

环境安装

由于已经将win10虚拟机和win10宿主机ping通，所以选择在win10宿主机上安装环境来进行实验
并且python&java&burp等环境之前均已安装，所以直接展示结果

安装python3.8

```
BexhOlder@DESKTOP-O4JCLR x + v
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

python3.8.0b4
Python 3.8.0b4 (tags/v3.8.0b4:d93605d, Aug 29 2019, 23:21:28) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> |
```

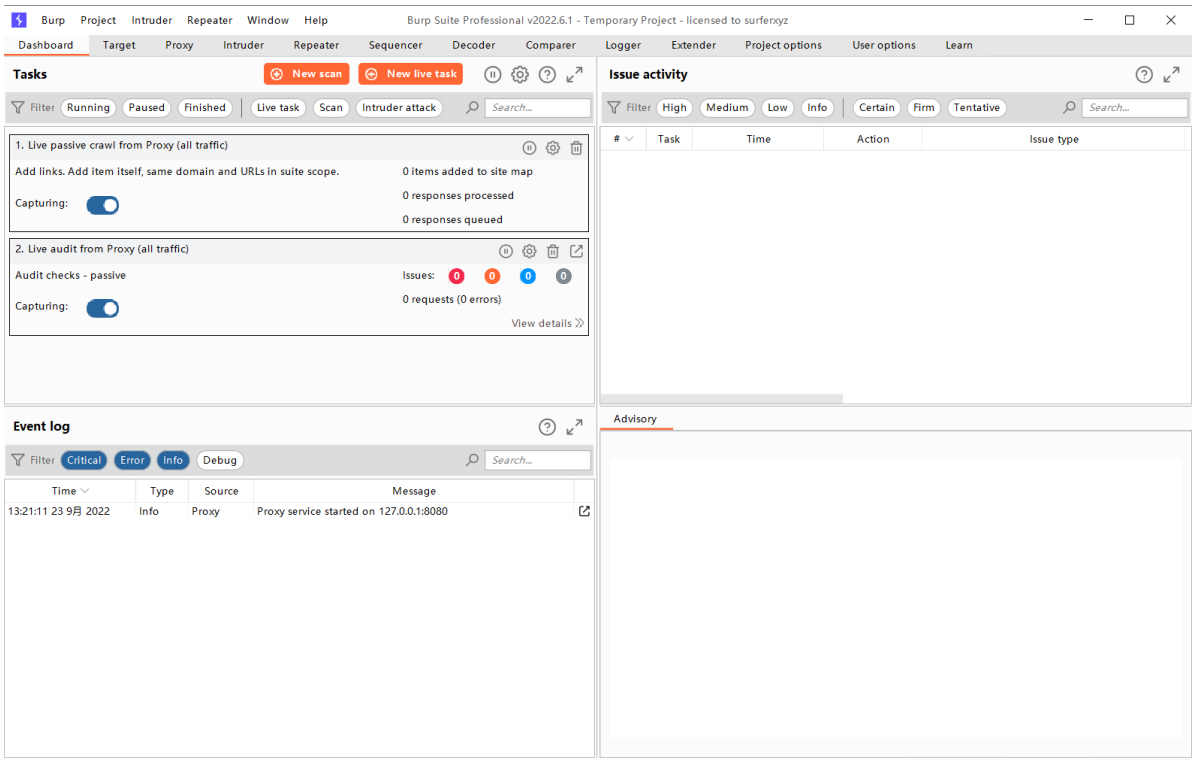
安装JDK18

```
BexhOlder@DESKTOP-O4JCLR x + v
加载本机代理库 <库名>，例如 -agentlib:jdwp
另请参阅 -agentlib:jdwp=help
-agentpath:< 路径名>[=<选项>]
按完整路径名加载本机代理库
-javaagent:<jar 路径>[=<选项>]
