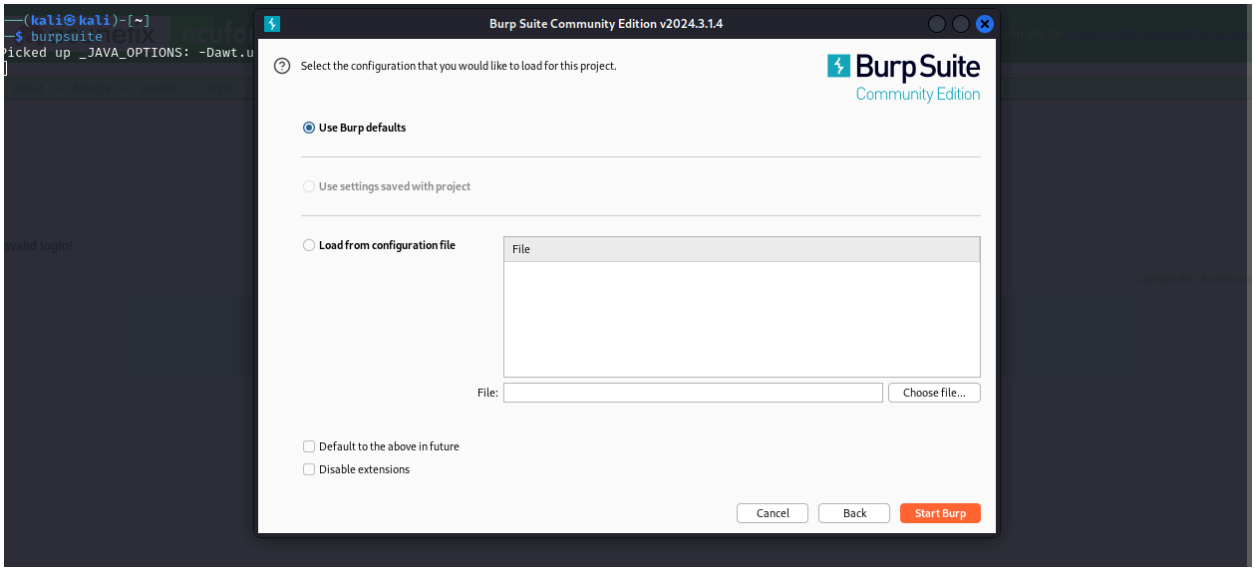
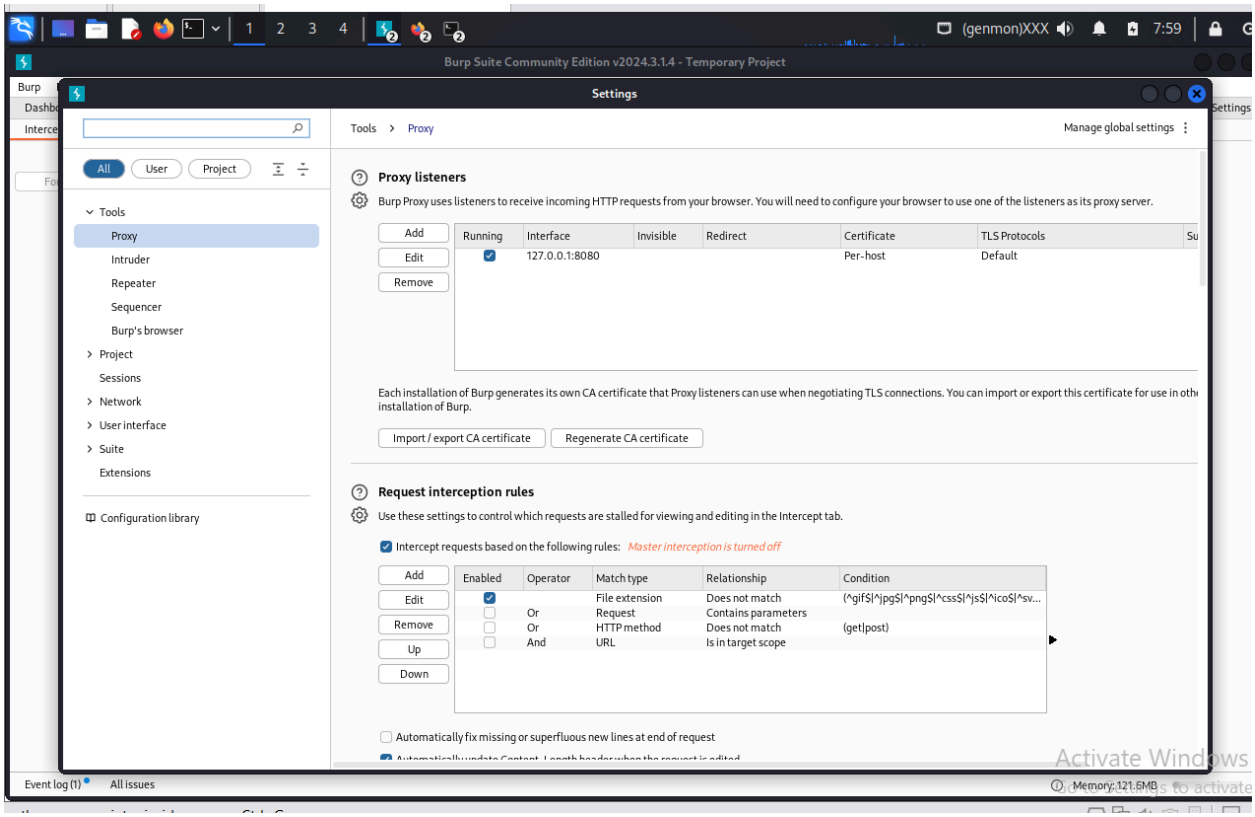
USING BURP SUITE TO INTERCEPT CLIENT SIDE REQUEST.

