CTF_web_study_信息获取

文件读取

目录扫描

目录扫描可以让我们发现这个网站存在多少个目录，多少个页面，探索出网站的整体结构。通过目录扫描我们还能扫描敏感文件，后台文件，数据库文件，和信息泄露文件，等等。

扫描的方式就是通过设置字典进行撞库匹配，探索网站的目录结构。字典需要靠平时积累，有时候会遇见一些骚气的目录，加进去就行。再就是要根据你所扫描的网站的特点构造专门的字典，所以**目录扫描的重点是字典的设置**

工具

[御剑（两个）]

使用御剑扫描器，主要是扫描网站敏感目录，包括网站后台等。其扫描原理也是爆破，即通过敏感目录的字典去匹配。

御剑有好多版本，功能也稍微有些许区别，有指纹识别、后台扫描、获取真实IP、检测注入等

配置文件里面是字典，可以添加和删除。

[dirsearch]

dirsearch是一个扫描网站的目录和文件的命令行工具，推荐在kali中使用，可以使用多线程快速扫描目标站点。它可以通过自定义字典进行扫描，同时支持正则表达式和自定义扩展名。

个人觉得最好的目录扫描工具

使用教程：

在终端中运行以下命令，使用kali中的dirsearch扫描目标URL

```
dirsearch -u <URL>
```

例如：

```
dirsearch -u http://www.baidu.com
```

更多的参数选项

```
-e：指定要排除的扩展名
例如：排除.html和.php文件
dirsearch -u http://www.baidu.com -e html,php

-f：指定要包含的拓展名
例如：只包含.html和.php文件
dirsearch -u http://www.baidu.com -f html,php

-x：指定要排除的目录
```

```
例如：排除index.php目录
dirsearch -u http://www.baidu.com -x index.php

-t：指定线程数
例如：使用50线程进行扫描
dirsearch -u http://www.baidu.com -t 50

-o：保存结果到某文件
例如：保存结果到result.txt文件
dirsearch -u http://www.baidu.com -o result.txt

-w WORDLIST：使用自定义字典
例如：设置passwd.txt为字典进行扫描
dirsearch -u http://www.baidu.com -w passwd.txt
```

汇总：

后缀	介绍
-h	查看帮助
-u URL	设置url
-L URLLIST	设置url列表
-e EXTENSIONS	网站脚本类型
-w WORDLIST	设置字典
-f	强制扩展字典里的每个词条
-s DELAY	设置请求之间的延时
-r	递归地扫描
-t	设置扫描线程
-x	排除指定的网站状态码(用逗号隔开)
-c	设置cookie
-F	跟随地址重定向扫描
-H	设置请求头

postman

关于目录扫描的使用即自动化接口测试

其原理就是构建js脚本进行批量发送请求，并利用js脚本进行对返回状态的分析

目前用的较少，总结一下就是会用的很厉害，不会就是不会