加载 Java 编程语言代理，请参阅 java.lang.instrument
-splash:< 图像路径>
使用指定的图像显示启动屏幕
自动支持和使用 HiDPI 缩放图像
(如果可用)。应始终将未缩放的图像文件名 (例如, image.ext)
作为参数传递给 -splash 选项。
将自动选取提供的最合适的缩放
图像。
有关详细信息，请参阅 SplashScreen API 文档
@argument 文件
一个或多个包含选项的参数文件
-disable-@files
阻止进一步扩展参数文件
--enable-preview
允许类依赖于此发行版的预览功能
要为长选项指定参数，可以使用 --<名称>=<值> 或
--<名称> <值>。

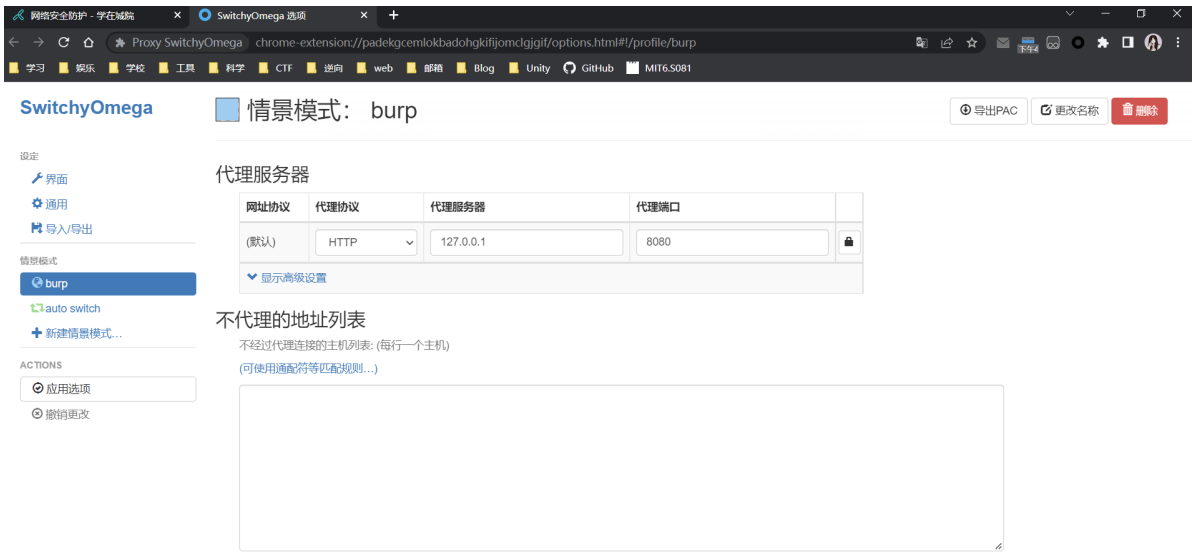
java -version
java version "18.0.1.1" 2022-04-22
Java(TM) SE Runtime Environment (build 18.0.1.1+2-6)
Java HotSpot(TM) 64-Bit Server VM (build 18.0.1.1+2-6, mixed mode, sharing)

14:38:46 75ms
```

