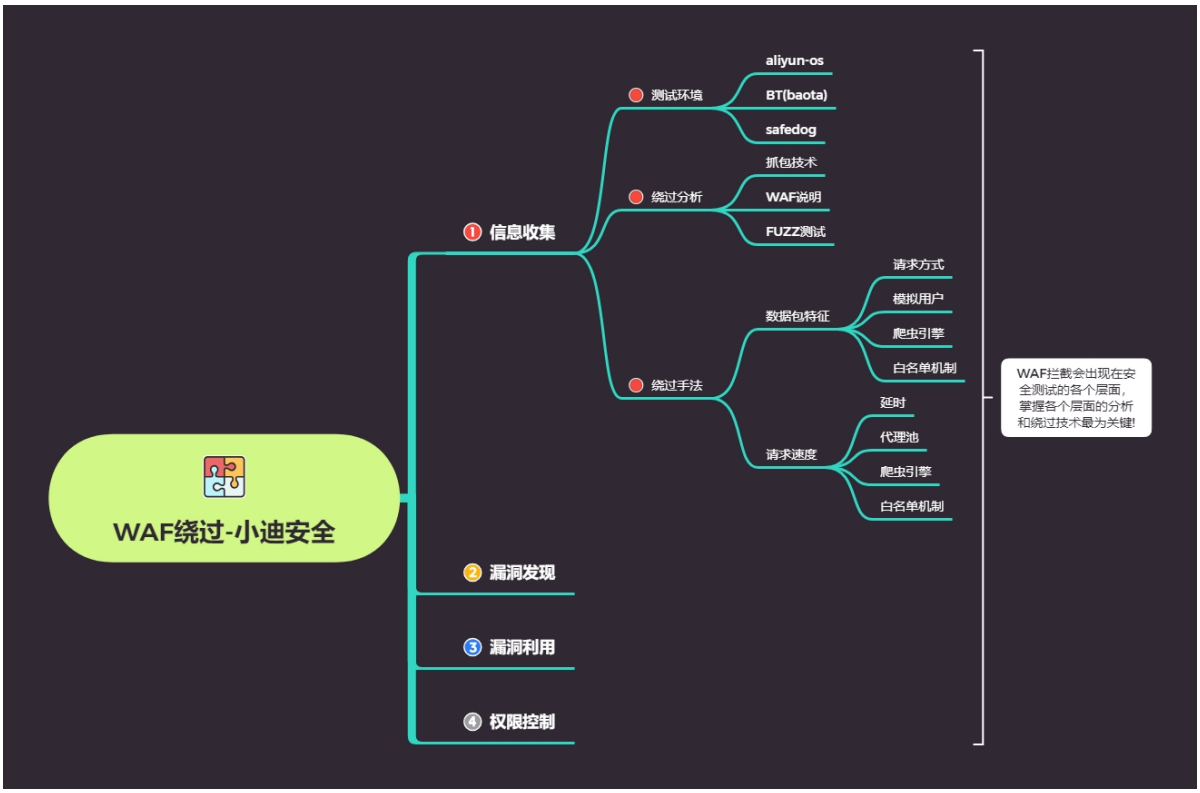
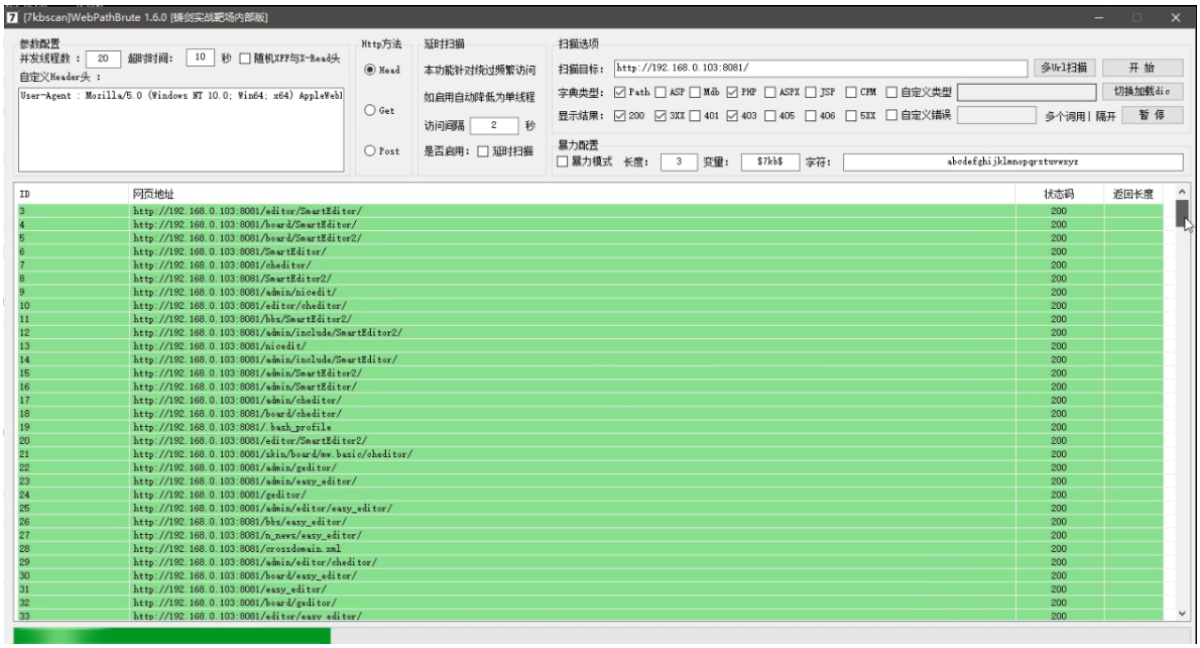
Day46　WAF绕过–信息收集之反爬虫延时代理池技术



