

main ▾

...

POC / Stored XSS



rsrahulsingh05 Create Stored XSS

[History](#)[1 contributor](#)

30 lines (17 sloc) | 971 Bytes

...

```
1 # Exploit Title: Simple Cold Storage Management System v1.0 - Stored XSS in "First Name"
2 # Exploit Author: Rahul Singh
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: Windows 10, Apache
8
9
10 Description : A Stored XSS in Simple Cold Storage Management System v1.0 allows an attacker to inp
11
12
13 Vulnerable Parameters:
14 First Name
15
16
17
18 Steps:
19 1) Login into account
20 2) Go to My Account
21 3) Now in Parameters "First Name" put your payload
22
23
24
25 Payload: <script>alert(1)</script>
26
27
28
29 4) Now save the user and our Java script payload will be stored.
```

30 | 5) As the payload has been stored in the database, the alert will trigger everytime user will go t

