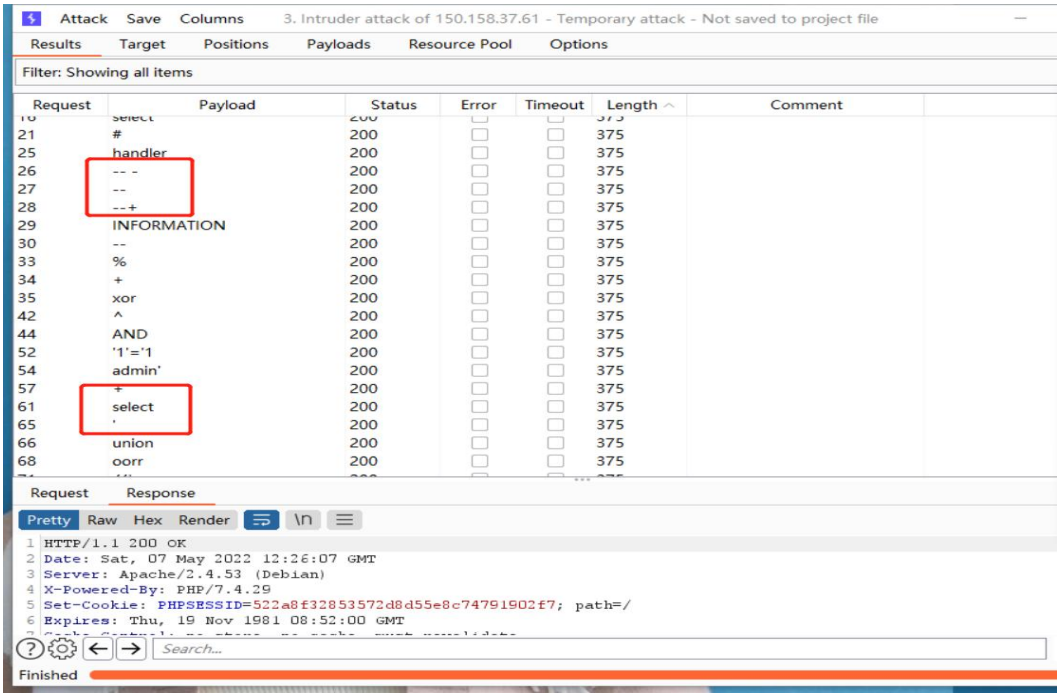
太菜了做出 minisql, include 两个 web 题。Checkin 那个题脚本写出来了不知道哪里有错误一直出不来尝试搭本地环境然后寄了）纠结了几天放弃了….框架漏洞之前没有接触过，学了两天 springboot&Struts2 但是没有把题做出来。

1. miniSQL:

打开是个登录框。查看源代码发现 SQL 执行语句为:

```
select * from users where username='admin' and password='$password'
```

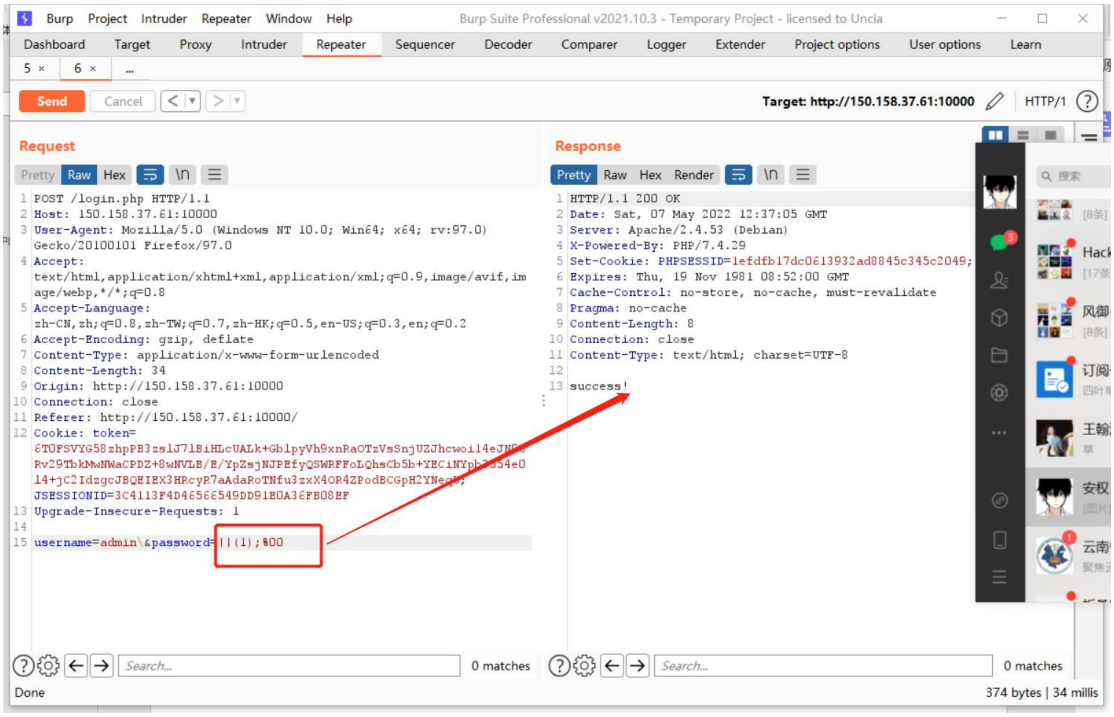
然后 fuzz：发现把注释符过滤，单引号，select 过滤等等大多数关键字过滤