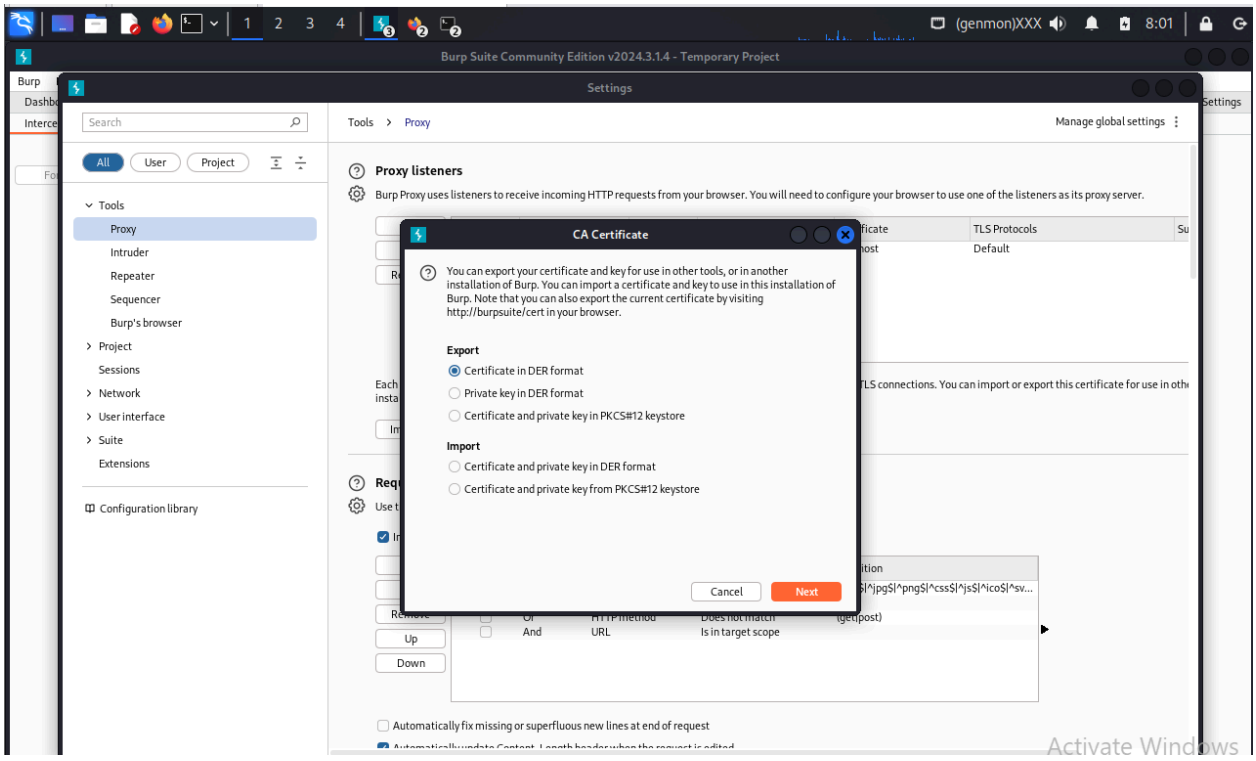
TOOLS : Kali Linux [BURP SUITE]

