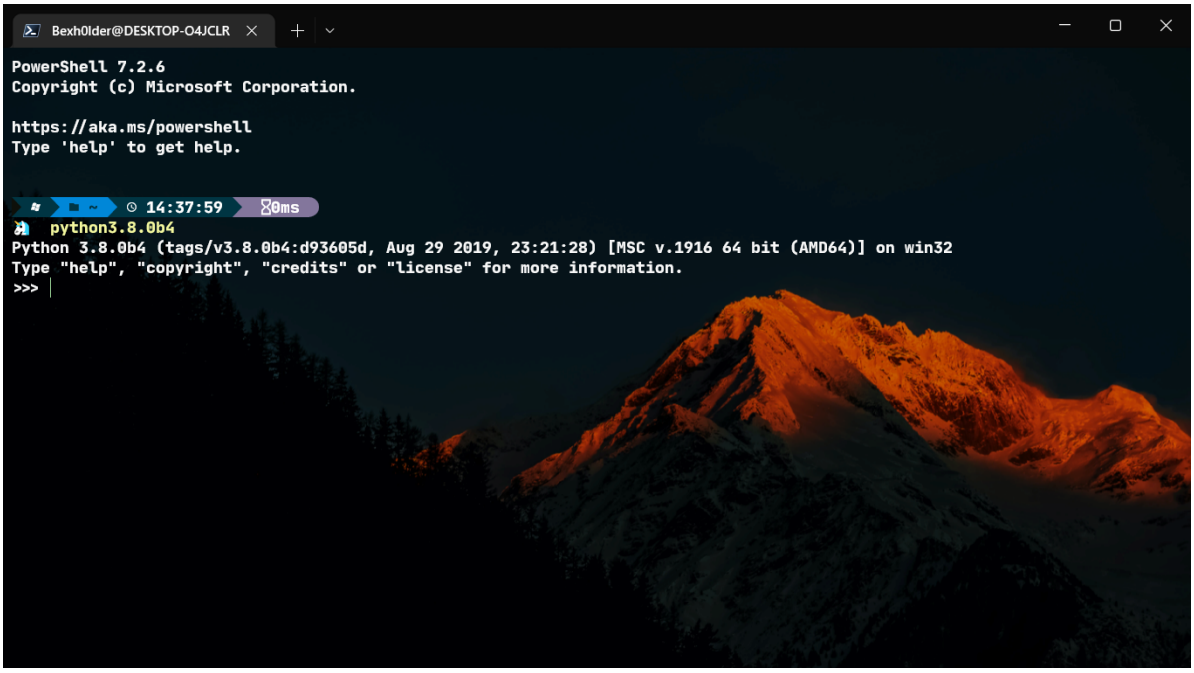
环境安装

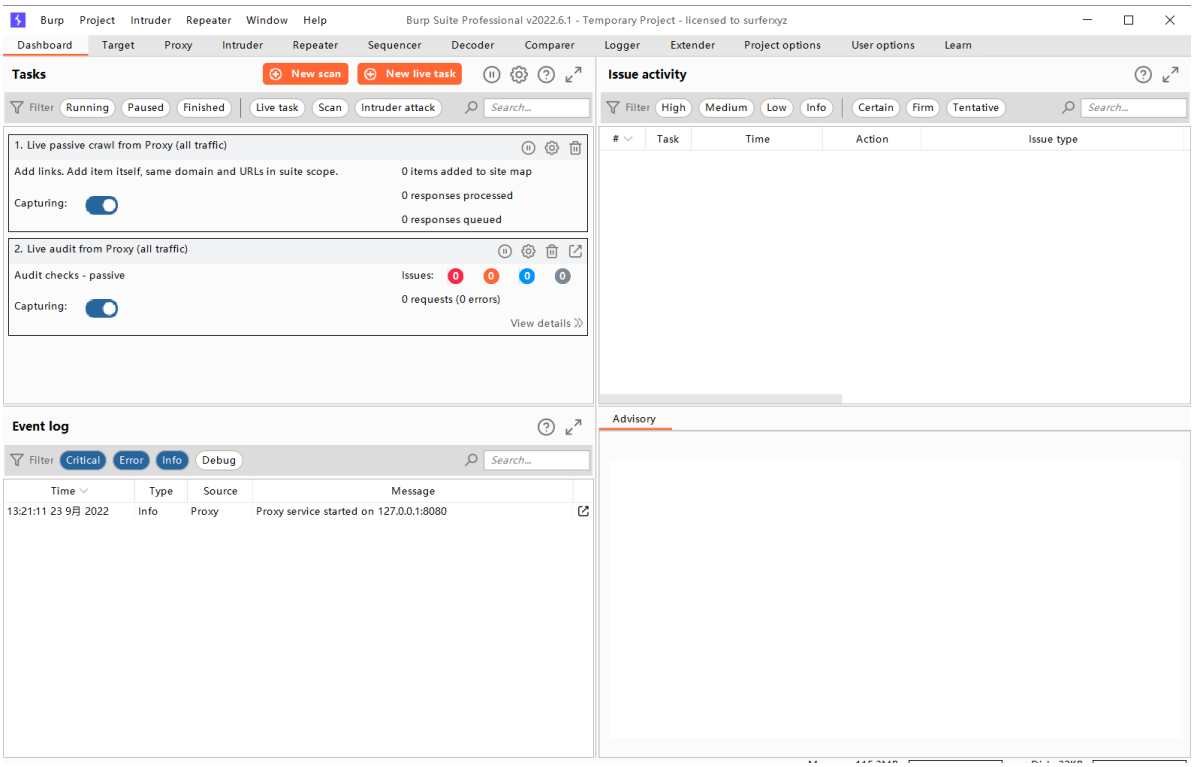
> 由于已经将win10虚拟机和win10宿主机ping通，所以选择在win10宿主机上安装环境来进行实验
>
> 并且python&java&burp等环境之前均已安装，所以直接展示结果

