

TITLE: - CROSS SITE SCRIPTING

Domain: Vulnweb.com Subdomain: testasp.vulnweb.com

Steps to Reproduce: -

Step 1: Visit hNp://testasp.vulnweb.com/Step 2: On the top of the menu, you will find a search option.

Step 3: Click on it and you will be prompted with the search Box.

Step 4: You can intercept the request in

Burp Suite

Step 5: Now you can find different payloads for XSS.

Step 6: Send the request to intruder and paste all the payloads.

Step 7: Try to find a successful payload for XSS.

Step 8: Prepare a report for it.

Impact: Cross Site Scripting can lead to stealing of your user data can be Harmful for your website/company.

Mitigation: If you want to prevent your website to be vulnerable of Cross Site Scripting then you can just enable no script on browser.

Included Screenshot is included in the report which is attached below.

🔍

📁

📧

🌐

📺

🔧

Firefox

07:43 AM 🔊 🔔 🔒 🔑

acuforum search - Mozilla Firefox

Inbox (1,366) - vinaym23 ✕

acuforum search ✕ +

⬅ ➡ 🔄 🏠

🔒 🔗 testasp.vulnweb.com/Search.asp

⋮ 📑 ⭐

🔍 📄 👤 ☰

about - forums - search - login - register - SQL scanner - SQL vuln help

:<script>alert(1)</script> _____ searCh osls_t

Warning. This forum is deliberately vulnerable to SQL injections, directory traversal, and other web based attacks. It is only using ASP and it is here to help you test Acunetix. The entire content of the forum is changed daily. All the posts are real i.e. examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links or attachments posted by malicious parties.

X +

açu forum

" se h posts "

You searched for "

1

OK

Acunetix Web VulnerabilityShe

Talk about Acunetix Web vulnerability Scanner

7

7

8/14r2021 M.46:S6 AM

Weather

Whai weatr+r is in your T0wn rlght noW

1

1

11/9/2005 12:16:35 PM

Miscellaneous

AnythiFI\$ Cfosstng your mind can be posted here

0

C

Warning: This forum is deliberately vulnerable to SQL injections, directory reveal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is updated daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.