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:

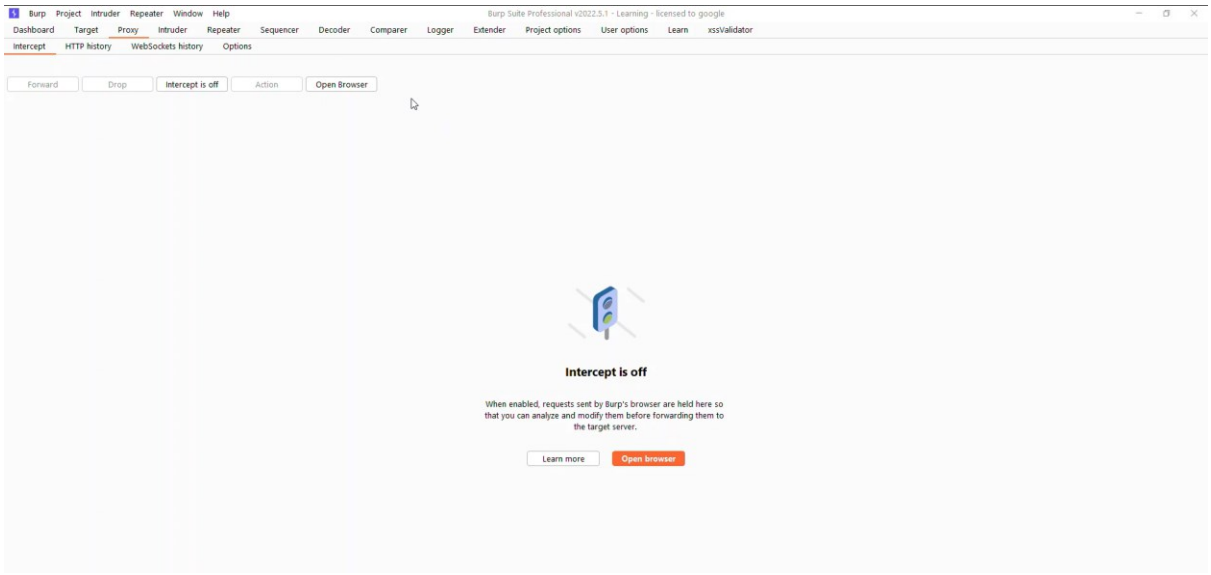
The Reflected XSS involves immediate return of output to the user. It ensures that the server is been sent a malicious javascript code and the data response is GET without validation.

Impact:

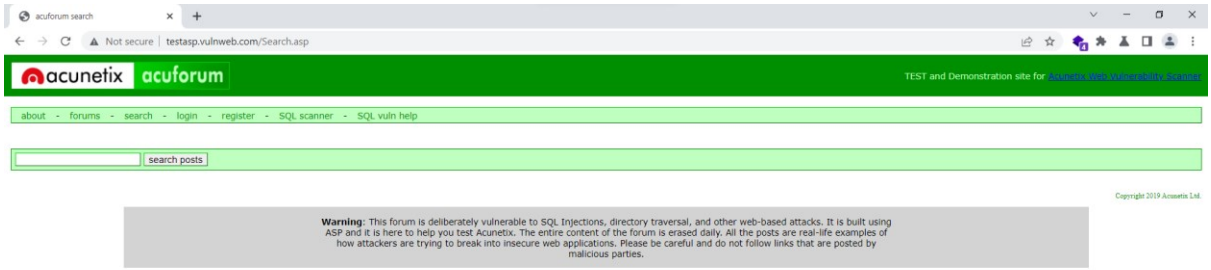
It allows adversaries to send a payload to the server consisted of list of malicious javascript codes and checks the response for exploitation. It may be exploited by sending a remote execution command for remote code execution, thus giving access to the adversary.