安装python3.8

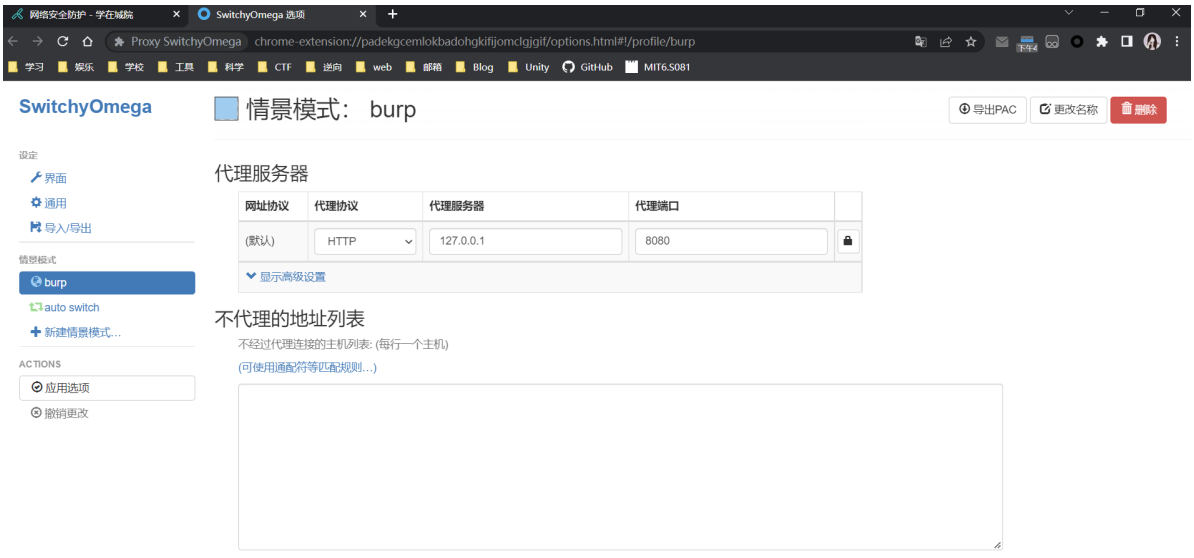


安装JDK18

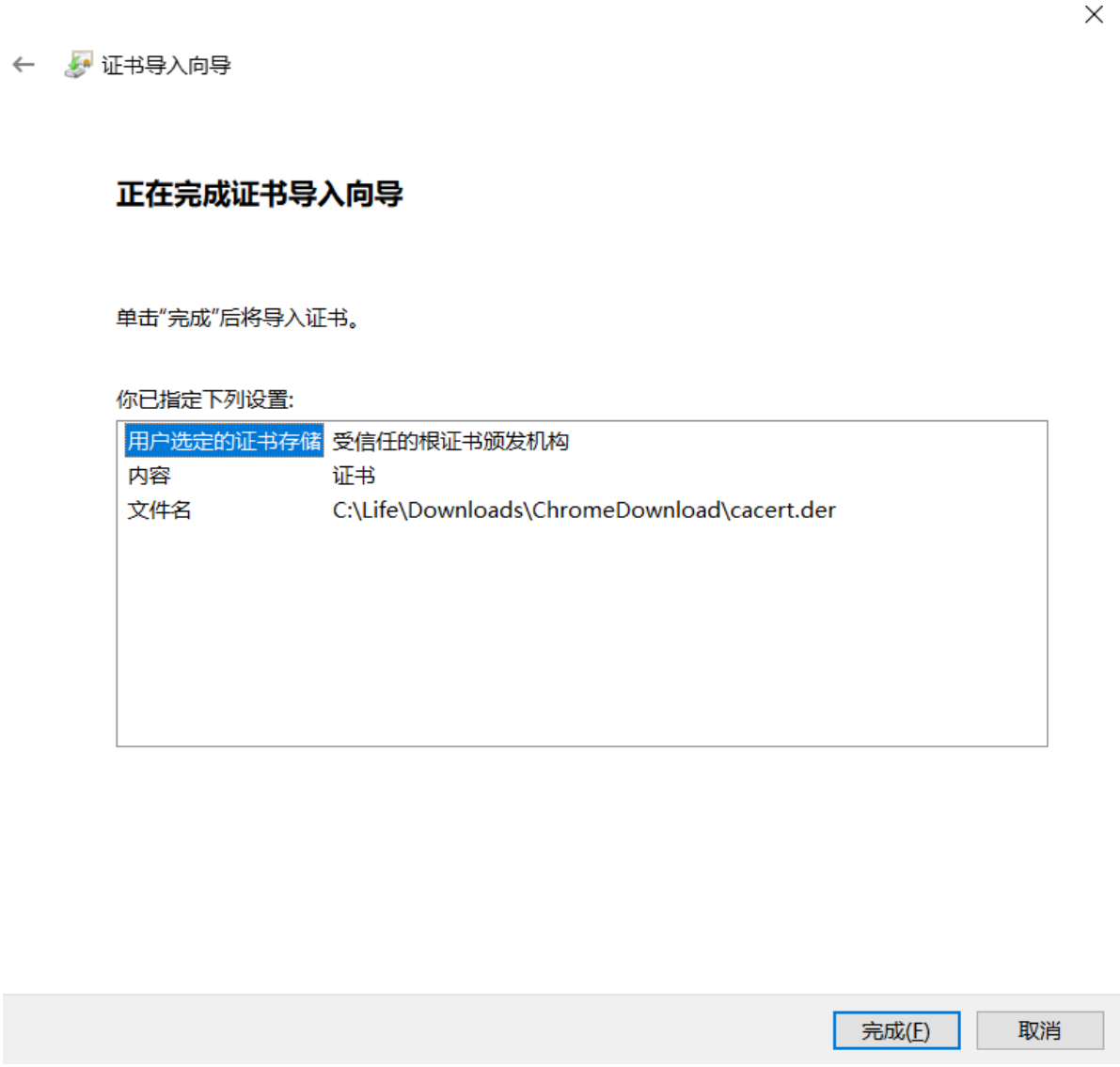
安装Burp



