风险：

高

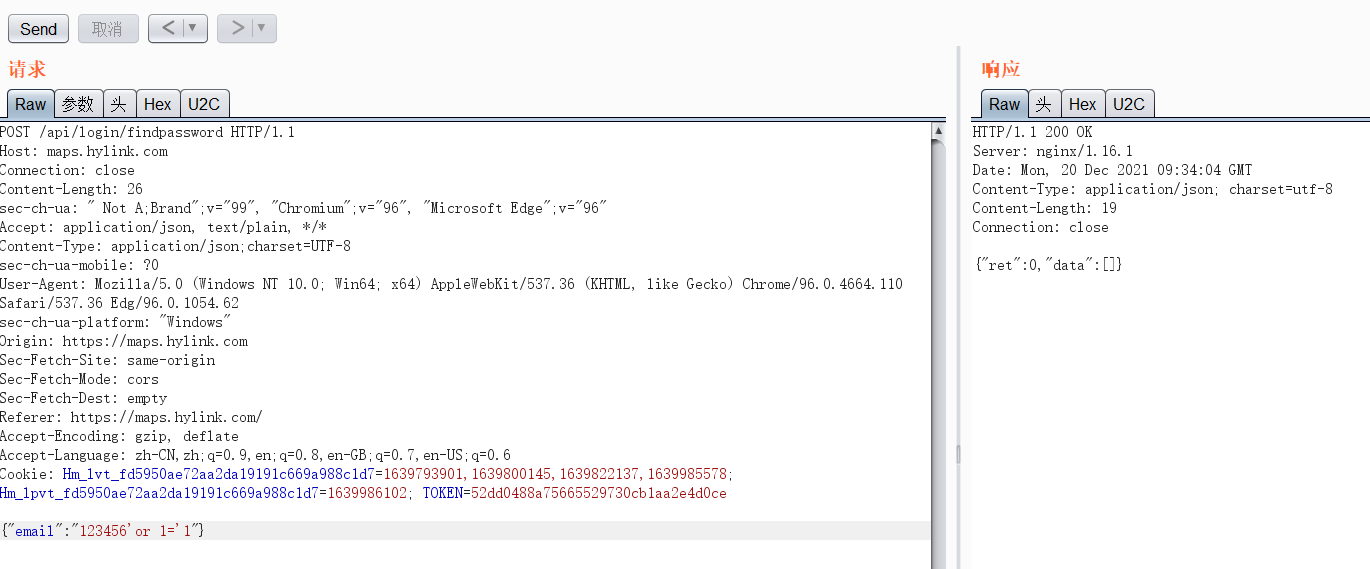
链接：

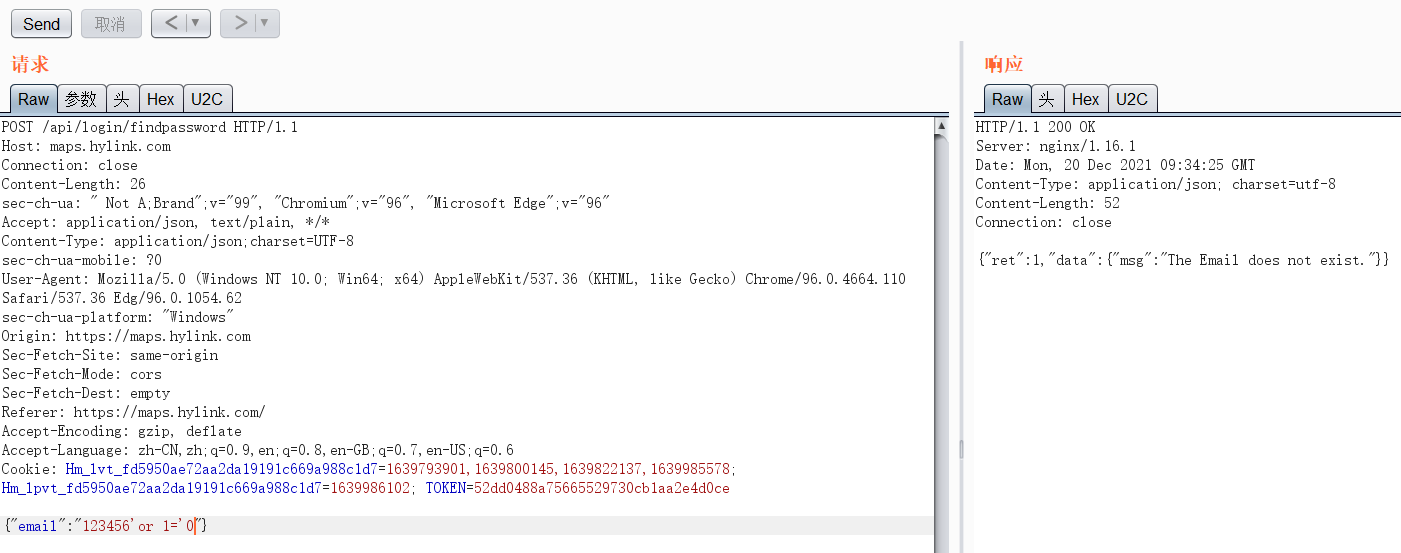
https://maps.hylink.com/#/user/password\_reset

