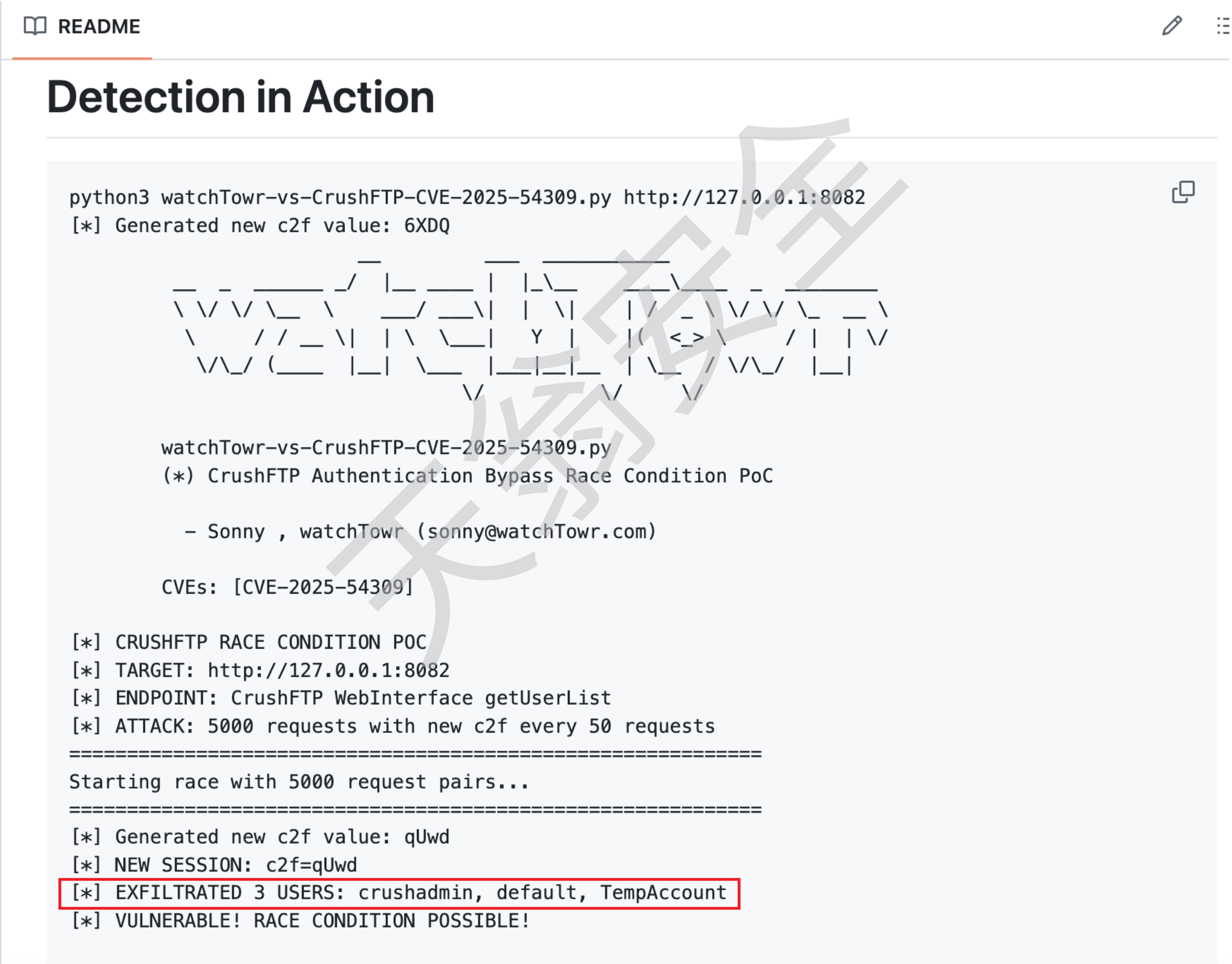
【已复现】CrushFTP条件竞争导致的任意管理员用户添加漏洞（CVE-2025-54309）被在野积极利用

为什么写这篇文章

近日刷到了CrushFTP曝出了一个任意管理员添加漏洞，但是看了网上Watchtowr安全团队公布的POC却只是一个示意POC（只能列出当前存在的用户）。

POC地址：https://github.com/watchtowrlabs/watchTowr-vs-CrushFTP-Authentication-Bypass-CVE-2025-54309/

