main

CVE / CVE-2022-45214.txt

Rajeshwar40 Add files via upload   History

1 contributor

47 lines (46 sloc) | 1.13 KB

```
 1   > [Suggested description]
 2   > A cross-site scripting (XSS) vulnerability in Sanitization Management
 3   > System v1.0.0 allows attackers to execute arbitrary web scripts or HTML
 4   > via a crafted payload injected into the username parameter at
 5   > /php-sms/classes/Login.php.
 6   >
 7   > ----------------------------------------
 8   >
 9   > [Vulnerability Type]
10   > Cross Site Scripting (XSS)
11   >
12   > ----------------------------------------
13   >
14   > [Vendor of Product]
15   > https://www.sourcecodester.com
16   >
17   > ----------------------------------------
18   >
19   > [Affected Product Code Base]
20   > Sanitization Management System - V 1.0.0
21   >
22   > ----------------------------------------
23   >
24   > [Affected Component]
25   > username
26   >
27   > ----------------------------------------
28   >
29   > [Attack Type]
30   > Local
31   >
32   > ----------------------------------------
33   >
34   > [Impact Code execution]
35   > true
36   >
37   > ----------------------------------------
38   >
39   > [Reference]
40   > https://www.sourcecodester.com/php/15770/sanitization-management-system-project-php-and-mysql-free-source-code.html
41   >
42   > ----------------------------------------
43   >
44   > [Discoverer]
45   > Rajeshwar Singh
46
47   Use CVE-2022-45214.
```