详情：

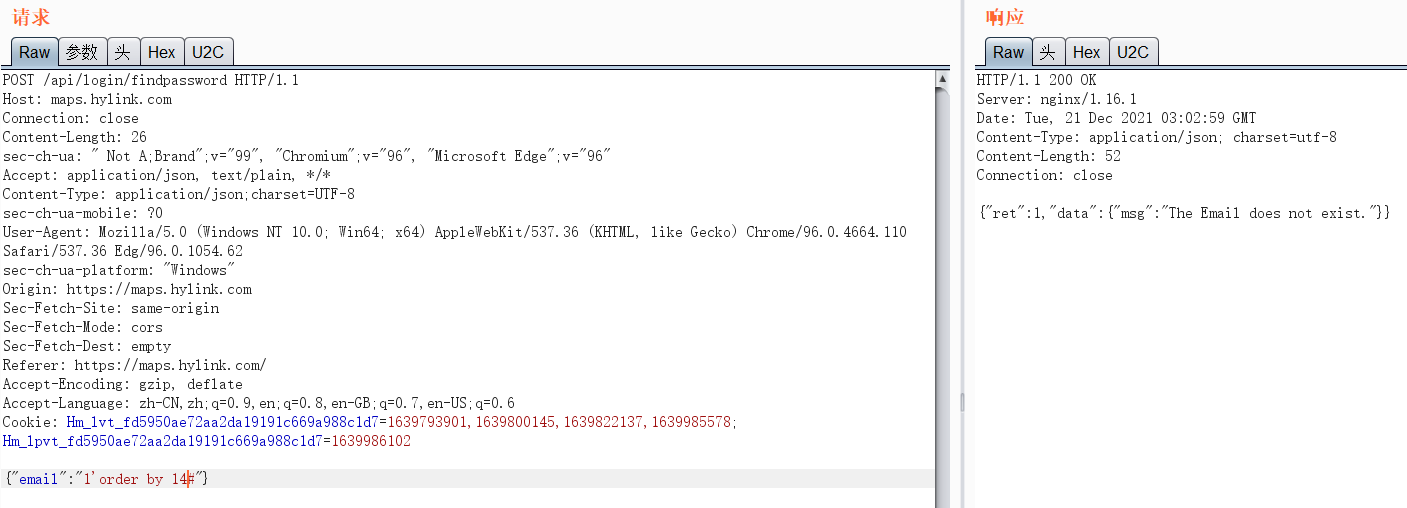
Sql注入

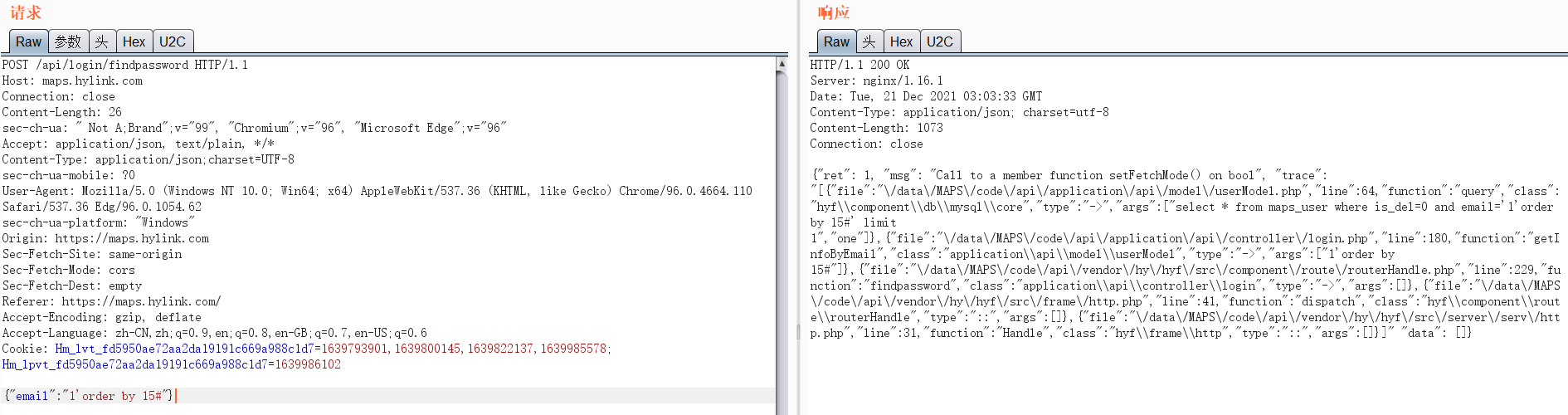
截图：



