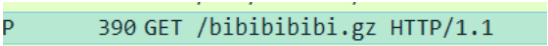


来看看自己是怎么日自己的

打开后直奔 http，发现是在 sql 注入，直接拉到最下面去找成功爆出数据的，一个一个看过来就找到了。

```
'qqvvqhgame{sqlmap_Anddd_wireshark2333}qjqpq1' for key 'group_key'
```

考眼力喽

打开，http，看了下太多了，就过滤了下 not ip.src == 219.138.24.12 and not ip.dst == 10.211.55.4 and http，然后一个个慢慢找就找到 bibibi.gz，
下载过来打开就是一张 png 图片 
Flag:hctf{hua_de_zhen_lei}

正在前往翻车大道

打开，http，发现是在跑 sqlmap，就去找数据，发现数据里没有 flag 迹象，用 wireshark 自带的搜索搜 flag，发现有个 hctf.flag 的注入语句，然后就没思路了想着去谷歌一下 ctf 比赛的 wp，佬们是怎么做流量分析的，然后就……



链接: <http://lorexar.cn/2016/04/06/hctfgame-llfx/>

感谢土爷 QAQ

LoRexxar 的渗透之战之二

因为不会那种可以获取 cookies 的 XSS(虽然和这题没关系),就开着 Tamper Data 各种页面点过来,发现改密码的时候可以把用户名改成别人的,于是就改管理员的密码,

Post Parameter	Value
form_data[name]	user
form_data[name]	\n\nLoRexxar
form_data[name]	\n\n
form_data[name]	38461635211934\n\nContent-

登陆就拿到 flag: hctf{y3wu_louj1_l1_h4i_l3}

LoRexxar 的渗透之战之三

Hint 是水平越权,去搜发现都是在网址上做文章,但是发现 getmessage.php 里有个 user,感觉有事情可以搞,就用火狐自带的网络改 user 然后发出去就拿到 flag 了

The screenshot shows a web browser window with a dark-themed interface. The page title is "HAMMER" and the main heading is "WELCOME, HAMMER". Below the heading, it says "TRY TO SEND MESSAGE TO OTHERS". The browser's developer tools are open, showing the "Network" tab. The list of requests includes:

- user.php (GET, 200)
- bootstrap.min.js (GET, 200)
- default.css (GET, 200)
- styles.css (GET, 200)
- jquery.min.js (GET, 200)
- LoRexxar.js (GET, 200)
- bootstrap.min.js (GET, 200)
- LoRexxar.js (GET, 200)
- getmessage.php (POST, 200)
- user.php (GET, 200)
- user.php (GET, 200)
- getmessage.php (POST, 200)

The "Details" view for the last request (getmessage.php) shows the request body with a highlighted payload: `<li class="list-group-item">hctf{y3wu_louj1_l1_h4i_l3}`.