Steps to Reproduce:

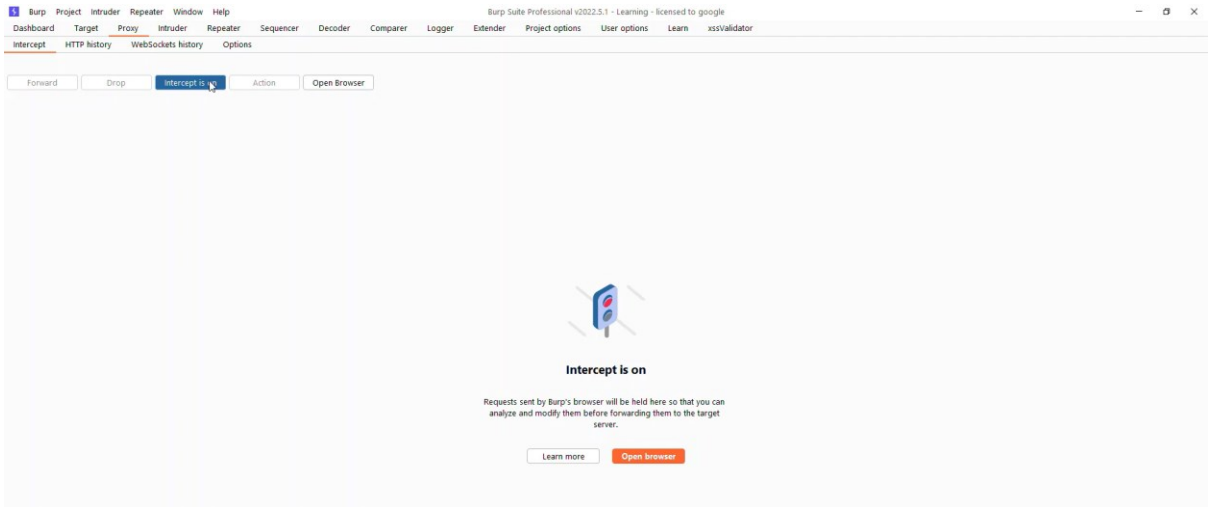
Step 1: Open Burpsuite → Proxy Tab



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

