**Cross- Site Scripting (XSS) Report**

By: SHREYA PANDEY

Email: csengineerspandey@gmail.com

**Title:** Cross- Site Scripting

**Domain:** Vulnweb.com

**Subdomain:** testasp.vulnweb.com

**Parameter used:** Search

**Summary:**

The website <http://testasp.vulnweb.com/> has an endpoint that is vulnerable to an injection vulnerability called as “Reflected Cross-Site Scripting” which arises when a website receives data in HTTP request and includes the data within immediate response in an unsafe way due to improper sanitization of user input done by GET parameters.

As defined by Portswigger,

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application.

Reflected XSS, where the malicious script comes from the current HTTP request.

In the process while checking whether the website has vulnerabilities or not, I used the JavaScript payload mentioned below:

<script>onerror= alert; throw 1 </script>

**Steps used to reproduce:**

**Step 1:** Open Oracle VM virtual box and start the virtual machine

**Step 2:** Then login into Kali Linux to your root account

**Step 3:** Open Burp Suite

**Step 4:** Check whether Intercept is on or not

**Step 5:** Open Mozilla Firefox browser and search “vulnweb”

**Step 6:** Click on http://testasp.vulnweb.com on the given interface

**Step 7:** Click on the search bar

**Step 8:** Click on FoxyProxy and turn on “Burp” then type <script>onerror=alert; throw 1</script> and search it

**Step 9:** After the request is made then firstly send it to the intruder then forward it

**Step 10:** Go to the Intruder and check target

**Step 11:** Then go to positions in intruder

**Step 12:** Add the payload position for required place

**Step 13:** Go to the payloads and add the payload from the system

**Step 14:** After loading the payloads, start the attack

**Step 15:** Check whether there is a sudden change in length and status

**Step 16:** Copy the URL to show the response for the payload that has been accepted

**Step 17:** Copy the URL and search it in Mozilla Firefox browser

**IMPACT:**

When the user will access the website then the attacker can breakthrough and do malicious activities such as: -

1. Whatever the user will search the attacker will be able to see it.
2. The login credentials will also be visible to the attacker.
3. The attacker can perform any undesirable changes in the interface which user is using.
4. Even the attacker can impersonate the user without user’s knowledge and can do whatever he wants.

**REMEDY:**

In order to prevent cross-site scripting vulnerabilities following measures need to be taken in that direction such as-:

1. Filtering the input which is being entered by the user on that time only
2. Then encoding the data on output to prevent it being interpreted as active content. To encode the data, HTML, JavaScript or CSS encoding can be used in combination.
3. Use appropriate response headers such as Content-Type and X-Content-Type-Options.
4. Using CSP i.e. “Content Security Policy” to reduce the existing vulnerabilities.