在Linux系统中，可以使用 ls 命令结合管道符 | 和其他命令来查看目录相关信息。

比如ip=127.0.0.1|ls

上传用户登录信息使用的一定是http里的post方法

补充知识：用户登录操作常用的有两种方式，GET和POST
使用GET方法所有参数都包含在URL中，所有访问网站的URL都会记录在服务器的访问日志中
相比于GET而言，POST就安全得多。
POST是通过携带数据体传递用户登录信息，登录的数据并不会出现在URL和服务器访问日志中。
但这也并不十分安全，只要拦截到了传递的数据体，用户名和密码就能轻松获取。

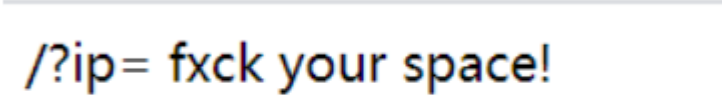
zip伪加密在文件头的加密标记位做修改，进而再打开文件时识被别为加密压缩包
伪加密原理：通过修改压缩源文件数据区和目录区的全局方式位标记，达到将伪压缩文件恢复到未加密的状态的目的

```
1  未加密：
2
3  文件头中的全局方式位标记为00 00
4
5  目录中源文件的全局方式位标记为00 00
6
7  伪加密：
8
9  文件头中的全局方式位标记为00 00
10
11 目录中源文件的全局方式位标记为09 00
12
13 真加密：
14
15 文件头中的全局方式位标记为09 00
16
17 目录中源文件的全局方式位标记为09 00
18
19 ps:也不一定要09 00或00 00，只要是奇数都视为加密，而偶数则视为未加密
```

过滤空格的解决方法

IFS1　　//$1改成$加其他数字都行，都能当作空格来用

?ip=127.0.0.1|catIFS1flag.php



以下方法可以绕过空格

1. ${IFS}替换
2. IFS1替换
3. ${IFS替换
4. %20替换
5. <和<>重定向符替换
6. %09替换

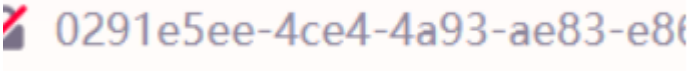
a的值覆盖，然后进行绕过

/?ip=127.0.0.1;a=g;catIFS1fla$a.php

如何判断一个网站是Linux系统?

文件路径格式：Linux系统下的文件路径使用 / 作为分隔符，如 /var/www/html/index.html 。如果在网站的URL中看到这种以 / 分隔的路径格式，很可能是Linux系统。

权限设置：访问网站的一些文件或目录时，若出现权限相关的错误提示，其权限表示方式可能暗示系统类型。Linux系统的文件权限通常用 rwx （读、写、执行）表示，如 drwxr-xr-x 。



