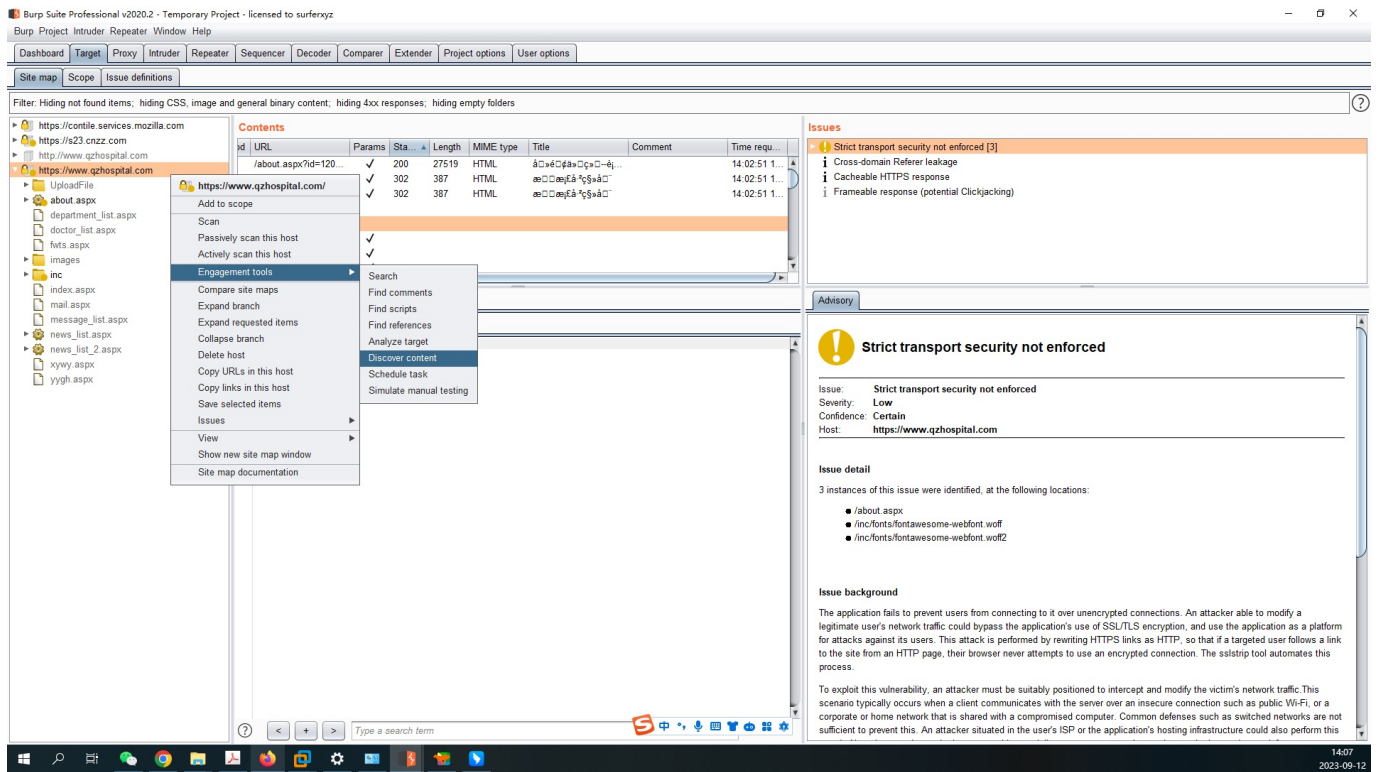


# 1. 使用 Burp 的 Discover Content 功能爬取任意站点的目录，给出爬取过程的说明文档、站点树截图；

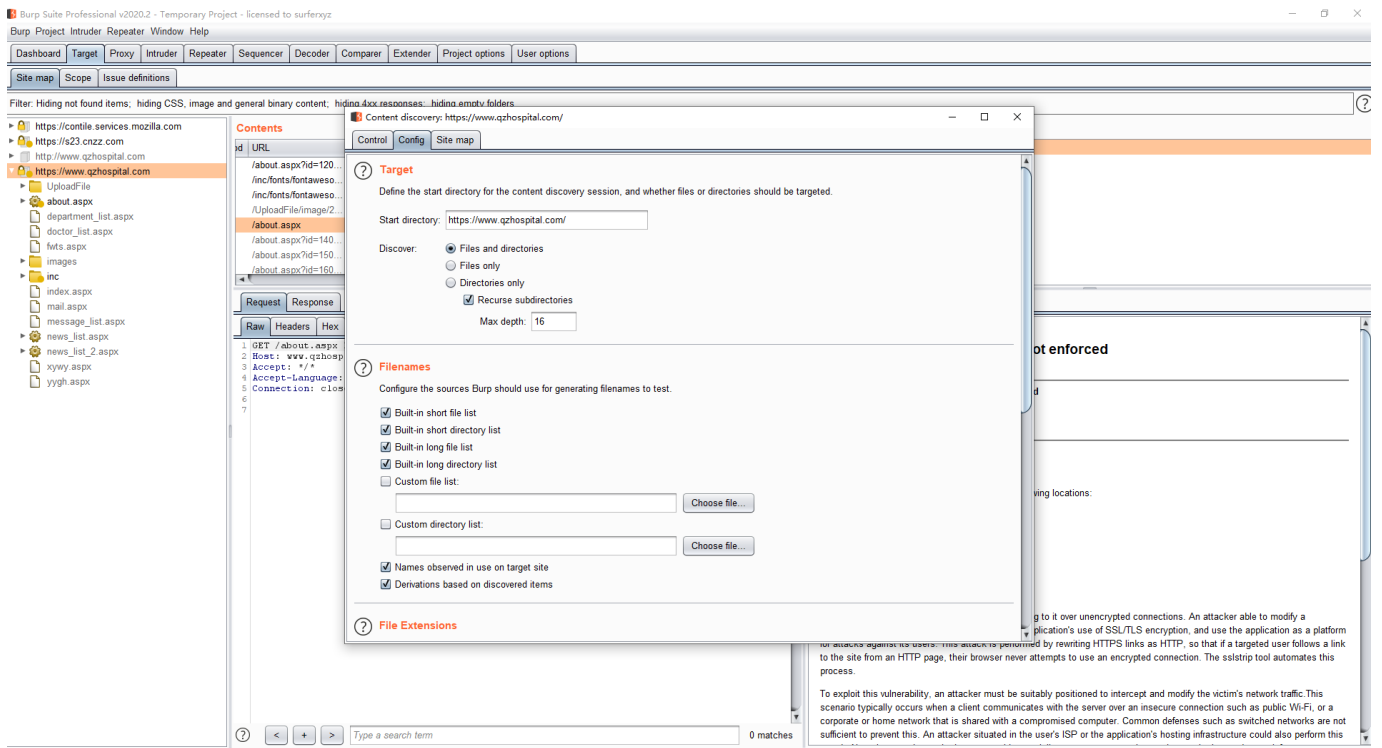
