Task 3:Report on XSS Vulnerability

Name:Aakanksha Kalyani

Title : Cross Site Scripting

Domain : http://testasp.vulnweb.com/

Subdomain : http://testasp.vulnweb.com/Search.asp

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.

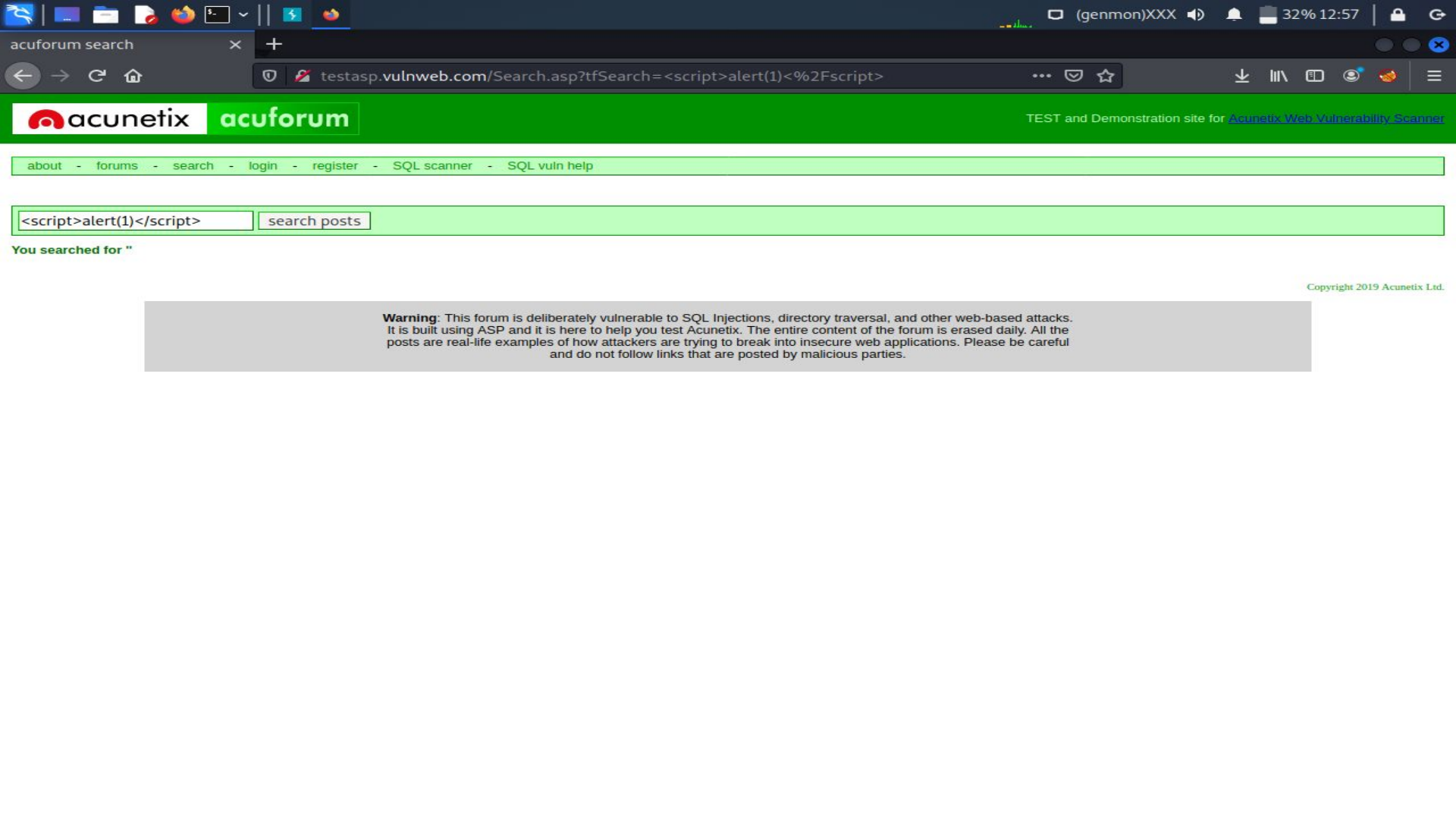
Step 7: Try to find a successful payload for XSS.

Step 8: Prepare a report for it.

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.
If the victim user has administrative privileges, it might lead to severe damage such as modifications in code or databases to further weaken the security of the web application, depending on the rights of the account and the web application.

