

Vulnerability: **Reflected XSS**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L (9.6 : Critical)

Description:

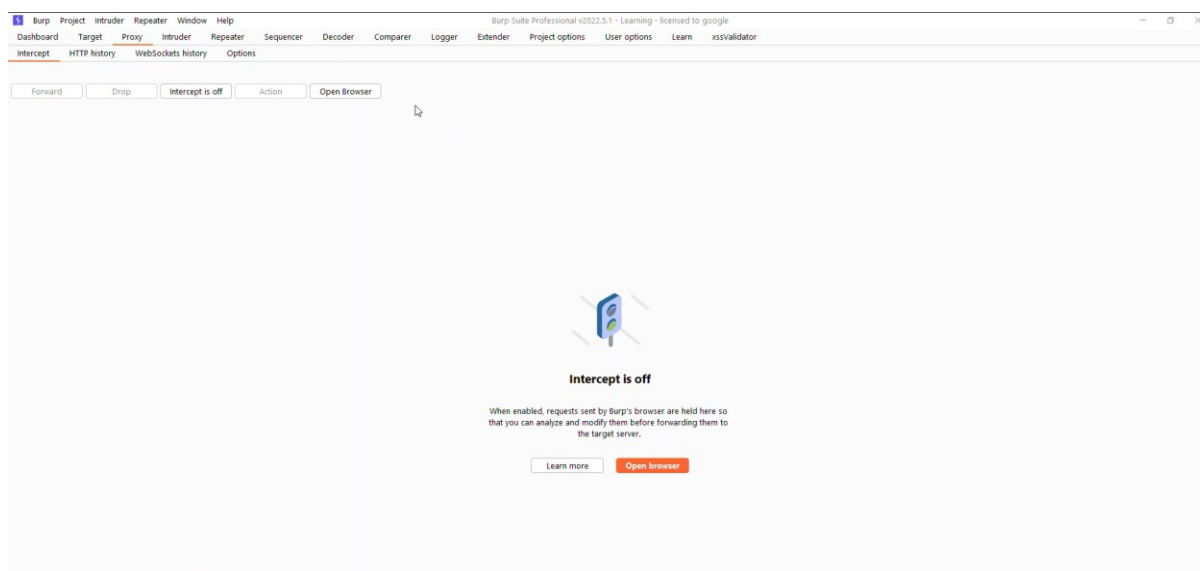
The Reflected XSS involves immediate return of output to the user. It ensures that the server is been sent a malicious javascript code and the data response is GET without validation.

Impact:

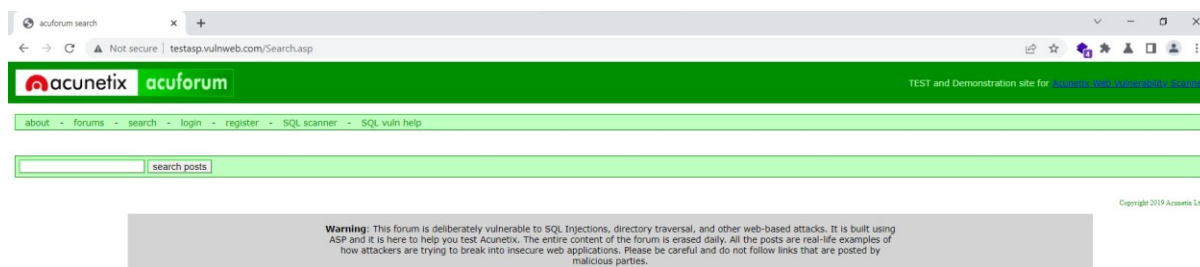
It allows adversaries to send a payload to the server consisted of list of malicious javascript codes and checks the response for exploitation. It may be exploited by sending a remote execution command for remote code execution, thus giving access to the adversary.

Steps to Reproduce:

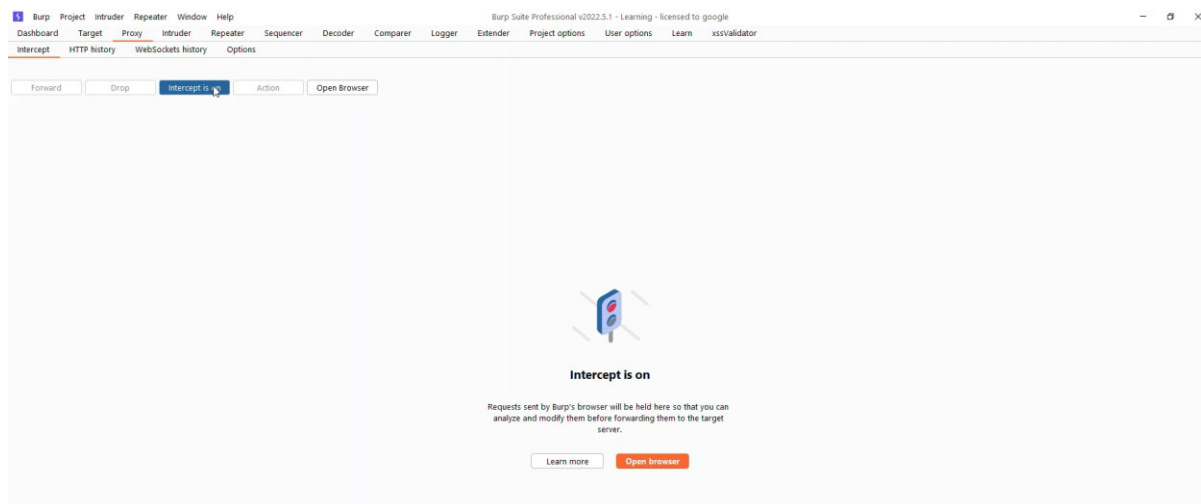
Step 1: Open Burpsuite → Proxy Tab



Step 2: Open Browser → go to <http://testasp.vulnweb.com/Search.asp>

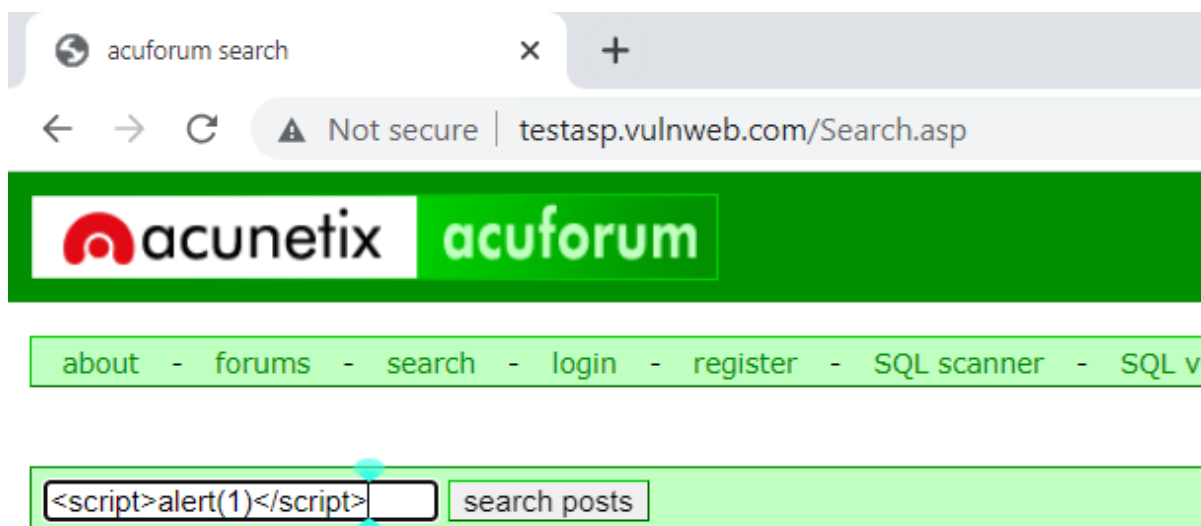


Step 3: go to BurpSuite → Turn on Intercept



Step 4: Enter javascript code

0



Warning: This
ASP and it is h
how attacke

Step 4: Send to Intruder and upload Payloads

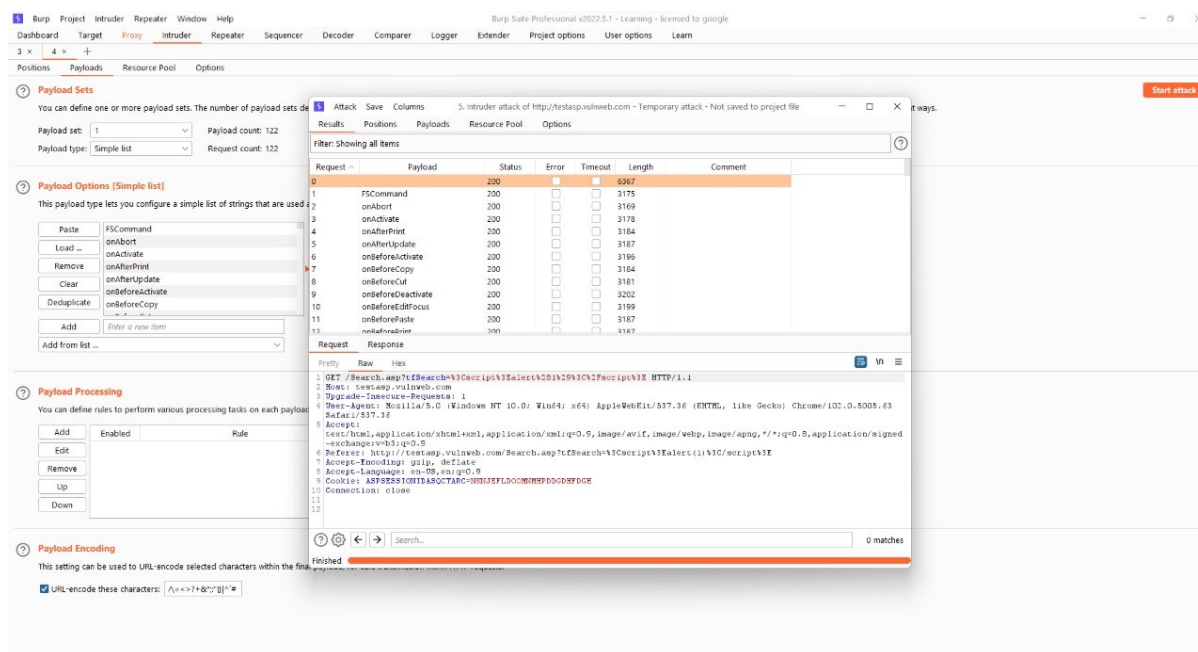
The screenshot shows the Burp Suite interface with the **Intruder** tab selected. The **Payloads** sub-tab is active, displaying the **Payload Sets** section. It indicates that you can define one or more payload sets, with the number depending on the attack type. The configuration shows **Payload set: 1** and **Payload count: 1,192**. The **Payload type** is set to **Simple list**, and the **Request count** is also **1,192**.