## 一、打开火狐浏览器，开启burp代理



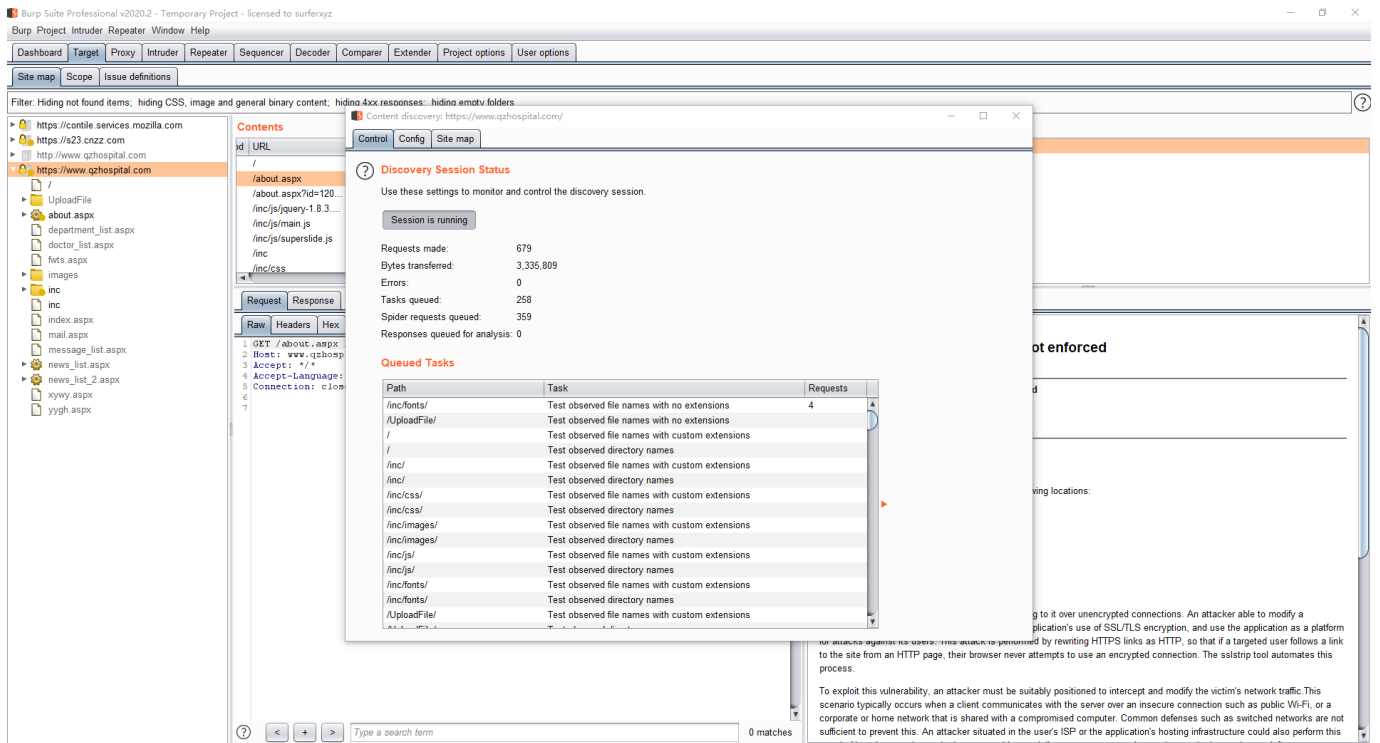
## 二、打开burp,点击target里面的Engagement tools的Discover content.