46.1 Safedog-默认拦截机制分析绕过-未开 CC

safedog ——CC攻击防护默认是关闭的:

用目录扫描工具扫:



字典的所有的结果都有，明显错误！抓取进程的抓包工具抓包，与浏览器数据包对比，明显请求方式不同:

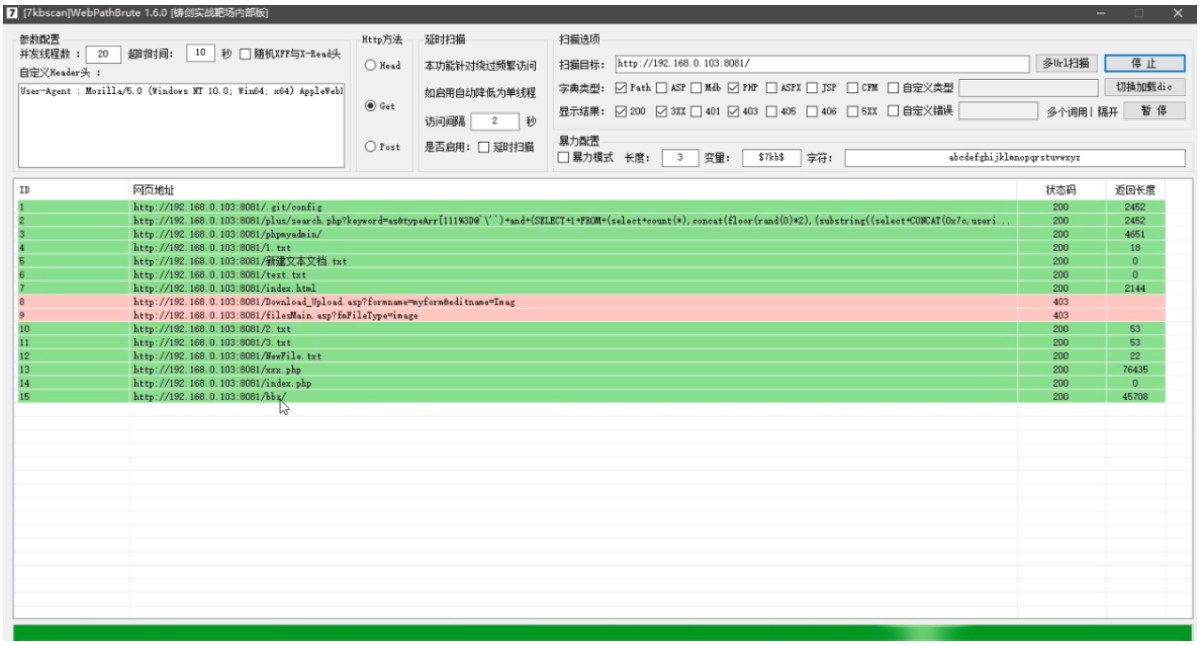
```
HEAD /bbs/easy_editor/ HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US, en; q=0.8, zh-Hans-CN; q=0.5, zh-Hans; q=0.3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Host: 192.168.0.103:8081
Connection: Close


GET /sssada HTTP/1.1
Host: 192.168.0.103:8081
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=1723ba091ce6a-030410c3773dff-3f6b490f-384000-1723ba091cfb3f; CNZZ
```