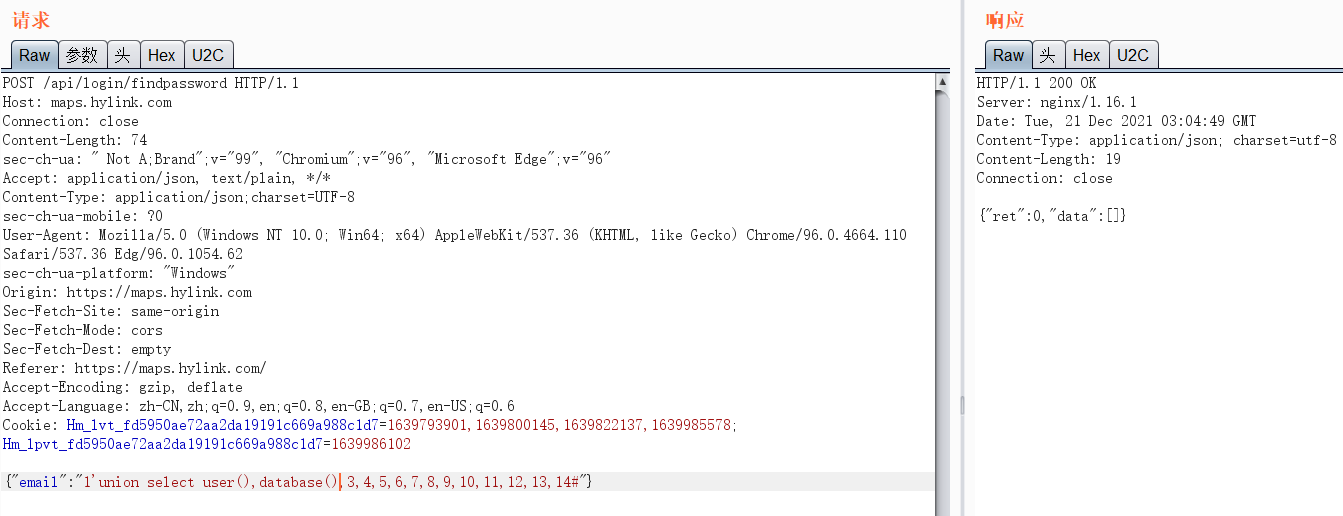


Order by 发现14个字段



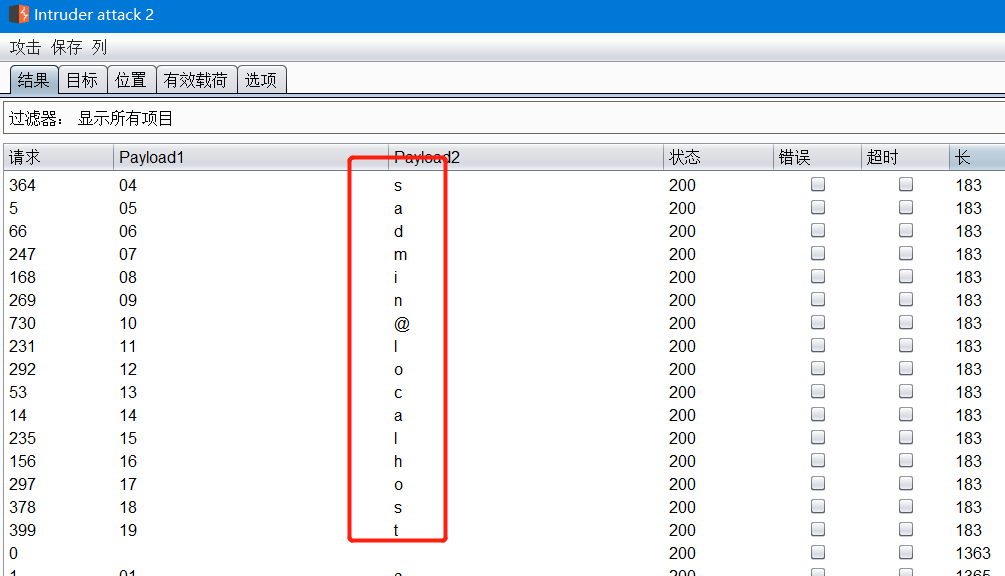