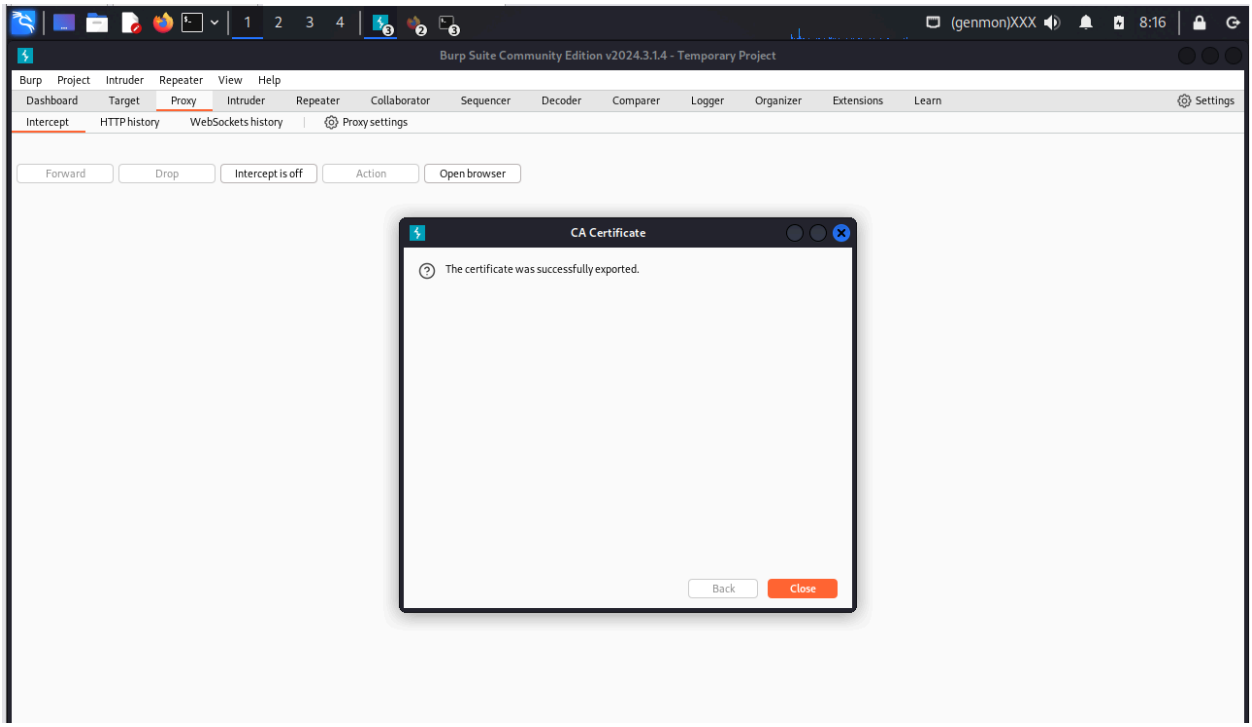
Project-Site : http://testasp.vulnweb.com

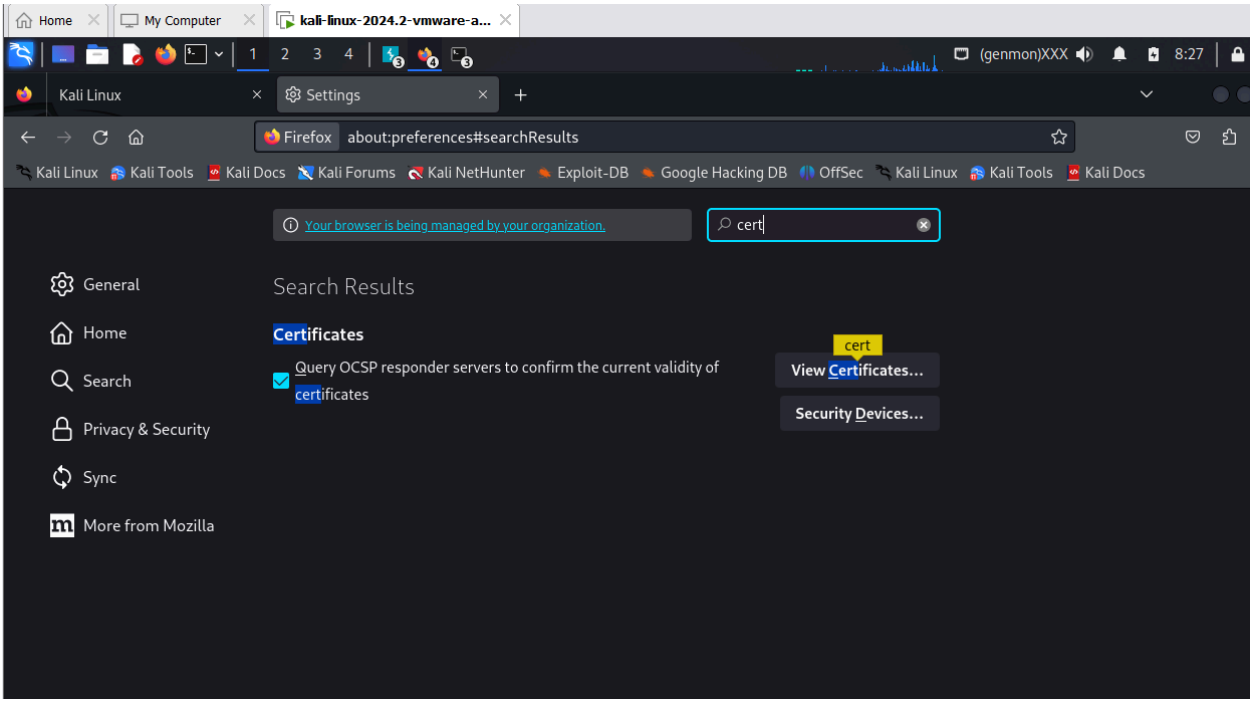
Burp suite is a popular web application security testing tool used by penetration testers and security professionals, it provides a range of features for web application security assessment like proxy, scanner, intruder, repeater, decoder, comparer. In this lab we will be focusing on the local proxy feature, which allows us to intercept the requests being sent from our machine to a server. This provides us with the ability to alter the requests being sent to the server.

