

# 来看看自己是怎么日自己的

pcapng 文件，丢到 **wireshark**，粗看了一下包的内容，为 **sql** 的注入过程，对分组列表进行字符串搜索“**flag**”，找到一些包含有“**flag**”的注入语句，在这些语句对应的 **http** 回应中（**text/html**）找到 **flag**。

No.	Time	Source	Destination	Protoc	Length	Info
1...	31.895...	127.0.0.1	127.0.0.1	TCP	66	38090→80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=22618947 TSecr=22618947
1...	31.899...	127.0.0.1	127.0.0.1	HTTP	772	GET /hgame/user.php?id=test%20AND%20%28SELECT%203552%20FROM%28SELECT%20COUNT%28%2A%29%20C
1...	31.899...	127.0.0.1	127.0.0.1	TCP	66	80→38086 [ACK] Seq=1 Ack=707 Win=45184 Len=0 TSval=22618948 TSecr=22618948
1...	31.903...	127.0.0.1	127.0.0.1	HTTP	407	HTTP/1.1 200 OK (text/html)
1...	31.903...	127.0.0.1	127.0.0.1	TCP	66	38086→80 [ACK] Seq=707 Ack=342 Win=44800 Len=0 TSval=22618949 TSecr=22618949

Transfer-Encoding: chunked\r\n  
Connection: close\r\n  
Vary: Accept-Encoding\r\n  
X-Powered-By: PHP/5.5.36\r\n  
Content-Encoding: gzip\r\n  
\r\n  
[HTTP response 1/1]  
[Time since request: 0.003964241 seconds]  
[\[Request in frame: 15401\]](#)  
> HTTP chunked response  
Content-encoded entity body (gzip): 114 bytes -> 102 bytes  
File Data: 102 bytes

Line-based text data: text/html  
Could not get data: Duplicate entry 'qqvvqhgame{sqlmap\_Anddd\_wireshark2333}qjkkp1' for key 'group\_key'

0000 43 6f 75 6c 64 20 6e 6f 74 20 67 65 74 20 64 61  
0010 74 61 3a 20 44 75 70 6c 69 63 61 74 65 20 65 6e  
0020 74 72 79 20 27 71 71 76 76 71 68 67 61 6d 65 7b  
0030 73 71 6c 6d 61 70 5f 41 6e 64 64 64 5f 77 69 72  
0040 65 73 68 61 72 6b 32 33 33 33 7d 71 6a 6b 70 71  
0050 31 27 20 66 6f 72 20 6b 65 79 20 27 67 72 6f 75  
0060 70 5f 6b 65 79 27

Could not get data: Duplicate entry 'qqvvqhgame{sqlmap\_Anddd\_wireshark2333}qjkkp1' for key 'group\_key'