# 攻防世界web ics-06 writeup

原创

Sprint#51264 于 2020-07-10 17:19:55 发布 135 收藏 1

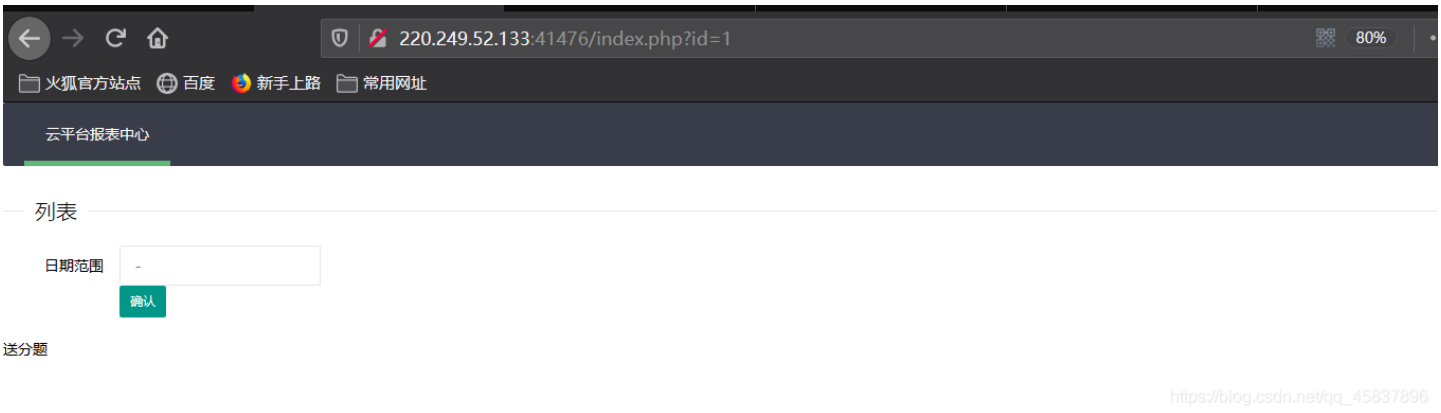
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_45837896/article/details/107255832
版权