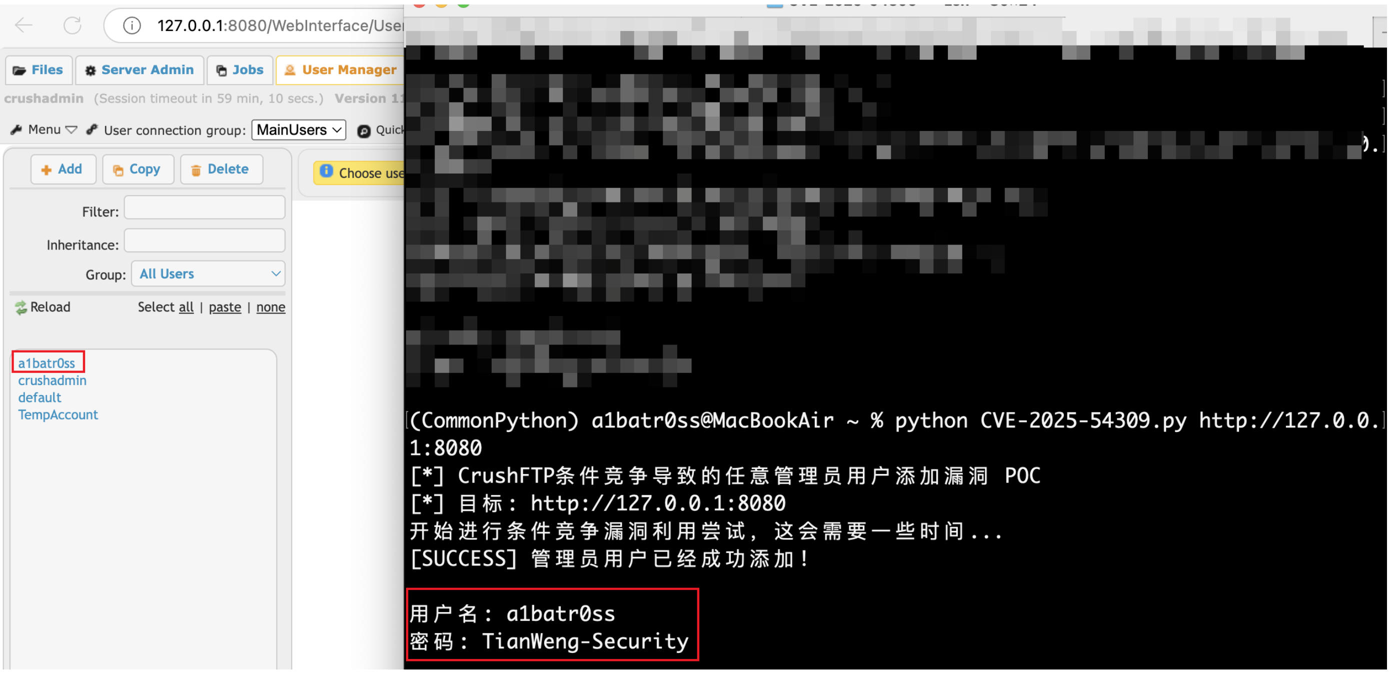


README

Detection in Action

```
python3 watchTowr-vs-CrushFTP-CVE-2025-54309.py http://127.0.0.1:8082
[*] Generated new c2f value: 6XDQ
                         __         ___  ___________
         __  _  ______ _/  |__ ____ |  |_\__    ____\____  _  ________
         \ \/ \/ \__  \    ___/ ___\|  |  \|    | /  _ \ \/ \/ \_  __ \
          \     / / __ \|  | \  \___|   Y  |    |(  <_> \     / |  | \/
           \/\_/ (____  |__|  \___  |___|__|__  | \__  / \/\_/  |__|
                                  \/          \/     \/

        watchTowr-vs-CrushFTP-CVE-2025-54309.py
        (*) CrushFTP Authentication Bypass Race Condition PoC

          - Sonny , watchTowr (sonny@watchTowr.com)

        CVEs: [CVE-2025-54309]

[*] CRUSHFTP RACE CONDITION POC
[*] TARGET: http://127.0.0.1:8082
[*] ENDPOINT: CrushFTP WebInterface getUserList
[*] ATTACK: 5000 requests with new c2f every 50 requests
============================================================
Starting race with 5000 request pairs...
============================================================
[*] Generated new c2f value: qUwd
[*] NEW SESSION: c2f=qUwd
[*] EXFILTRATED 3 USERS: crushadmin, default, TempAccount
[*] VULNERABLE! RACE CONDITION POSSIBLE!
```