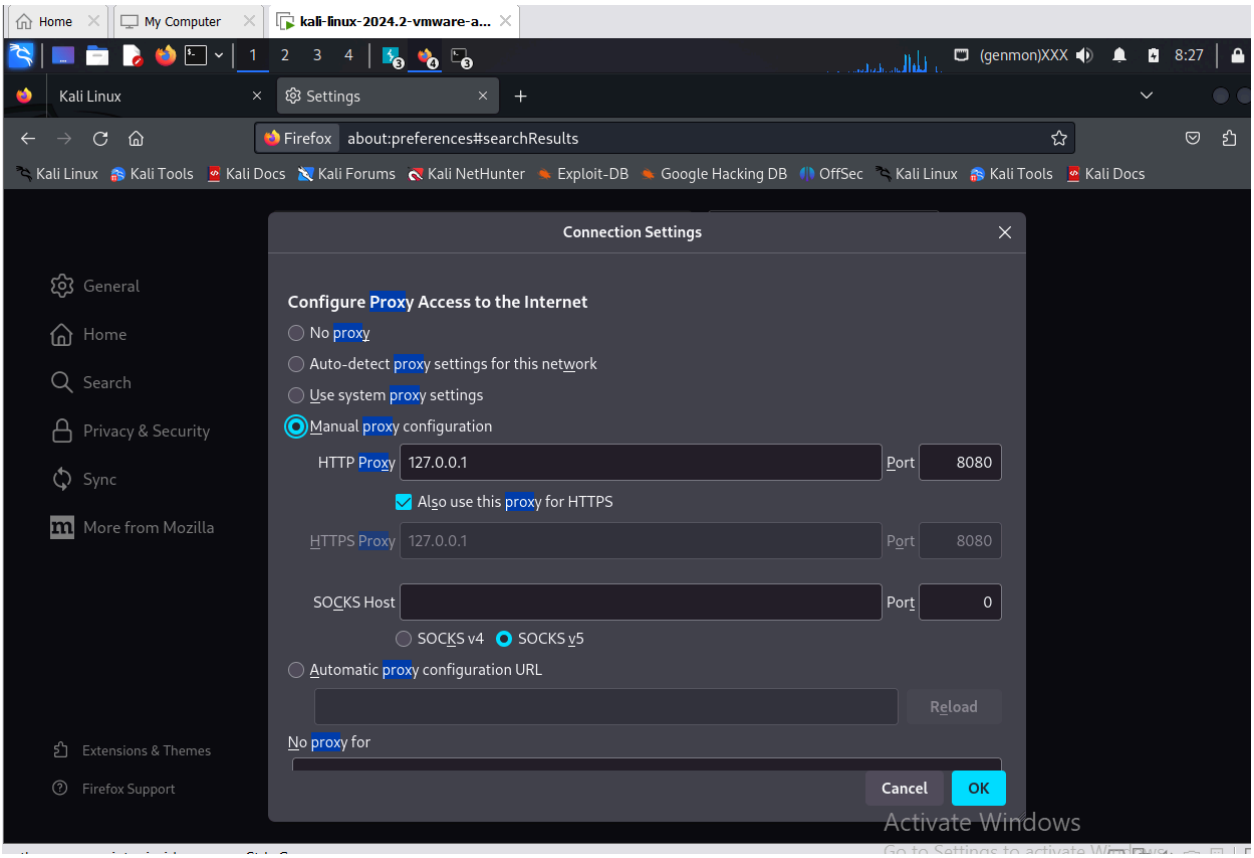

(kali㉿kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.u
Burp Suite Community Edition v2024.3.1.4
Select the configuration that you would like to load for this project.
Burp Suite
Community Edition
Use Burp defaults
Use settings saved with project
Load from configuration file
File
File:
Choose file...
Default to the above in future
Disable extensions
Cancel
Back
Start Burp

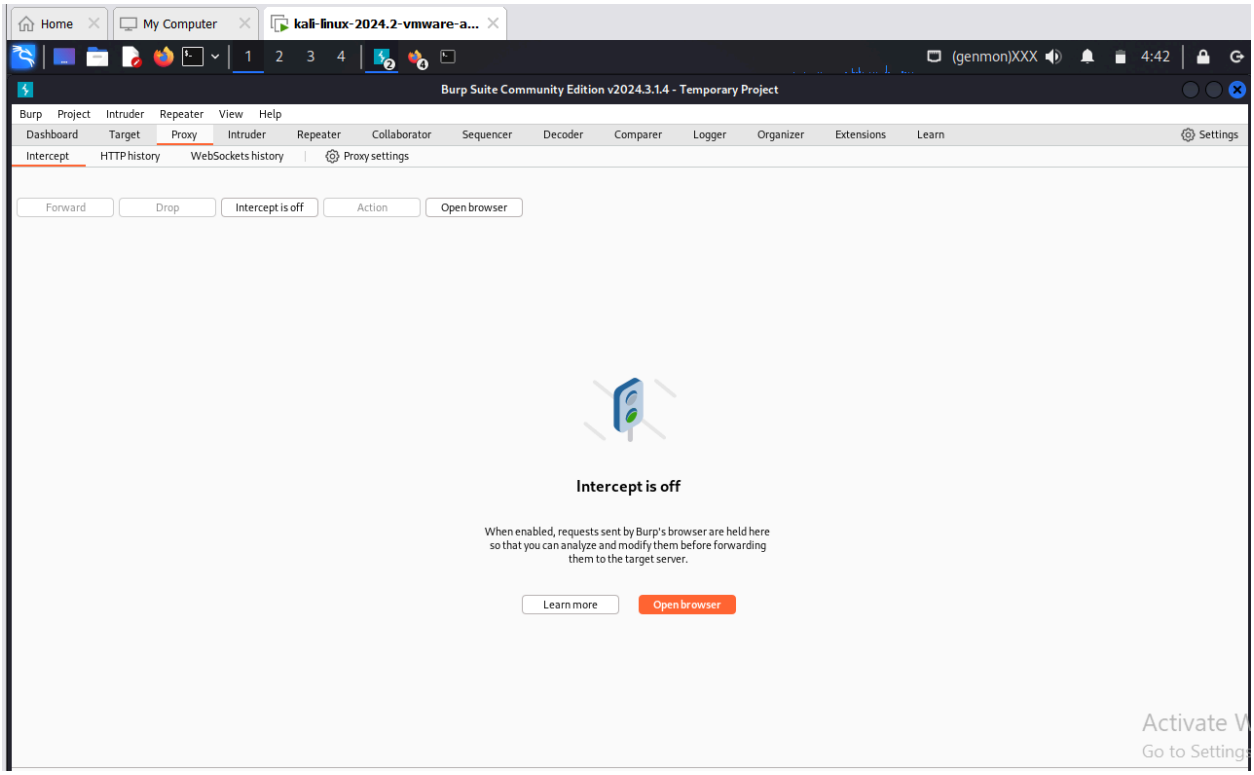

Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Settings
Tools
Proxy
Manage global settings
All
User
Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Proxy listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
TLS Protocols
127.0.0.1:8080
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 oth
installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Request interception rules
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Master interception is turned off
Add
Edit
Remove
Up
Down
Enabled
Operator
Match type
Relationship
Condition
File extension
Does not match
(^gif$|^jpg$|^png$|^css$|^js$|^ico$|^sv...
Or
Request
Contains parameters
Or
HTTP method
Does not match
(get|post)
And
URL
Is in target scope
Automatically fix missing or superfluous new lines at end of request
Event log (1)
All issues
Memory: 121.6MB
Activate Windows