先尝试解决闭合问题：看到转义符: \ 没有过滤于是利用 \, %00 截断符闭合原来的语句变为:

```
select * from users where username='admin\' and
password='||mid(version(),1,1)=num;%00'
```

闭合以后 or 被过滤了利用||绕过查看闭合回显是否改变



看到回显 success ， 盲注。

根据执行的 SQL 语句 知道了有表 user，以及提示要注出用户名，密码才能有 flag。

但是因为过滤了 select 尝试 bypass 试了很久发现没什么用然后考虑新方法

参考到文章：https://www.crisprx.top/archives/203#ezsql

https://xz.aliyun.com/t/8646

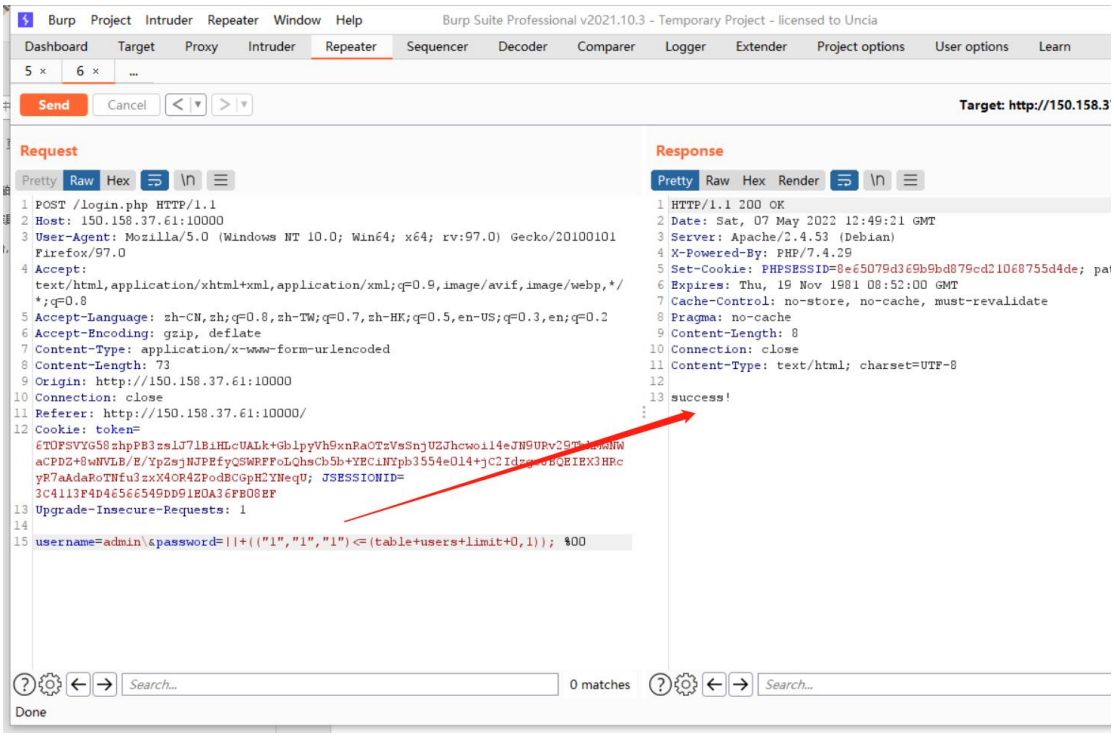
发现可以利用 MySQL8 的特性来继续注入

```
利用 username=admin\and password=||mid(version(),1,1)=$num$;%00'
```

