**Vulnerability Report – Task 3**

Report ID: #Task3-XSS-Intruder

Vulnerability: Reflected Cross-site Scripting (XSS)

Target URL: http://testasp.vulnweb.com/search.asp

Affected Parameter: searchFor

Severity: Medium

Description:

The searchFor parameter is vulnerable to reflected XSS. Payloads passed through this parameter are rendered without sanitization, leading to execution of arbitrary JavaScript.

Steps to Reproduce:

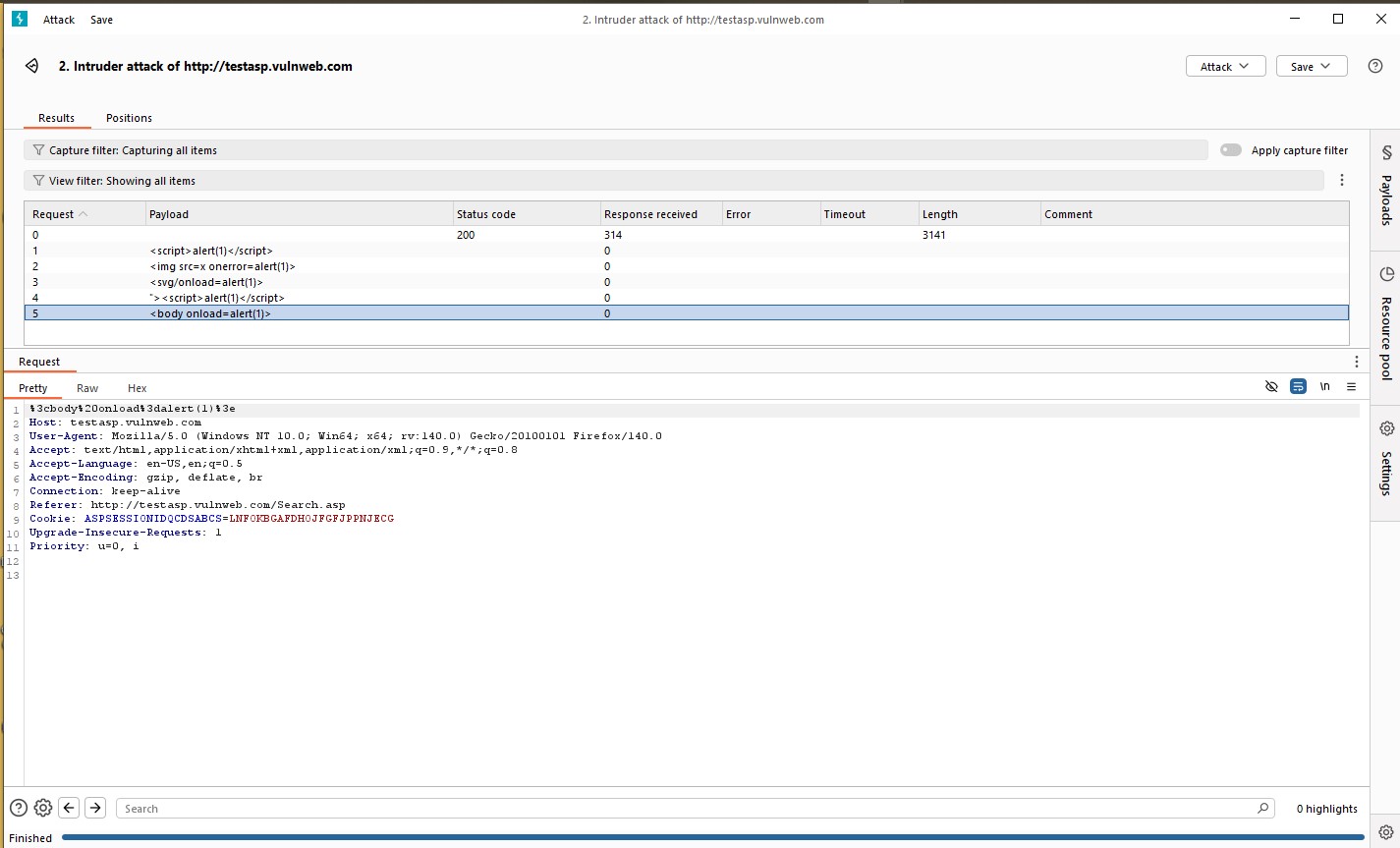
* Visit http://testasp.vulnweb.com/
* Click on the "Search" tab.
* Intercept the search request using Burp Suite Proxy.
* Send the intercepted request to Intruder.
* Add payloads in Intruder like:
* <script>alert(1)</script>
* <img src=x onerror=alert(1)>
* "><svg/onload=alert(1)>
* Launch attack and check responses.
* Observe successful JavaScript execution in the browser.

Impact:

* Allows attackers to inject and execute arbitrary JavaScript.
* Could steal cookies, session tokens, or perform phishing/redirection.
* Can be used to pivot toward more dangerous attacks (e.g., session hijacking).

Mitigation:

* Use output encoding to properly sanitize reflected content.
* Implement Content Security Policy (CSP) headers.
* Validate and filter all input on both client and server side.
* Use security libraries like DOMPurify to clean HTML.



Video Link- <https://drive.google.com/file/d/1Mmhwabtar7siOawta5RpX-rB7IByxJ7_/view?usp=sharing>