于是在本地搭建环境进行研究，成功研究出可以添加任何管理员用户的POC。

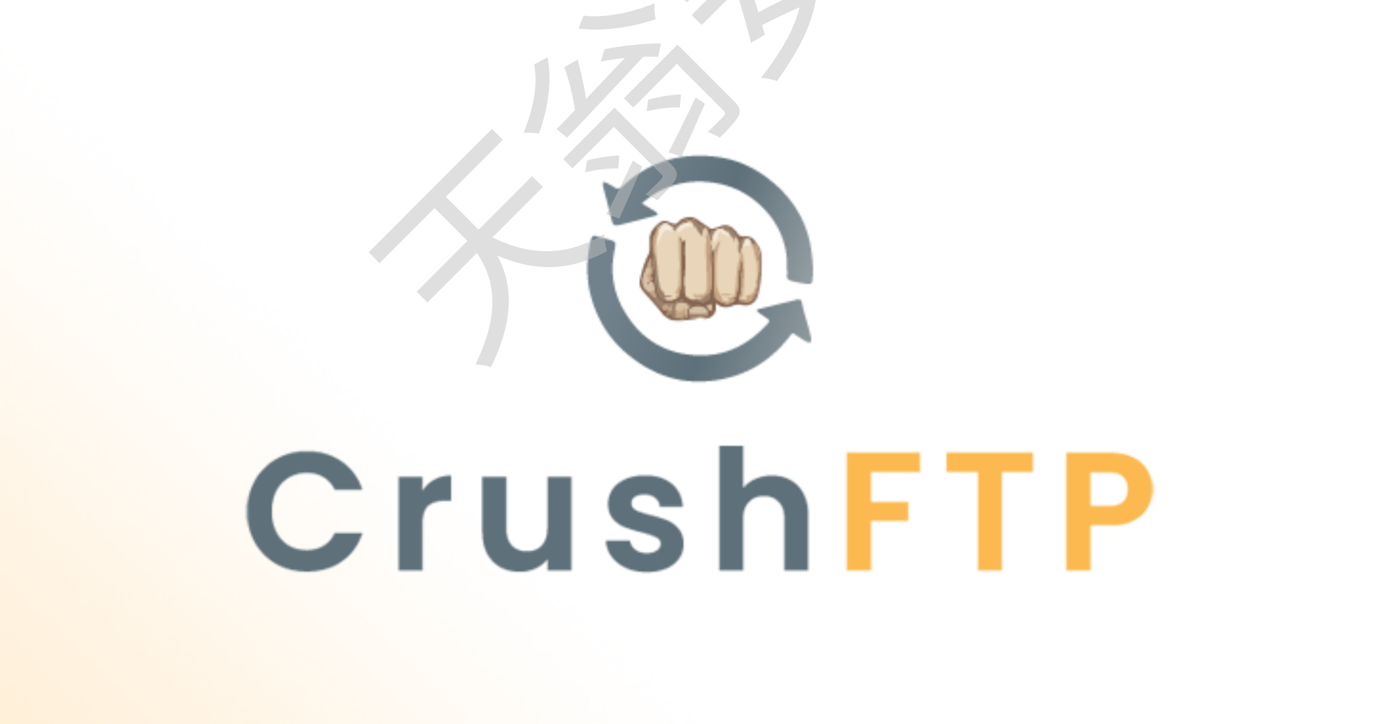

127.0.0.1:8080/WebInterface/User
Files
Server Admin
Jobs
User Manager
crushadmin (Session timeout in 59 min, 10 secs.) Version 1
Menu
User connection group: MainUsers
Quick
Add
Copy
Delete
Choose use
Filter:
Inheritance:
Group: All Users
Reload
Select all | paste | none
a1batr0ss
crushadmin
default
TempAccount

[redacted]

```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-54309.py http://127.0.0.
1:8080
[*] CrushFTP条件竞争导致的任意管理员用户添加漏洞 POC
[*] 目标：http://127.0.0.1:8080
开始进行条件竞争漏洞利用尝试，这会需要一些时间...
[SUCCESS] 管理员用户已经成功添加！

用户名：a1batr0ss
密码：TianWeng-Security
```

漏洞介绍

CrushFTP 是一款跨平台的企业级文件传输服务器软件，支持 FTP、FTPS、SFTP、HTTP(S)、WebDAV 等多种协议，能够运行在 Windows、Linux、macOS 等环境中。它提供用户友好的 Web 管理界面，支持高并发文件传输、压缩与解压缩、自动化任务、事件触发、日志审计和权限管理等功能。相比传统 FTP 服务器，CrushFTP 更强调安全性和可扩展性，常用于企业内部文件共享、对外数据交换以及自动化传输流程的搭建。