工具扫描数据包

浏览器访问数据包

改为GET请求方式，就是正常的扫描结果:

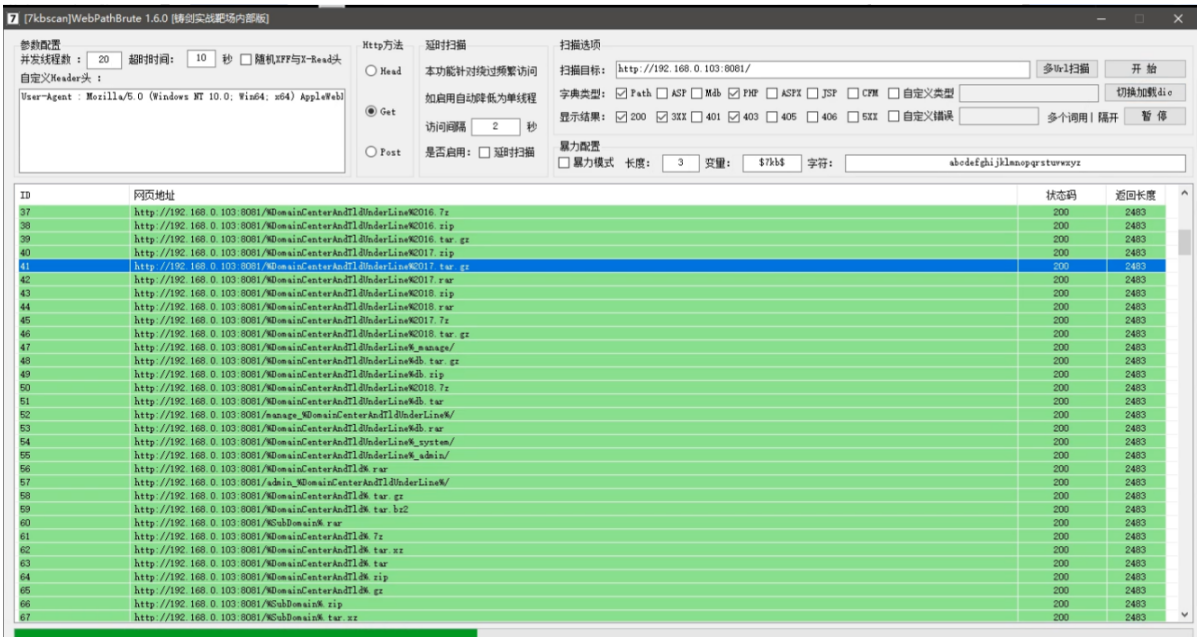


46.2 Safedog-默认拦截机制分析绕过-开启 CC

开启CC防护:

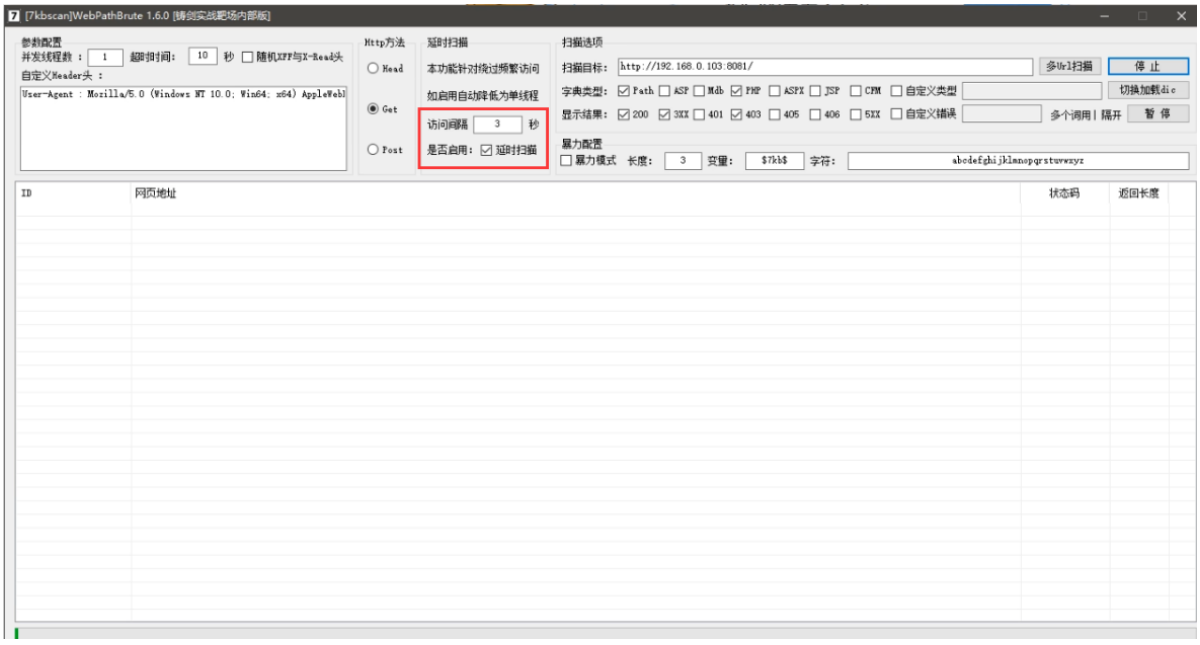
查看防护规则:

开启CC之后，再次使用扫描工具，并且访问网站:



频繁访问（访问频率过快，绝对是工具），触发安全狗防护机制，被拦截:

设置延时扫描时间:



或者也可以通过白名单:

模拟搜索引擎请求头User-Agent就可以了,进行扫描:

```
谷歌搜索引擎蜘蛛爬虫：
Mozilla/5.0 (compatible; Googlebot/2.1;
+http://www.google.com/bot.html)
Googlebot/2.1
(+http://www.googlebot.com/bot.html)
Googlebot/2.1 (+http://www.google.com/bot.html)
Googlebot-Image/1.0
```

```
百度搜索引擎蜘蛛爬虫：

移动 UA:
Mozilla/5.0 (Linux;u;Android 4.2.2;zh-cn;)
AppleWebKit/534.46 (KHTML,likeGecko) Version/5.1
Mobile Safari/10600.6.3 (compatible;
Baiduspider/2.0;
+http://www.baidu.com/search/spider.html)
PC UA: Mozilla/5.0 (compatible; Baiduspider/2.0;
+http://www.baidu.com/search/spider.html）

移动 UA：
Mozilla/5.0 (iPhone; CPU iPhone OS 9_1 likeMac
OS X) AppleWebKit/601.1.46 (KHTML, like Gecko)
Version/9.0 Mobile/13B143 Safari/601.1
(compatible; Baiduspider-render/2.0;
+http://www.baidu.com/search/spider.html)

PC UA：
Mozilla/5.0 (compatible; Baiduspider-render/2.0;
+http://www.baidu.com/search/spider.html)
```

```
搜狗搜索引擎蜘蛛爬虫:
Sogou web spider/4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)

图片蜘蛛:
Sogou Pic Spider/3.0(+http://www.sogou.com/docs/help/webmasters.htm#07)
```