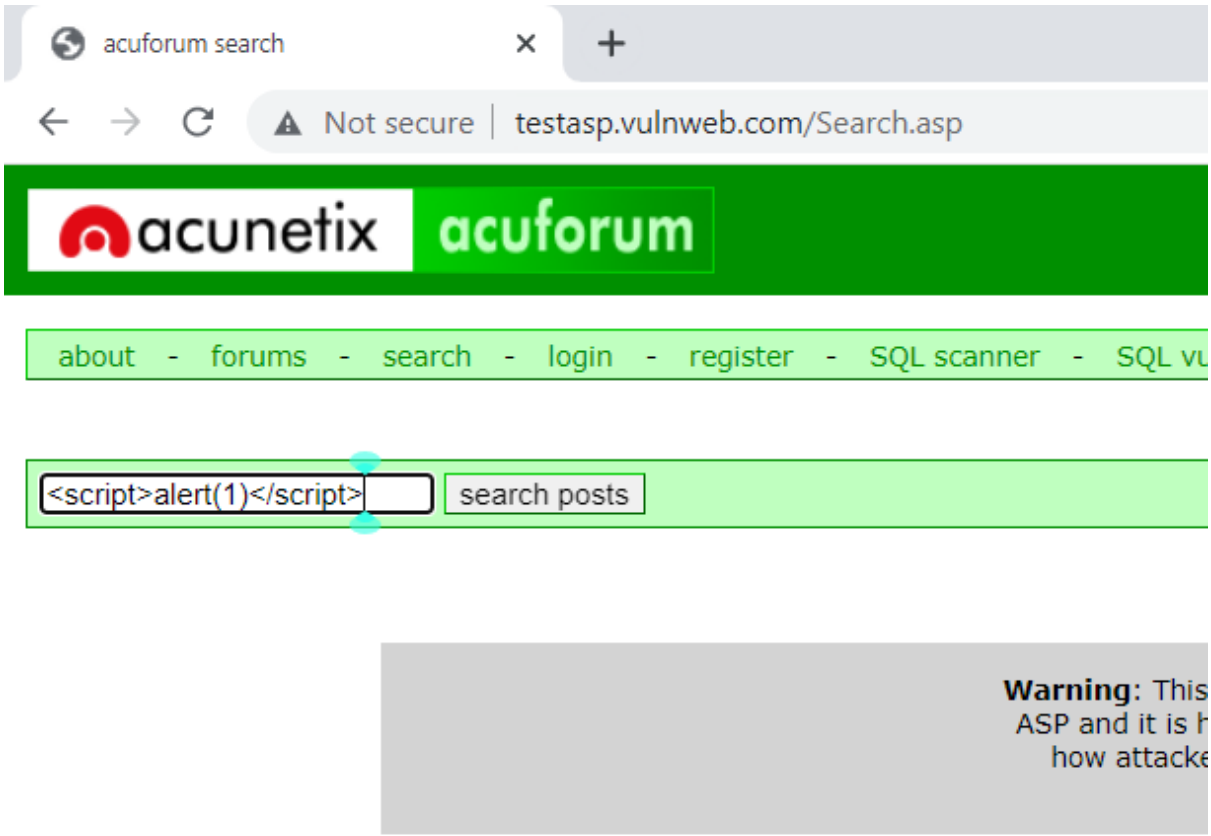


Step 3: go to BurpSuite → Turn on Intercept

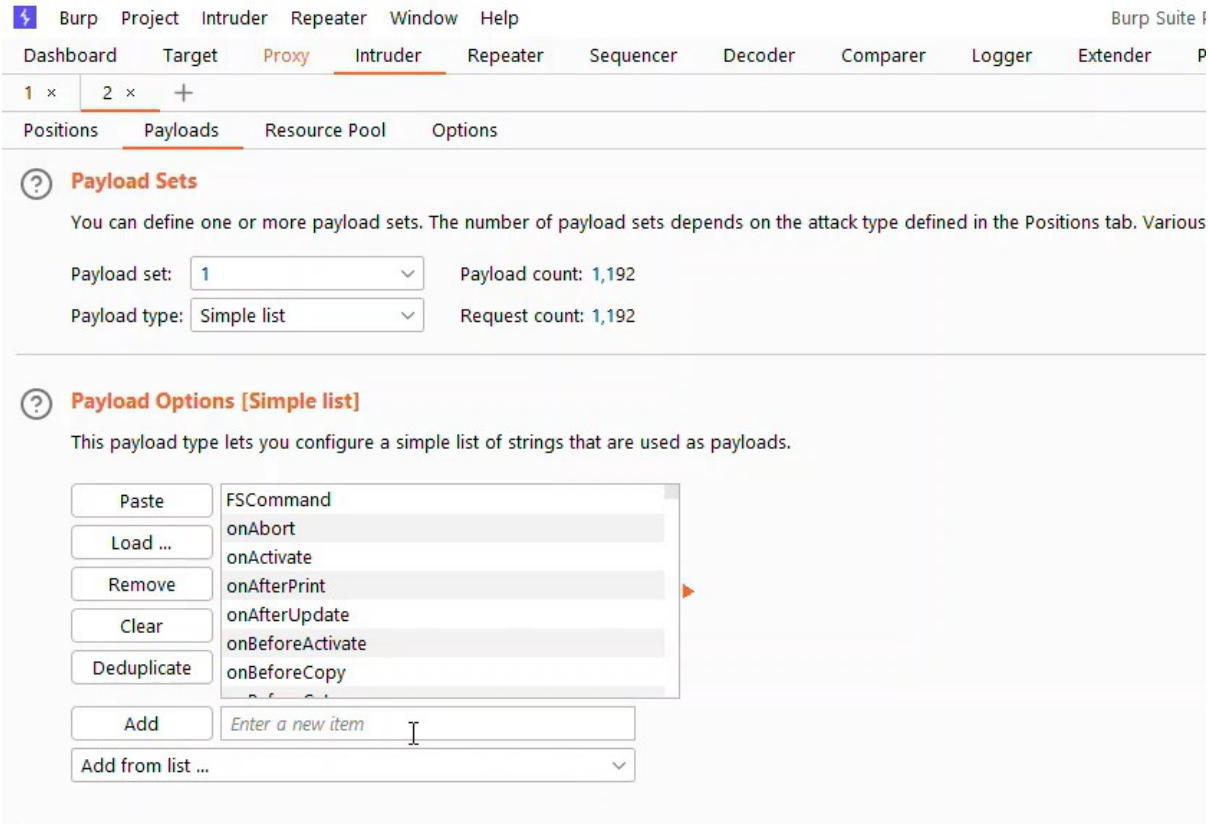