使用工具：burpsuite pro（一定要用pro，不然线程不能更改得跑一年）


首先看这个题目描述，说只有一处留下了入侵者的痕迹，现在并不能推断出什么。

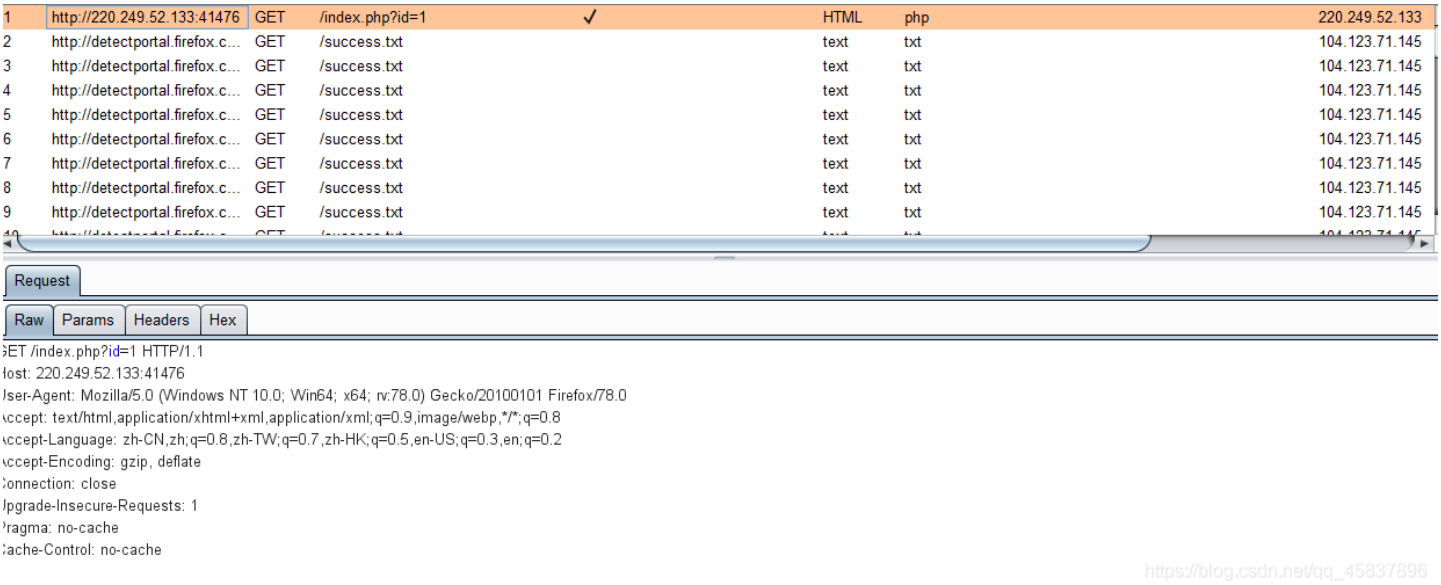
然后我们进入题目场景：


发现一个网站，并且貌似有很多网页，对左侧的选项进行点击，但是页面没有发生任何变化，唯独“*报表中心*”这一项会引导到另外一个页面。




下方描述“送分题”，还是先观察网页的url，发现后面有一个可以改变的id值，改变其值没有明显的变化出现，想到题目说只有一处留下痕迹，可能是某个id值会有不同的页面，于是决定使用burp来爆破

抓包



| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | http://220.249.52.133:41476 | GET | /index.php?id=1 | ✓ | HTML | php | 220.249.52.133 |
| 2 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 3 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 4 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 5 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 6 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 7 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 8 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |
| 9 | http://detectportal.firefox.c... | GET | /success.txt | | text | txt | 104.123.71.145 |

Request

Raw Params Headers Hex

```
GET /index.php?id=1 HTTP/1.1
Host: 220.249.52.133:41476
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

https://blog.csdn.net/qq_45837896

发送到intruder
多次尝试之后发现密id范围在0-10000

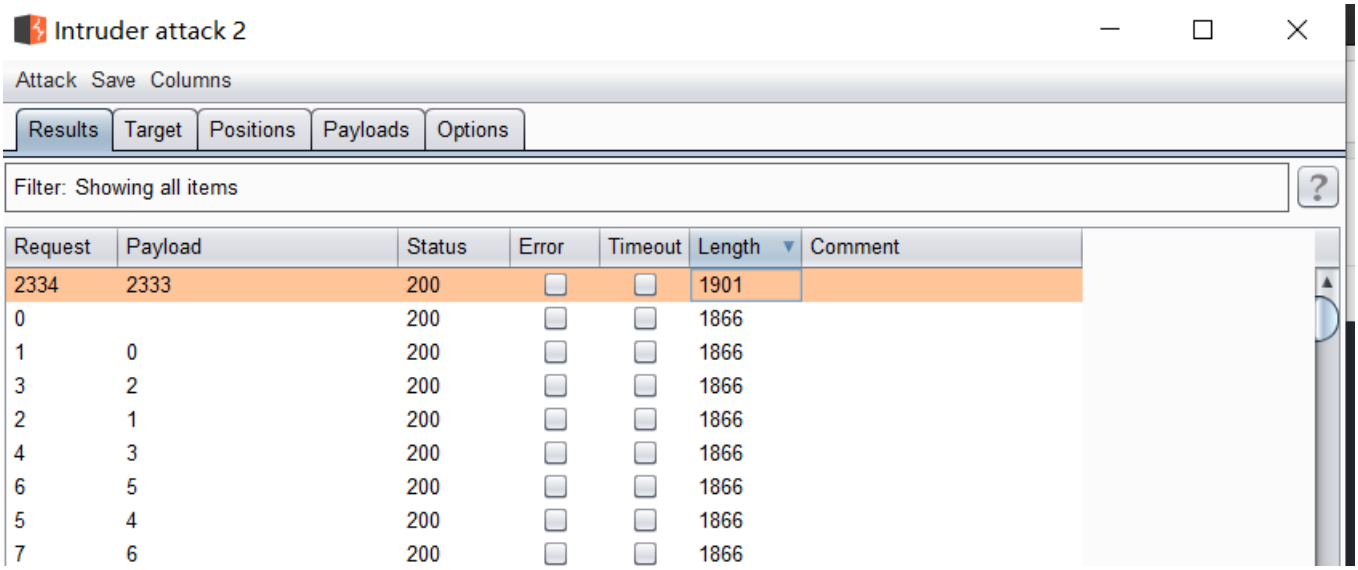
c代码生成字典文件

