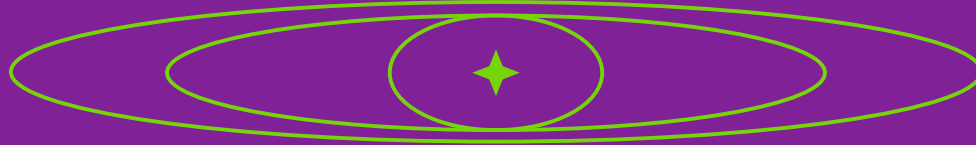


INTERNSHIP STUDIO INTERNSHIP FOR ETHICAL HACKING TASK-2

-Shibunewin@gmail.com



Task 2:

In this task you are completely free.
<http://testasp.vulnweb.com/> - This is the website. Explore the website and try to find vulnerabilities in the website and report it to us. You will be evaluated on your methods and the report you submit. Don't worry about evaluation, just report the vulnerabilities as you feel comfortable.

Title: Cross Site Scripting



Domain: <http://vulnweb.com>

Subdomain: <http://testasp.vulnweb.com>

Will see steps followed in the next slide...

STEPS INVOLVED

- 1) Use burp suit for this method.
- 2) Open Firefox and set the proxy setting as burp suit proxy.
- 3) Turn on intercept in burp suit.
- 4) In Firefox open the link
<http://testasp.vulnweb.com>
- 5) Forward in intercept in burp suit and connect.
- 6) Try the XSS script `<script>alert(1)</script>` in search box.
- 7) In burp suit forward the response in intruder.
- 8) In intruder section, post the XSS scripts.

- 
- 
- 9) start attack.
 - 10) Check which XSS script that intruded.
 - 11) Copy the response of it and paste it in Firefox browser.
 - 12) It will work (as shown in proof).
 - 13) Here `<script>alert(1)</script>` works and gives out an response of script injection.
 - 14) Stop.

Impact: Cross site scripting is harmful and dangerous where it can steal and access user data, user data is in risk.

PROOF:

The screenshot displays the Burp Suite Community Edition v2021.10.3 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main toolbar contains various tools like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The 'Proxy' tab is active, showing the 'Proxy Listeners' section. Below this, a table lists the configured listeners. The first listener is running on 127.0.0.1:8080 with a per-host certificate and default TLS protocols. Below the table are buttons for 'Import/Export CA certificate' and 'Regenerate CA certificate'. The 'Intercept Client Requests' section follows, with a checkbox for 'Intercept requests based on the following rules:' which is checked. Below this is a table of rules. The first rule is enabled and matches file extensions. The second rule is disabled and matches HTTP methods. The third rule is disabled and matches URLs. At the bottom, there are checkboxes for 'Automatically fix missing or superfluous new lines at end of request' (unchecked) and 'Automatically update Content-Length header when the request is edited' (checked).

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

	Running	Intrude	Invisible	Redirect	Certificate	TLS Protocols
	<input checked="" type="checkbox"/>				Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy Listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