Union select 没有显示位

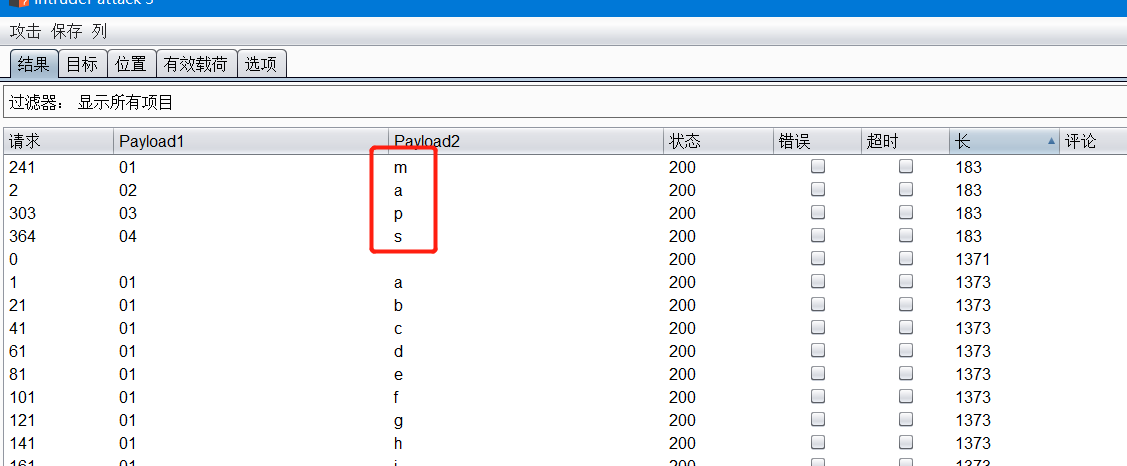


只能使用盲注

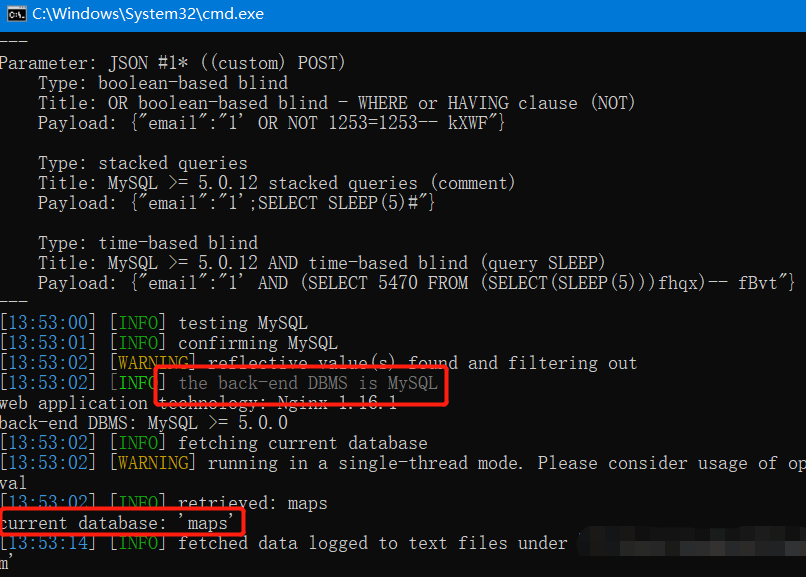