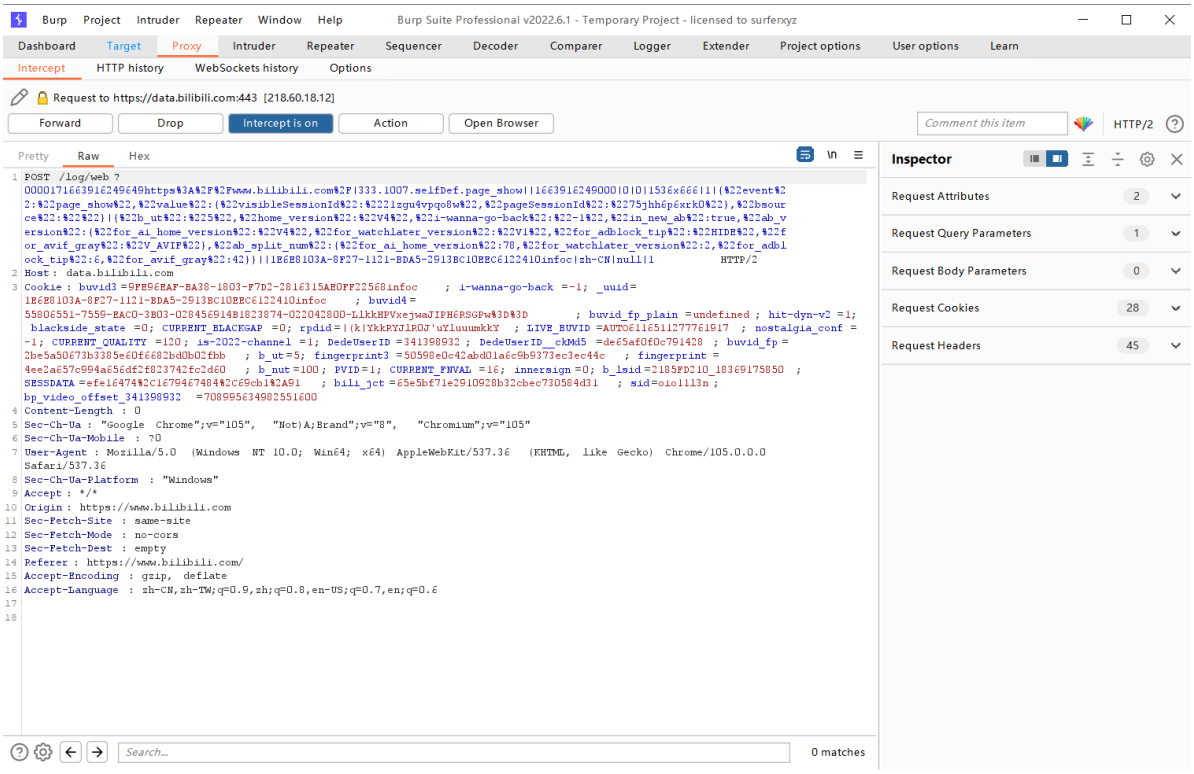
安装代理插件并配置代理



安装CA证书

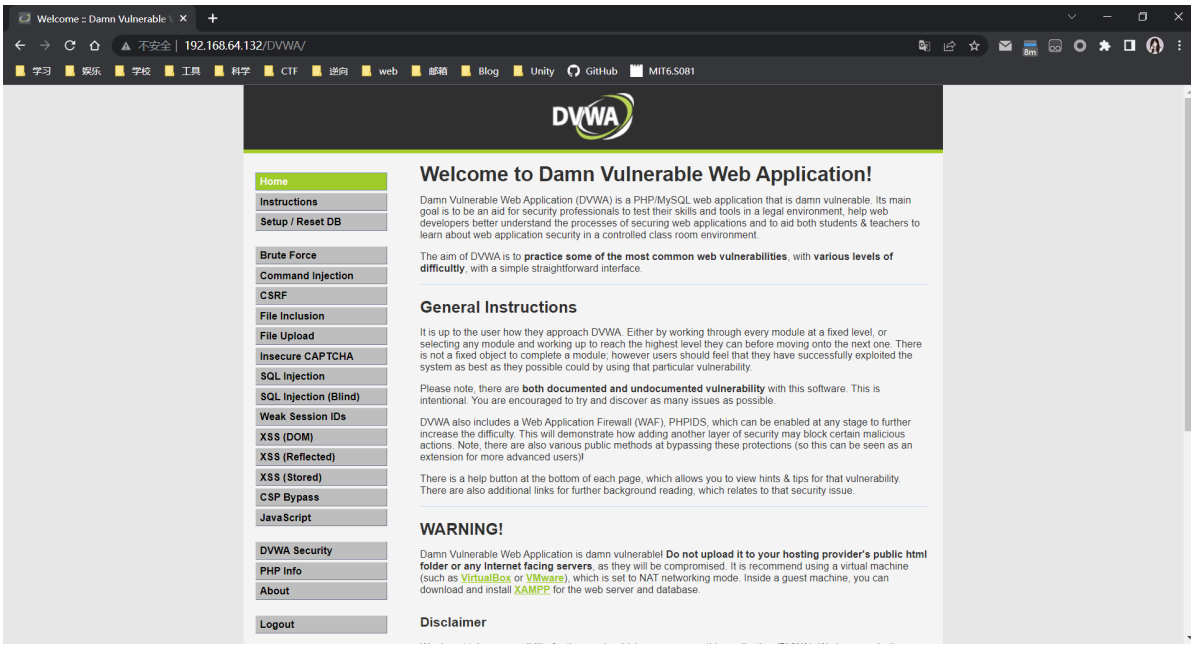

证书导入向导
正在完成证书导入向导
单击"完成"后将导入证书。
你已指定下列设置:
用户选定的证书存储
受信任的根证书颁发机构
内容
证书
文件名
C:\Life\Downloads\ChromeDownload\cacert.der
完成(F)
取消