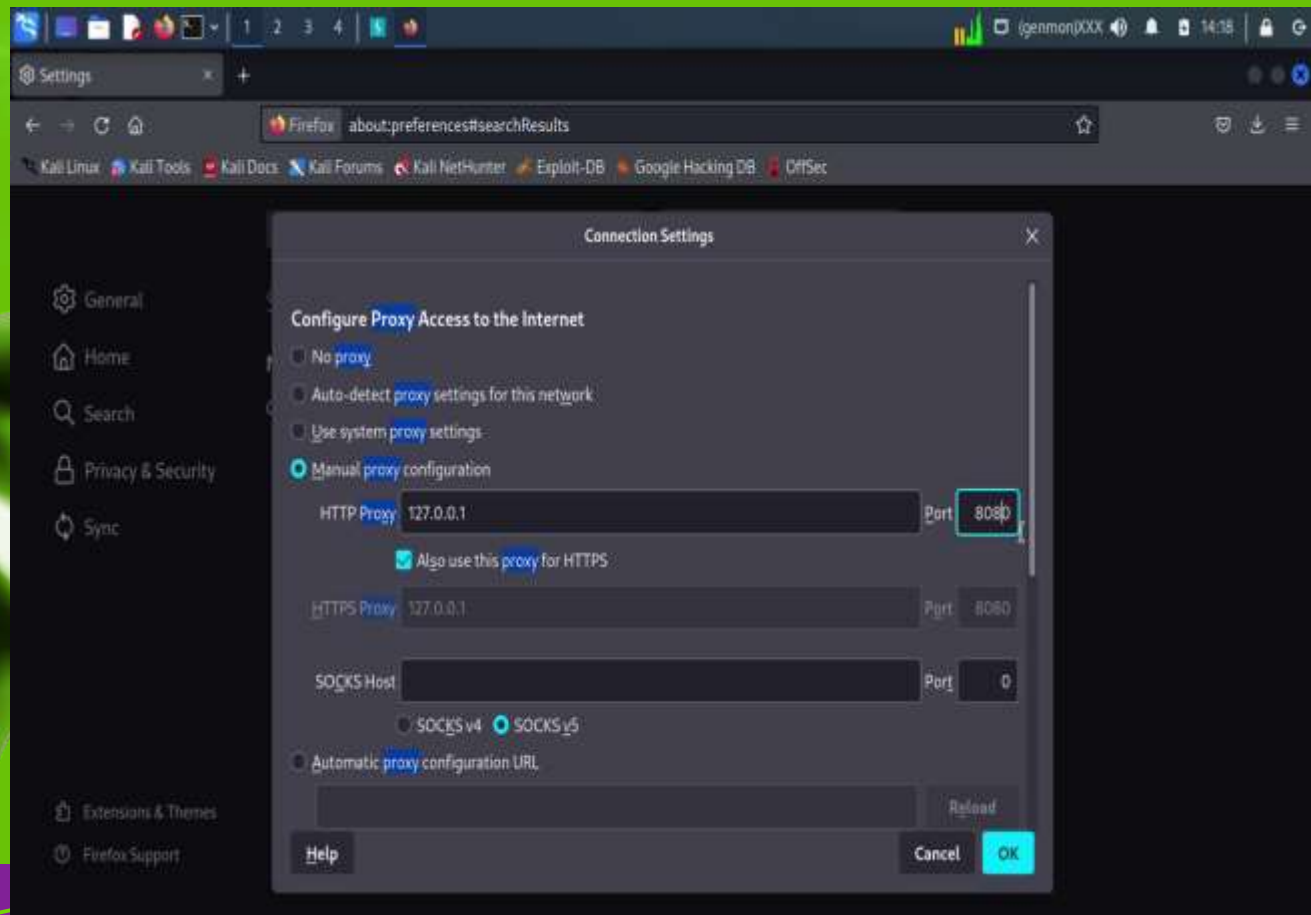
☒ Intercept requests based on the following rules:

	Enabled	Operator	Match type	Relationship	Condition
	<input checked="" type="checkbox"/>		File extension	Does not match	(*gif/*png/*jpeg/*css/*js/*ico...
	<input type="checkbox"/>	Or	Request	Contains parameters	
	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
	<input type="checkbox"/>	And	URL	Is in target scope	