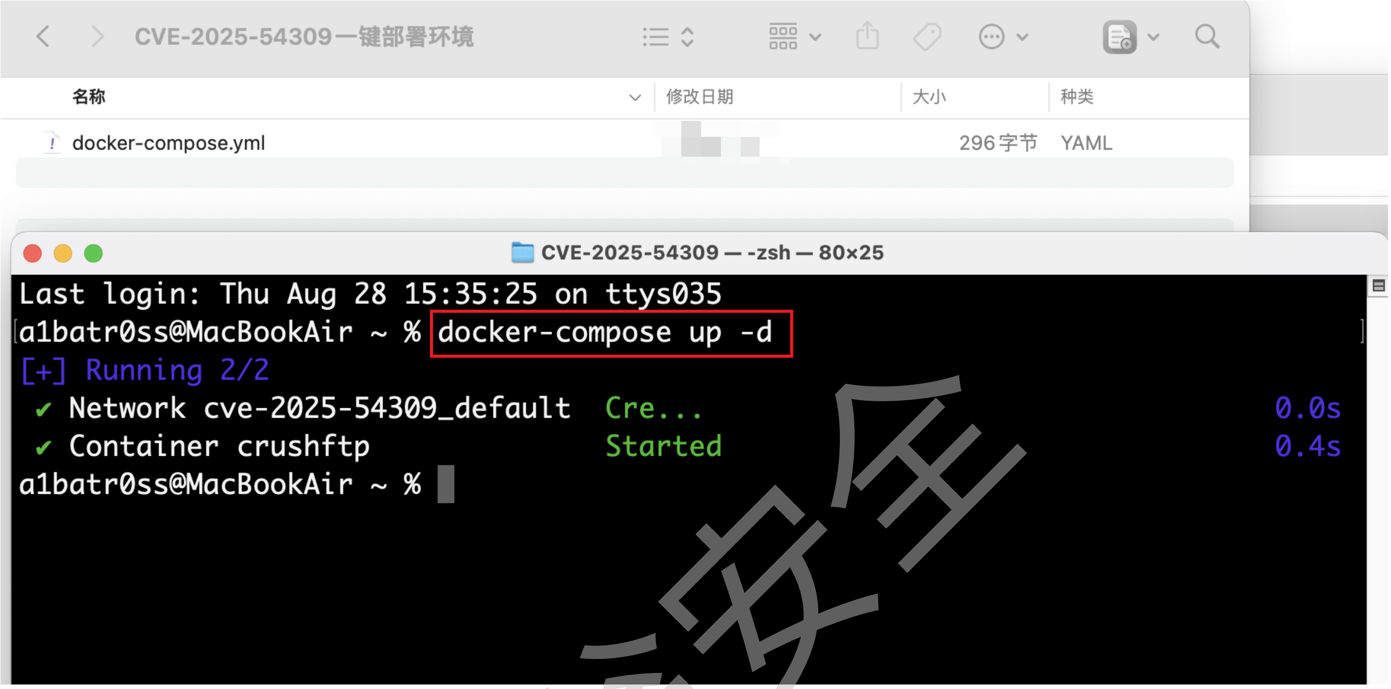
CVE-2025-54309 是 CrushFTP 中的一个严重漏洞（CVSS 评分高达 9.0+），影响 10.8.5 之前的 10.x 版本和 11.3.4_23 之前的 11.x 版本。CrushFTP在处理 AS2 验证逻辑上存在缺陷，攻击者可通过精心构造的请求绕过认证，获取管理员权限。该漏洞已在 2025 年 7 月被黑客在实际攻击中利用，危害范围广泛，官方已发布修复版本，受影响用户需立即升级并加强防护。

