Info Sec Helper Follow

Nov 19, 2020 · 1 min read · Listen

Cross site scripting Vulnerability in admin panel :-

Hello all, I am Parshwa Bhavsar again.

I have found another Vulnerability in one project called : Online news portal using PHP/MySQLi.

Download link :

Click here.

Steps to reproduce

1. Open the web application in your browser and login to admin panel
2. Then go to posts page and click on Add new button to add new post.
3. After that, You will notice one input field named “Title”.
4. In that field put Xss payload , select any category.(Any Xss payload will work)
5. In News Content field write anything than in the the news cover photo select any image.
6. Click on save.
7. You will notice that your Xss payload has triggered.
8. After that, once you visit your website, Your payload will execute every time you visit the site.

Impact

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Remediation

Apply context-dependent encoding and/or validation to user input rendered on a page.

Thanks and Regards,

Parshwa Bhavsar