爆用户名：



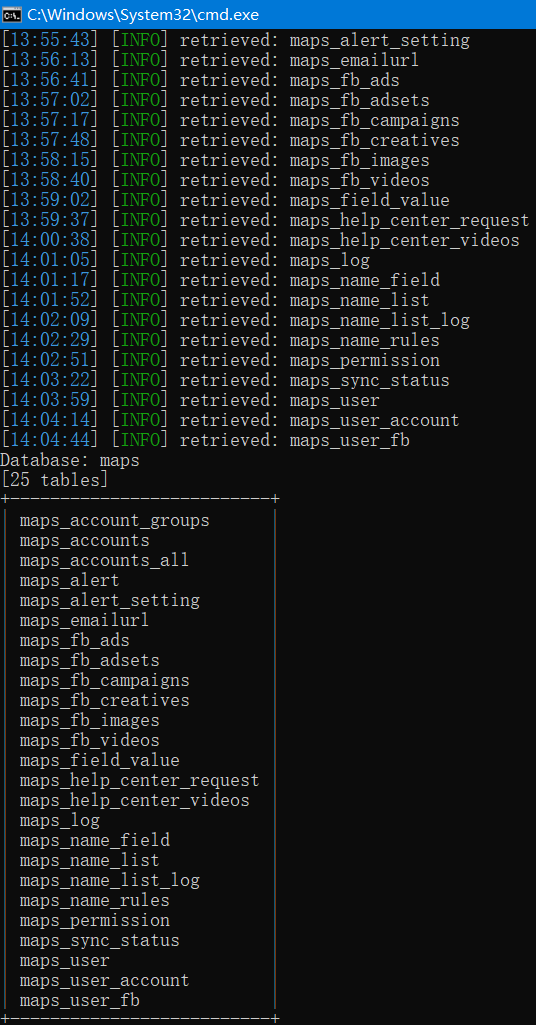
爆数据库名：



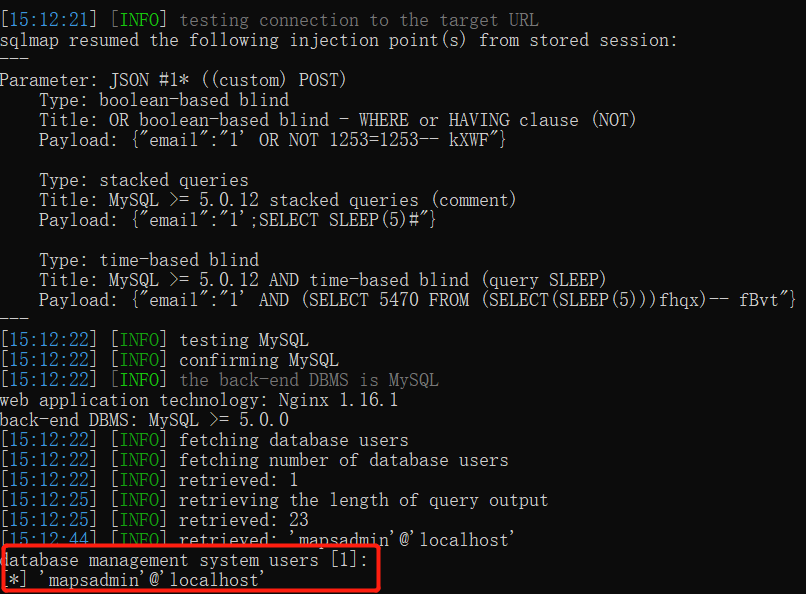
