|  |  |
| --- | --- |
| **Observation No. 1** | |
| **Vulnerability** | XSS |
| **Status** | Open |
| **Severity** | **High** |
| **Description** | Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. |
| **Remediation** | The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet. Also, it’s crucial that you turn off HTTP TRACE support on all web servers. An attacker can steal cookie data via Javascript even when document.cookie is disabled or not supported by the client. This attack is mounted when a user posts a malicious script to a forum so when another user clicks the link, an asynchronous HTTP Trace call is triggered which collects the user’s cookie information from the server, and then sends it over to another malicious server that collects the cookie information so the attacker can mount a session hijack attack. This is easily mitigated by removing support for HTTP TRACE on all web servers. |
| **Affected URLs** | * http://localhost:3000/observation/create/65019513646866b0ae1ee87d |
| **References** | https://owasp.org/www-community/attacks/xss/ |
| **Proof Of Concept** | Screenshot shared below. |
| http://localhost:3000/observation/create/65019513646866b0ae1ee87d | |
| http://localhost:3000/observation/create/65019513646866b0ae1ee87d | |
| http://localhost:3000/observation/create/65019513646866b0ae1ee87d | |