

【xctf】comment, git泄露git修复

原创

南方古猿 已于 2022-03-24 17:03:59 修改 20 收藏

文章标签: [git](#)

于 2022-03-24 17:02:42 首次发布

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_39167911/article/details/123714056

版权

dirsearch -u发现git目录, burpsuits的spider爬虫发现login等目录

githacker拿源码

```
sudo pip3 install GitHacker

//创建软连接放到 /usr/bin 或者 /usr/sbin 目录下
cd /usr/sbin
sudo ln -s /home/<用户名>/local/bin/githacker

//添加到环境变量中
sudo vi /etc/profile

:/home/<用户名>/local/bin/

//使环境变量生效
source /etc/profile
```

如果软连接创建失误, 提示

In: failed to create symbolic link './githacker': File exists

sudo rm -rf ./githacker命令删除错误的软连接

:/home/<用户名>/local/bin/添加位置

```
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).
if [ "`id -u`" -eq 0 ]; then
    PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/home/kali/.local/bin/"
else
    PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games"
fi
```

CSDN @南方古猿

根据提示写命令获取源码

```
(kali@kali)-[~/Desktop/GitHacker-1.1.0]
└─$ githacker --url http://111.200.241.244:58440/.git/ --folder ./111
usage: githacker [-h] (--url URL | --url-file URL_FILE) --output-folder OUTPUT_FOLDER [--brute]
               [--enable-manually-check-dangerous-git-files] [--threads THREADS] [--version]
githacker: error: the following arguments are required: --output-folder

(kali@kali)-[~/Desktop/GitHacker-1.1.0]
└─$ githacker --url http://111.200.241.244:58440/.git/ --output-folder ./111
2022-03-24 04:36:41 INFO 1 urls to be exploited
2022-03-24 04:36:41 INFO Exploiting http://111.200.241.244:58440/.git/ into ./111
2022-03-24 04:36:41 INFO Downloading basic files ...
```

```
githacker --url http://111.200.241.244:58440/.git/ --output-folder ./111
```

cd 到111释放的文件夹，git修复

```
//查看历史commit  
git log --reflog  
  
//(HEAD -> master, origin/master, origin/HEAD)的是当前git下载  
git reset --hard 最新commit编号  
  
//重新查看文件  
cat 文件名
```