Step 4: Enter javascript code

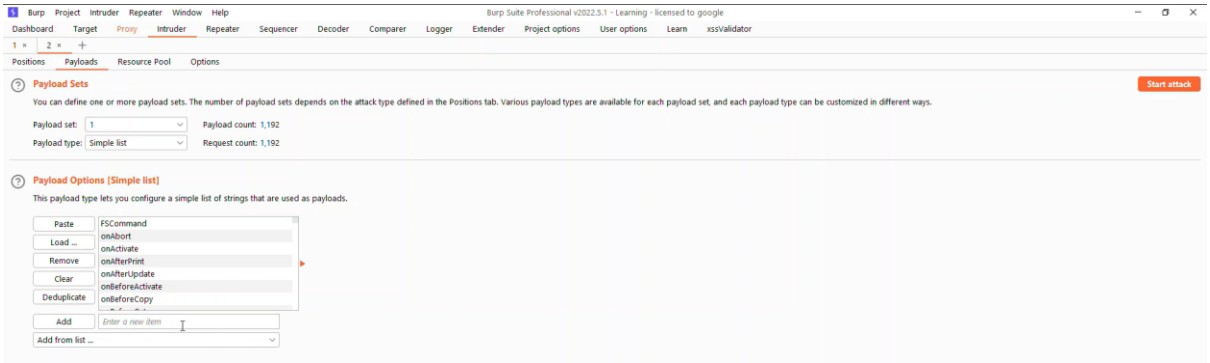
0



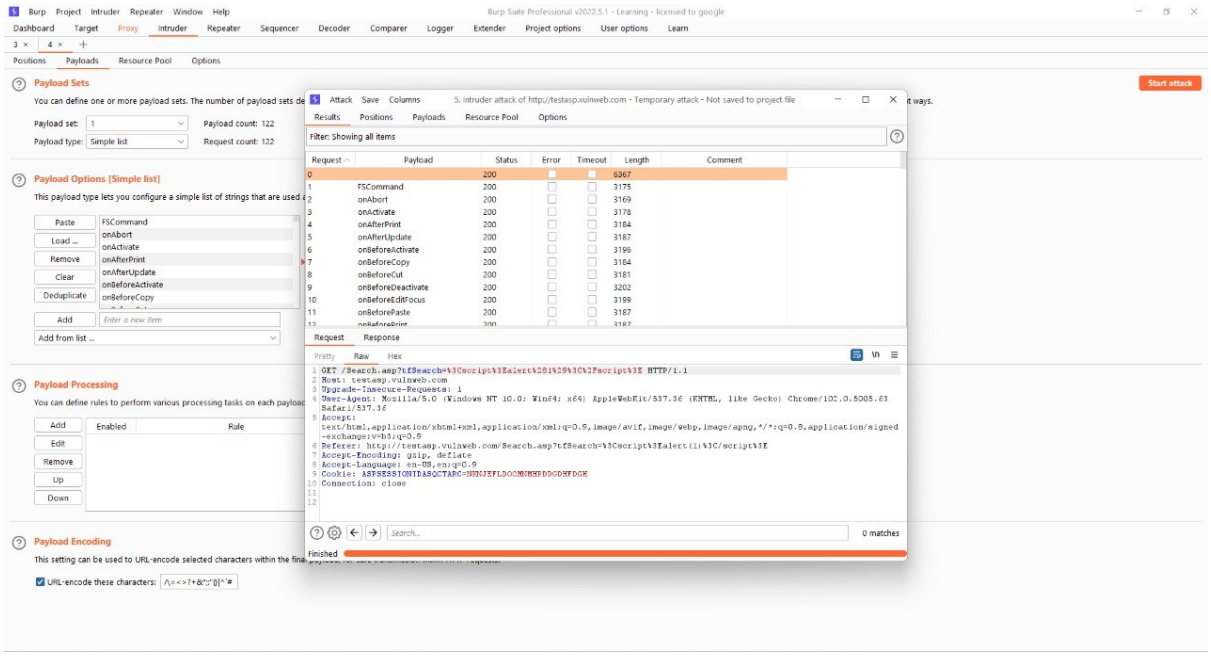
Step 4: Send to Intruder and upload Payloads



