

🔑 main ▼

...

POCs / POC



lakshaya0557 Create POC

🕒 History

👤 1 contributor

26 lines (20 sloc) | 1018 Bytes

...

```

1  # Exploit Title: Simple Cold Storage Management System v1.0 - Stored XSS in "Settings"
2  # Exploit Author: Lakshaya Bawa
3  # Vendor Name: oretnom23
4  # Vendor Homepage: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-
5  # Software Link: https://www.sourcecodester.com/php/15088/simple-cold-storage-management-system-us
6  # Version: v1.0
7  # Tested on: Kali Linux, Apache
8
9
10 Description: A multiple stored XSS in Simple Cold
11 A multiple stored XSS in Simple Cold Storage Management System v1.0 allows an attacker to input ar
12
13 Vulnerable Parameters:
14 System Name
15 System Short Name
16 Payload:
17 <script>alert(1)</script>
18
19 Steps:
20 1) Login into admin account
21 2) Now go to "http://localhost/csms/admin/?page=system_info".
22 3) Now in Parameters "System Name" and "System Short Name" put your payload
23
24 Payload: <script>alert(1)</script>
25
26 4) Now update the settings and our payload will be executed.
```