

```
# Exploit Title: EgavilanMedia My To Do List 1.0 - Stored Cross Site Scripting
# Exploit Author: Dwiki Kusuma
# Vendor Homepage: http://egavilanmedia.com
# Software Link: https://egavilanmedia.com/my-to-do-list/
# Demo: http://demo.egavilanmedia.com/My%20To-Do%20List/
# Version: 1.0
# Tested on: Chrome 87.0.4280.88 (Official Build) (x86_64) , Firefox Version 84.0.1 (64-bit)
# Contact: https://twitter.com/qlkwej
```

Vulnerable Parameters: Title and Description

Steps for reproduce:

1. Open the project / open the demo webpage
2. fill in the details & put <marquee></marquee> payload in Title or Description field
3. Our payload got executed!

4. Poc

The screenshot shows a browser window with a 'Not Secure' warning at the top. Below it is the 'My To-Do List' application interface. On the left, there's a form with 'Title' and 'Description' fields. The 'Description' field contains the payload: <marquee></marquee>. A green 'Save' button is at the bottom of the form.

This screenshot shows the 'My To-Do List' application after saving the item. The 'Description' field now displays the injected payload: <marquee></marquee>. The 'Save' button is visible at the bottom of the form.

The screenshot shows the application after the exploit has been triggered. A confirmation dialog box is displayed in the center, showing the message "demo.egavilanmedia.com says qlkwej" with "Cancel" and "OK" buttons. In the background, the main application interface shows the saved item with the exploit payload in the description field. A red 'X' button is visible next to the item.