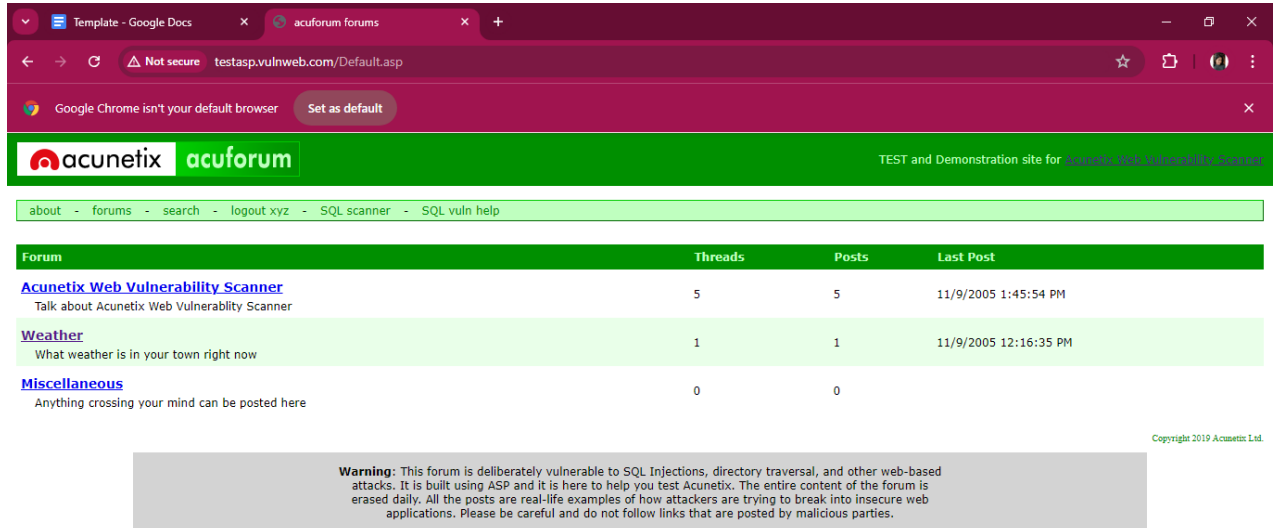


## TASK 3

Screenshots :

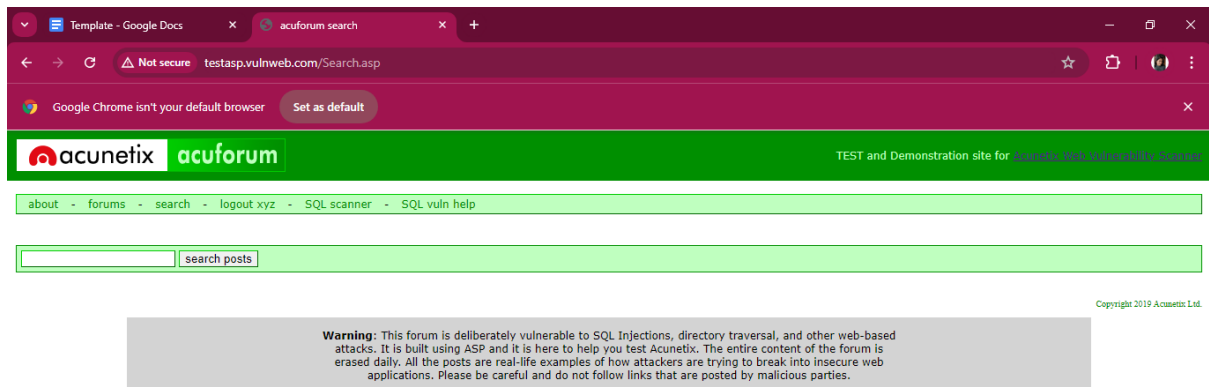


The screenshot shows the Acunetix forums page. The browser address bar indicates the URL is `testasp.vulnweb.com/Default.asp`. The page features a navigation bar with links: [about](#), [forums](#), [search](#), [logout xyz](#), [SQL scanner](#), and [SQL vuln help](#). Below this is a table listing forum topics.

