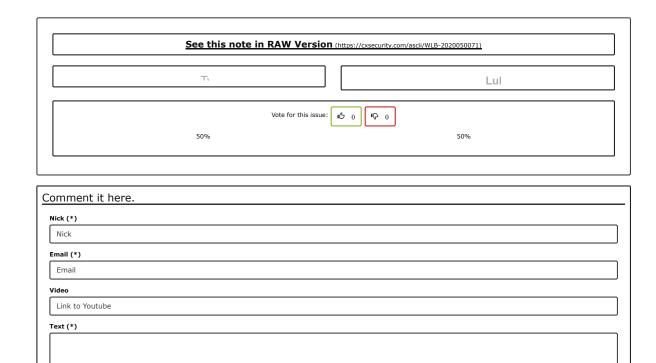
## Create-Project Manager 1.07 Cross Site Scripting / HTML Injection

Greate-Project Manager 1.07 Cross Site Scripting / TriME Injection
2020.05.09
Credit: thelastvvv (https://cxsecurity.com/author/thelastvvv/1/)
Risk: Low Local: No Remote: Yes
Risk: Low Local: No Remote: Yes
CVE: N/A  CWE: CWE-79 (https://cxsecurity.com/cwe/CWE-79)
CVE: N/A  CWE: CWE-79 (https://cxsecurity.com/cwe/CWE-79)
# Exploit Title: Create-Project Manager 1.07 Multi XSS /HTML injection Vunlerabilities
# Google Dork:N/A
# Date: 2020-05-06
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://codecanyon.net/item/create-project-manager-with-authenticator/20483329?s_rank=3
# Version: 1.6 # Tested on: 5.4.0-kali4-amd64
# Tested On: 5.4.0-Xall4-amod4
About :
Create! freelancer manager is a complete project management solution for developers, freelancers and software companies, it offers powerf
ul tools for project development, tracking each developer work time for each project, generating invoices for online payment, complete so cial network with chat and news feed for developers, and powerful financial section for income and expenses.
Summary:
Multi Persistent Cross-site Scripting and HTML injection in Create 1.07 - Freelancer Project Manager
PoC:
1- Go to any of following:
A-Online chat
B-Social feed
C-Message (title-tag)  B-Add new client (all-tags)
2 100 100 02200 (022 0030)
2- In the text field type your payload :
<h>&gt;vvv</h> >
<pre><svg onload="confirm()"></svg></pre>
3-then hit Enter
3-then hit Enter
4- Once the admin or users receive the message or read /visit the post feed they will be xssed
Impact:
XSS can lead the adminstators & users Session Hijacking, it can also lead to disclosure of sensitive data and other critical attacks on administrators and the webapp directly.
distributions and the medical first
Screentshoots:
A-Online chat https://i.imgur.com/nNGVoXI.png B-Social feed https://i.imgur.com/yQle2Mn.png
C-Message (title-tag) https://i.imgur.com/8usFkJ7.png

B-Add new client (all-tags) https://i.imgur.com/oWYA88d.png



Copyright 2022, cxsecurity.com