Mitigation : XSS typically involve sanitizing data input (to make sure input does not contain any code), escaping all output (to make sure data is not presented as code), and re-structuring applications so code is loaded from well-defined endpoints.

If you want to prevent your website to be vulnerable of cross site scripting then you can jst enable noscript on browser.


acuforum search
testasp.vulnweb.com/Search.asp?tfSearch=<script>alert(1)<%2Fscript>
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register - SQL scanner - SQL vuln help
<script>alert(1)</script>
search posts
You searched for ''
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.

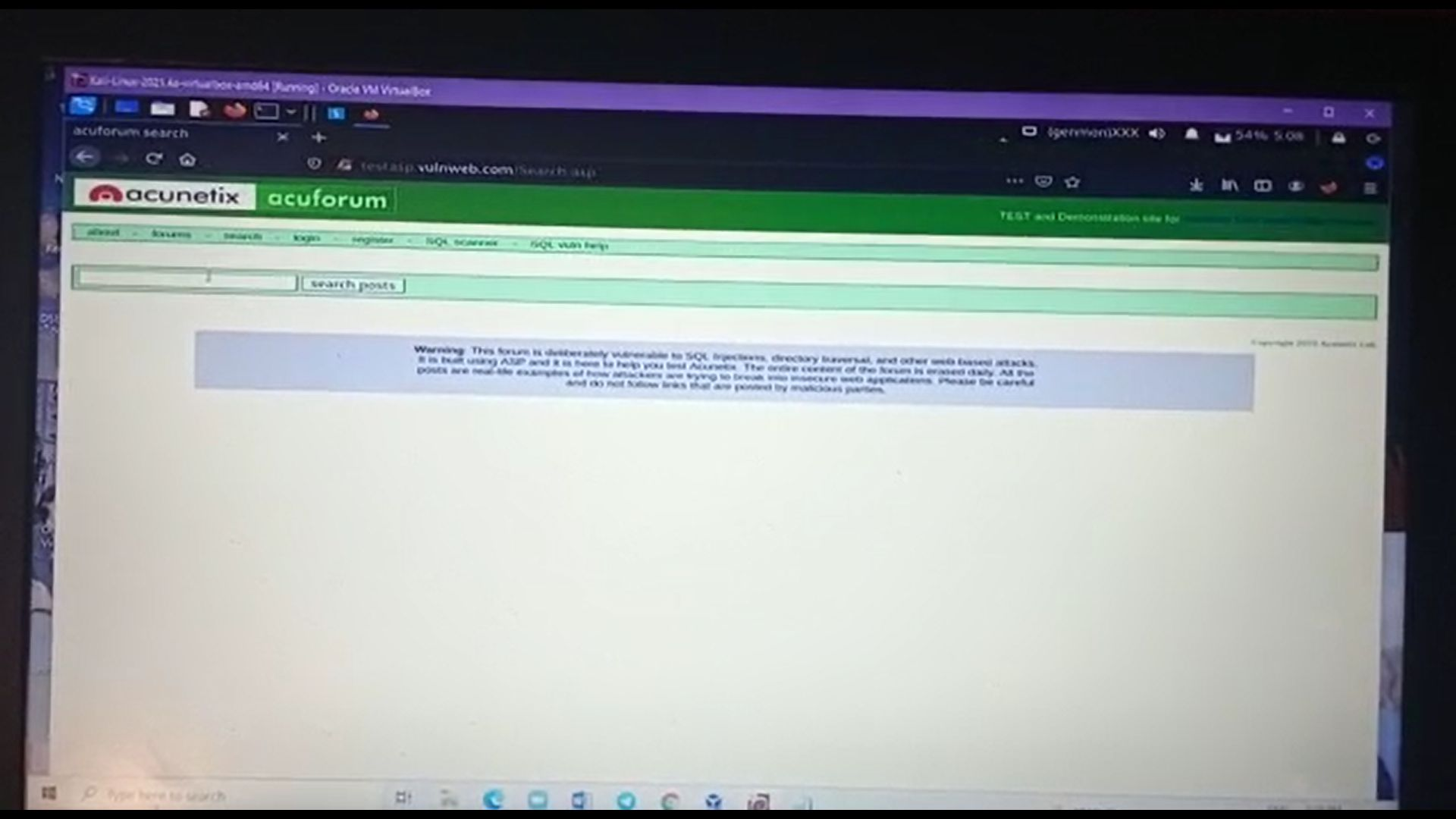
acunetix acuforum

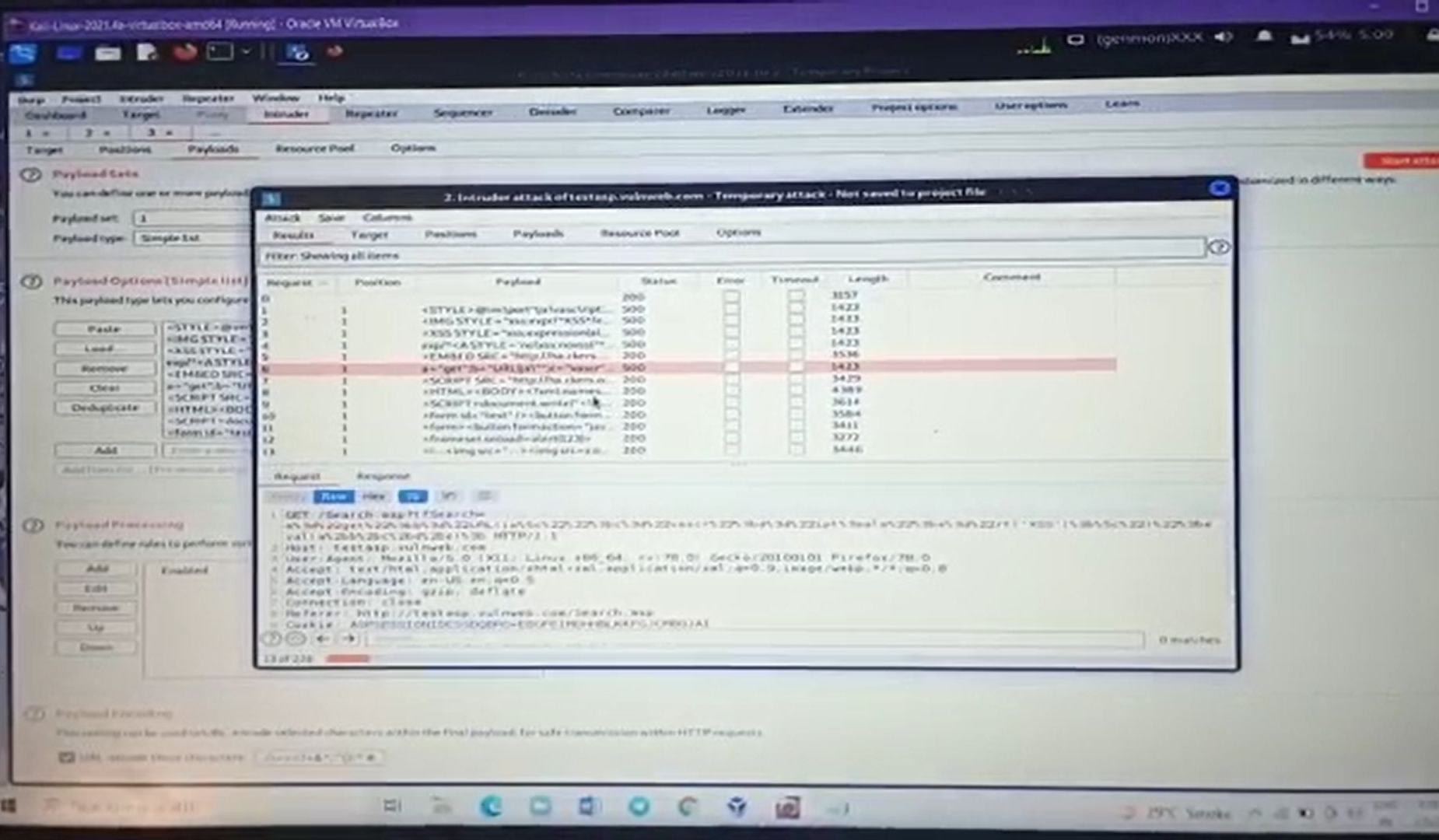
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