安装Burp



安装代理插件并配置代理



安装CA证书

正在完成证书导入向导

单击“完成”后将导入证书。

你已指定下列设置:

用户选定的证书存储	受信任的根证书颁发机构
内容	证书
文件名	C:\Life\Downloads\ChromeDownload\cacert.der

完成(F)

取消

成功拦截

Burp Suite Professional v2022.6.1 - Temporary Project - Licensed to surferoxy

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

Intercept HTTP history WebSockets history Options

Request to https://data.bilibili.com:443 [218.60.18.12]

Forward Drop Intercept is on Action Open Browser

Comment this item HTTP/2

Pretty Raw Hex

```
1 POST /log/web?
000U0171663916249649http%3A%2F%2Fwww.bilibili.com%2F1333.1007-selfDef.page_show%1166391624900010101536x66611(%22event%2
2:%22page_show%22,%22value%22:(%22visibleSessionId%22:%2212guvqvqob%22,%22pageSessionId%22:%2275ghhh6pxck0K2C),%22source
ce%22:%22%22))(%22b_ut%22:%225482c,%22home_version%22:%22V482c,%221-wanna-go-back%22:%221-%22,%22in_new_ab%22:true,%22vid_v
ersion%22:%222for_ai_home_version%22:%22V482c,%22for_watchlater_version%22:%22V1%22,%22for_adblock_tlp%22:%23HIDE%22,%22cf_e
or_avif_gray%22:%22V AVIF%22),%22ab_split_num%22:(%22for_ai_home_version%22:78,%22for_watchlater_version%22:2,%22for_adbl
ock_tlp%22:6,%22for_avif_gray%22:42)))|1BE8B103A-8F27-11D1-BDA5-2913BC10E8C6122410info{zh-CN|null||} HTTP/2
2 Host: data.bilibili.com
3 Cookie: buvid4=9P856AP-BA38-1803-F7D2-2816315AB0FF22568info; i-wanna-go-back=-1; uuid=
1BE8B103A-8F27-11D1-BDA5-2913BC10E8C6122410info; buvid4=
5506C551-7559-BAC0-3803-02945691481823874-D2C043800-L1kXHVvzwaIPHG8SGpw3d3nQ; buvid_fp_plain=undefined; hit-dyn-v2=1;
blackside_state=0; CURRENT_BLACKGAP=0; rpidid=(k|YkHPV1PD3|uYluumkky; LIVE_BUVID=AUTO616511277761917; nostalgia_conf=
-1; CURRENT_QUALITY=120; is-2022-channel=1; DedeUserID=341398932; DedeUserID_ckm5=de5af0f0c791428; buvid_fp=
2be5a50673b385e0f6682bd0b02fbb; b_ut=5; fingerprint3=50599e0c42abd01acc9b9373ec3ec44c; fingerprint=
4ee2ac57c694ae5edf2f82374fc2cd60; PVID=1; CURRENT_FINAL=16; innerSign=0; h_lcid=2185FD210_18369175850;
SESSDATA=eef647482c16794674842cc69cb12A91; b_jlt_ct=65e5bf71e2910928b32cbec730584d31; sid=oioil113n;
bp_video_offset_341398932=708995634682551600
4 Content-Length: 0
5 Sec-Ch-Ua: "Google Chrome";v="105", "Not(A)Brand";v="8", "Chromium";v="105"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0
Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept: */*
10 Origin: https://www.bilibili.com
11 Sec-Fetch-Site: same-site
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: empty
14 Referer: https://www.bilibili.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
17
18
```

