Introduction

Useful links :

- XSS attacks What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy
- CSRF attacks What is CSRF (Cross-site request forgery)? Tutorial & Examples | Web Security Academy
- XSF attacks Framing Attacks and Cross-frame scripting explained
- CSP basics Content Security Policy (CSP) - HTTP | MDN
- X Frame options header X-Frame-Options - HTTP | MDN
- CSRF token Cross-Site Request Forgery Prevention - OWASP Cheat Sheet Series
- XSS, CSRF and CSP vulnerabilities (lab root-me) Challenges/Web - Client [Root Me : Hacking and Information Security learning platform]
- samesite cookie attribute Set-Cookie - HTTP | MDN

TL;DR : Use the security built-in your framework, and do not use custom injection of code. Enable the different securities integrated in your framework, such as CSRF token. Deny all iframe, or scope it to trusted domains if needed

---

Revision #3
Created 12 April 2024 03:36:26 by Seaweedbrain
Updated 12 April 2024 03:38:45 by Seaweedbrain