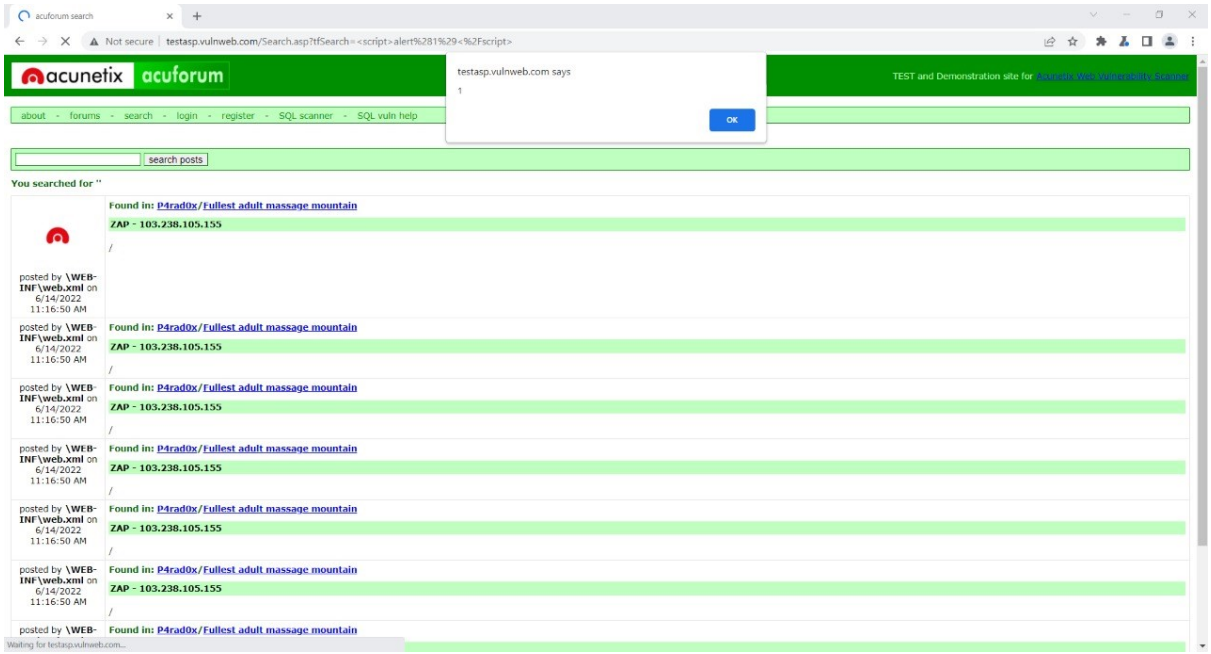
Step 4: Start attack



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