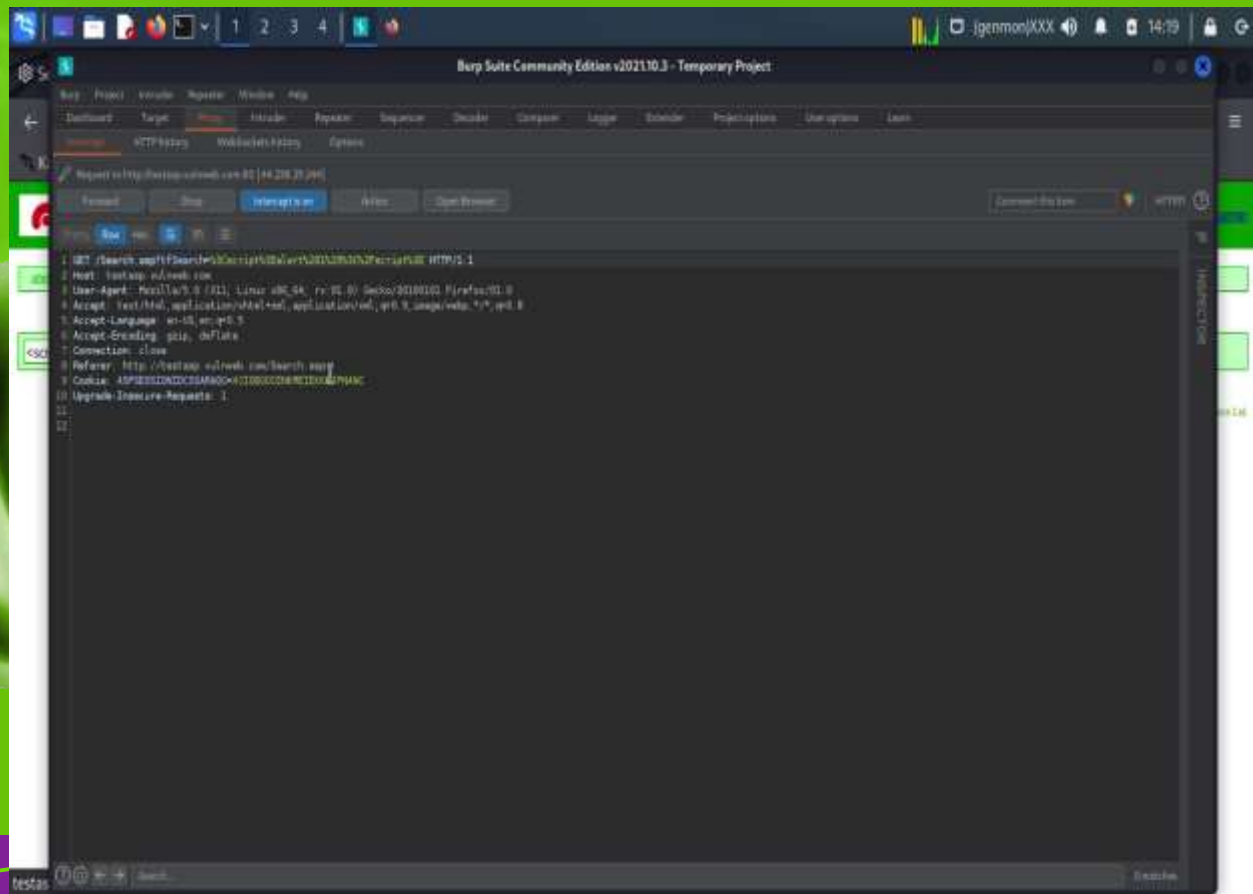
☐ Automatically fix missing or superfluous new lines at end of request.

☒ Automatically update Content-Length header when the request is edited.