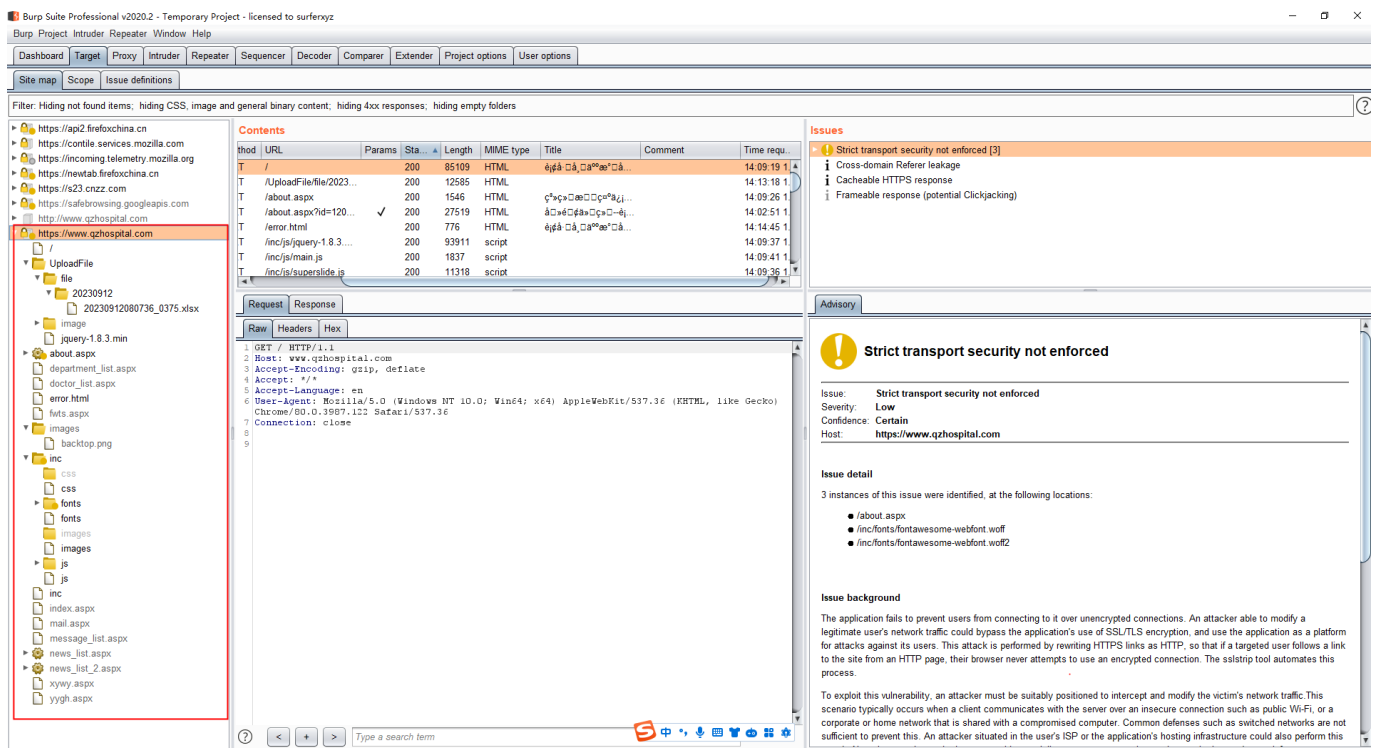
### 三、Discover content 设置



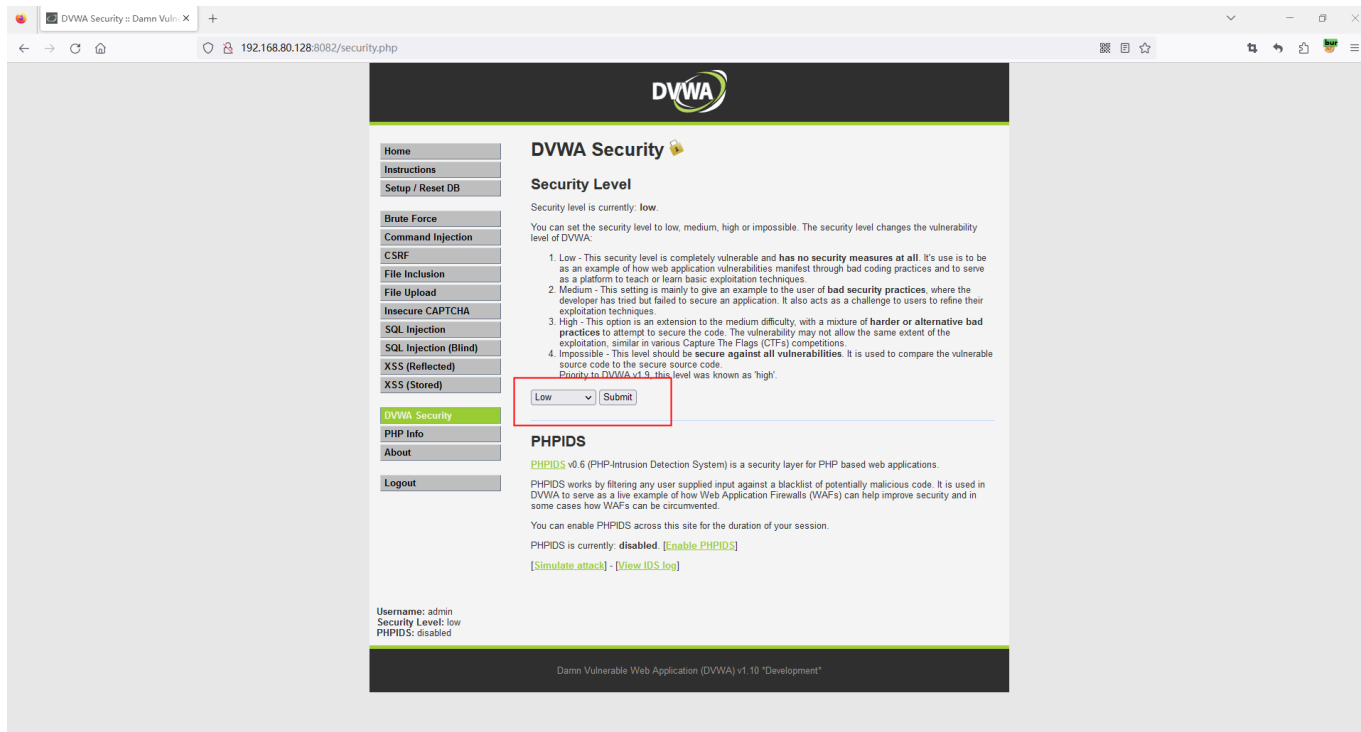
### 四、点击session running



