NAME OF AFFECTED PRODUCT(S)

Employee Record System

VERSION(S)

V1.0

submitter

LonTan0

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\edit_employee.php employeed_id ,first_name,middlename, lastname have Cross Site Scripting(XSS)

```php
if(isset($_GET['id'])){
    $record_id = mysqli_real_escape_string(mysql: $db_connect, string: $_GET['id']);

    $getinfo = mysqli_query(mysql: $db_connect, query: "SELECT * FROM sharp_emp WHERE id = '$record_id' ");
    $getinfocount = mysqli_num_rows(result: $getinfo);

    if($getinfocount == 1){
        if($fetch = mysqli_fetch_assoc(result: $getinfo)){
            $employee_id = $fetch['employee_id'];
            $firstname = $fetch['first_name'];
            $middlename = $fetch['middle_name'];
            $lastname = $fetch['last_name'];
            $phone = $fetch['phone'];
            $employee_image = $fetch['employee_image'];
            $id_type = $fetch['id_type'];
            $id_number = $fetch['id_number'];
            $residence_address = $fetch['residence_address'];
            $residence_location = $fetch['residence_location'];
            $residence_direction = $fetch['residence_direction'];
            $residence_gps = $fetch['residence_gps'];
            $next_of_kin = $fetch['next_of_kin'];
            $relationship = $fetch['relationship'];
            $phone_of_kin = $fetch['phone_of_kin'];
            $kin_residence = $fetch['kin_residence'];
            $kin_residence_direction = $fetch['kin_residence_direction'];
            $date_employed = $fetch['date_employed'];
            $job_type = $fetch['job_type'];
            $status = $fetch['status'];
        }
    }
} else {
    echo "Invalid Approach";
    exit();
}
```

```
ss="input-box input-small left">
t type="text" class="inputField emp_id" placeholder="Optional" name="employee_id" value="<?php echo $employee_id ?>">
class="error empiderror"></div>

ss="input-box input-small right">
l for="firstname">First Name</label><br>
t type="text" class="inputField firstname" name="firstname" value="<?php echo $firstname ?>">
class="error firstnameerror"></div>

ss="input-box input-small left">
l for="middlename">Middle Name</label><br>
t type="text" class="inputField middlename" placeholder="Optional" name="middlename" value="<?php echo $middlename ?>">
class="error middlenameerror"></div>

ss="input-box input-small right">
l for="lastname">Last Name</label><br>
t type="text" class="inputField lastname" name="lastname" value="<?php echo $lastname ?>">
class="error lastnameerror"></div>

ss="input-box input-small left">
l for="phone">Phone number</label><br>
t type="text" class="inputField phone" name="phone" value="<?php echo $phone ?>">
class="error phoneerror"></div>

ss="input-box input-small right">
l for="jobtype">Job Type</label><br>
t type="text" class="inputField jobtype" name="jobtype" value="<?php echo $job_type ?>">
class="error jobtypeerror"></div>

ss="input-box input-small left">
l for="dateemployed">Date employed</label><br>
t type="text" id="datepicker" class="inputField dateemployed" name="dateemployed" value="<?php echo $date_employed ?>">
class="error dateemployederror"></div>
```

POC

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