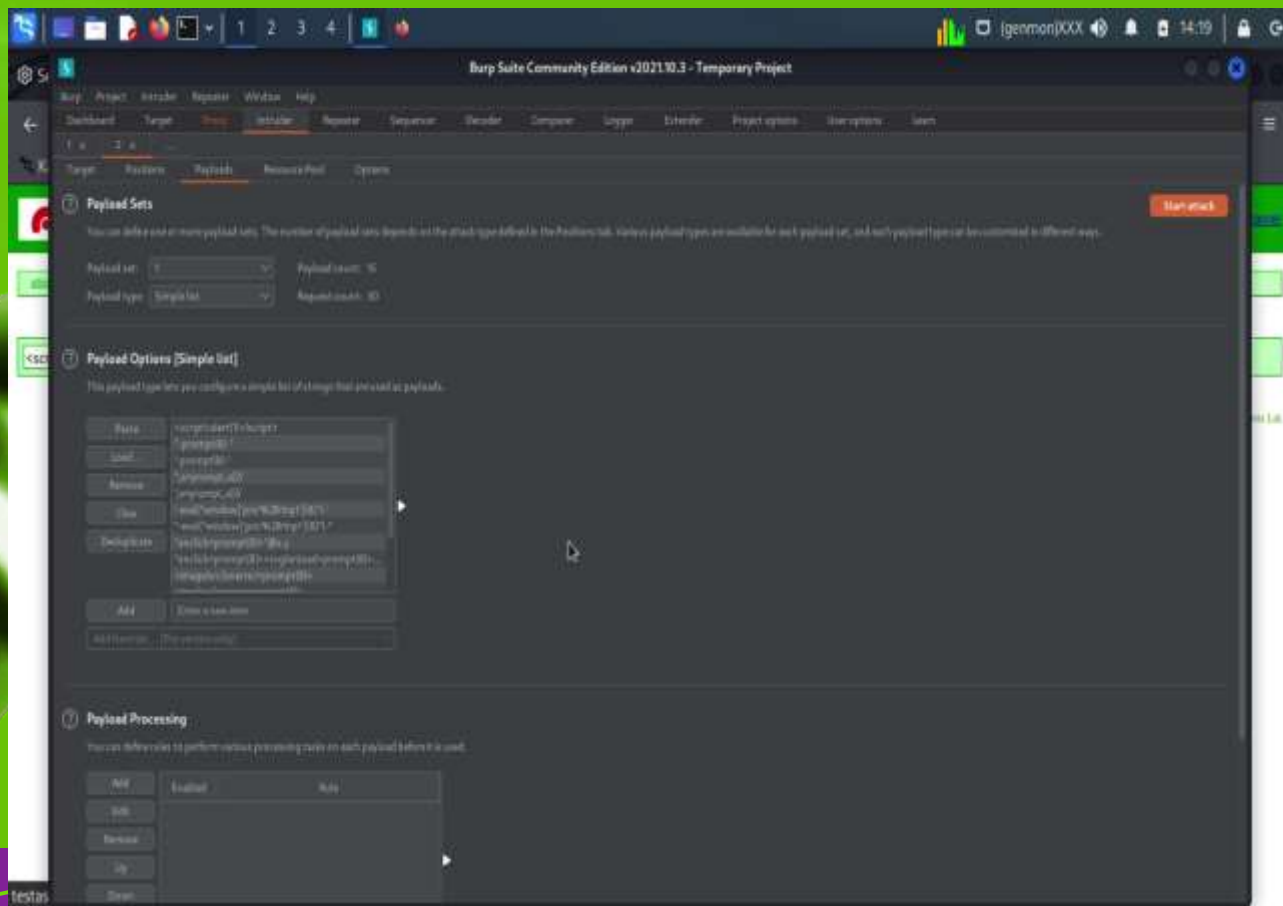
PROOF:



PROOF:



PROOF:



PROOF:

The screenshot displays the Burp Suite Community Edition interface. The main window shows a list of HTTP history items. The selected item is an HTTP GET request to `http://testasp.vulnweb.com/Search.asp?Search=script>alert(1)/&id=1`. The response is an HTTP 200 OK from `testasp.vulnweb.com`. A modal dialog titled "Show response in browser" is open, displaying the response body which contains the text `1. GET /Search.asp?Search=script>alert(1)/&id=1 HTTP/1.1`. The response body is visible in the bottom right pane.

Attack | **Target** | **Hosts** | **Payloads** | **Response** | **Options**

Filter: Showing all items

Request #	Response	Payload	Status	Error	Timeout	Length	Comment
1			200			3276	
2		script>alert(1)/&id=1	200			3282	
3		script(1)	200			3279	
4		script(1)	200			1423	
5		script(1)	200			3248	
6		script(1)	200			3276	

Show response in browser

To view the response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

`http://testasp.vulnweb.com/Search.asp?Search=script>alert(1)/&id=1` **Copy**

☐ In future, just copy the URL and don't show this dialog. **Ok**

Request | **Response**

1. GET /Search.asp?Search=script>alert(1)/&id=1 HTTP/1.1
2. Host: testasp.vulnweb.com
3. User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
4. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp;q=0.8
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Connection: close
8. Referer: http://testasp.vulnweb.com/Search.asp
9. Cookie: ASPSESSIONIDCSAFAD0HUIIIBKXEMKEDKADPMME
10. Upgrade-Insecure-Requests: 1
11.
12.

Search... **0 matches**

14 of 20

Payload Sets

You can define one or more payload sets. The sample payload set below is included in the default installation.

Payload set: **Simple list**

Payload type: **Simple list**

Payload Options (Simple list)

This payload type lets you configure a simple list of payloads.