成功拦截

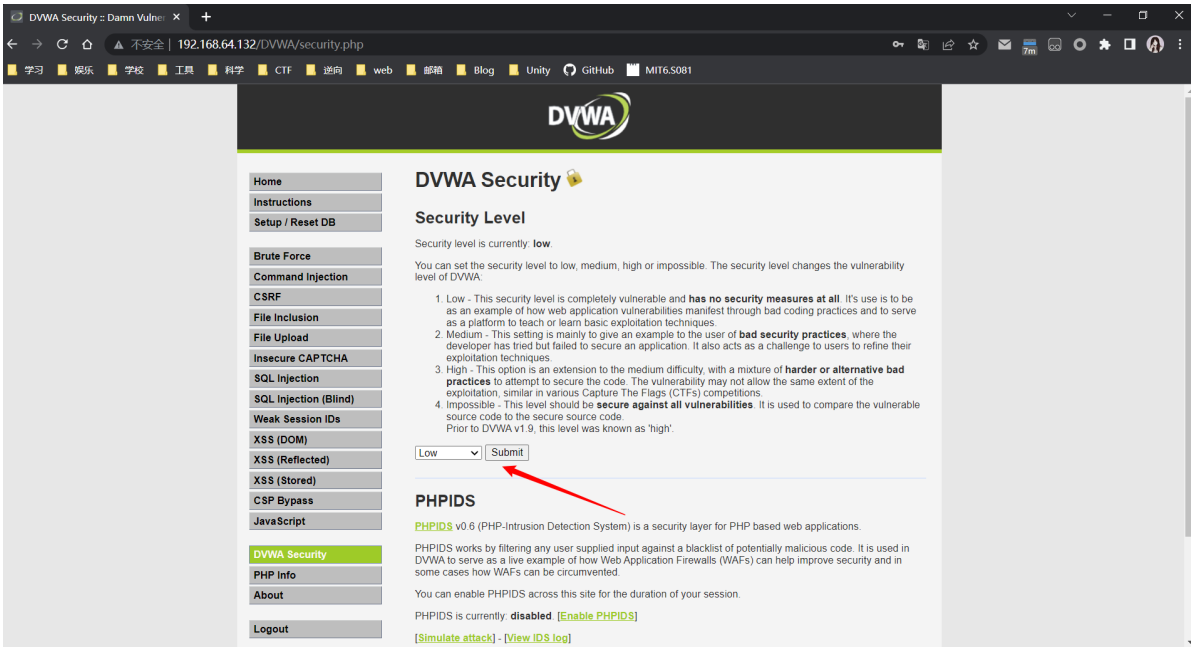

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.6.1 - Temporary Project - licensed to surferxyz
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to 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
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 28
Request Headers 45
Search...
0 matches