漏洞版本

- 10.x 版本：< 10.8.5版本
- 11.x 版本：< 11.3.4_23版本

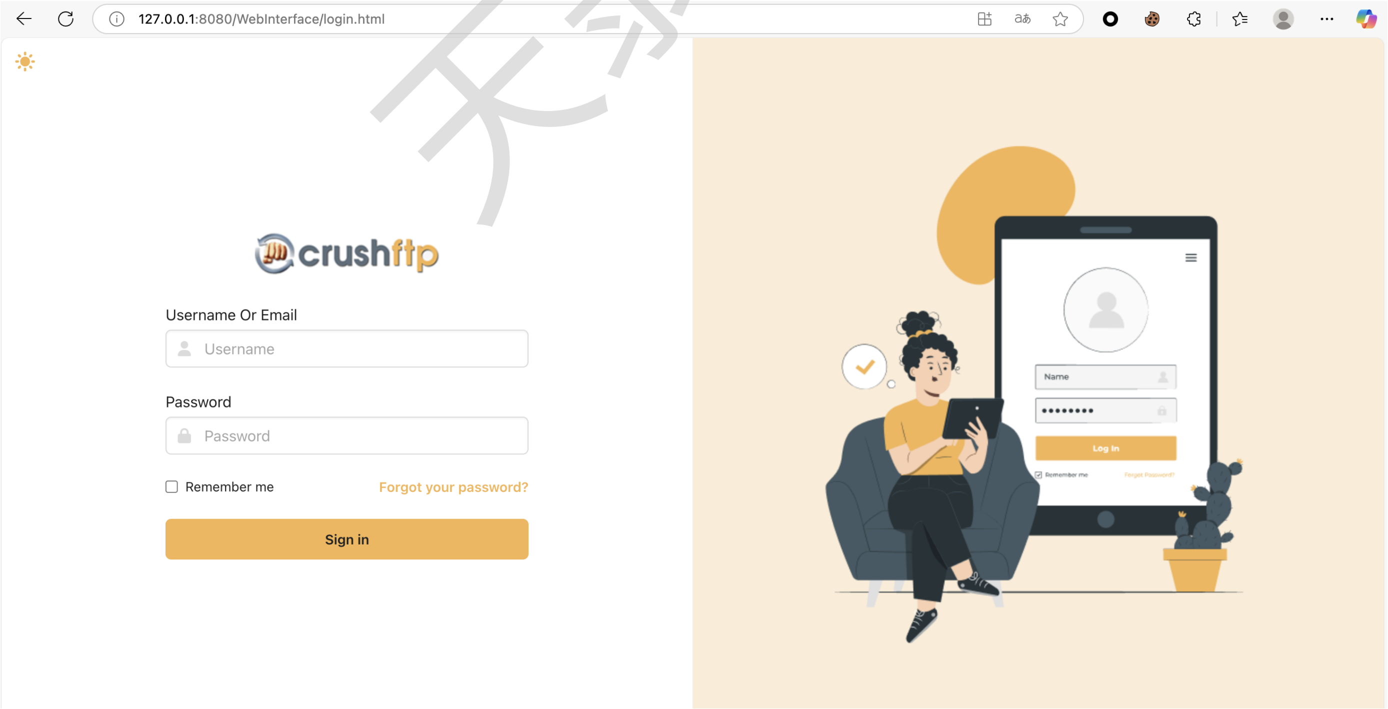
一键部署-漏洞环境

在“CVE-2025-54309一键部署环境”文件夹执行`docker-compose up -d`即可部署CVE-2025-54309漏洞环境



```
Last login: Thu Aug 28 15:35:25 on ttys035
a1batr0ss@MacBookAir ~ % docker-compose up -d
[+] Running 2/2
 ✔ Network cve-2025-54309_default  Cre...                               0.0s
 ✔ Container crushftp              Started                              0.4s
a1batr0ss@MacBookAir ~ %
```

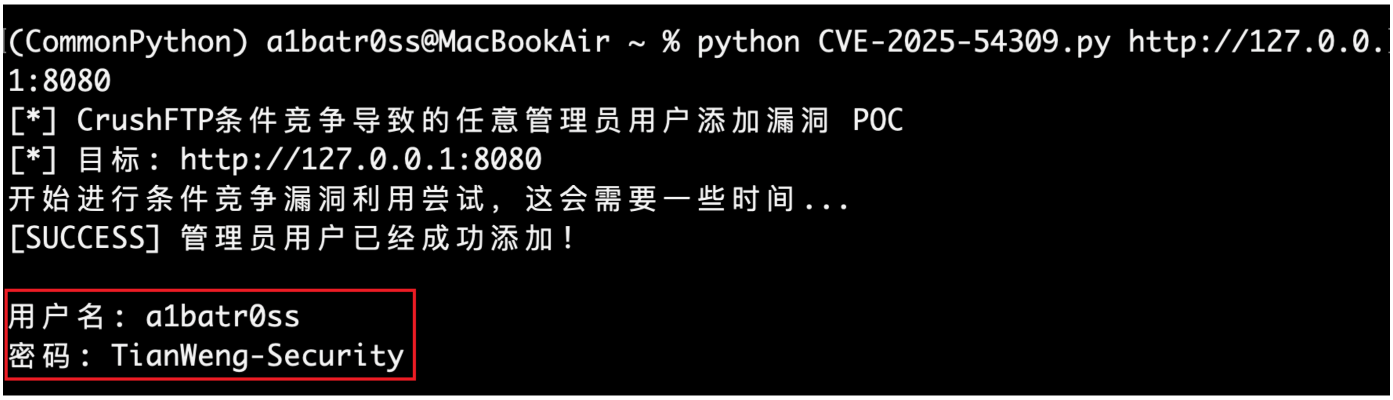
CVE-2025-54309环境搭建完成后，访问 http://127.0.0.1:8080 即可看到CrushFTP后台的web界面，



