

Instantly share code, notes, and snippets.



chao112122 / [gist:504e224e63c9a966ba233df1d523ce4f](#)

Secret

Last active yesterday

<> Code

Revisions 2

Stars 1

Embed ▼

<script src="https://i



Download ZIP

[gistfile1.txt](#)

```
1 CVE-2025-45236 - DBSyncer v2.0.6: Stored Cross-Site Scripting (XSS)
2 Vulnerability Type: Stored XSS
3 Attack Vector: Nickname field in the user profile
4
5 Reproduction Steps:
6
7 Log in to the DBSyncer web application as a valid user.
8
9 Navigate to the top-right section and click on "Edit Profile".
10
11 Locate the "Nickname" field and inject the following payload:
12
13 <script>alert('XSS');</script>
14 Save the changes.
15
16 Refresh the page or visit any part of the site where the nickname is displayed.
17
18 Result: The JavaScript payload is executed in the victim's browser session, demonstrating a persistence
19
20 Impact: Allows attackers to execute arbitrary JavaScript in the context of other users, potentially
```