Forum	Threads	Posts	Last Post
<a href="#">Acunetix Web Vulnerability Scanner</a> Talk about Acunetix Web Vulnerability Scanner	5	5	11/9/2005 1:45:54 PM
<a href="#">Weather</a> What weather is in your town right now	1	1	11/9/2005 12:16:35 PM
<a href="#">Miscellaneous</a> Anything crossing your mind can be posted here	0	0	

Copyright 2019 Acunetix Ltd.

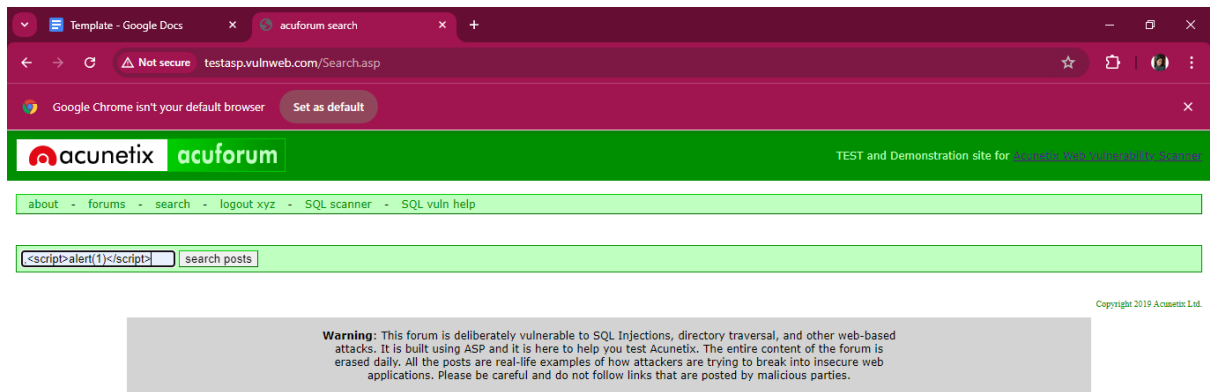
**Warning:** This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to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



The screenshot shows the Acunetix forums search page. The browser address bar indicates the URL is `testasp.vulnweb.com/Search.asp`. The page features a navigation bar with links: [about](#), [forums](#), [search](#), [logout xyz](#), [SQL scanner](#), and [SQL vuln help](#). Below this is a search bar with the text "search posts".

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.





[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

Username:	<input type="text"/>
Real name:	<input type="text"/>
Email:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Register me"/>	

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.



[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

Username:	<input type="text" value="joy"/>
Real name:	<input type="text" value="joyshua"/>
Email:	<input type="text" value="hello123@hello.com"/>
Password:	<input type="password" value="*****"/>
<input type="button" value="Register me"/>	

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.



[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

Username:	<input type="text"/>
Password:	<input type="password"/>
<input type="button" value="Login"/>	

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.



[about](#) - [forums](#) - [search](#) - [login](#) - [register](#) - [SQL scanner](#) - [SQL vuln help](#)

Username:	<input type="text" value="joy"/>
Password:	<input type="password" value="*****"/>
<input type="button" value="Login"/>	

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.

## **Video:**

[https://drive.google.com/file/d/1T1nMyc-ANJbtkS3Z2cRpScKG9\\_peGKG1/view?usp=drive link](https://drive.google.com/file/d/1T1nMyc-ANJbtkS3Z2cRpScKG9_peGKG1/view?usp=drive_link)

## **REPORT :**

Vulnerability Type: Cross-Site Scripting

URL : <http://testvulnweb.com>

Domain: <http://testasp.vulnweb.com/Search.asp>

### **Steps to Reproduce:**

Step 1: Identifying the Vulnerable Input

Navigate to <http://testvulnweb.com/Search.asp>

Step 2: Testing for XSS

XSS payload: `<script>alert(1)</script>`

Step 3: Observing the Results

If the script alert box appears with the message '1',  
the vulnerability is confirmed.

### **Impact:**

An XSS vulnerability allows attackers to inject malicious scripts into web pages viewed by other users.

### **Mitigation:**

Ensure that all user inputs are validated and sanitized on the server side.