漏洞利用

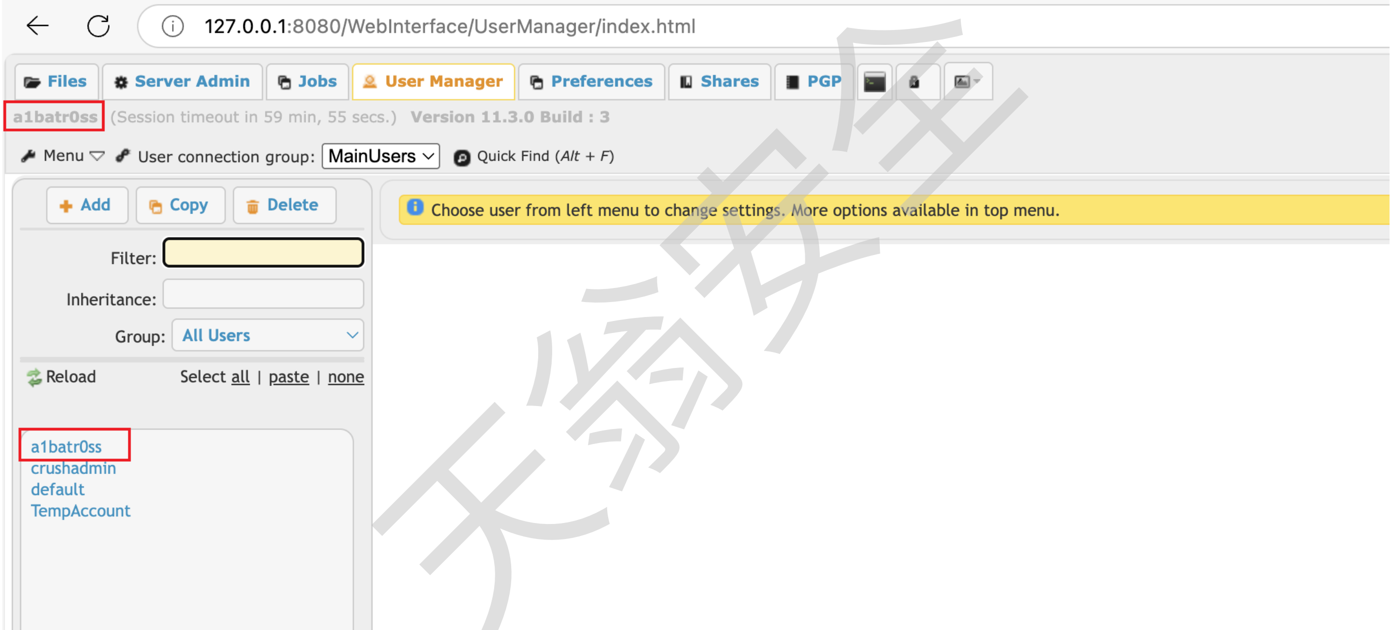
执行一下命令对目标环境进行CVE-2025-54309漏洞利用，执行成功后会给CrushFTP增加一个用户名为a1batr0ss、密码为TianWeng-Security的**管理员用户**。

```
python CVE-2025-54309.py【CrushFTP的地址】
```



```
(CommonPython) a1batr0ss@MacBookAir ~ % python CVE-2025-54309.py http://127.0.0.
1:8080
[*] CrushFTP条件竞争导致的任意管理员用户添加漏洞 POC
[*] 目标: http://127.0.0.1:8080
开始进行条件竞争漏洞利用尝试，这会需要一些时间...
[SUCCESS] 管理员用户已经成功添加！

用户名: a1batr0ss
密码: TianWeng-Security
```

我们利用刚才生成的管理员a1batr0ss的用户名和密码，可以成功登录到CrushFTP的后台



127.0.0.1:8080/WebInterface/UserManager/index.html

a1batr0ss (Session timeout in 59 min, 55 secs.) Version 11.3.0 Build : 3

User connection group: MainUsers

Choose user from left menu to change settings. More options available in top menu.