State: script(1)/&id=1
Level: script(1)
Remove: script(1),id=1
Close
Debugging

Add **State a new item**

Add a new item... (the window only)

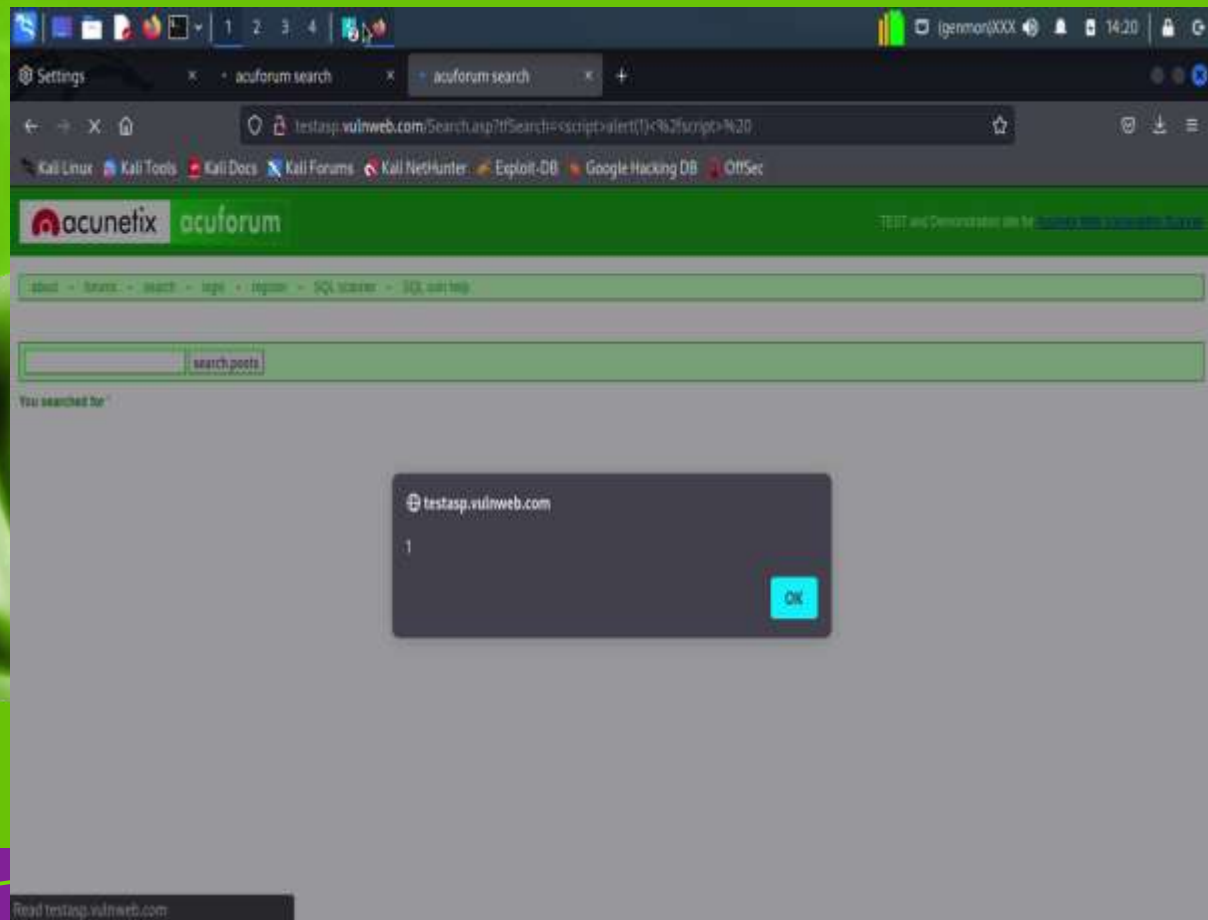
Payload Processing

You can define rules to perform various processing on the payloads.

Add **Enabled** **Name**

Test

PROOF:



Title: Sql Injection (2)

Domain: <http://vulnweb.com>

Subdomain: <http://testasp.vulnweb.com>

Login bypass-

PROOF:

Applications login

testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.a

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

acunetix acuforum

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

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

Username:

Password:

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.

PROOF:

acuforum login

testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.aspx

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

acunetix acuforum TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

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

Username: admin

Password: [masked]

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.