对 num 爆破对 num 爆破发现为数据库版本确实为 8.xx

构造 payload：

```
||+(("1","1","1")<=(table+users+limit+0,1)); %00
```



第一个 1 id 例 第二是 username 例 第三个为 password

首先对爆 username 位爆破根据回显 success 得到 username：w3lc0me_t0_m1n1lct5

这里 username 关键词没有过滤还可以利用

```
username=admin\ and password=||ascii(mid(username,1,1))=num;%00
```

对 num 来爆然后一样可以得到

然后对 password 位爆破得到：cd51c1005cab68be2f7e6112a4de3e89

登录得到 flag

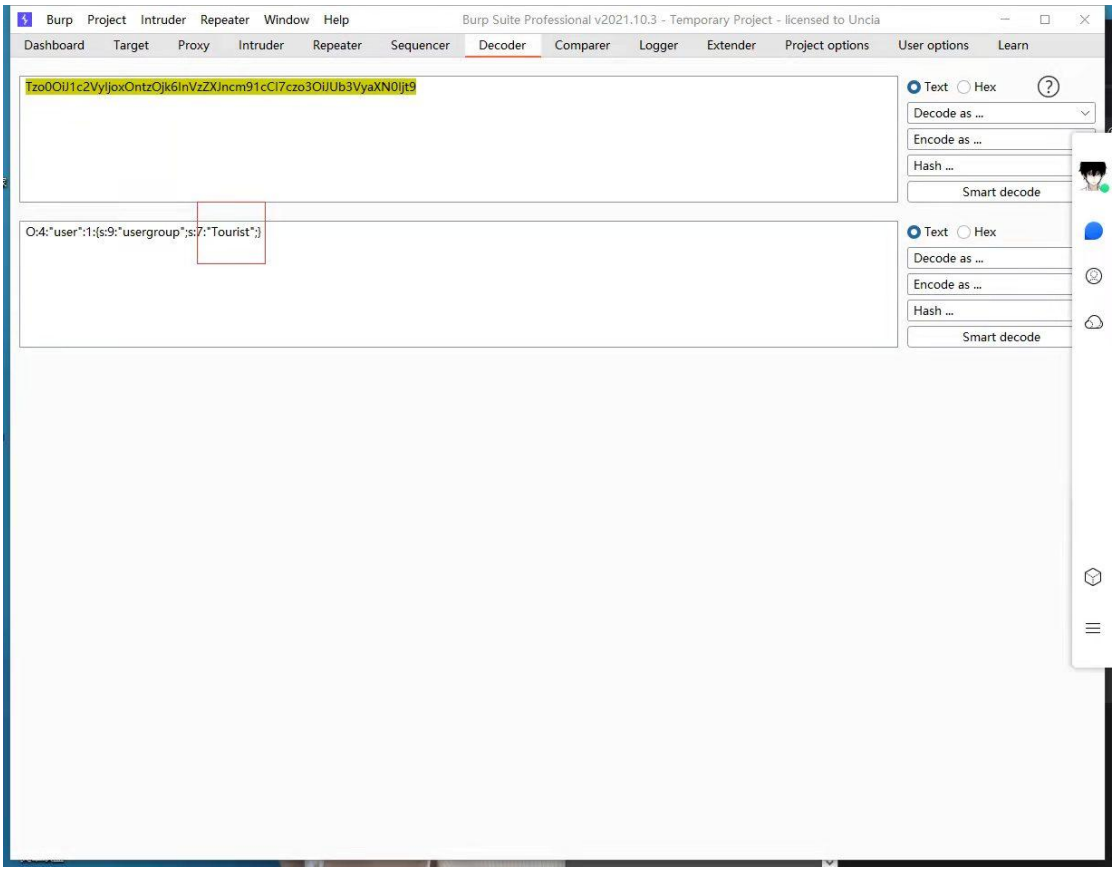
这里做题的时候没想到密码用户名这么长所以当时手工爆…

做完之后写了个脚本，，脚本有问题还在改（呜呜呜编程能力太菜了）

2．Include

文件上传：打开上传题目发现只有 Lteam 可以使用上传功能

抓包发现 cookie 解码



把 Touist 换成 Lteam 编码

访问可以上传文件 直接 getshell 用蚁剑直连根目录找到 flag