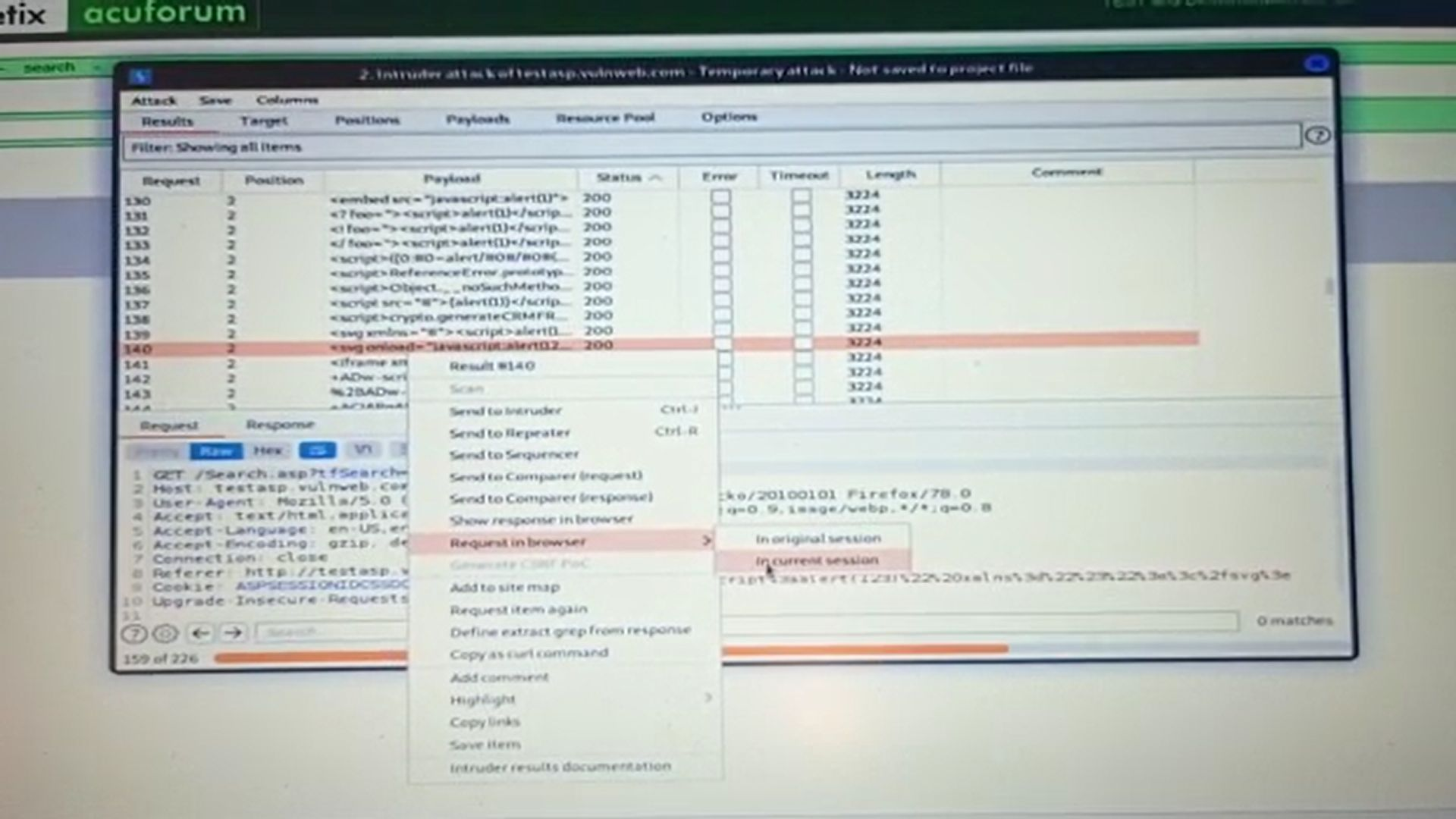
about - forums - search - login - register - SQL scanner - SQL vuln help

