# 1: Cross Site Scripting

|  |
| --- |
| **Vulnerability / Risk** |
| Stored XSS (Cross-Site Scripting) occurs when an application stores untrusted user input in a database and later retrieves and displays it without proper sanitization or encoding. This makes it possible for an attacker to inject malicious JavaScript, which executes when another user views the compromised content.   * *Persistent Execution***:** Unlike Reflected XSS, which requires user interaction, Stored XSS is permanently embedded in the database and automatically executes whenever an affected page is accessed. * *Automated Attack Trigger:* Each time a user clicks the compromised button(Update Info), the malicious script runs without requiring any further action from the victim. * *Content Manipulation & Phishing:* Attackers can modify webpage content, redirect users to fraudulent login pages, or embed keyloggers to capture sensitive information. |
|  |