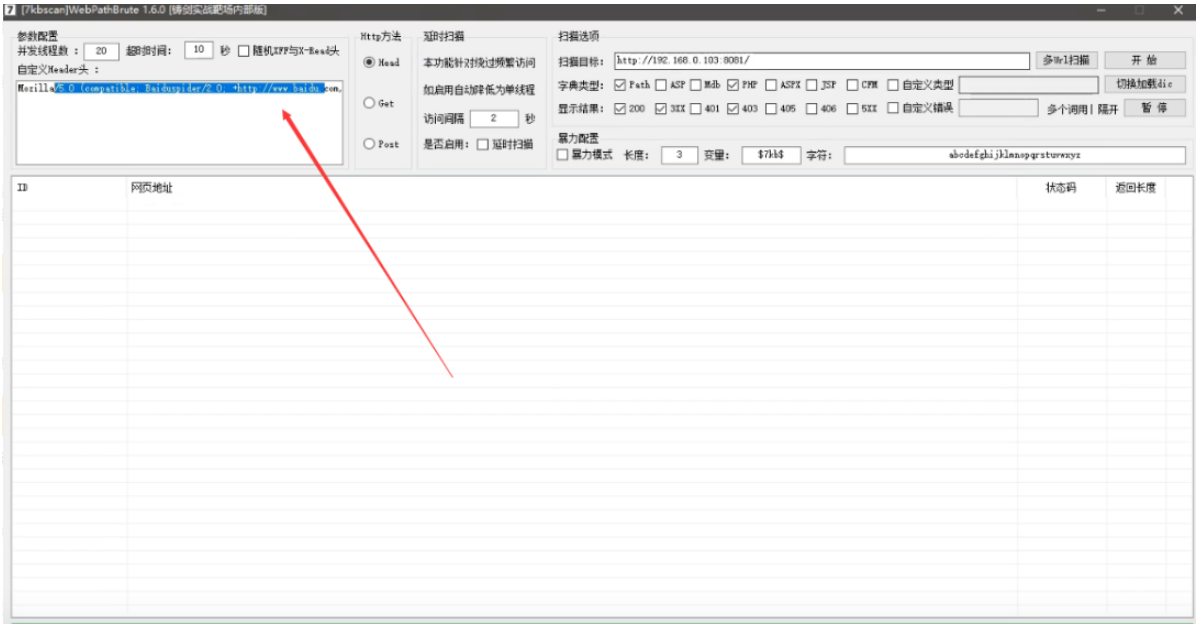
```
360 搜狗搜索引擎蜘蛛爬虫:
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36; 360Spider
```

```
Bing 搜索引擎蜘蛛爬虫:
Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
```

```
Yandex 搜索引擎蜘蛛爬虫:
Mozilla/5.0 (compatible; YandexBot/3.0; +http://yandex.com/bots)
```

```
https://www.imtqy.com/amp/spider-ua-ip.html
https://ziyuan.baidu.com/college/articleinfo?id=1002
http://www.webkaka.com/tutorial/zhanzhang/2017/061068/
https://www.cnblogs.com/iack/p/3557371.html
```

此时更换完user-agent后发现并没有任何结果。因为单单只修改了user-agent，如果对方对你请求包的内容进行检测的话，还是会被发现是工具进行的访问:



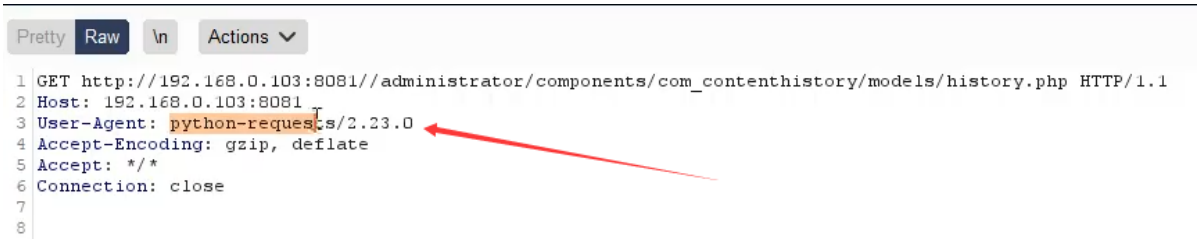
1.可以使用python脚本自定义请求包来访问:

可以通过python自定义来模拟正常用户的请求数据包，以及更改为百度谷歌等搜素引擎的user-agent来对网站进行访问请求，此时对方不会拦截.