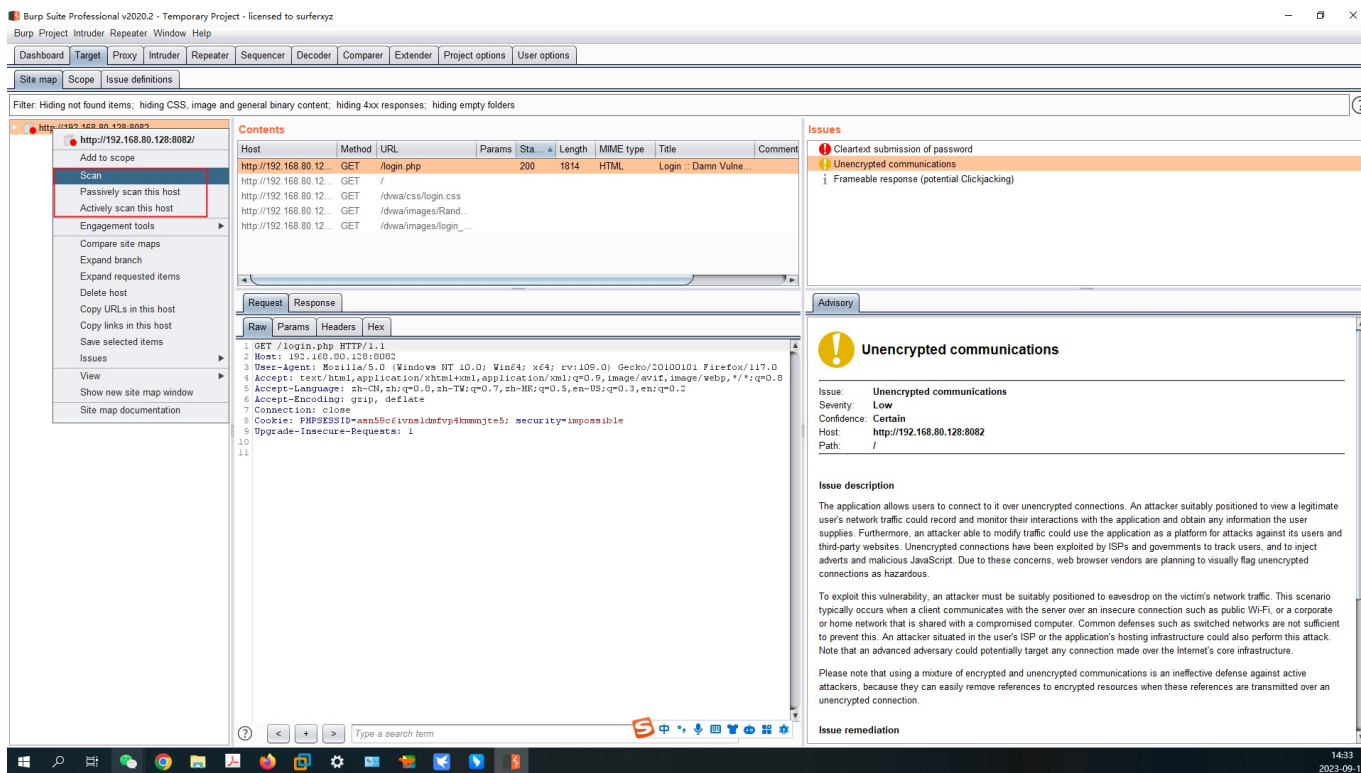
## 五、树状图展示



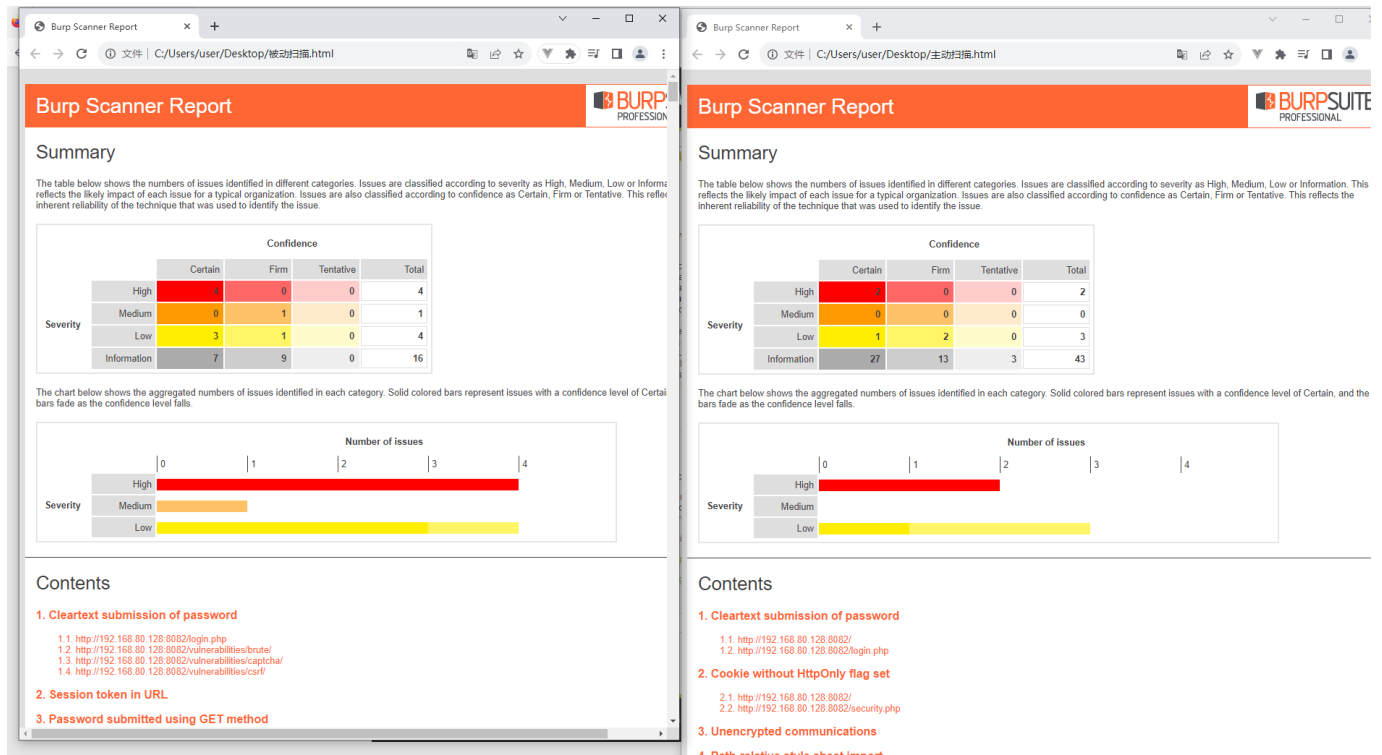
## 2. 分别使用 Burp Scan 的主动扫描和被动扫描功能对 DVWA 站点进行扫描，输出扫描报告；



