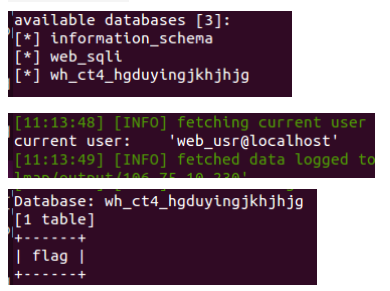
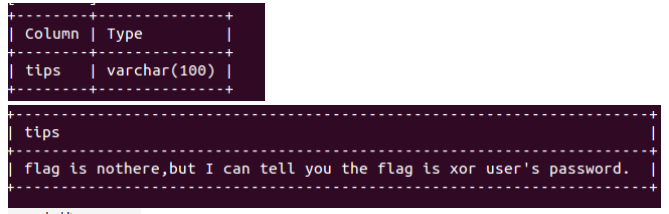
信息

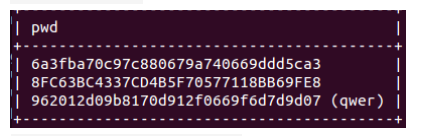
根据报文，将包给还原出来得出a.zip，提示华科官网，直接把网址www.hust.edu.cn填上去成功解压。在flag3.docx里面找到了flag

窃取

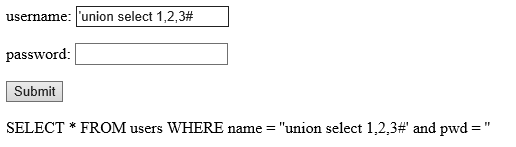
Sqlmap 跑下：



  
===去找 users：

  
前两个破不出来的异或下：  
e5f981b4fa005cb38ea23777166bc34b  
解密是 hust，加上 whctf{}即可。

忘了账户和密码



输入'union select 1,2,3#跳出flag

**find**

看到一串正则：



前面两个很好确定，应该是wh  
猜测为 whctf+7 个数字。七个数字无法爆破。  
按照 tips 找到某 qq

七位猜到是生日，试几个年份

正则最后匹配为：whctf1999512，拿到 flag  
http://106.75.10.230:9798/css/whctf1999512.css

**beat it**

解题思路：

用wireshark打开packet.pcap内容为同一个ip数据包的三个分片ip数据包。观察其中

分片1：偏移为0，

分片2：偏移为24，

分片3：偏移为40，

由第一个分片的长度为40字节，第三个分片片偏移刚好为40，故第一个分片和第三个合起来刚好为一个完整的包，第一个分片为udp，去除udp头8字节和明显无意义的首部0，拼起来的数据部分为：77686374667B30303020686572652069742069732074686520666C6167203030307D 用base16解码为答案：whctf{000 here it is the flag 000}

**忘记密码怎么办**

解题思路：

看题目提示猜测是一个sql注入的题目。使用 ' or 1=1 # 和 ‘) or 1=1 #注入测试验证猜想。

看提示框每次大概只出一个结果，所以结合sql 的limit进行注入。

‘) or 1=1 limit 1,1#

注入到第五行出现whctf{的答案。

继续如下：

') or 1=1 limit 5,1 #

') or 1=1 limit 6,1 #

') or 1=1 limit 7,1 #

') or 1=1 limit 8,1 #

拼接即可得到whctf{hello$$##itisme&---&&&}

**看图说话**

解题思路：

本题提示是ctf脚本不能访问，在浏览器地址栏请求ctf.php发现转跳。猜测应该要通过首页index.php转跳才可以访问。

然后观察输入框，应该是xss注入或和html 注入之类，用带<a/>html标签对测试

输入框：<a href="ctf.php">....</a>

点击 ... 看到一个图片，下载下来 对图片解压缩即可得到flag