PROOF:

acuforum login

testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.a

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

acunetix acuforum TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

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

Username:

Password:

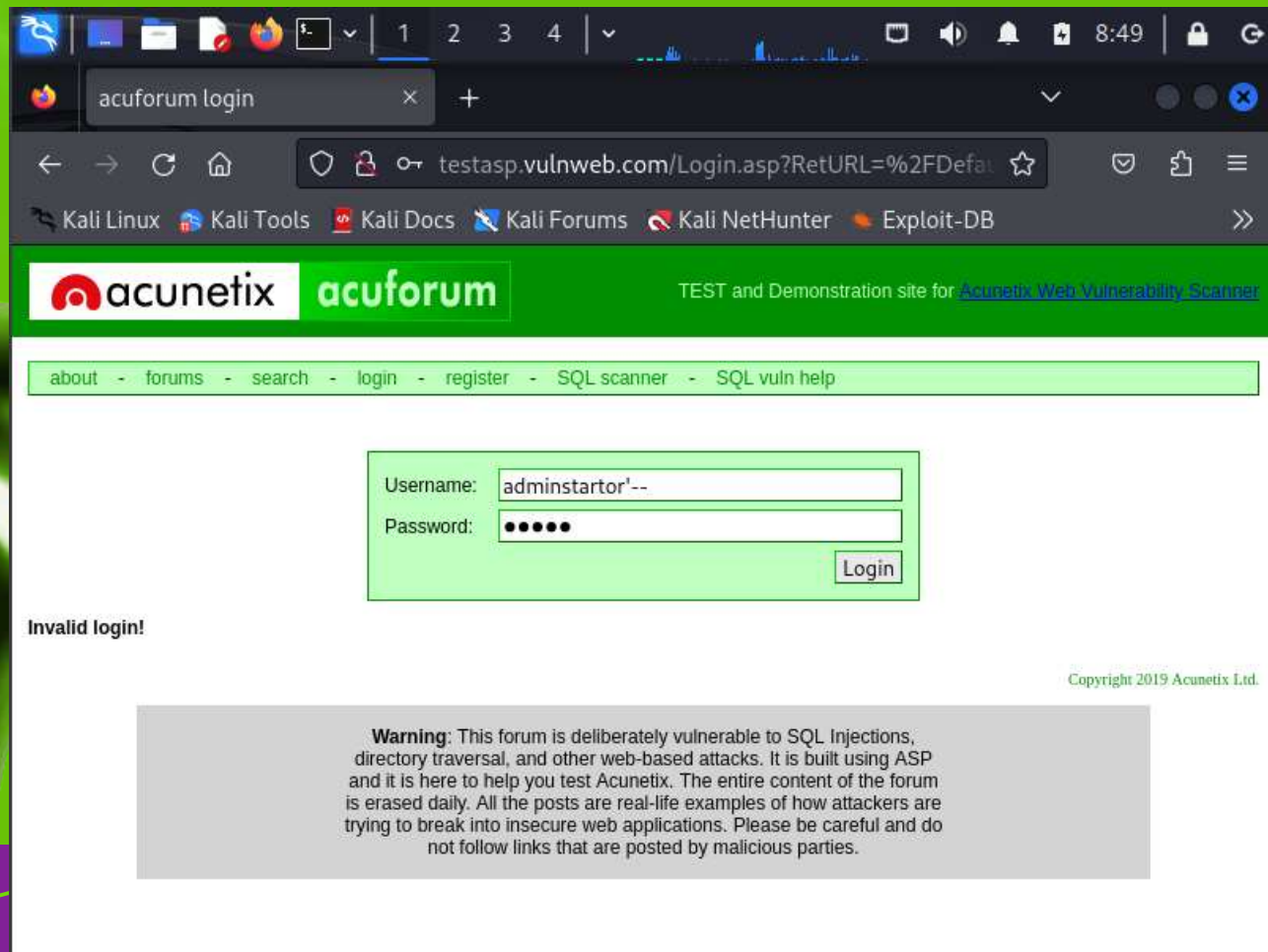
Login

Invalid 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.

PROOF:



acunetix acuforum TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

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

Username:

Password:

Login

Invalid 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.

PROOF:

acuforum login

testasp.vulnweb.com/Login.asp?RetURL=%2FSearch.asp

Kali Linux Kali Tools

acunetix

about - forums - search - login

Invalid login!

Save login for vulnweb.com?

Username

administrator'--

Password

.....