## 主动扫描和被动扫描

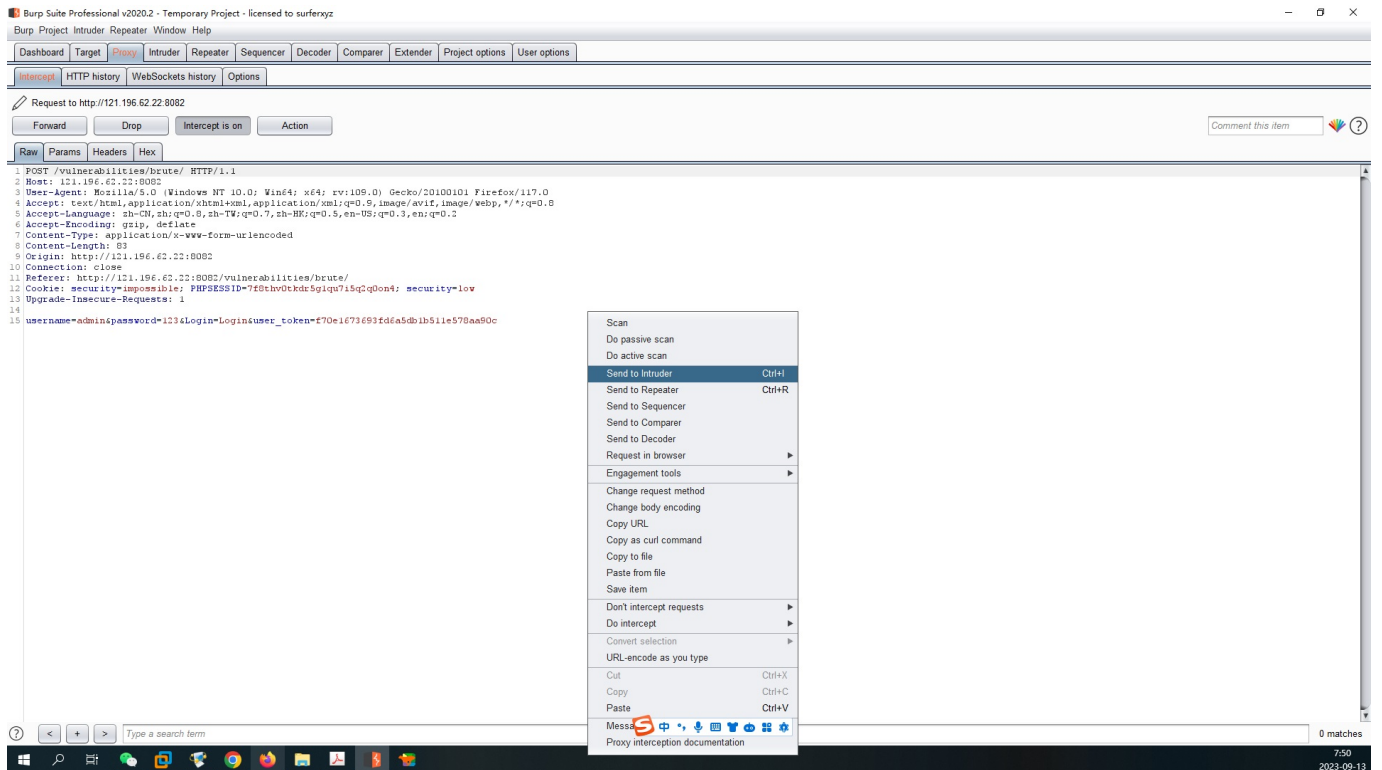


## 主动和被动扫描报告导出



### 3. Burp Intruder 爆破题目

#### (一) 生日日期爆破



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

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

2

Target Positions Payloads Options

**1 Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the number of positions.

Payload set: 1 Payload count: 365

Payload type: Dates Request count: 365

**2 Payload Options [Dates]**

This payload type generates date payloads within a given range and in a specified format.

From: 1 January 2023

To: 31 December 2023

Step: 1 Days

Format: 09/23

MMdd

Example: 0101

**3 Payload Processing**

You can define rules to perform various processing tasks on each payload before it is sent to the target.

Add Enabled Rule

Edit

Remove

Up

Down

**4 Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: /<>?&\*~'"|

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			5257	
1	0101	200			5198	
2	0102	200			5198	
3	0103	200			5198	
4	0104	200			5198	
5	0105	200			5198	
6	0106	200			5198	
7	0107	200			5198	
8	0108	200			5198	
9	0109	200			5198	

Finished

different ways.

Start attack

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

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

1 2

Target Positions Payloads Options

**1 Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the number of positions.

Payload set: 1 Payload count: 365

Payload type: Dates Request count: 365

**2 Payload Options [Dates]**

This payload type generates date payloads within a given range and in a specified format.

From: 1 January 2023

To: 31 December 2023

Step: 1 Days

Format: 23-9-13

MMdd

Example: 0101

**3 Payload Processing**

You can define rules to perform various processing tasks on each payload before it is sent to the target.

Add Enabled Rule

Edit

Remove

Up

Down

**4 Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		302			327	
1	0101	302			327	
2	0102	302			327	
3	0103	302			327	
4	0104	302			327	
5	0105	302			327	
6	0106	302			327	
7	0107	302			327	
8	0108	302			327	
9	0109	302			327	

Request Response

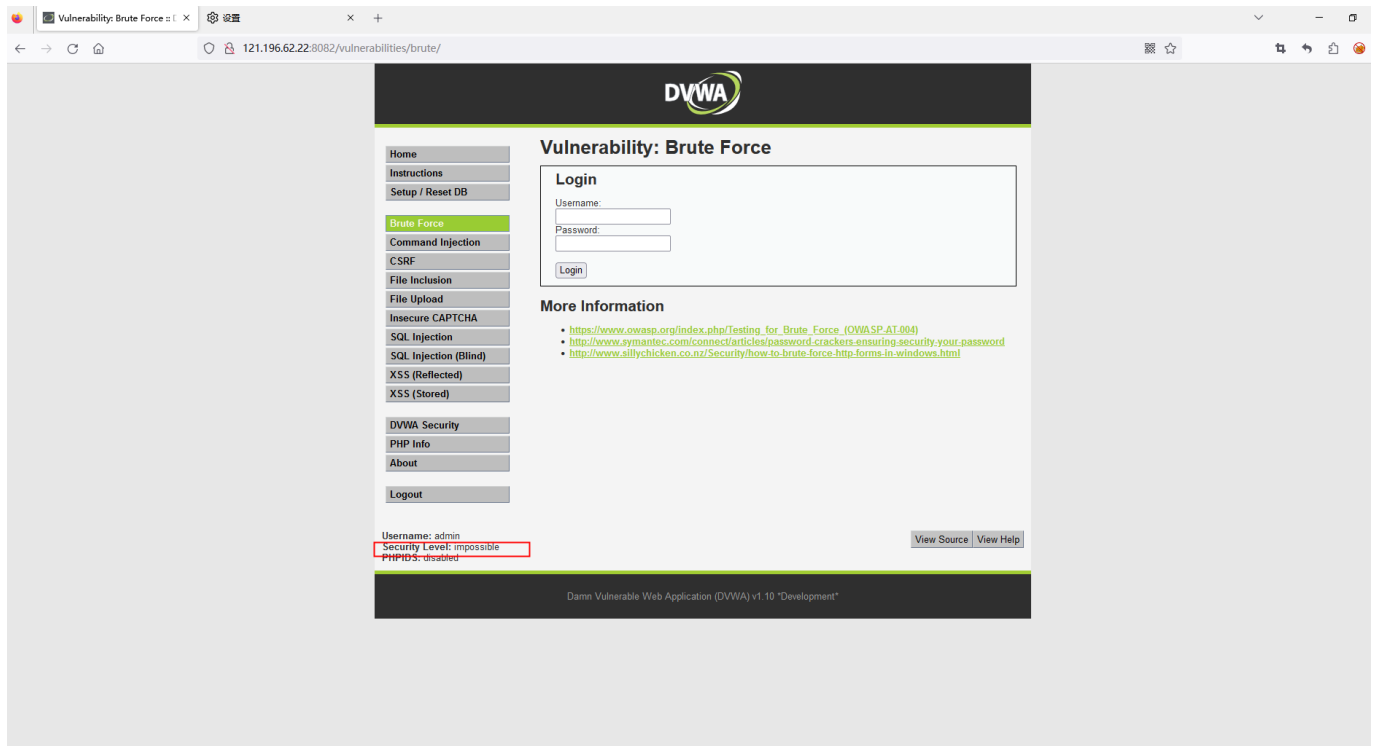
Raw Headers Hex

```
1 HTTP/1.1 302 Found
2 Date: Tue, 12 Sep 2023 23:52:54 GMT
3 Server: Apache/2.4.18 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
6 Pragma: no-cache
7 Location: index.php
8 Content-Length: 0
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
```