抓包分析：此处为python脚本自定义的请求数据包

```
GET http://192.168.0.103:8081//administrator/components/com_contenthistory/models/history.php HTTP/1.1
Host: 192.168.0.103:8081
User-Agent: Mozilla/5.0 (compatible; Baiduspider-render/2.0; +http://www.baidu.com/search/spider.html)
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: bdshare_firstime=1581597934650; PHPSESSID=ncsajdvh39qse0q1sgqokshuc4; yx_auth=
dc4fq8FAEkyiAUZ54b5z19GGStCxXoRb1TFaAaozygMiSc5uZYHjR3gCQm%2BtKNz3bcjbTi8BRgcd%2F7LvRO1HN1j319CI6x29Z2QDI38
```

如果不使用自定义的请求数据包：



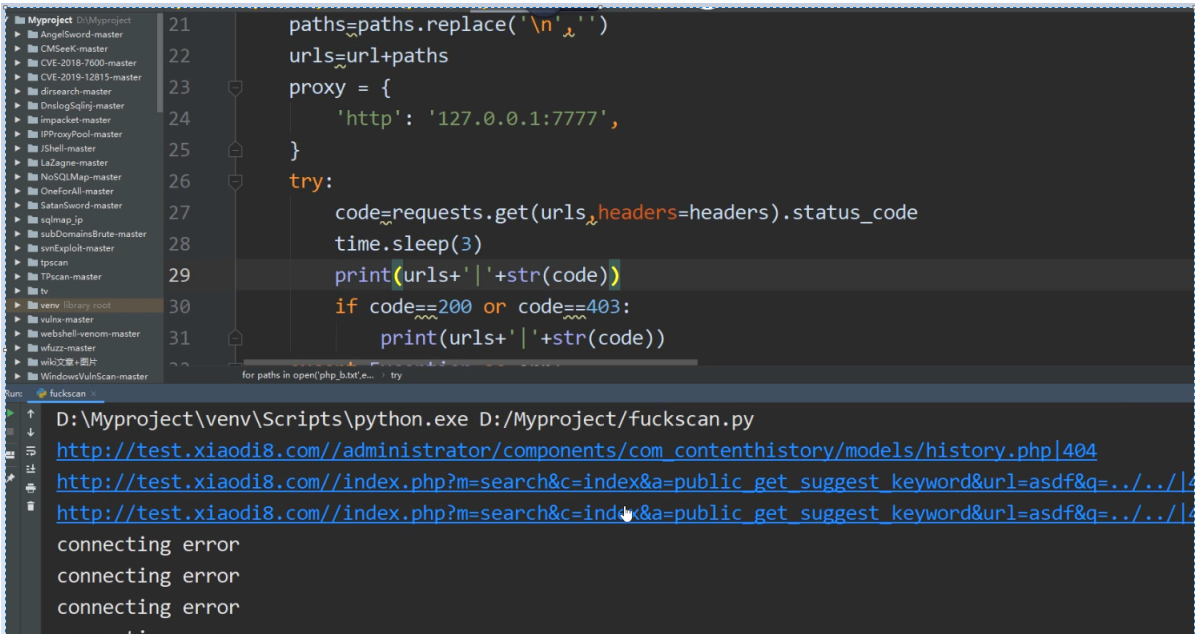
2.代理池

可通过python写的脚本不停更换代理ip访问进行测试,检测ip代理，一般是CC防护，但是使用代理，扫描目录，大概率是可行的:

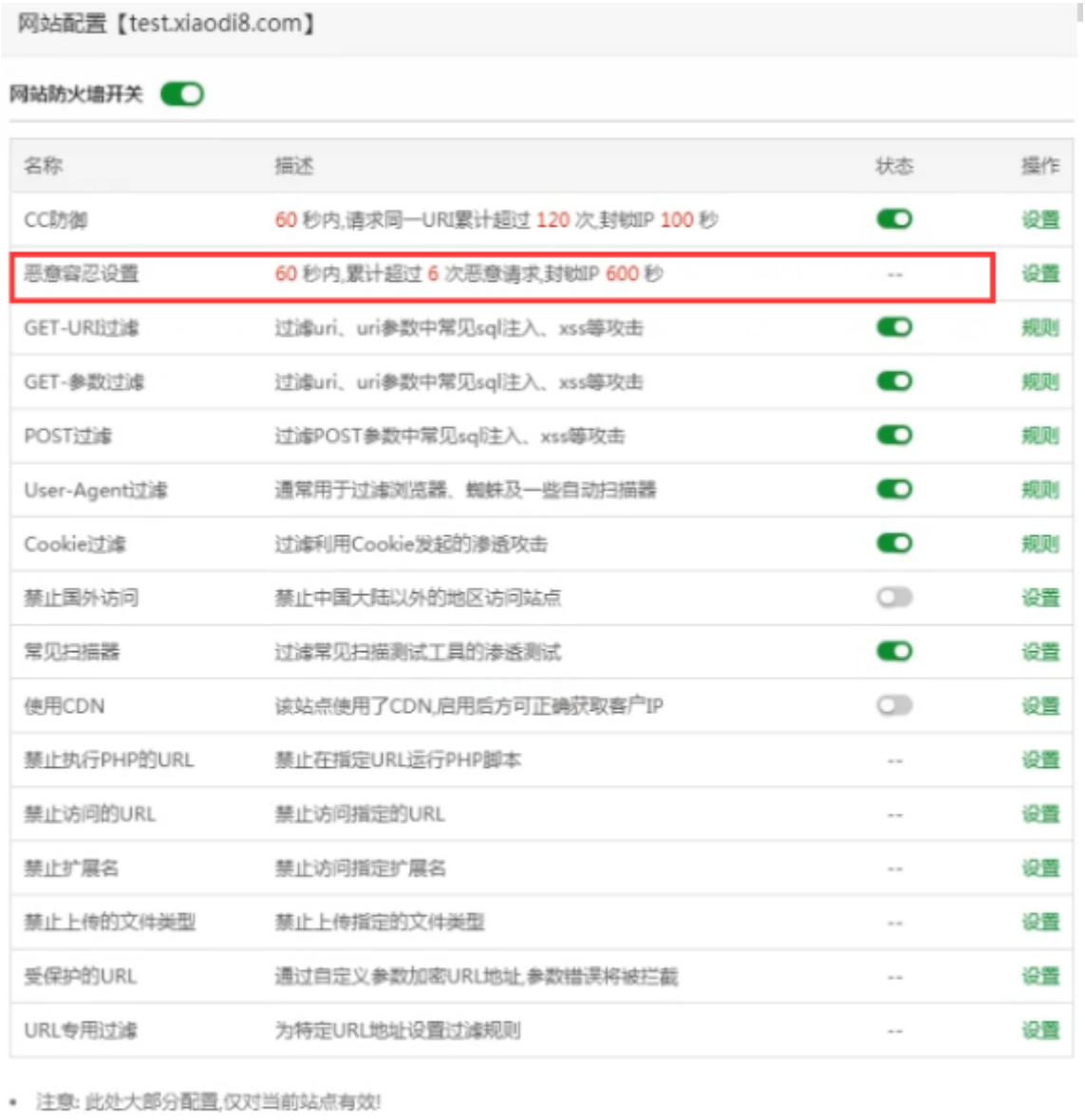
46.3 Aliyun_os-默认拦截机制分析绕过-简要界面

- 阿里云-无法模拟搜索引擎爬虫绕过，只能采用代理池或者延时。
- 一般访问频率过快，站点直接就访问不了，一个小时后才可以访问。

46.4 BT(防火墙插件)-默认拦截机制分析绕过-简要界面

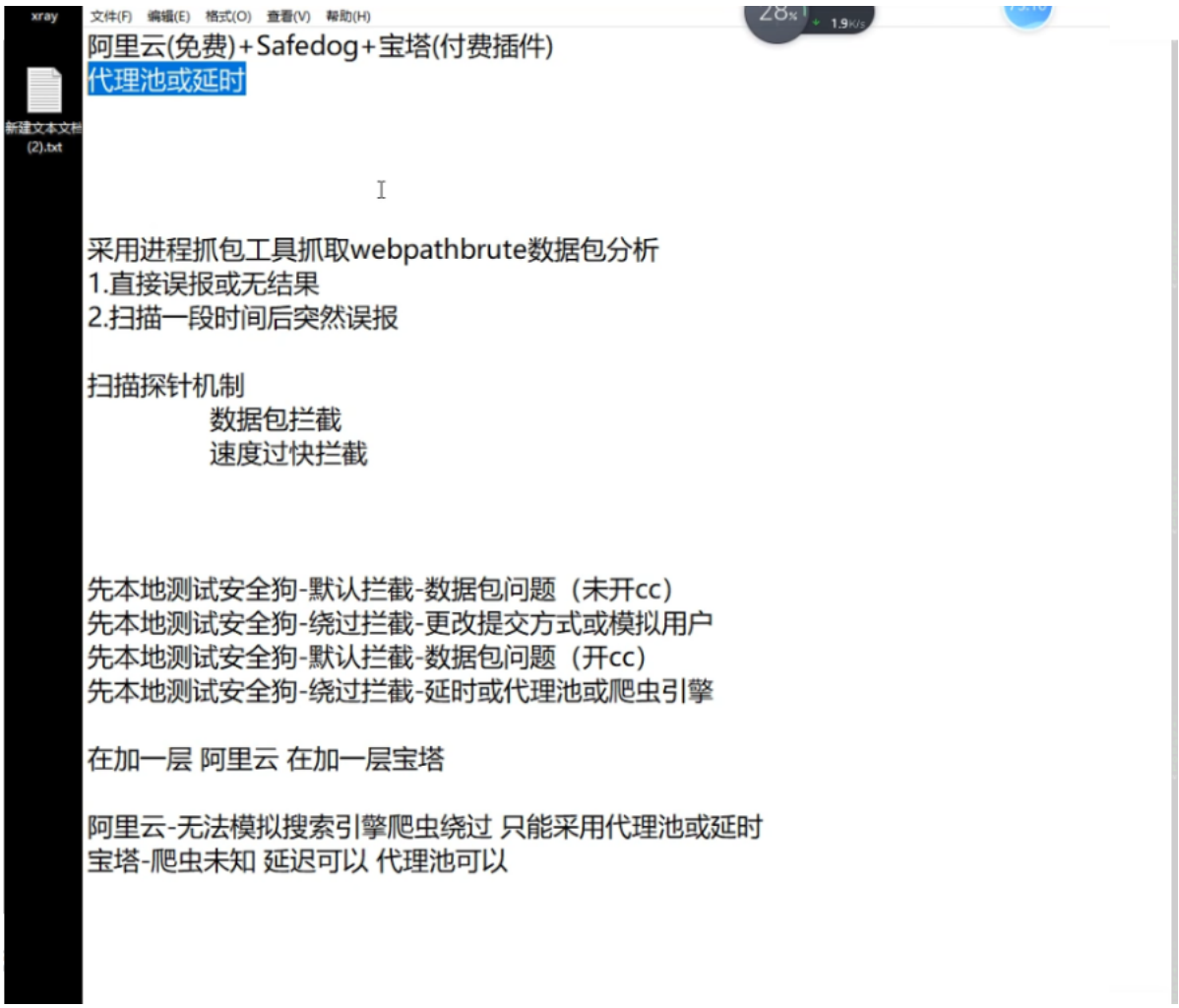


扫描3个后就不行，不是alliyun拦截的，而是BT的防火墙拦截的:



```
绕过:
字典拆开使用 ， 绕过他的恶意容忍机制60秒内6次
字典优化
index.php.bak ------> index.php.bak.
```

46.5 总结



资源:

```
https://www.bt.cn/
http://free.safedog.cn/website_safedog.html
https://www.cnblogs.com/iack/p/3557371.html
```