爆破过程

打开DVWA靶场

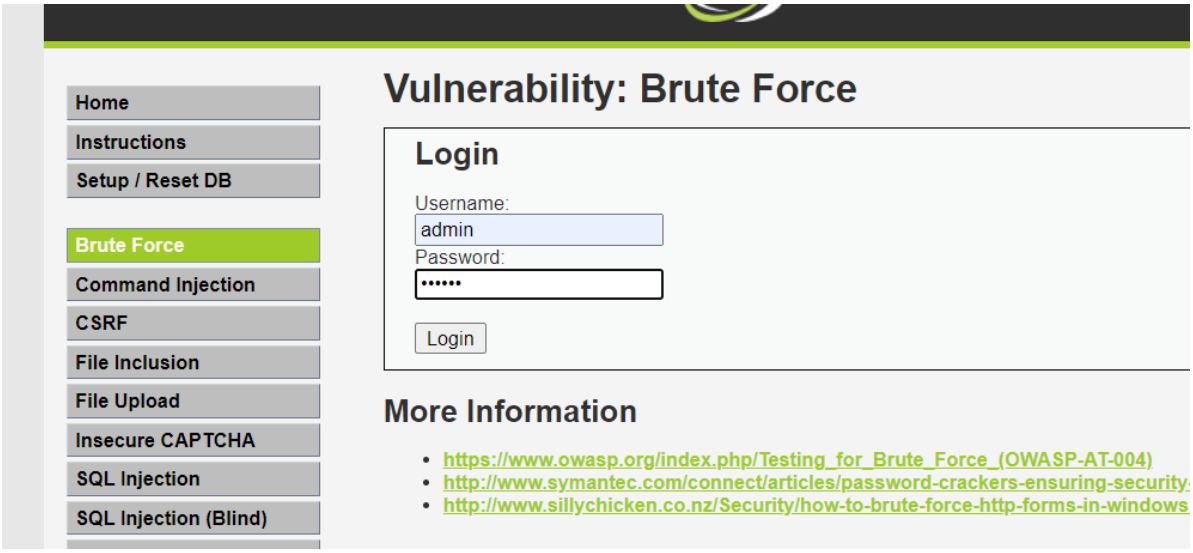


打开DVWA Security将Security Level设置为low并submit

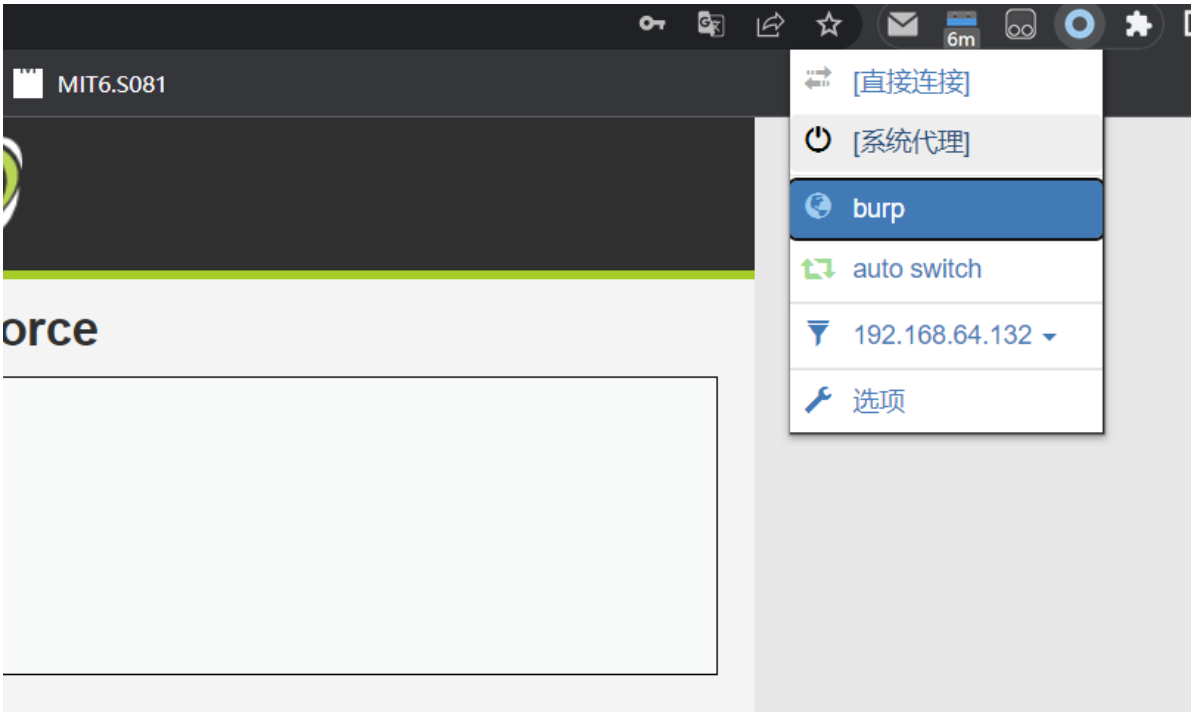


选择Brute Force关卡

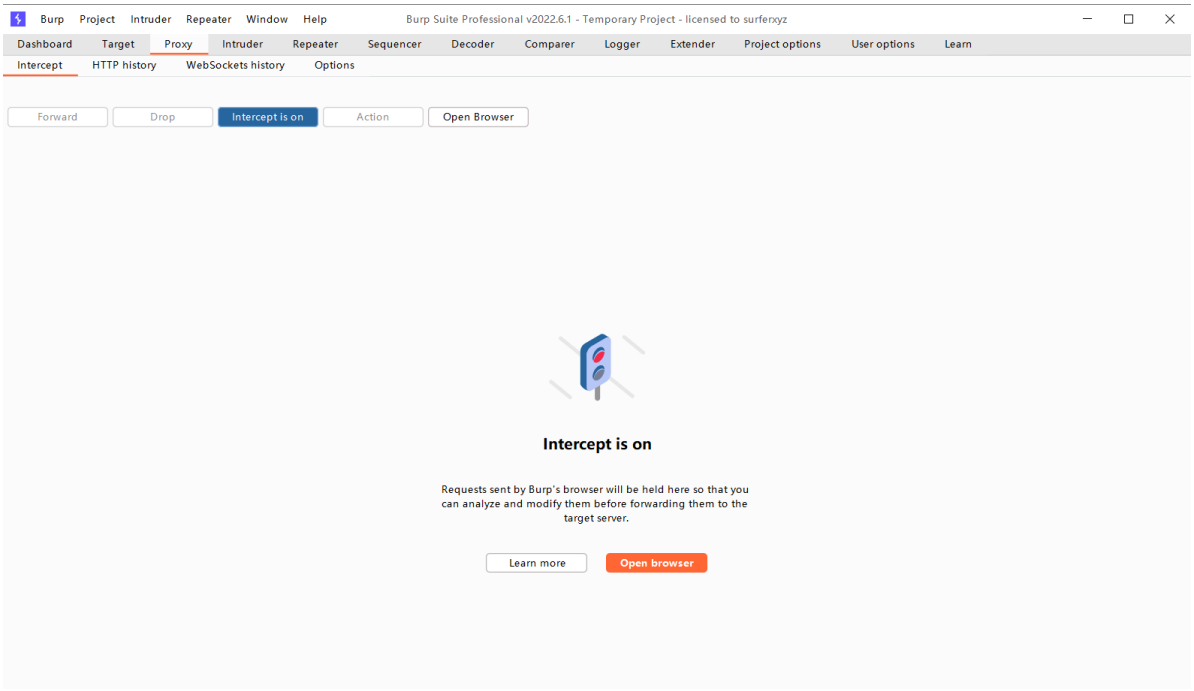
输入用户名admin和任意密码



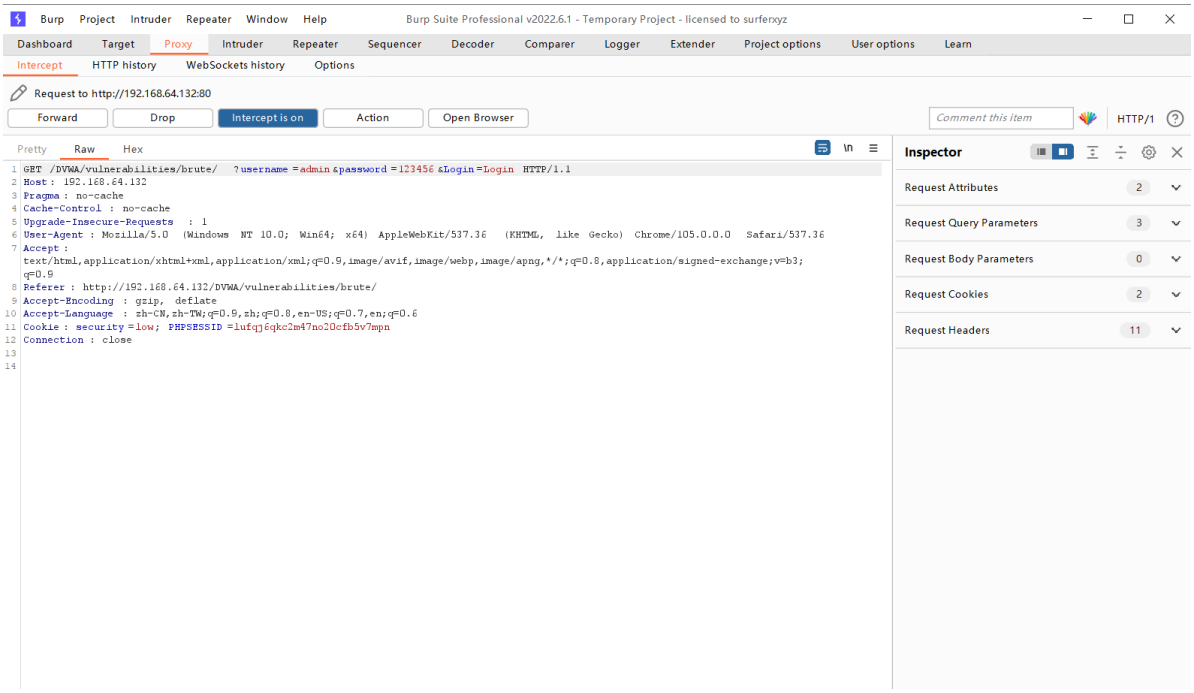
将代理切换到burp



