

**Reflected XSS on Search Page**

**on 28 July 2018**

**by** **Overfl0w**

|  |  |
| --- | --- |
| **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.  An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page |
| **Affected Endpoint** | **https://www.tokopedia.com/search** |
| **Impact** | 1. Steal credentials in non-HTTPOnly cookies. 2. send requests to a server with the user's credentials. Think XSRF 3. steal secrets that are stored in JS variables. 4. prompt the user to download content by submitting a form 5. display a password input, log keystrokes, and send the result to a site of your choosing |
| **Steps to Reproduce** | 1.  2.  3. |
| **POC** | List of screenshoot |
| **Remediation** | 1.  2. |
| **References** | 1. <https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)> |