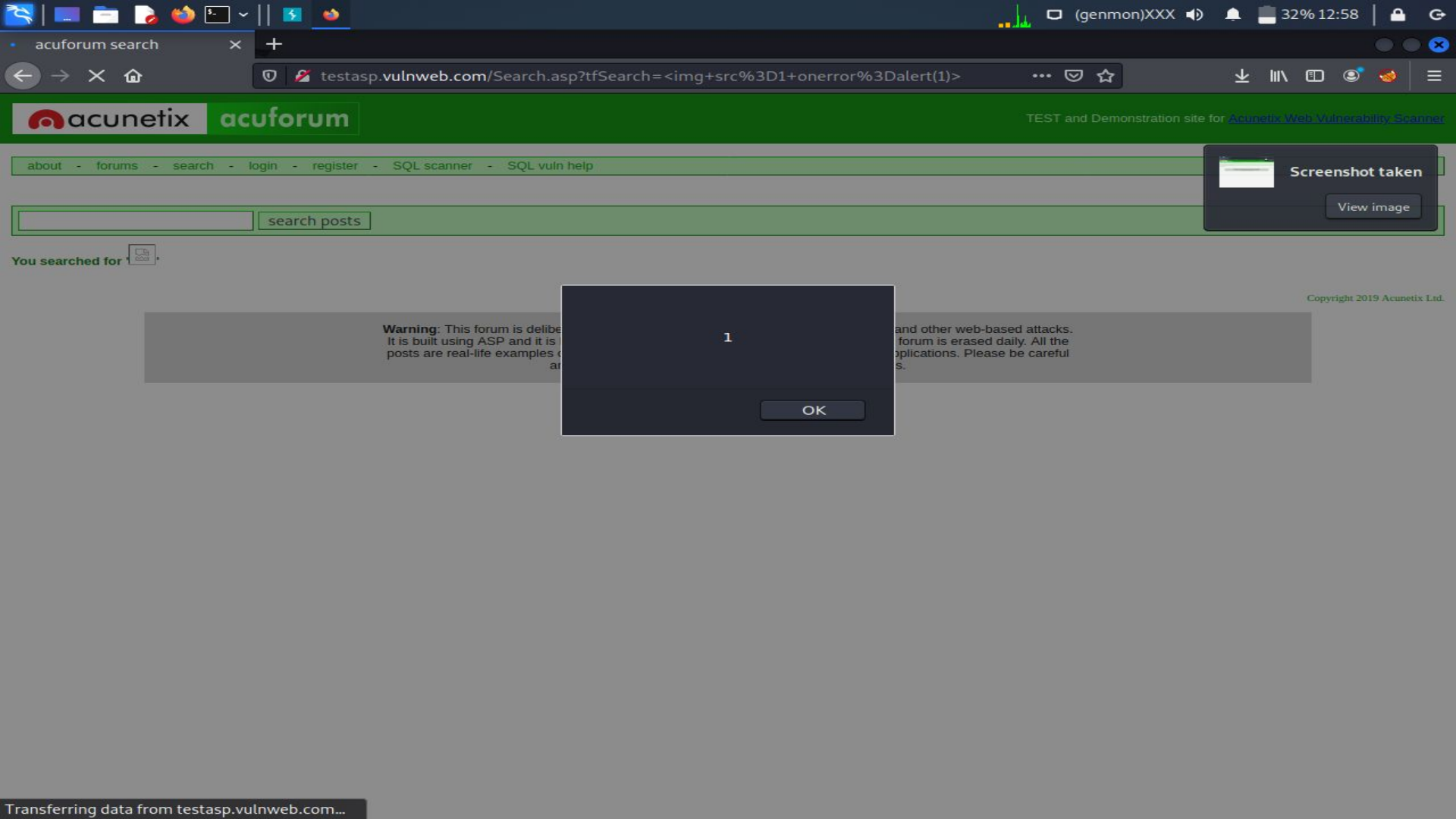
search posts

You searched for '


acuforum search
testasp.vulnweb.com/Search.asp
acunetix
acuforum
search posts
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.


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
2. Intruder attack of testasp.vulnweb.com - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
Request Response
GET /Search.asp?tfSearch=
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://testasp.vulnweb.com/Search.asp
Payload Sets
Payload Options [Simple list]
Payload Processing
Payload Encoding


acuforum
2. Intruder attack of testasp.vulnweb.com - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Position Payload Status Error Timeout Length Comment
Result #140
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
In original session
In current session
Add to site map
Request item again
Define extract grep from response
Copy as curl command
Add comment
Highlight
Copy links
Save item
Intruder results documentation
Request Response
0 matches
159 of 226


acuforum search
testasp.vulnweb.com/Search.asp?tfSearch=<img+src%3D1+onerror%3Dalert(1)>
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
Screenshot taken
View image
1
OK
Copyright 2019 Acunetix Ltd.
Warning: This forum is delibe
and other web-based attacks.
It is built using ASP and it is
forum is erased daily. All the
posts are real-life examples
plications. Please be careful
Transferring data from testasp.vulnweb.com...