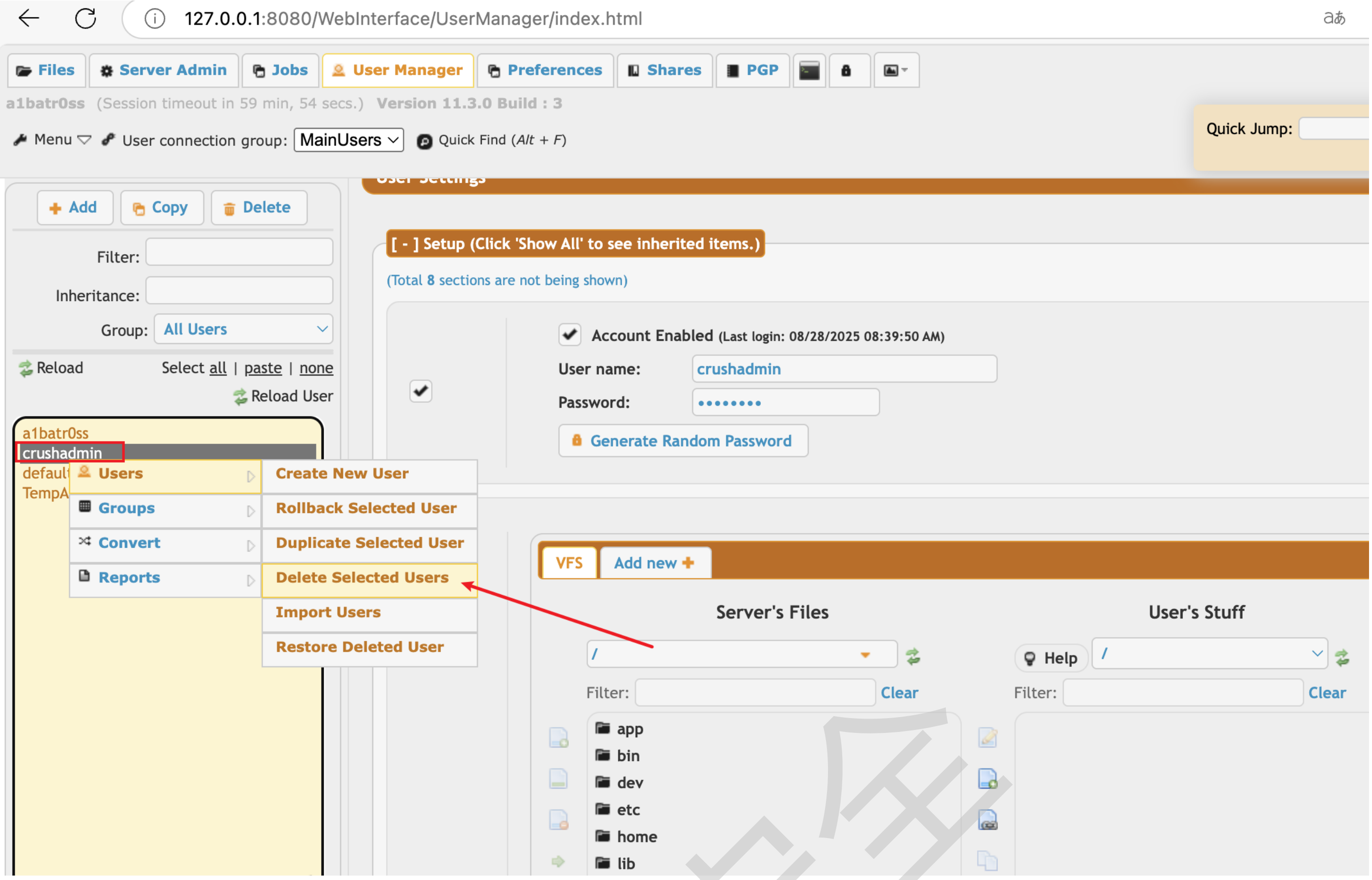
Filter:

Inheritance:

Group: All Users

a1batr0ss
crushadmin
default
TempAccount

我们拥有的权限甚至可以把原来存在的管理员删除掉



a1batr0ss (Session timeout in 59 min, 54 secs.) Version 11.3.0 Build : 3

User connection group: MainUsers

[-] Setup (Click 'Show All' to see inherited items.)