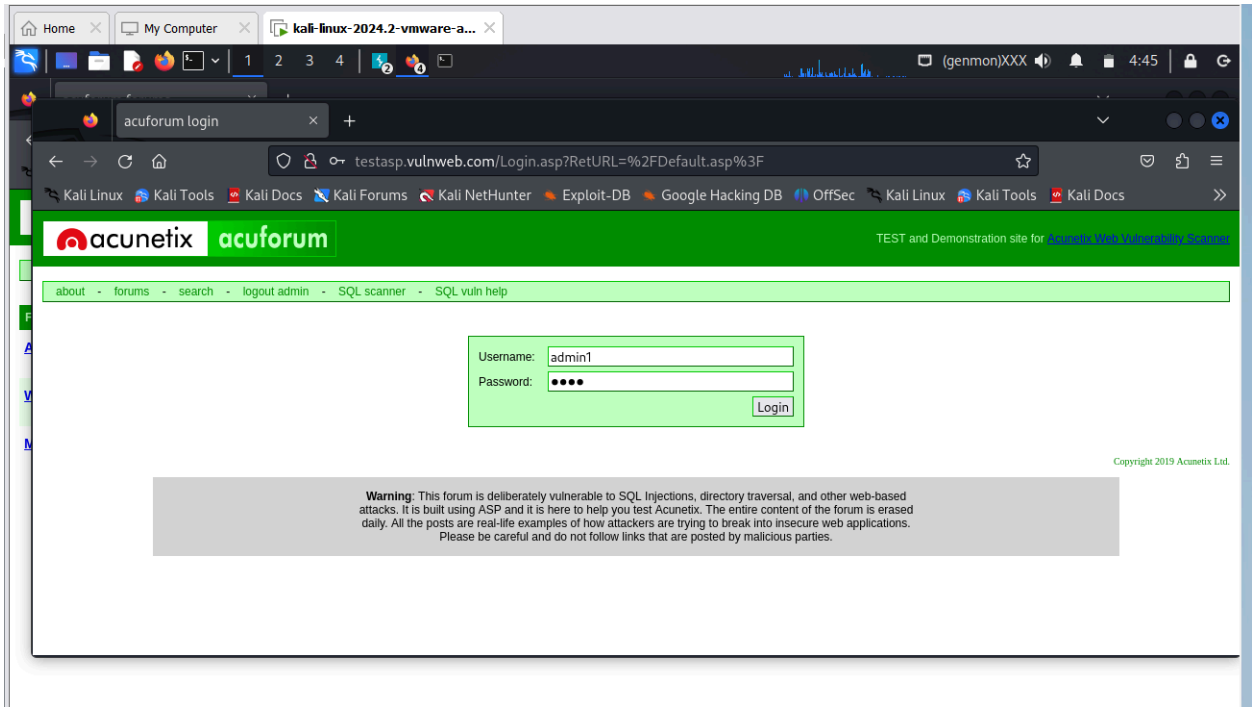

Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Settings
Search
All
User
Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
Sessions
Network
User interface
Suite
Extensions
Configuration library
Tools › Proxy
Manage global settings
Proxy listeners
Burp Proxy uses listeners 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.
TLS Protocols
Default
CA Certificate
You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burpsuite/cert in your browser.
Export
Certificate in DER format
Private key in DER format
Certificate and private key in PKCS#12 keystore
Import
Certificate and private key in DER format
Certificate and private key from PKCS#12 keystore
Cancel
Next
Up
Down
And
URL
Is in target scope
Automatically fix missing or superfluous new lines at end of request
Activate Windows