0 matches

Finished

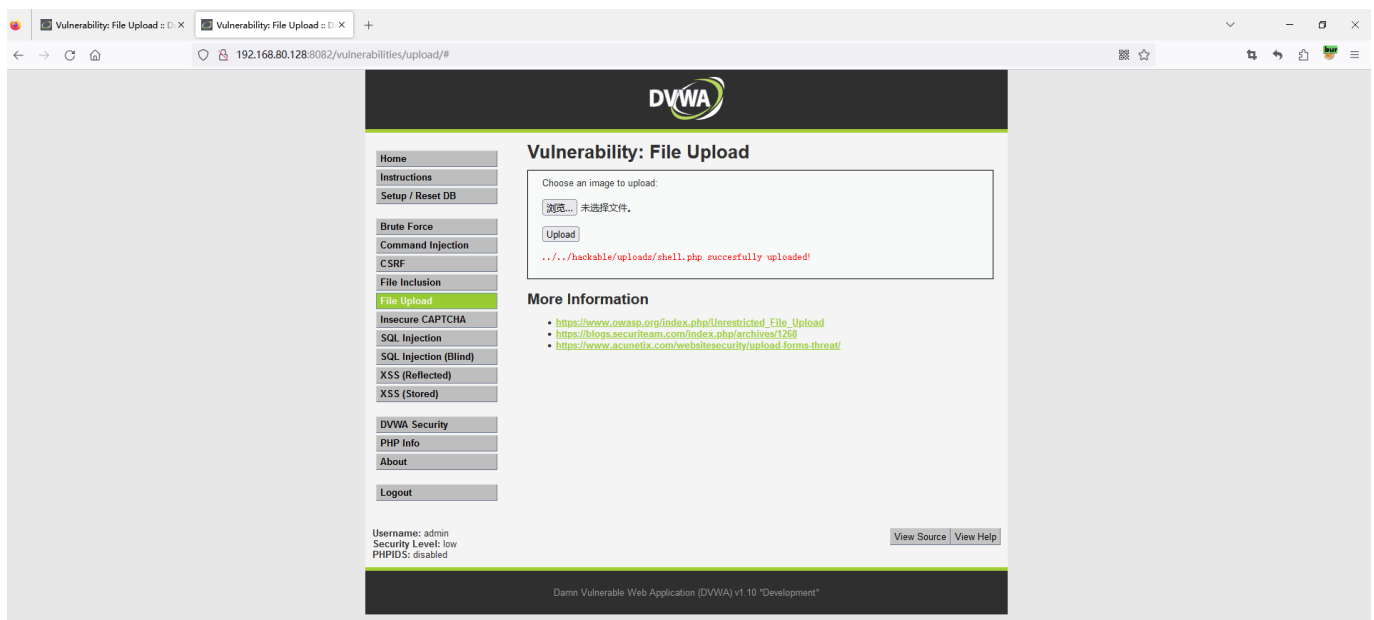




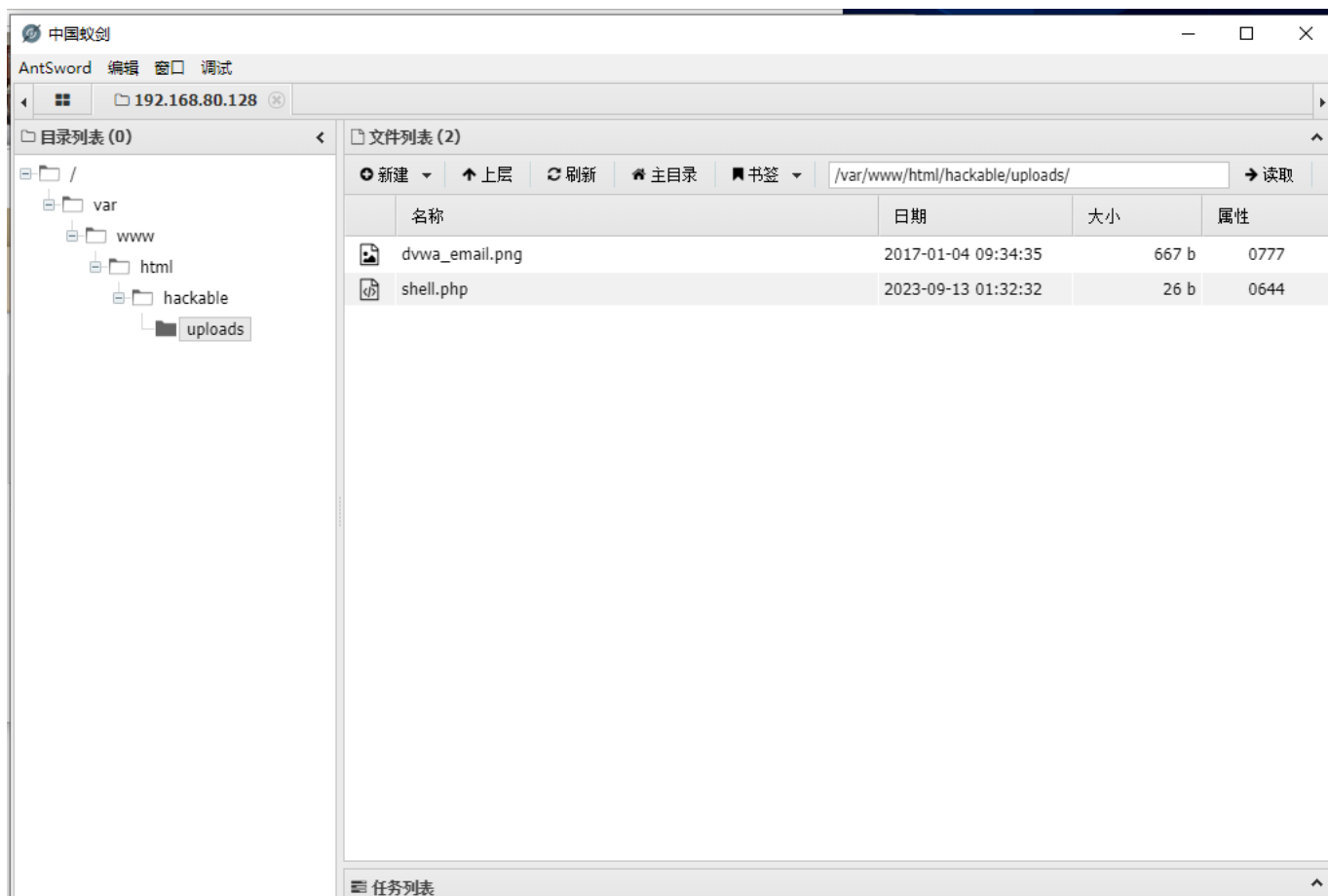