Inspector

Request Attributes 2

Request Query Parameters 1

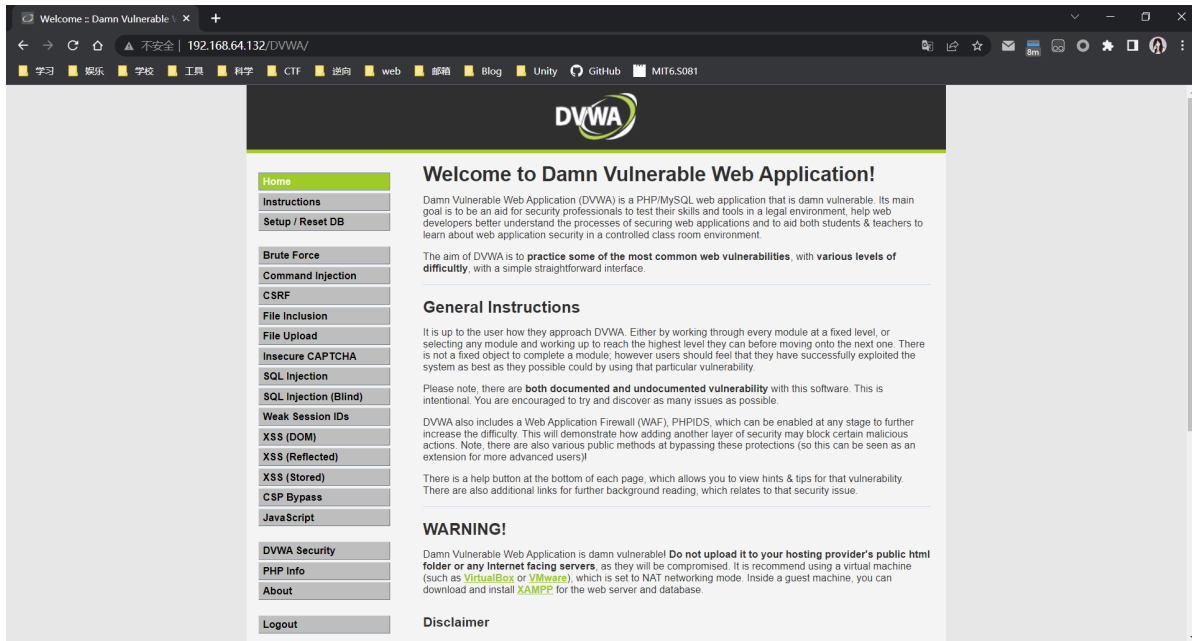
Request Body Parameters 0

Request Cookies 28

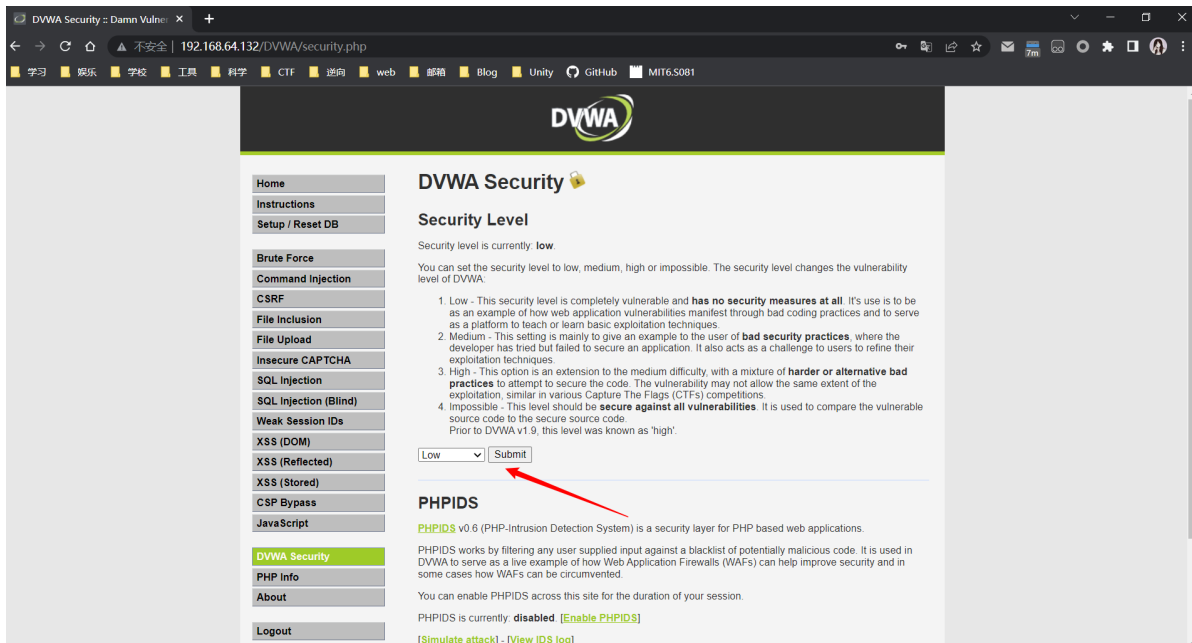
Request Headers 45

爆破过程

打开DVWA靶场

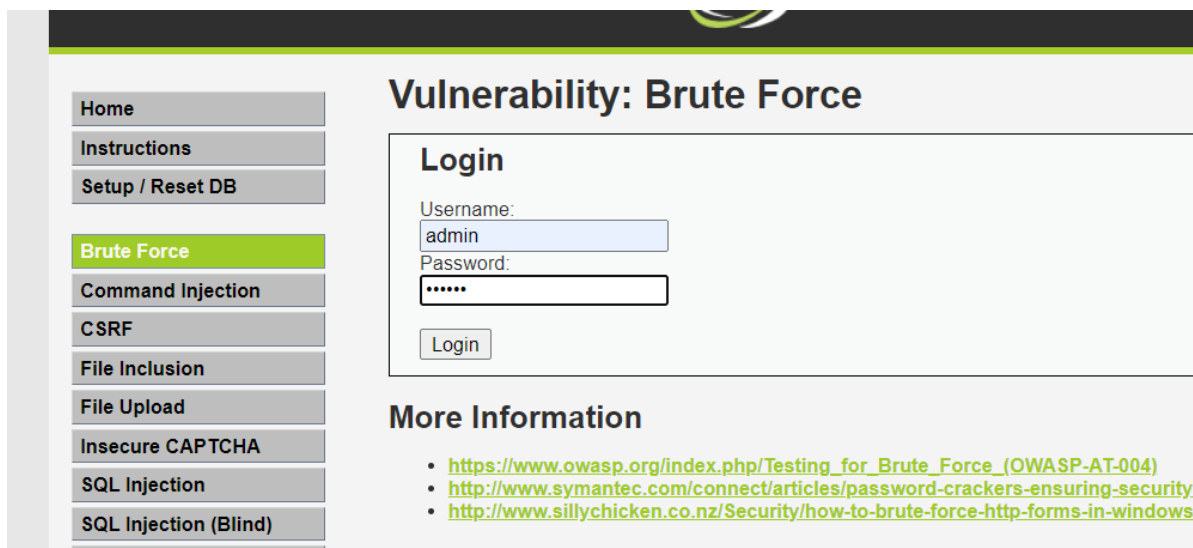


打开DVWA Security将Security Level设置为low并提交

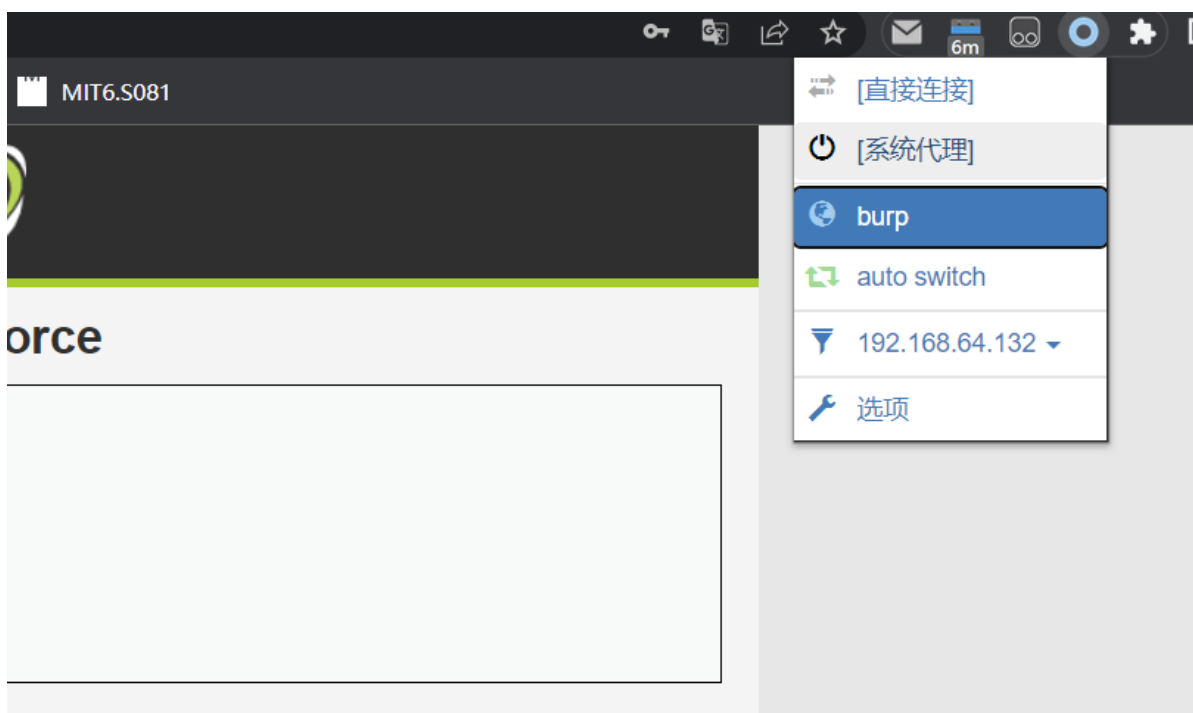


选择Brute Force关卡

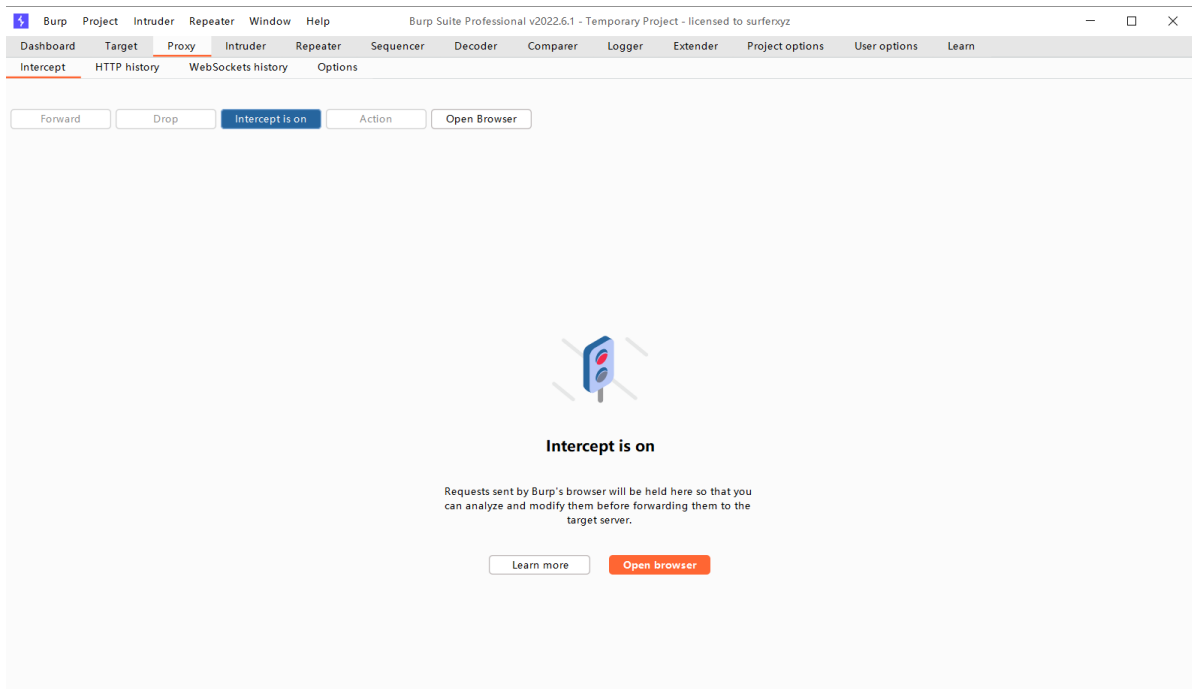
输入用户名admin和任意密码