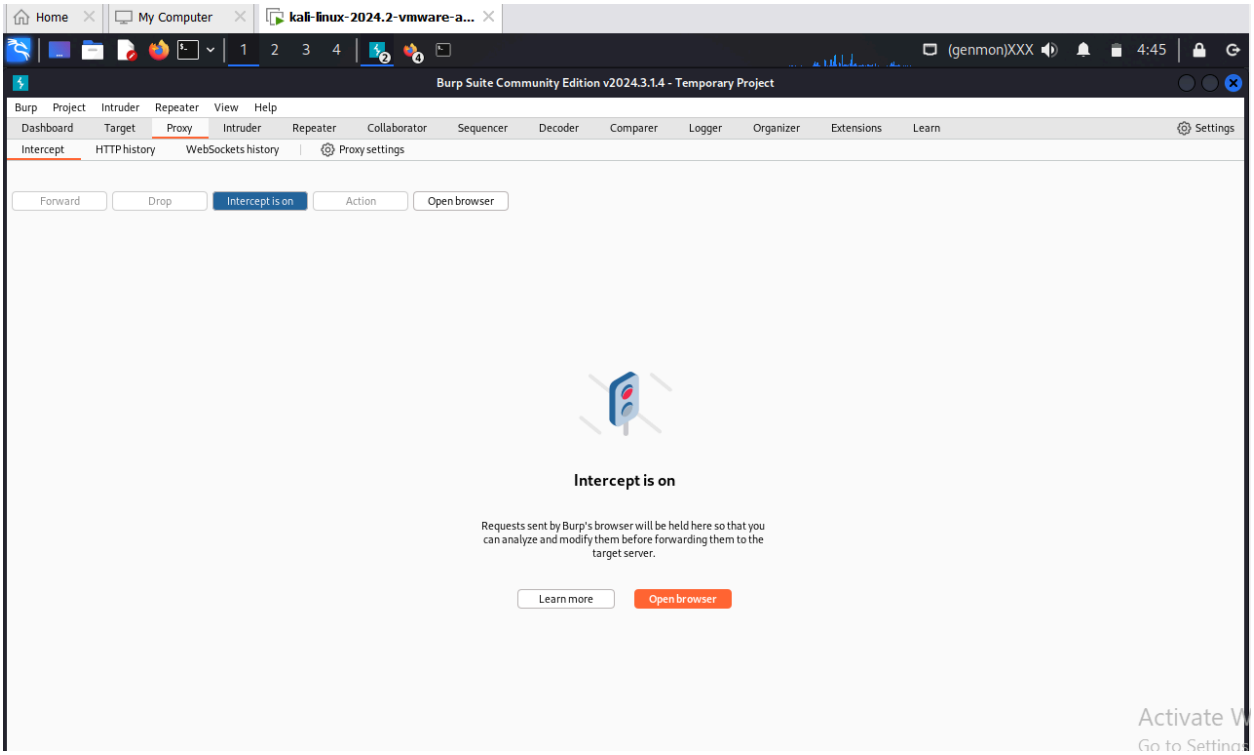

(genmon)XXX
8:16
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
CA Certificate
The certificate was successfully exported.
Back Close

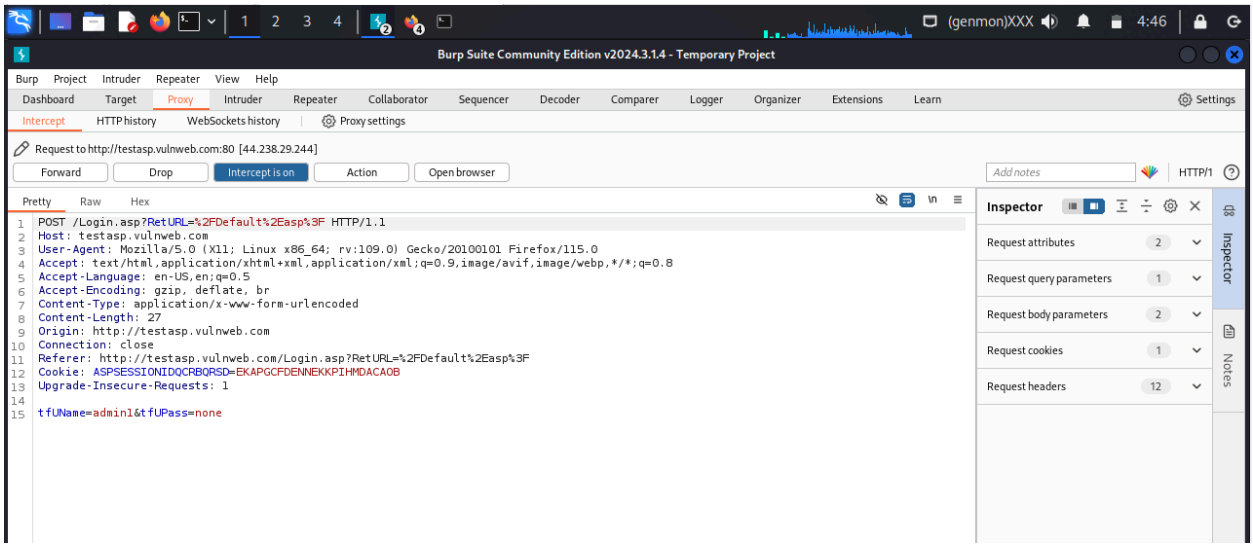

Home
My Computer
kali-linux-2024.2-vmware-a...
(genmon)XXX
8:27
Kali Linux
Settings
Firefox
about:preferences#searchResults
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Kali Linux
Kali Tools
Kali Docs
Your browser is being managed by your organization.
cert
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Search Results
Certificates
Query OCSP responder servers to confirm the current validity of certificates
cert
View Certificates...
Security Devices...

