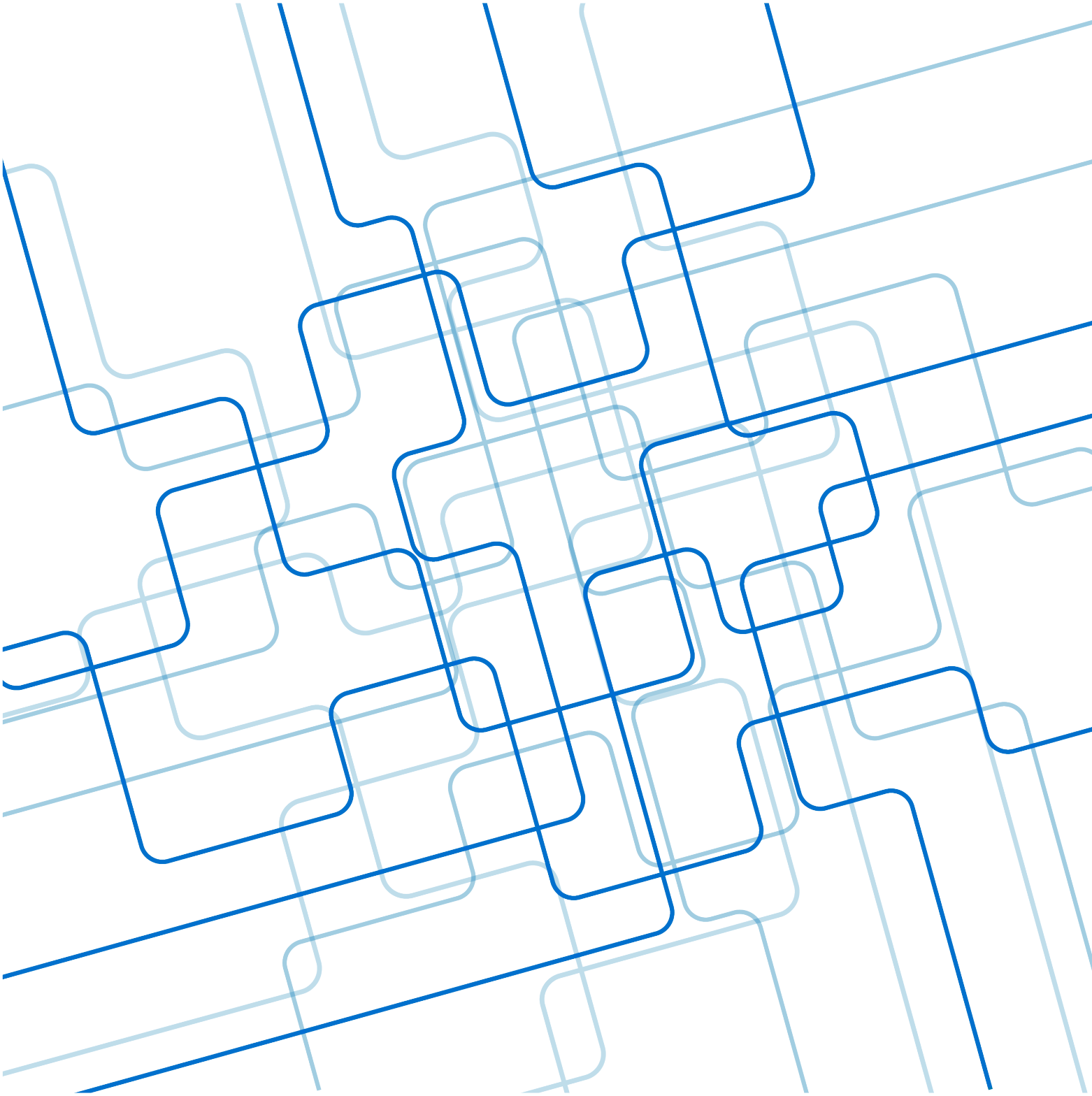

CTF 学习笔记

作者：shijy16

时间：March 13, 2021

特别声明

本册是 CTF 学习笔记，按照从 0 到 1：CTFer 成长之路的章节一步一步学习，会记录一些笔记。

供初学 CTF 的同学们参考交流。

shijy16

目录

第一章 web 入门

web 类题目是 CTF 比赛的主要题目，和二进制、逆向题目相比，不需要掌握底层知识。本章介绍 web 题目最常见的三类漏洞。

1.1 信息收集

信息搜集涵盖的面很广泛，包含备份文件、目录信息、Banner 信息等，信息搜集主要依赖经验。

1.1.1 敏感目录泄露

通过敏感目录泄露通常可以获取网站的源代码和敏感的 URL 地址。

git 泄露

常规 git 泄露 直接用现成工具或脚本获取网站源码或 flag。如：在确保目标 URL 含有.git 的情况下，可以直接使用scrabble来获取网站源码。命令如下：

```
./scrabble http://example.com/
```

git 回滚 利用 scrabble 获取网站源码后，部分情况下，flag 会在之前的 commit 中被删除/修改，这时需要回滚。

```
git reset --hard HEAD^ #回滚到上一版本
git log -stat #查看每个commit修改了什么
git diff HEAD commit-id #查看当前版本与目标版本的区别
```

git 分支 有时候 flag 不在默认分支中，需要切换其他分支，但大部分现成 git 泄露工具不支持分支，还原其他分支代码需要手工进行文件提取。功能较强的工具有GitHacker，用法：

```
python GitHacker.py [Website]
```

而后使用 $git\ reflog$ 命令查看 checkout 记录，可以发现其他分支，然后修改/复用 GitHacker 代码来自动恢复分支。

git 泄露其他利用 泄露的 git 中可能还有其他有用信息，比如说.git/config 文件夹里面可能有 access_tocken 信息，用来访问用户其他仓库。

SVN 泄露

SVN 是源代码版本管理软件，管理员可能疏忽将 SVN 隐藏文件夹暴露在外。可以利用.svn/entries 或 wc.db 获取服务器源码。

工具：https://github.com/kost/dvcs-ripper/,Seay-svn(windows)。

HG 泄露

HG 会创建.hg 隐藏文件记录代码、分支信息。

工具：https://github.com/kost/dvcs-ripper/

总结经验

CTF 线上赛往往有重定向问题，如访问.git 后重定向，再访问.git/config 后有内容返回，就有.git 泄露问题。

目录扫描工具：https://github.com/maurosoria/dirsearch

1.1.2 敏感备份文件

gedit 备份文件

gedit：文件保存后会有一个后缀为'～' 的文件。如 $flag\sim$。

vim 备份文件

vim 崩溃时会有一个 $.swp$ 文件，可以用 $vim\ -r$ 命令恢复。

常规文件

- robots.txt:CMS 版本信息
- readme
- www.zip/rar/tar.gz: 常常是网站的备份源码

1.1.3 Banner 识别

Banner: 网站服务器对外显示的一些基础信息，如网站使用的框架等。可以据此尝试框架历史漏洞。

自行搜集指纹库

github 上有 CMS 指纹库，也有扫描器。

使用已有工具

Wappalyzer 工具：python 工具，使用 pip 安装即可。

总结经验

随意输入一些 URL 有时可以通过 404 或 302 跳转页面发现一些信息。

1.2 SQL 注入

1.3 任意文件读取