offsecin Create stored-xss History

1 contributor

20 lines (17 sloc) | 848 Bytes

```
Exploit Title: Rescue Dispatch Management System 1.0 : Stored XSS

Date: 26-04-2022
Exploit Author: Saket Saurav
Vendor Homepage:
https://www.sourcecodester.com/php/15296/rescue-dispatch-management-system-phpoop-free-source-code
Software Link: https://www.sourcecodester.com/php/15296/rescue-dispatch-management-system-phpoop-f
Version: 1.0
Tested on: Kali Linux 2020

Steps to reproduce the stored XSS.

1. Login as Low Privileged user (Staff) on :
http://localhost/rdms/admin/login.php
2. Go to http://localhost/rdms/admin/?page=teams . Click on 'CREATE NEW'
3.In the Team Leader/Code Field enser XSS Payload :
<script>alert(document.cookie)</script>
4.Login as Admin and visit the same Endpoint as step 1. It can be seen
that XSS gets executed.
It can be used to steal Admin Cookies and thus take over an Admin Account.
```