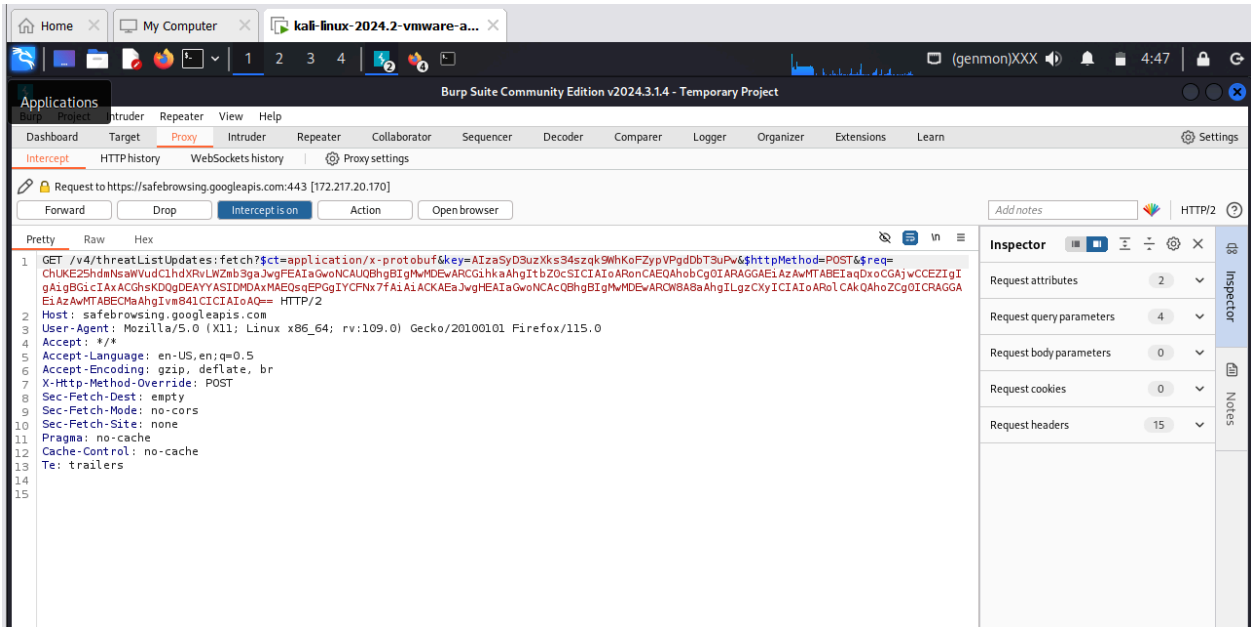

Home
My Computer
kali-linux-2024.2-vmware-a...
(genmon)XXX
8:27
Kali Linux
Settings
Firefox
about:preferences#searchResults
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Kali Linux
Kali Tools
Kali Docs
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Extensions & Themes
Firefox Support
Connection Settings
Configure Proxy Access to the Internet
No proxy
Auto-detect proxy settings for this network
Use system proxy settings
Manual proxy configuration
HTTP Proxy
127.0.0.1
Port
8080
Also use this proxy for HTTPS
HTTPS Proxy
127.0.0.1
Port
8080
SOCKS Host
Port
0
SOCKS v4
SOCKS v5
Automatic proxy configuration URL
Reload
No proxy for
Cancel
OK
Activate Windows


Home
My Computer
kali-linux-2024.2-vmware-a...
(genmon)XXX
4:42
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Intercept is off
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
Activate W
Go to Settings


Home
My Computer
kali-linux-2024.2-vmware-a...
(genmon)XXX
4:45
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout admin - SQL scanner - SQL vuln help
Username: admin1
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.


Home
My Computer
kali-linux-2024.2-vmware-a...
(genmon)XXX
4:45
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Intercept is on
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser
Activate W
Go to Setting


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://testasp.vulnweb.com:80 [44.238.29.244]
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
1 POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
2 Host: testasp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 27
9 Origin: http://testasp.vulnweb.com
10 Connection: close
11 Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
12 Cookie: ASPSESSIONIDQCRBQRSD=EKAPGCFDENNEKKPIHMDACAOB
13 Upgrade-Insecure-Requests: 1
14
15 tfUName=admin1&tfUPass=none
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 2
Request cookies 1
Request headers 12
Inspector
Notes



RESULT AND PROCEDURE FOR USING BURP SUITE TO INTERCEPT
CLIENT-SIDE REQUEST.