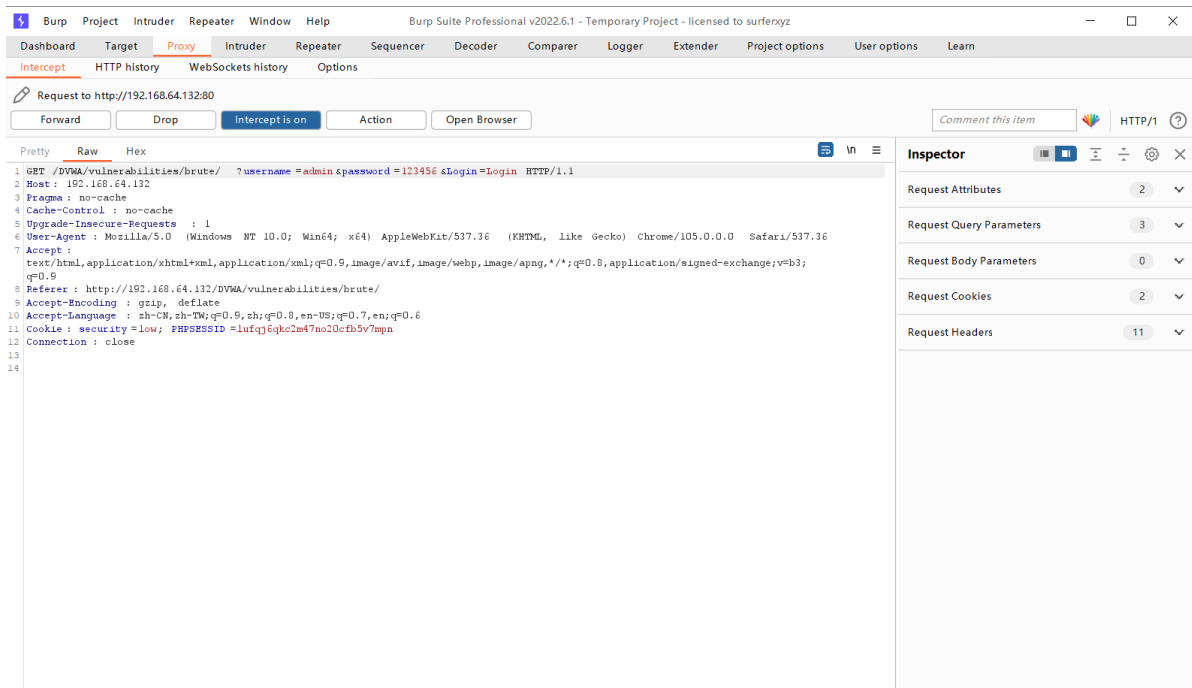
将代理切换到burp



将burp拦截打开

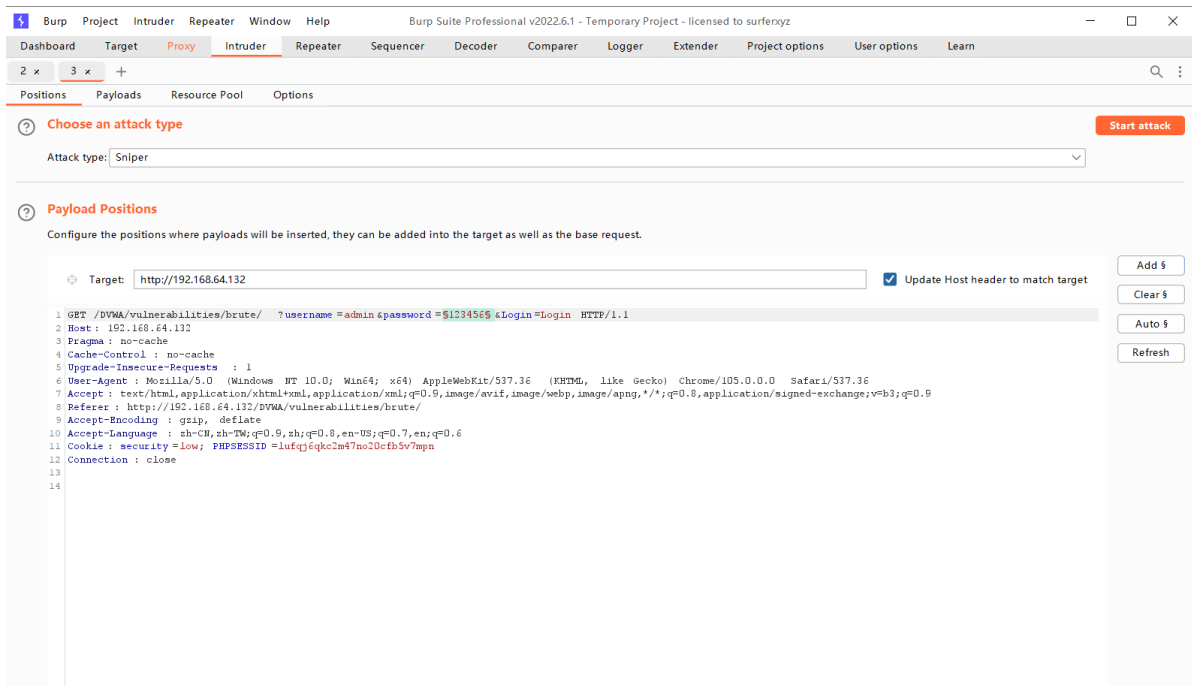


然后在网页中点击login按钮即可看到抓包

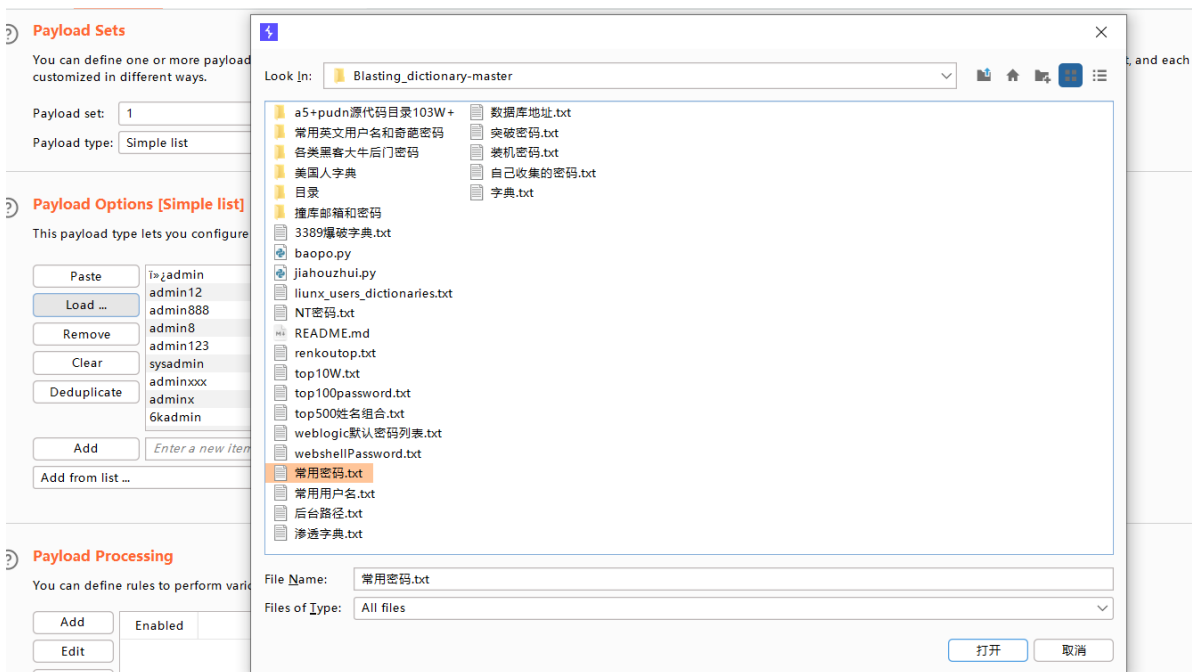


将其发送到Intruder爆破板块并设置爆破位置

选择Sniper模式



添加字典



开始爆破

完成后可以根据length发现不同

AttackSaveColumns5. Intruder attack of http://192.168.64.132 - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
19	password	200			4594	
0		200			4545	
1	admin	200			4545	
2	admin12	200			4545	