将burp拦截打开

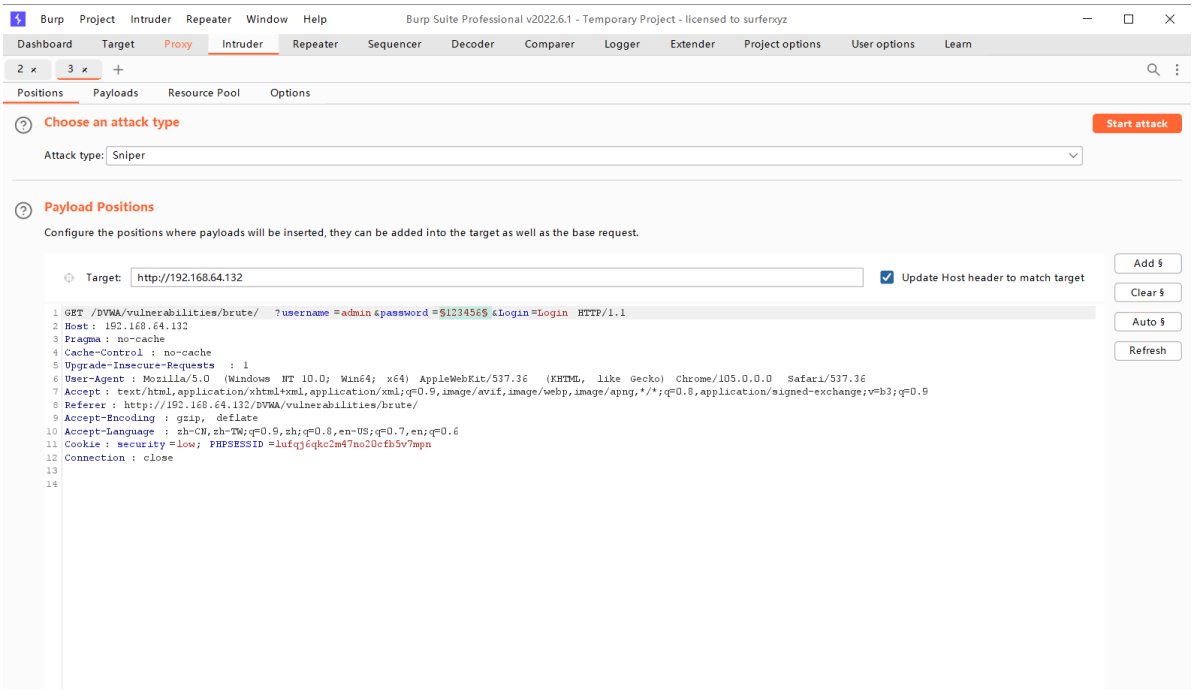


然后在网页中点击login按钮即可看到抓包

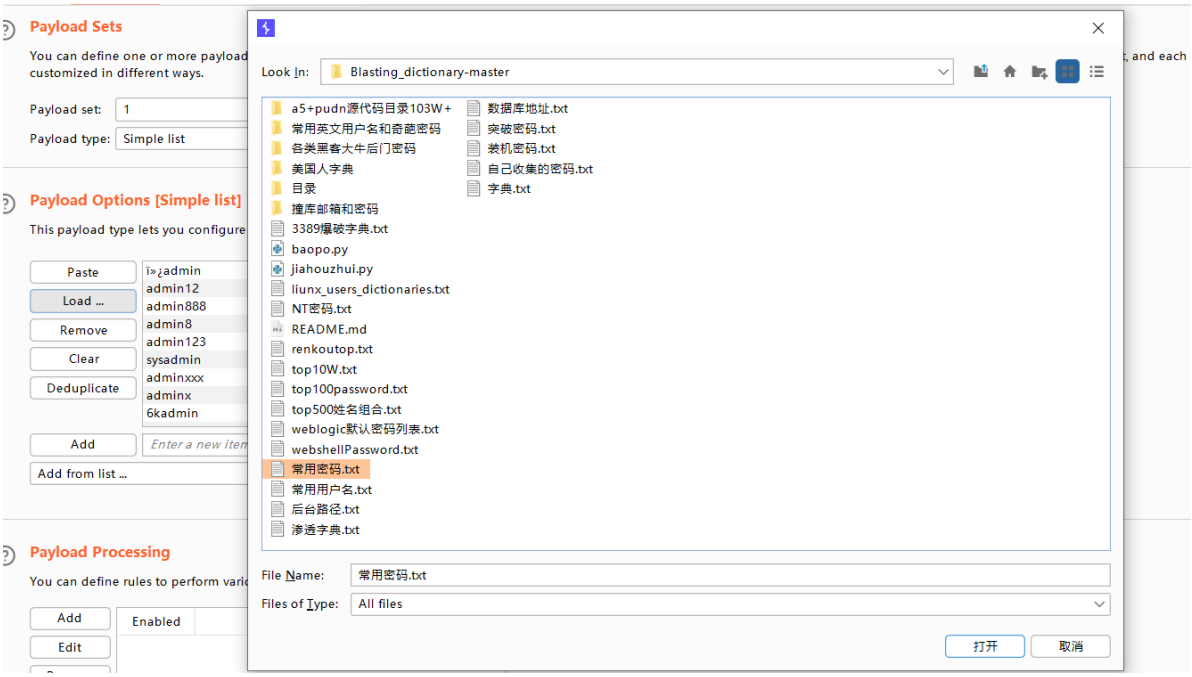


将其发送到Intruder爆破板块并设置爆破位置

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

Attack Save Columns 5. Intruder attack of http://192.168.64.132 - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
19	password	200			4594	
0		200			4545	
1	ï»¿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	

Request Response

Pretty Raw Hex

```
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:
```

Search... 0 matches

Finished

实验密码是否正确

可以看到密码正确