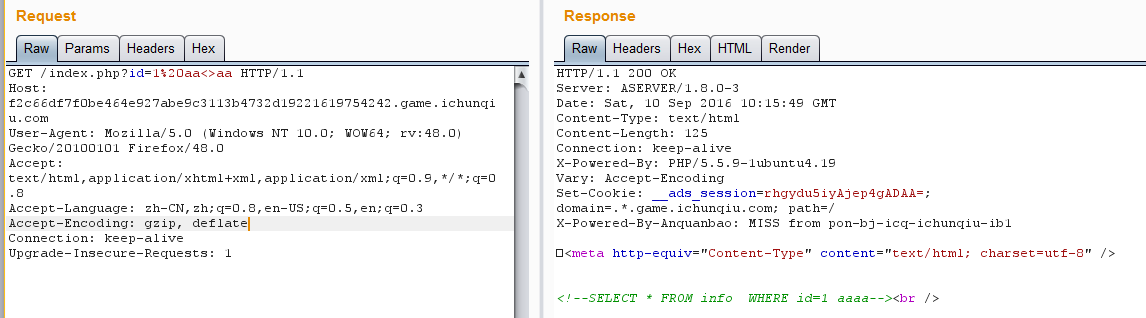
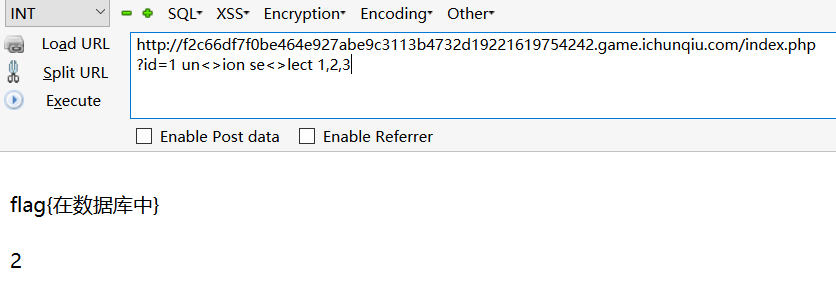
**第二场 WriteUp**

1. SQL

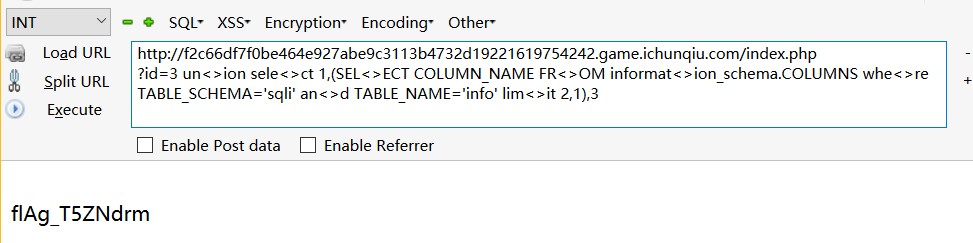
通过测试得知过滤了<>，以此重组payload可以绕过waf



手工注入后得知有3个字段，且输出第2个字段



构造payload查询出flag字段



再构造Payload union select 1,(select flAg\_T5ZNdrm from info limit 1),3 即可获得Flag

1. 再见CMS

通过查下面备案号得知这是齐博cms，这里我用wooyun-2014-080259





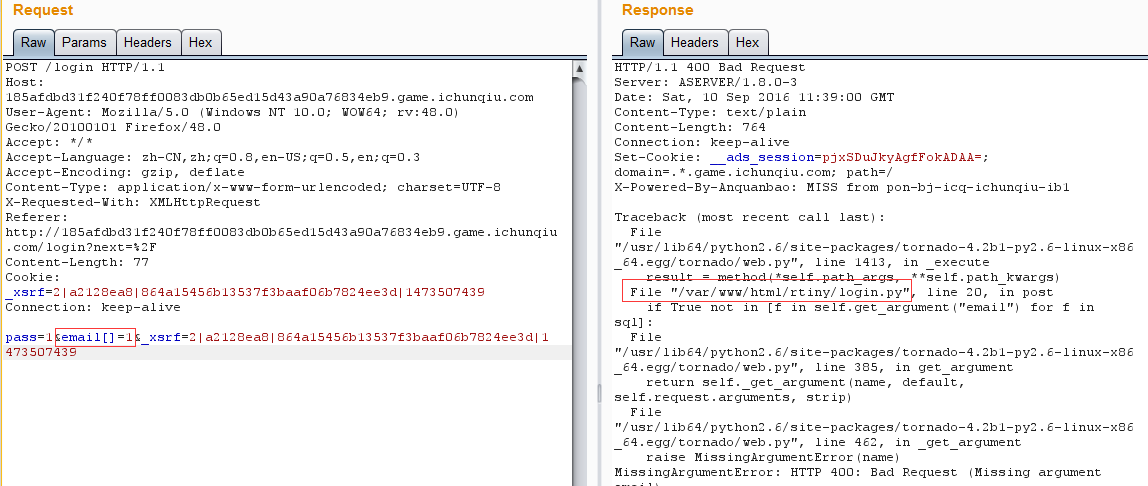
刚开始搞错方向了，一直在尝试解管理员密码，后面想到了用load\_file读flag.php (这就是小脑洞吧)



