

Instantly share code, notes, and snippets.



unklerunkle / [gist:73e2ab58d1a5b9129be5de55765ea4fe](#)

Created last week

<> **Code** Revisions 1

Embed ▼

<script src="https://i



Download ZIP

Stored and Reflected Cross Site Scripting (XSS) in Multiple Locations

[gistfile1.txt](#)

```
1 Version Affected: 1.6.10
2 Version Fixed: 1.6.11
3
4 Researchers: Ray Truex (Github - rt1252) and Jason Giusto (Github - unklerunkle)
5
6 Description: There were multiple sections of Koillection v 1.6.10 that were vulnerable to Stored XSS
7
8 Proof of Concept Exploit
9 The Collection, Wishlist, and Album section of Koillection 1.6.10 are vulnerable to Stored and/or Re
10
11 Usage/Exploitation
12 To exploit the Stored XSS the following payload "<img src=x onerror=prompt(1)>" can be used in the C
13 To exploit the Reflected XSS in the Wishlists section, the same payload can be used via creating or
14 To exploit the Relfected XSS in the Albums section, the same payload can be used via creating or edi
15
16
```