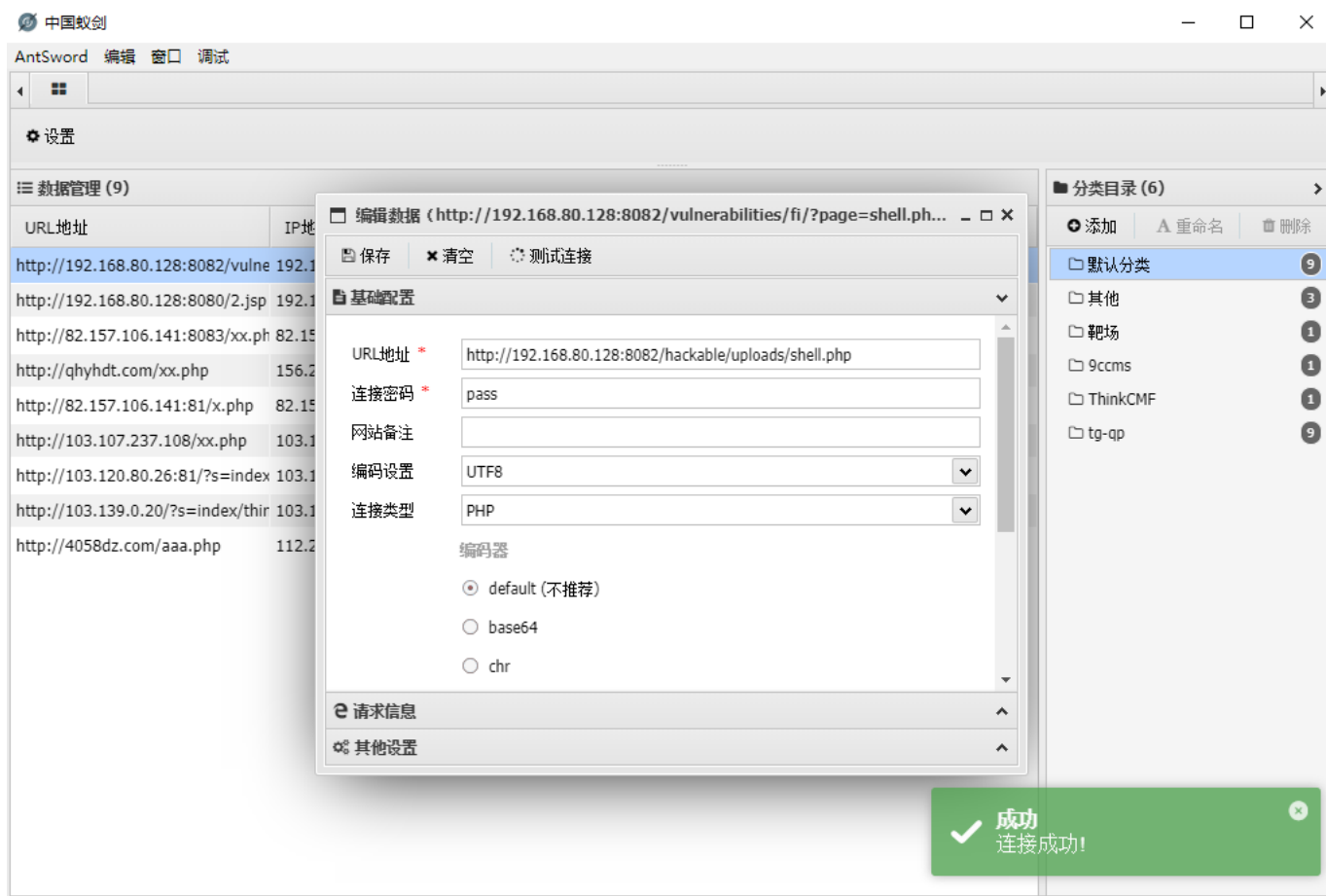
靶场环境level一直是impossible,无法爆破