使用sqlmap



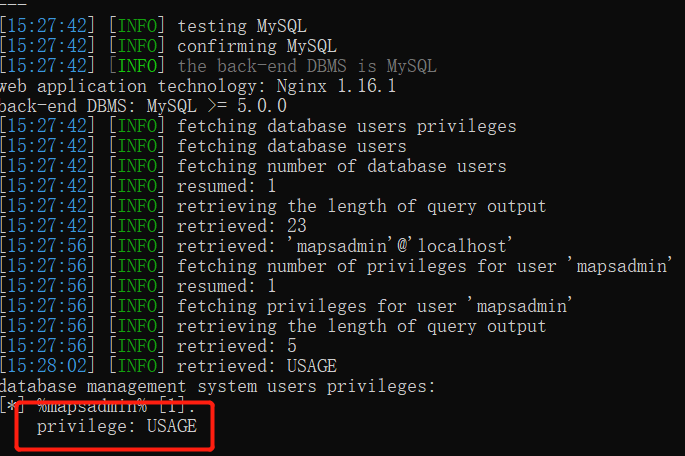
跑表名



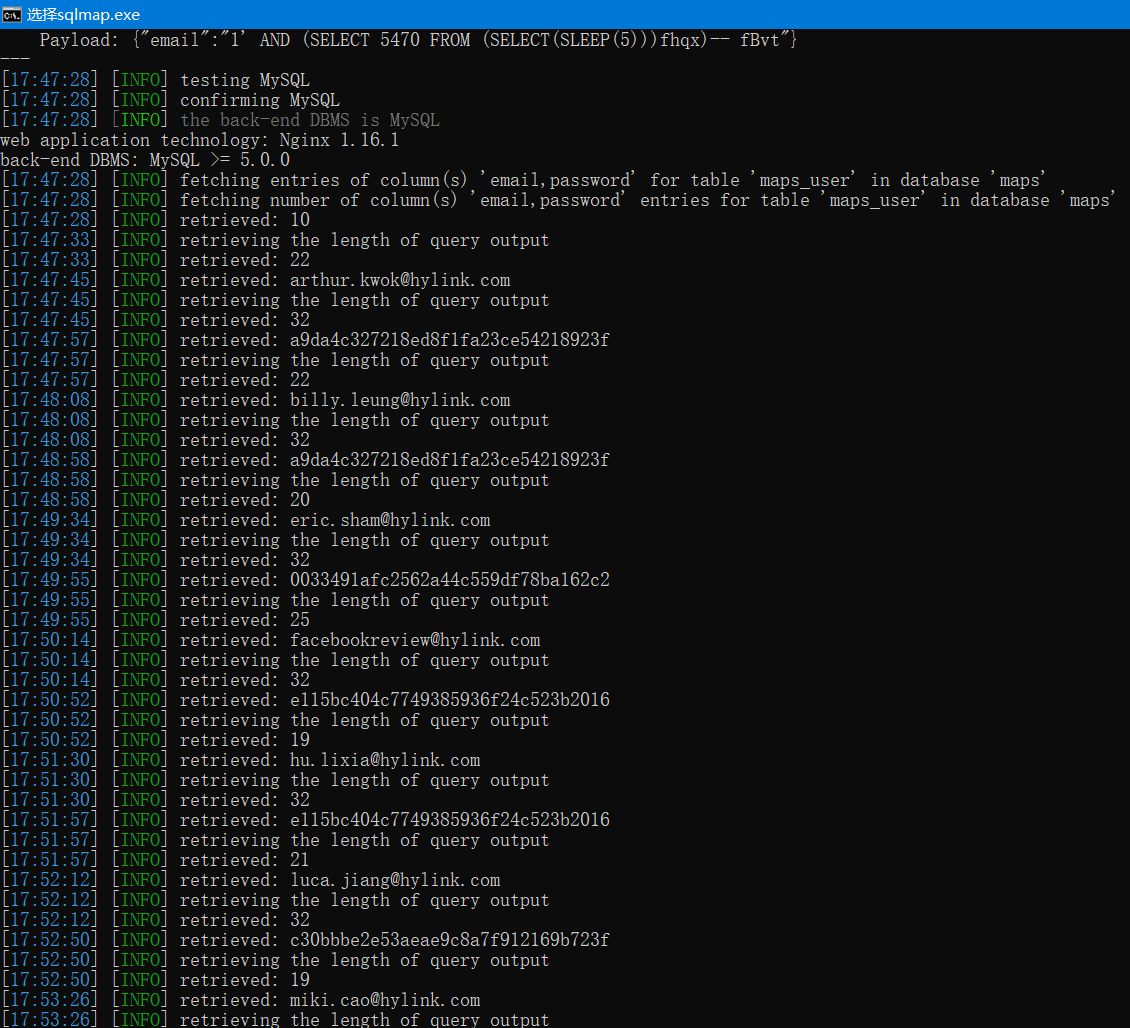
