bugsdisclose / xss

offsecin Create xss History

1 contributor

17 lines (13 sloc) | 704 Bytes

```
1  Exploit Title: Simple Food Website 1.0 : Stored XSS
2
3  Date: 26-04-2022
4  Exploit Author: Saket Saurav
5  Vendor Homepage:
6  https://www.sourcecodester.com/php/12510/simple-food-website-php.html
7  Software Link: https://www.sourcecodester.com/php/12510/simple-food-website-php.html
8  Version: 1.0
9  Tested on: Kali Linux 2020
10
11 Affected Endpoint: http://127.0.0.1:1234/food/admin/all_users.php
12
13 Steps to reproduce the stored XSS.
14
15 1. Login as Low Privileged user (Moderator) on :
16 2.Then a Moderator needs to enter XSS Payload: <script>alert(document.cookie)</> in Full User Name
17 This causes stored xss on the web portal.It can be then used as for privilege escalation from mode
```