

Stash

发表于 2021-01-04 分类于 [Skill](#) , [Web](#) , [信息泄露](#) , [Git泄露](#)
[Skill](#) | [Web](#) | [信息泄露](#) | [Git泄露](#) | [Stash](#)

[点击此处](#)获得更好的阅读体验

考点

- git 泄露 `.git/refs/stash`
- `stash` 用于保存 git 工作状态到 git 栈，在需要的时候再恢复。

解题思路

1. 尝试访问敏感目录，发现 `.git` 目录

`http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/config`

1. 利用 `GitHack` 工具将网站源代码 `clone` 到本地

```
1 python GitHack.py http://challenge-f8e28984e486f969.sandbox.ctfhub.com:10080/.git/
```

□

解法一

1. 执行 `git stash list` 发现有 `stash`

□

1. 执行 `git stash pop` 发现从 `git` 栈中弹出来一个文件，这个文件的内容就是 `flag`

□

解法二

如果你使用的 `GitHack` 工具执行完 `git stash show` 之后没有显示 `stash` 记录，那么不妨来尝试这个方法

1. 查看 `.git/refs/stash` 找到 `stash` 对应的 `hash`

□

1. `git diff e71ada` 即可看到 `flag`

□

Flag

动态 flag

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Skill/Web/信息泄露/Git泄露/vE36FuCiMl3DKT2VWumFHz.html>
- 版权声明： 本博客所有文章除特别声明外，均采用 [BY-NC-SA](#) 许可协议。转载请注明出处！

[#Skill](#) [#Web](#) [#信息泄露](#) [#Git泄露](#)

[Log](#)

[请求方式](#)