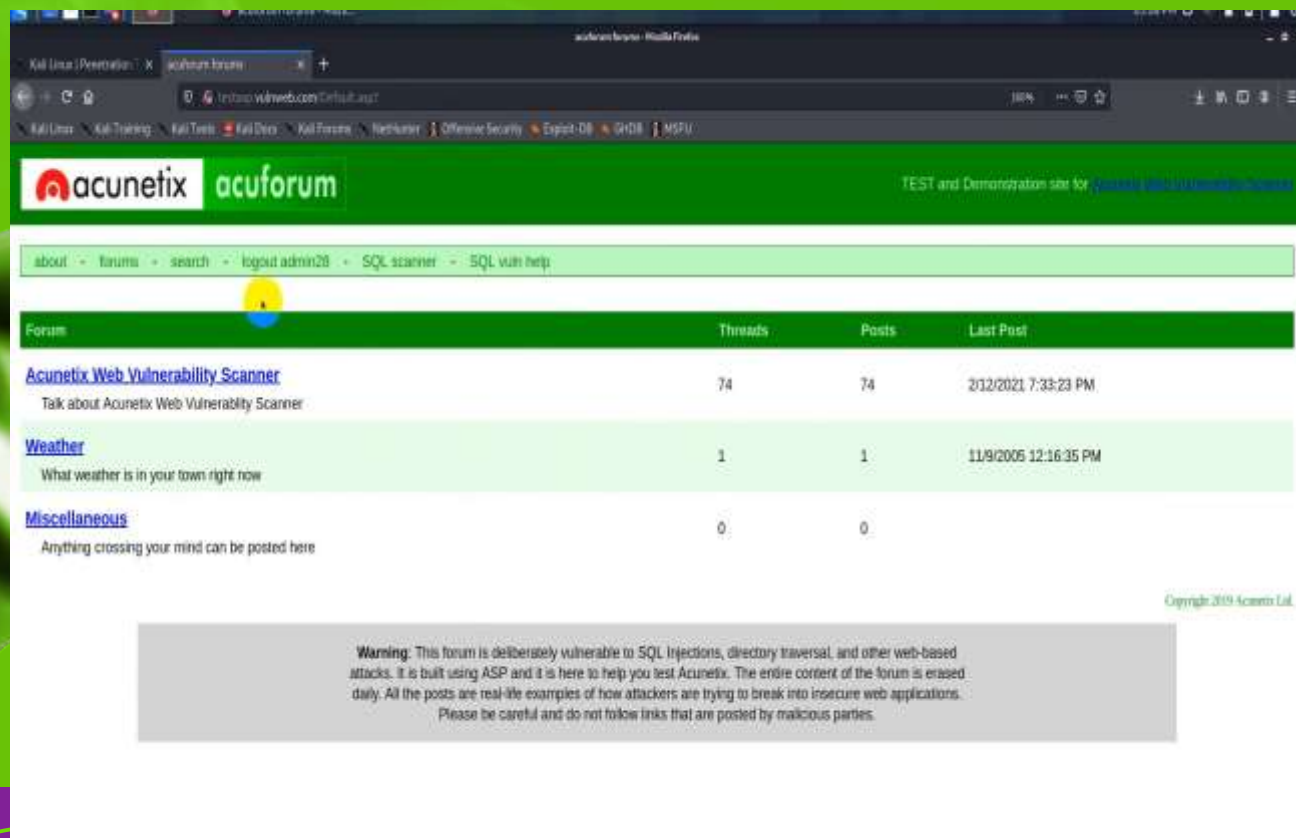
☐ Show password

Don't save Save

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.

Copyright 2019 Acunetix Ltd

PROOF:



The screenshot shows a web browser window displaying the Acunetix Forum. The browser's address bar shows the URL `https://www.acunetix.com/Default.asp?...`. The forum's header includes the Acunetix logo and the text "TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)". Below the header is a navigation bar with links: [about](#), [forums](#), [search](#), [logout admin20](#), [SQL scanner](#), and [SQL vuln help](#). The main content area features a table with forum topics. The table has four columns: "Forum", "Threads", "Posts", and "Last Post". The topics listed are "Acunetix Web Vulnerability Scanner", "Weather", and "Miscellaneous". A warning message is displayed at the bottom of the forum content.

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	74	74	2012/2021 7:33:23 PM
Weather What weather is in your town right now	1	1	11/9/2006 12:16:35 PM
Miscellaneous 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.



THANK YOU
-Shibu Newin