Project 3 Report

- Title – Cross Site Scripting
- Domain- Vulnweb.com
- Subdomain – testasp.vulweb.com
- Steps to reproduce
  - Step 1: Visit http://testasp.vulnweb.com/
  - Step 2: On the top 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 the intruder and paste all the payloads.
  - Step 7: Try to find a successful payload for XSS.

- Impact – The impact of cross-site scripting vulnerabilities can vary from one web application to another. It ranges from session hijacking to credential theft and other security vulnerabilities. By exploiting a cross-site scripting vulnerability, an attacker can impersonate a legitimate user and take over their account.

- Mitigation - Preventing cross-site scripting isn't a simple fix that you can turn on or off. Depending on the web application, protection strategies will differ. That said, it's important to consider the following strategies for how to mitigate cross-site scripting.

- POC including Screenshot Is included In The Report Which Is Atached Below :-

testasp.vulnweb.com says

1

OK

Not secure | testasp.vulnweb.com/Search.asp?tfSearch=<script>alert%281%29<%2Fscript>

acunetix **acuforum**

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

[ ] search posts

You searched for "

Found in: Acunetix Web Vulnerability Scanner/Mr.

Mr. - 46.11.187.39

1

posted by
KfnqDuxw on
2/28/2022
12:40:15 PM

Found in: Acunetix Web Vulnerability Scanner/Mr.

posted by
KfnqDuxw on
2/28/2022
12:40:15 PM

Mr. - 46.11.187.39

1

posted by
KfnqDuxw on
2/28/2022
12:40:15 PM

Found in: Acunetix Web Vulnerability Scanner/Mr.

Mr. - 46.11.187.39

1

posted by
KfnqDuxw on
2/28/2022
12:40:15 PM

Found in: Acunetix Web Vulnerability Scanner/Mr.

Mr. - 46.11.187.39

1

posted by
KfnqDuxw on
2/28/2022
12:40:15 PM

Found in: Acunetix Web Vulnerability Scanner/Mr.

Mr. - 46.11.187.39

1

Activate Windows   Copyright 2019 Acunetix Ltd.
Go to PC settings to activate Windows.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, 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 erased 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

6:43 PM
ENG
28/02/2022

Not secure | testasp.vulnweb.com/showforum.asp?id=0

acunetix **acuforum**

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

Acunetix Web Vulnerability Scanner

Thread	Posts	Posted by	Last Post
";print(md5(31337));$a="	21	KfnqDuxw	2/28/2022 12:51:16 PM
"'	98	KfnqDuxw	2/28/2022 12:54:02 PM
-1 OR 3*2<(0+5+773-773) --	30	KfnqDuxw	2/28/2022 12:56:58 PM
showforum.asp/.	77	KfnqDuxw	2/28/2022 1:00:03 PM
http://xfs.bxss.me	2	KfnqDuxw	2/28/2022 1:03:10 PM
${@print(md5(31337))}	1	KfnqDuxw	2/28/2022 12:39:39 PM

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, 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 erased 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.

Activate Windows
Go to PC settings to activate Windows.

ENG 6:44 PM 28/02/2022