(Total 8 sections are not being shown)

☑ Account Enabled (Last login: 08/28/2025 08:39:50 AM)

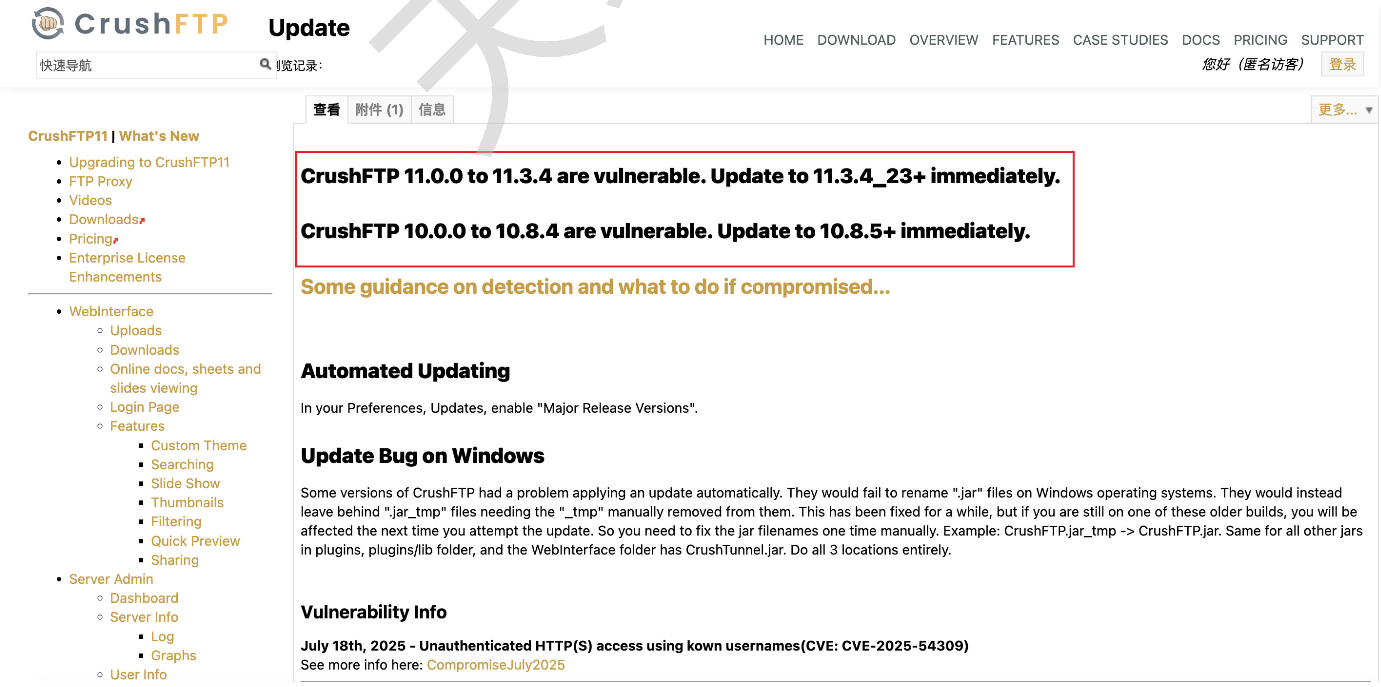
User name: crushadmin

Password: ••••••••

漏洞修复

修复需要将版本升级

- 10.x 版本：升级到10.8.5版本及以上
- 11.x 版本：升级到11.3.4_23版本及以上



CrushFTP 11.0.0 to 11.3.4 are vulnerable. Update to 11.3.4_23+ immediately.

CrushFTP 10.0.0 to 10.8.4 are vulnerable. Update to 10.8.5+ immediately.

Some guidance on detection and what to do if compromised...

Automated Updating

In your Preferences, Updates, enable "Major Release Versions".

Update Bug on Windows

Some versions of CrushFTP had a problem applying an update automatically. They would fail to rename ".jar" files on Windows operating systems. They would instead leave behind ".jar_tmp" files needing the "_tmp" manually removed from them. This has been fixed for a while, but if you are still on one of these older builds, you will be affected the next time you attempt the update. So you need to fix the jar filenames one time manually. Example: CrushFTP.jar_tmp -> CrushFTP.jar. Same for all other jars in plugins, plugins/lib folder, and the WebInterface folder has CrushTunnel.jar. Do all 3 locations entirely.

Vulnerability Info

July 18th, 2025 - Unauthenticated HTTP(S) access using kown usernames(CVE: CVE-2025-54309)

See more info here: CompromiseJuly2025