```c
#include <stdio.h>
int main ()
{
FILE * pFile;
int n;
pFile = fopen ("myfile.txt","w");
for(n=0;n<=10000;n++)
fprintf (pFile, " %d\n",n);
fclose (pFile);
return 0;
}
```

设置线程为100

要查找长度不同的payload值；

点击length进行排序



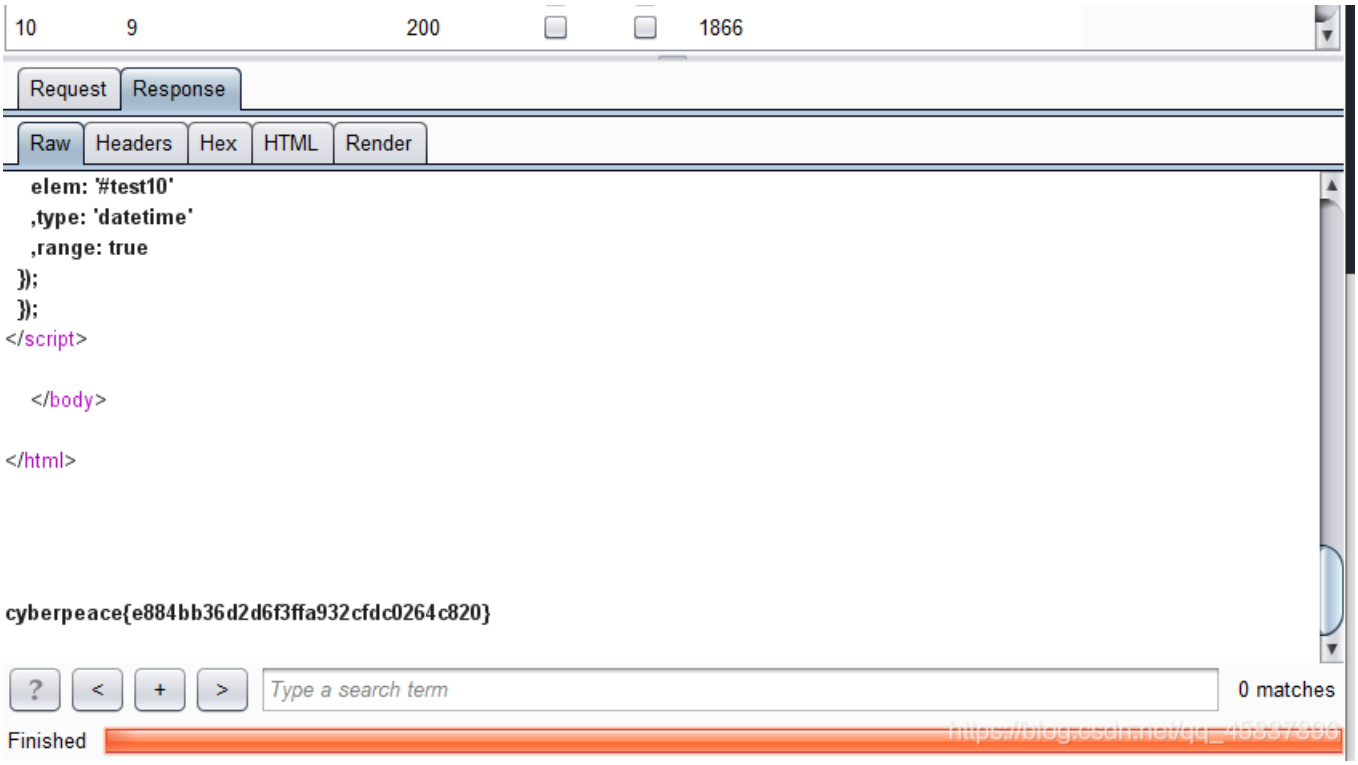
Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

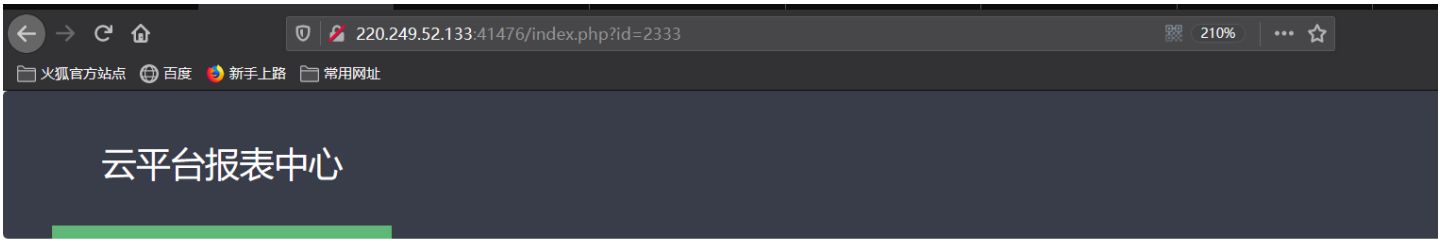
| Request | Payload | Status | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|
| 2334 | 2333 | 200 | | | 1901 | |
| 0 | | 200 | | | 1866 | |
| 1 | 0 | 200 | | | 1866 | |
| 3 | 2 | 200 | | | 1866 | |
| 2 | 1 | 200 | | | 1866 | |
| 4 | 3 | 200 | | | 1866 | |
| 6 | 5 | 200 | | | 1866 | |
| 5 | 4 | 200 | | | 1866 | |
| 7 | 6 | 200 | | | 1866 | |




发现

id=2333时出现flag

查看response，得到flag，或者访问该页面




列表

日期范围 -

确认

cyberpeace{e884bb36d2d6f3ffa932cfdc0264c820}