3	admin888	200			4545	
4	admin8	200			4545	
5	admin123	200			4545	
6	sysadmin	200			4545	
7	adminxxx	200			4545	
8	adminx	200			4545	
9	6kadmin	200			4545	
10	base	200			4545	
11	feitium	200			4545	
12	admins	200			4545	
13	root	200			4545	
14	roots	200			4545	
15	test	200			4545	
16	test1	200			4545	

RequestResponse

PrettyRawHex

```
1 GET /DVWA/vulnerabilities/brute/ ?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.64.132
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
7 Accept:
```

0 matches

Finished

实验密码是否正确

可以看到密码正确

Request

PrettyRawHex

```
1 GET /DVWA/vulnerabilities/brute/ ?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.64.132
3 Pragma: no-cache
4 Cache-Control: no-cache
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Referer: http://192.168.64.132/DVWA/vulnerabilities/brute/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
11 Cookie: security=low; PHPSESSID=lufqj6qkc2m47no20c6b5v7mpn
12 Connection: close
13
14
```

Response

PrettyRawHexRender

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Vulnerability: Brute

Login

Username:

Password:

Login

Welcome to the password protect

More Information

Inspector

Request Attributes2

Request Query Parameters3

Request Body Parameters0

Request Cookies2

Request Headers11

Response Headers9