用户名



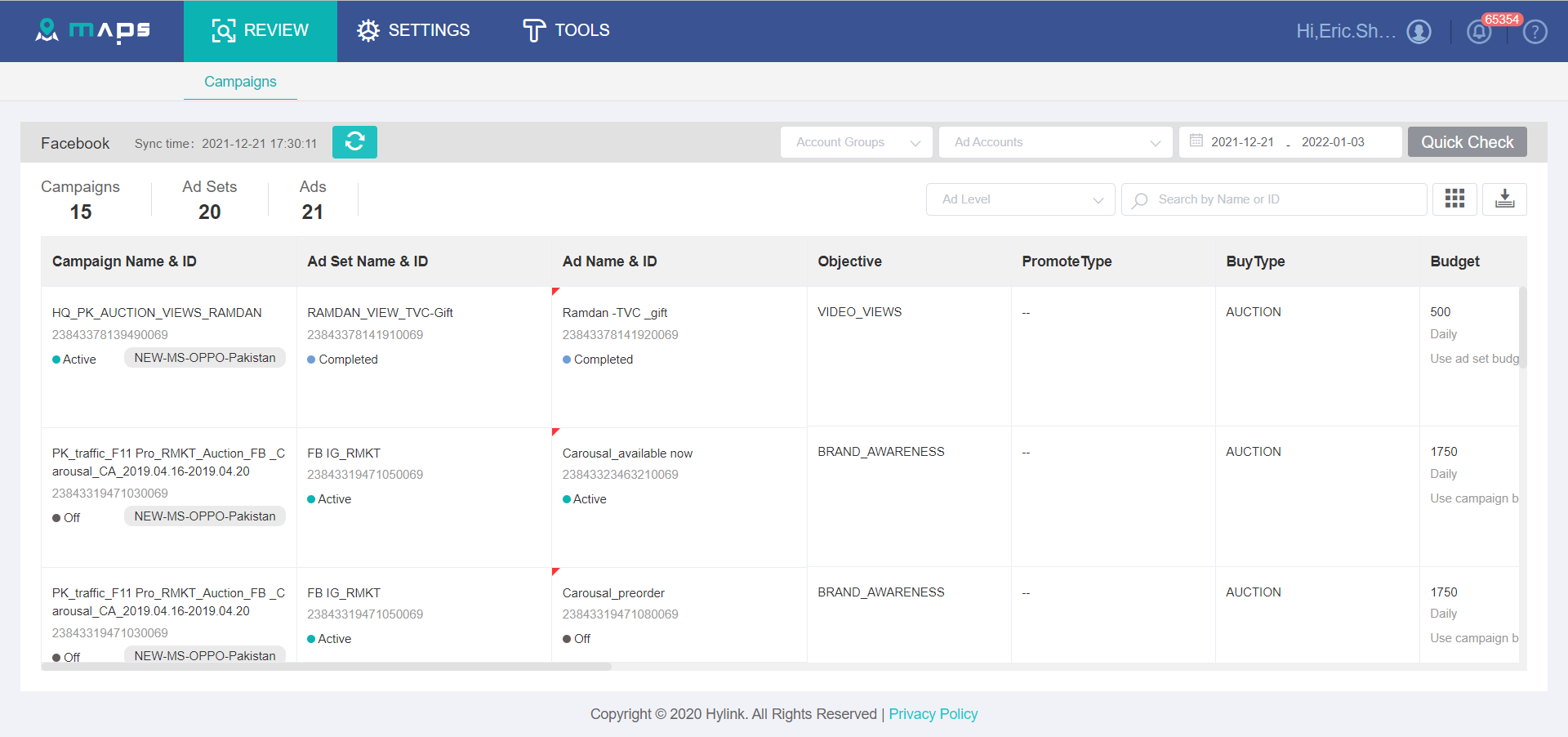
权限：普通用户



尝试—os-shell失败



跑出用户邮箱和密码哈希



成功登录系统