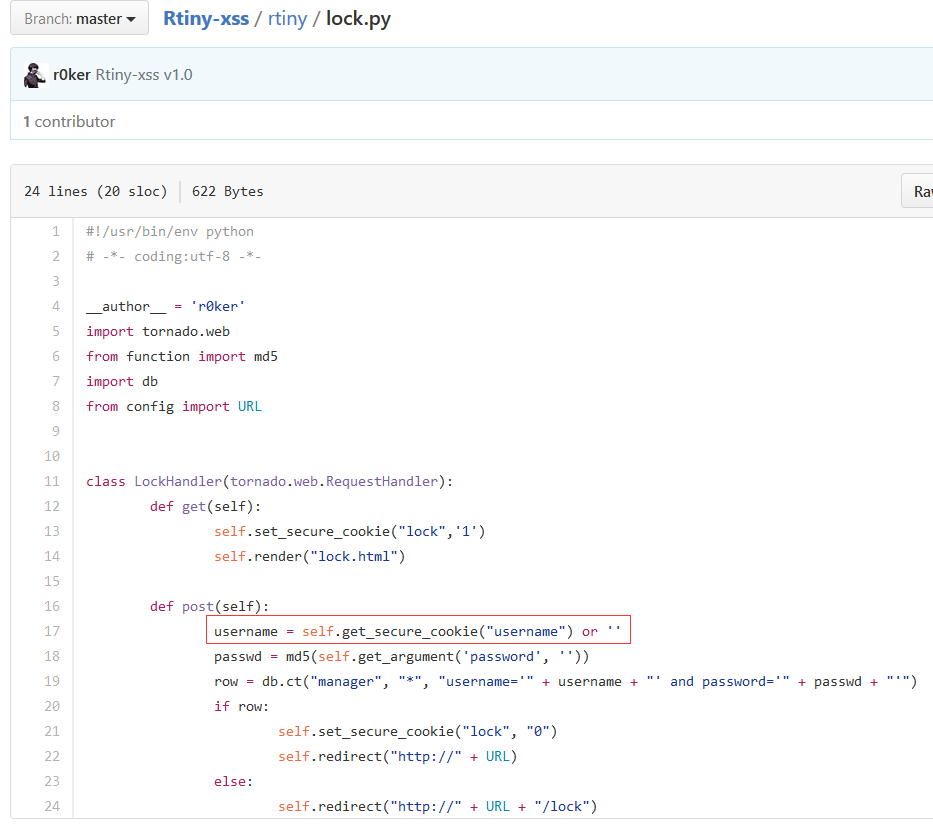
最后查看自己资料，flag就躺在那

1. XSS平台

登录抓包，把用户名改成数组，返回错误信息，从中得知该平台是基于tornado 编写的XSS平台

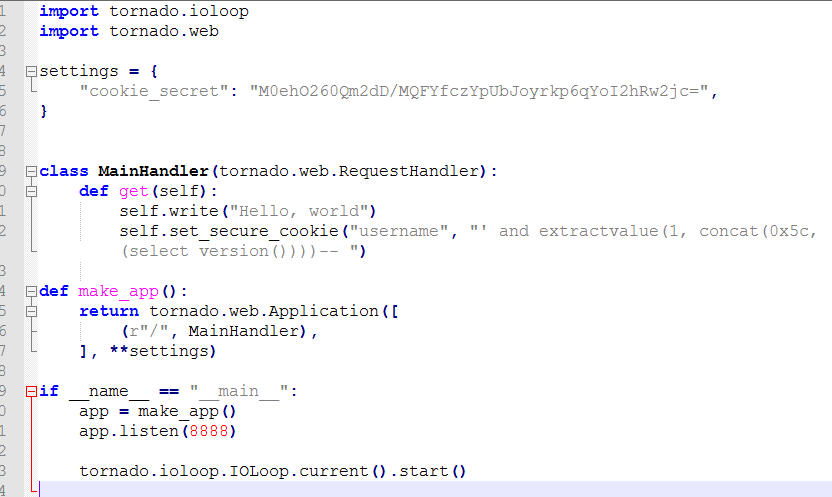


找到了该套源码，https://github.com/r0ker/Rtiny-xss，审计代码，/rtiny/lock.py 存在注入漏洞

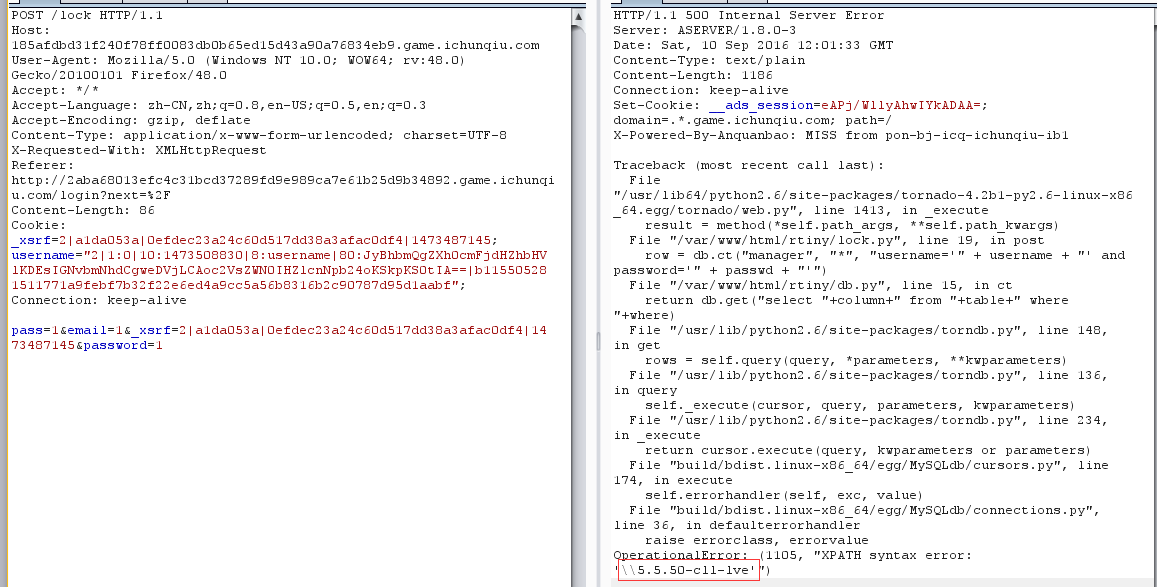