(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

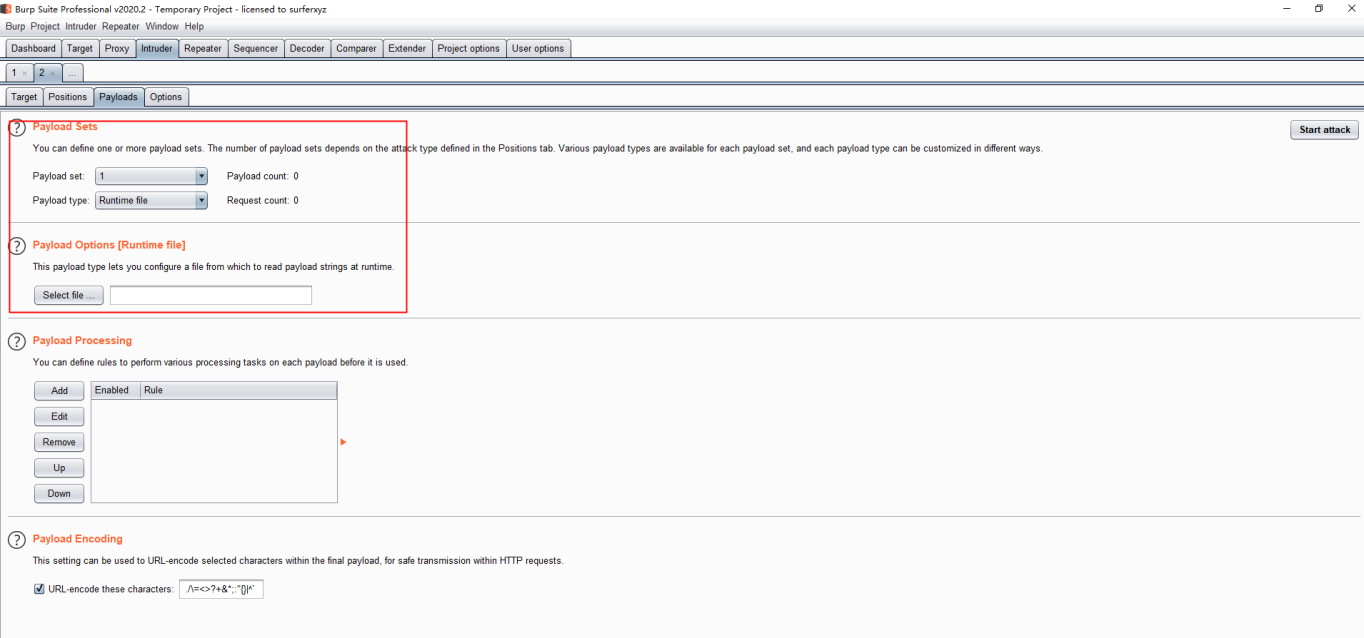


(2) 通过蚁剑连接, 进行目录暴露, geektime文件查找



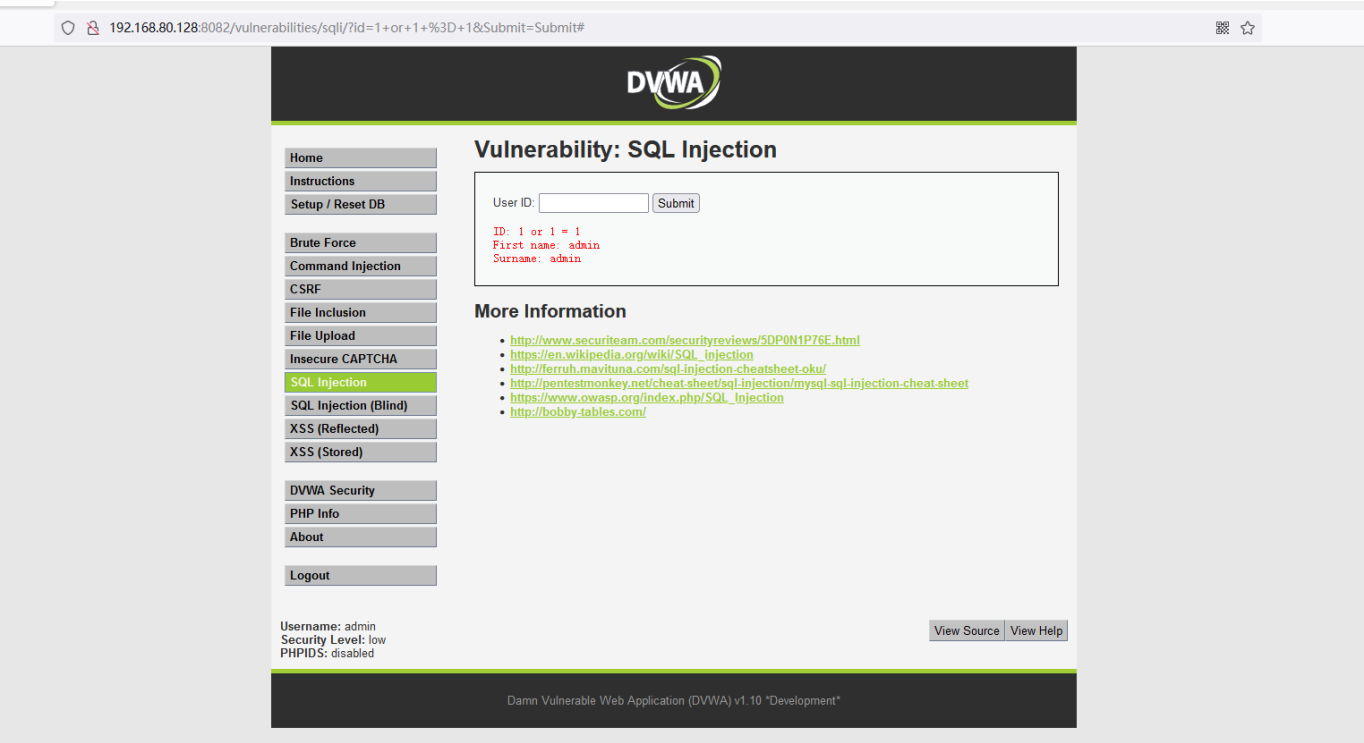


### (3)利用导入文件进行密码爆破



### 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](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](https://www.owasp.org/index.php/SQL_injection)
- <http://bobby-tables.com/>