Below this, the **Payload Options [Simple list]** section is shown. It explains that this type lets you configure a simple list of strings used as payloads. A list of JavaScript events is displayed, including **FSCommand**, **onAbort**, **onActivate**, **onAfterPrint**, **onAfterUpdate**, **onBeforeActivate**, and **onBeforeCopy**. Buttons for **Paste**, **Load ...**, **Remove**, **Clear**, and **Deduplicate** are on the left. An **Add** button is at the bottom, followed by a text input field with the placeholder *Enter a new item* and an **Add from list ...** dropdown.

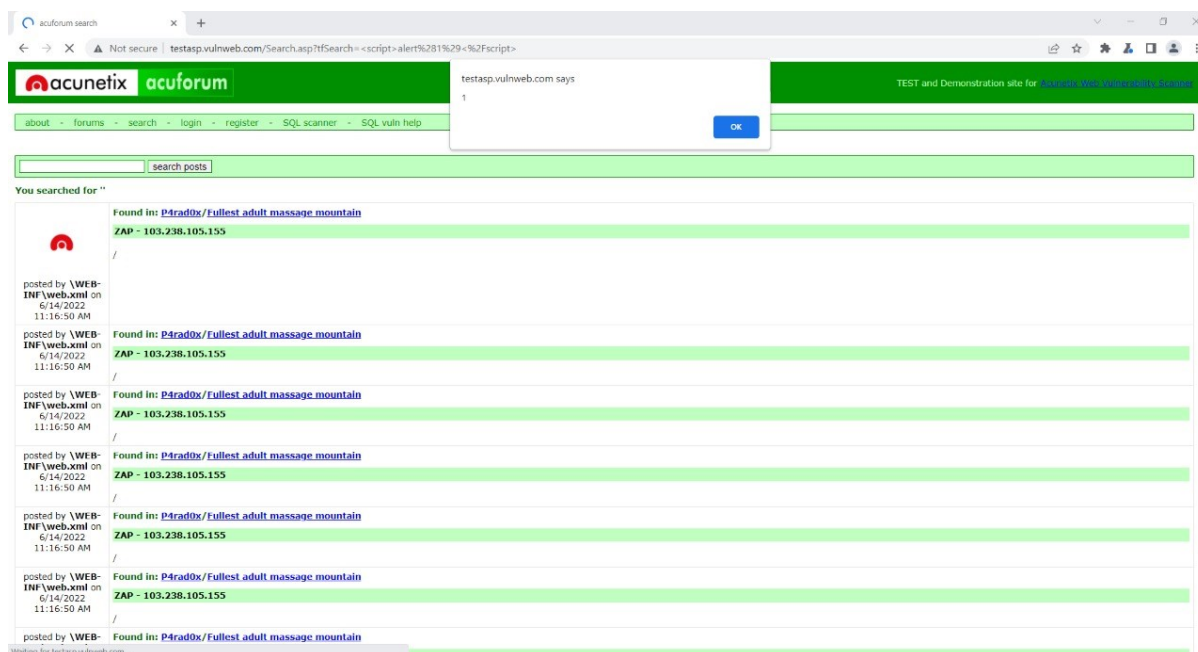
Step 4: Start attack

This screenshot shows the same Burp Suite interface as the previous one, but with the **Start attack** button highlighted in red in the top right corner. The configuration for the payload set remains the same: **Payload set: 1**, **Payload count: 1,192**, **Payload type: Simple list**, and **Request count: 1,192**. The **Payload Options [Simple list]** section is also visible, showing the same list of JavaScript events and control buttons.

Step 4: Open the attack response in browser



Step 4: Browser response to javascript code injection



Solution:

Do server site search input field code validations. Follow coding best practices for ASP.NET