

## Reflected XSS

---

**Reported to :** internshipstudio.com  
**Reported on :** 18 August 2021  
**Asset :** testasp.vulnweb.com  
**URL :** http://testasp.vulnweb.com/Search.asp  
**Weakness :** Reflected XSS  
**Severity :** Easy  
**Participants :** Roshan More

---

### Description:

Reflected XSS attacks, also known as non-persistent attacks, occur when a malicious script is reflected off of a web application to the victim's browser. The script is activated through a link, which sends a request to a website with a vulnerability that enables execution of malicious scripts. Attacker can perform a cross- site scripting attack that calls the alert function.

### Steps to Reproduce:

- Enter URL <http://zero.webappsecurity.com/login.html>
- In the search field, enter `<script>alert(1)</script>`
- Click 'search posts'.

- After user clicks ‘search posts’, website executes the alert function and a dialog box is displayed.

**Payload used:**

```
<script>alert(1)</script>
```

**Impact:**

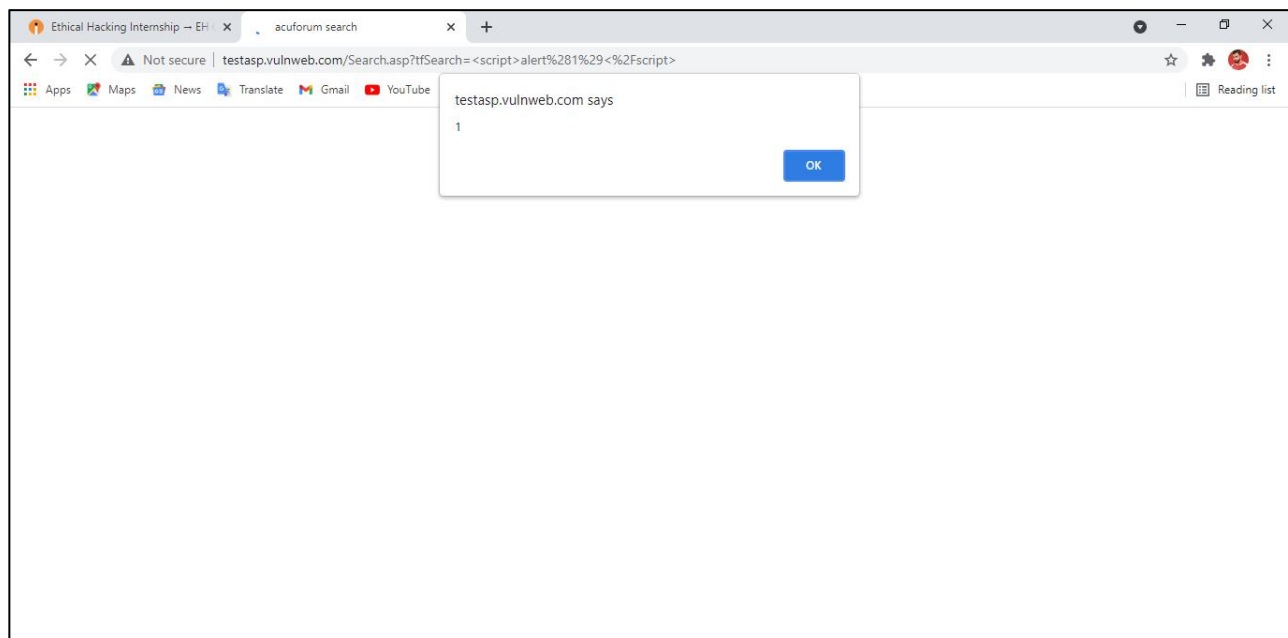
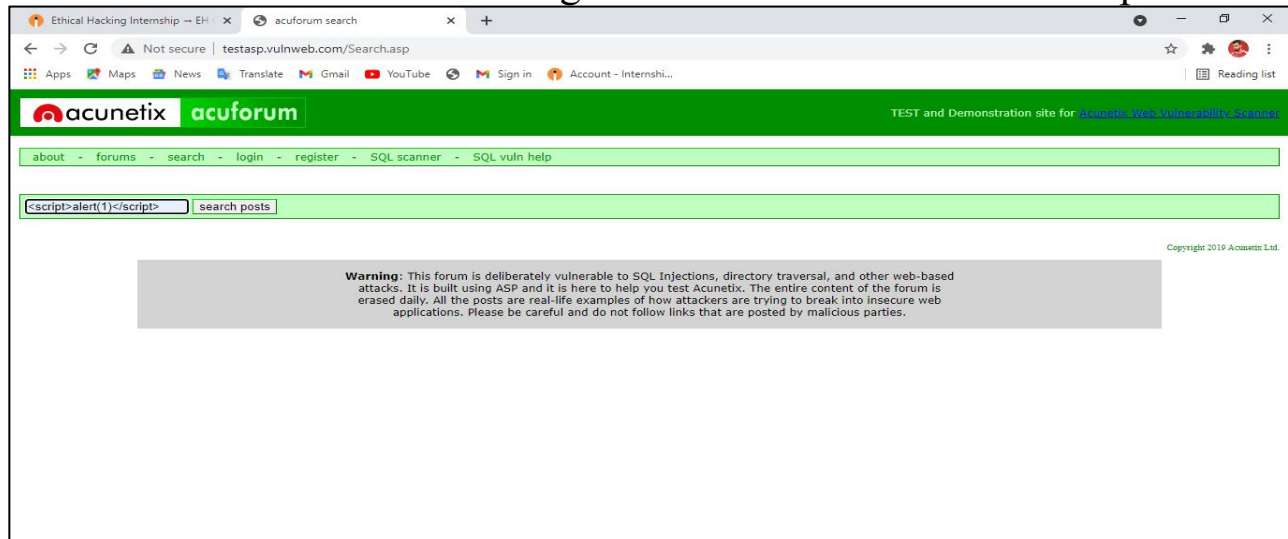
- Attacker can use this vulnerability to execute the alert function.
- View any information that the user is able to view.
- Modify any information that the user is able to modify.
- Initiate interactions with other application users, including malicious attacks, that will appear to originate from the initial victim user.

**Mitigation:**

- First of all user’s vigilance is the best way to avoid XSS.
- Disable execution of scripts in search field.

## Supporting Material/References:

Screenshots and video recording has been submitted with this report.



Ethical Hacking Internship – EH

acuforum search

testasp.vulnweb.com/Search.asp?tfSearch=<script>alert%281%29<%2Fscript>


AppsMapsNewsTranslateGmailYouTubeSign inAccount - Internshi...Reading list

acunetixacuforumTEST and Demonstration site for Acunetix Web Vulnerability Scanner


aboutforumssearchloginregisterSQL scannerSQL vuln help

search posts

You searched for "

  
posted by **admin**  
on 11/9/2005  
12:16:25 PM

**Found in: [Acunetix Web Vulnerability Scanner/1](#)**  
**1**  
1

  
posted by **admin**  
on 11/9/2005  
12:16:35 PM

**Found in: [Weather/1](#)**  
**1**  
1

Copyright 2019 Acunetix Ltd.