

How to Prevent XSS Attacks Cross-site scripting is a serious security vulnerability that can cause significant disruptions and malicious outcomes for unsuspecting users and organizations. Use of vulnerability scanning tools: Employ vulnerability scanning tools, penetration testing tools, and web application firewalls to help prevent XSS attacks and keep your website from being compromised. Implement a Content Security Policy (CSP): Set up CSP headers to restrict the source of resource loading to prevent attacker scripts from executing. Utilize cookie attributes and HTTP-only cookies: Take advantage of cookie attributes and HTTP-only cookies to change how JavaScript and browsers interact with cookies, thereby limiting the impact of XSS attacks. To prevent XSS attacks, it's essential to take the proper steps to shield your applications from these types of threats: Validate input: Always check and sanitize input from users or other systems. By scrutinizing user inputs for illegal characters and allowing only what's necessary, you reduce the risk of sneaky scripts slipping through.