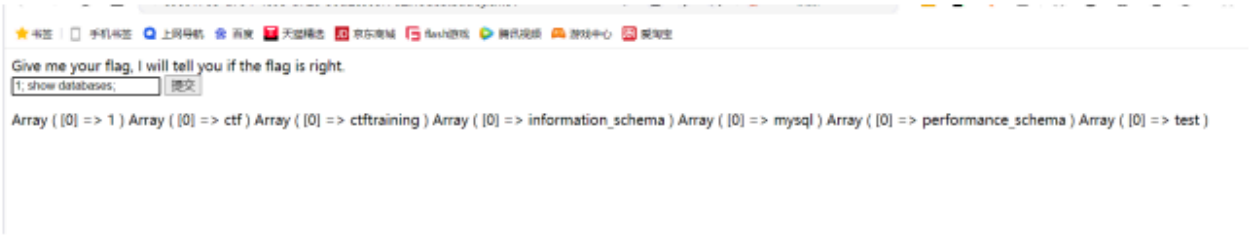
堆叠注入

在支持多语句执行的数据库系统中，如MySQL，攻击者可以通过在正常的SQL语句中插入分号来分隔不同的SQL命令，从而实现一次注入执行多个SQL语句。

先进行了万能密码注入，发现回显nonono,说明不行

进行堆叠注入

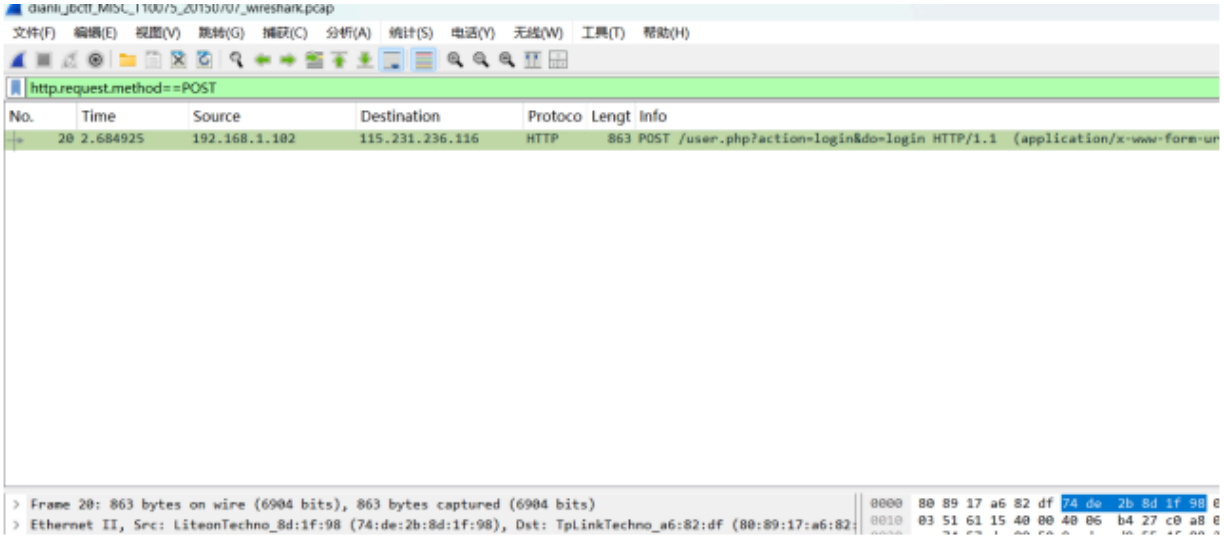
将多个SQL语句通过特定分隔符（如分号";"）连接起来一起提交执行。

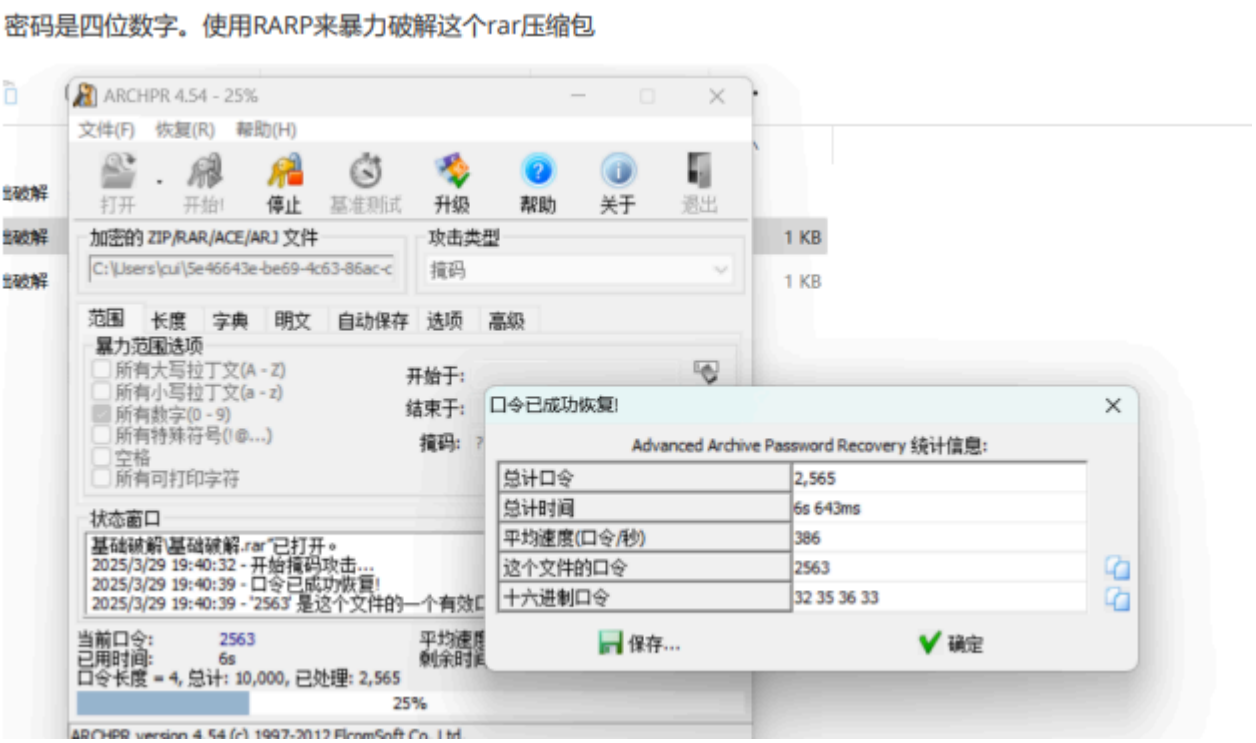


查看表名发现有Flag,猜测flag应该在Flag中

猜测查询语句select $_GET['query'] || flag from flag

知识点：上传用户登录信息使用的一定是http里的post方法
直接搜索 http.request.method==post





暴力破解这个rar压缩包

联合注入

当存在SQL注入，我们在密码出输入 1' or 1 = 1# 后，整条语句变成

$sql="select * from users where username='1' or 1 = 1#' and password='$pwd'";

> `#` 是注释符号，后面的内容被注释掉，`or` 是或，作用两边有一边为真，结果就为真，因为右边的 `1=1` 为真，所以上述语句等价于

select * from users where username='1' or 1 = 1

> 即使用户名不存在也没关系，`1=1` 为 `true`，等价于

select * from users

> 所以该语句的作用是爆破出所有字段

数字型注入

SQL中的语句格式：select * from users where id =x

判断方法：使用 1 and 1=1 ，1 and 1=2 来判断

当输入：and 1=1 时页面显示正常

select * from users where id =x and 1=1

输入：and 1=2 时页面显示异常

select * from users where id =x and 1=2

说明是数字型注入

字符型注入

SQL中的语句格式：select * from users where id ='x'

判断方法：使用 1' and '1'='1 ，1' and '1'='2 来判断

当输入：1’ and ‘1’='1 时页面显示正常

select * from users where id ='x' and '1'='1'

输入：1’ and ‘1’='2 时页面显示异常

select * from users where id ='x' and '1'='2'

说明是字符型注入