cookie中的username存在注入，但是tornado的cookie是密文传输的，所以我们也要对payload进行加密。

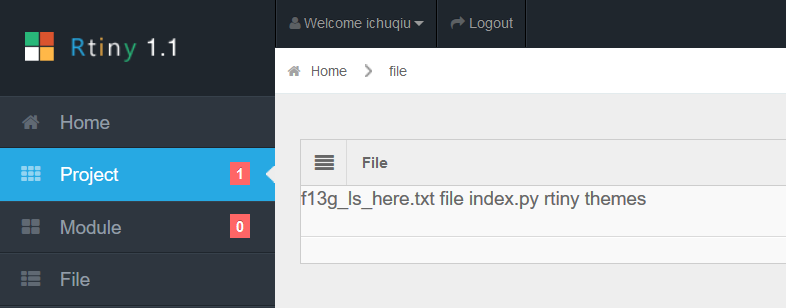
基于tornado写了个生成cookie的脚本



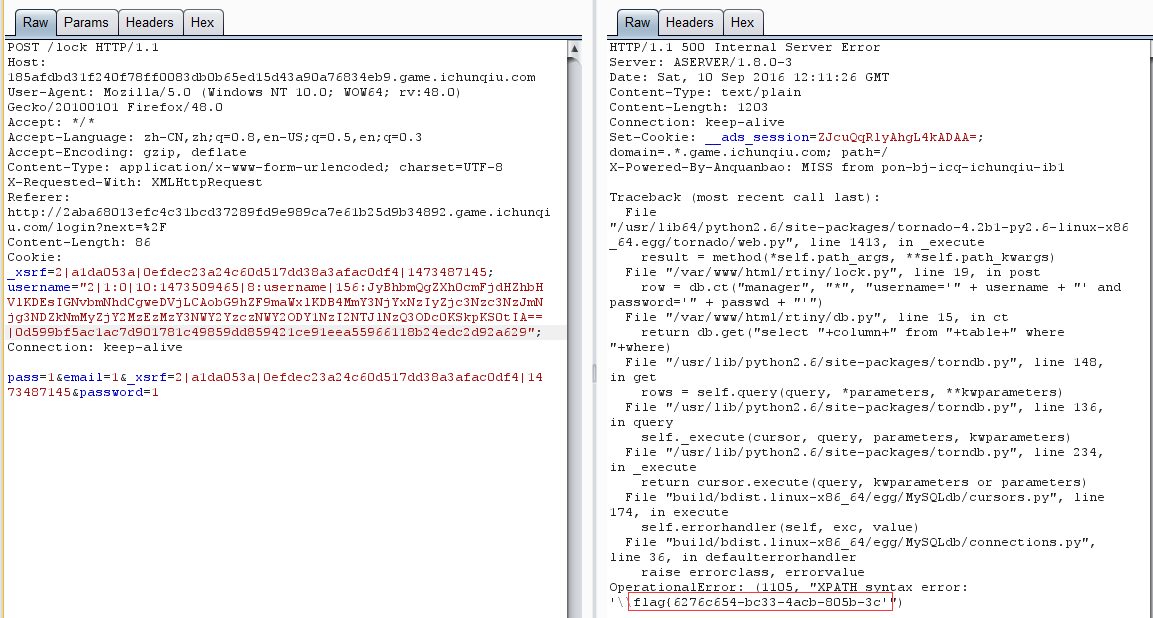
运行脚本，访问站点抓包取Cookie，注入 /lock



注入后得到帐号密码，登录XSS平台，/file 提示flag路径



文件不能直接访问，通过刚开始获取到的绝对路径，load\_file获取flag



用substring 分段获取就能得到完整flag