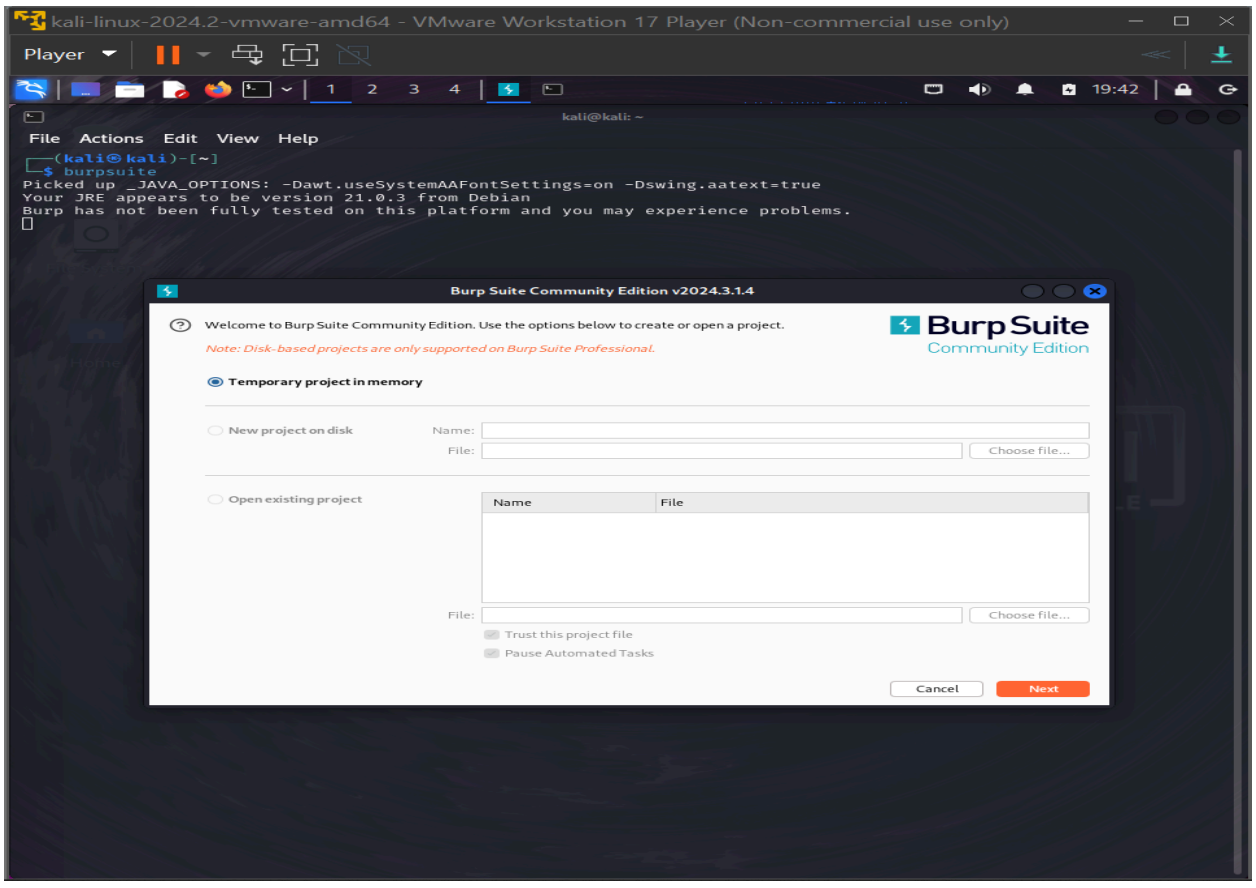
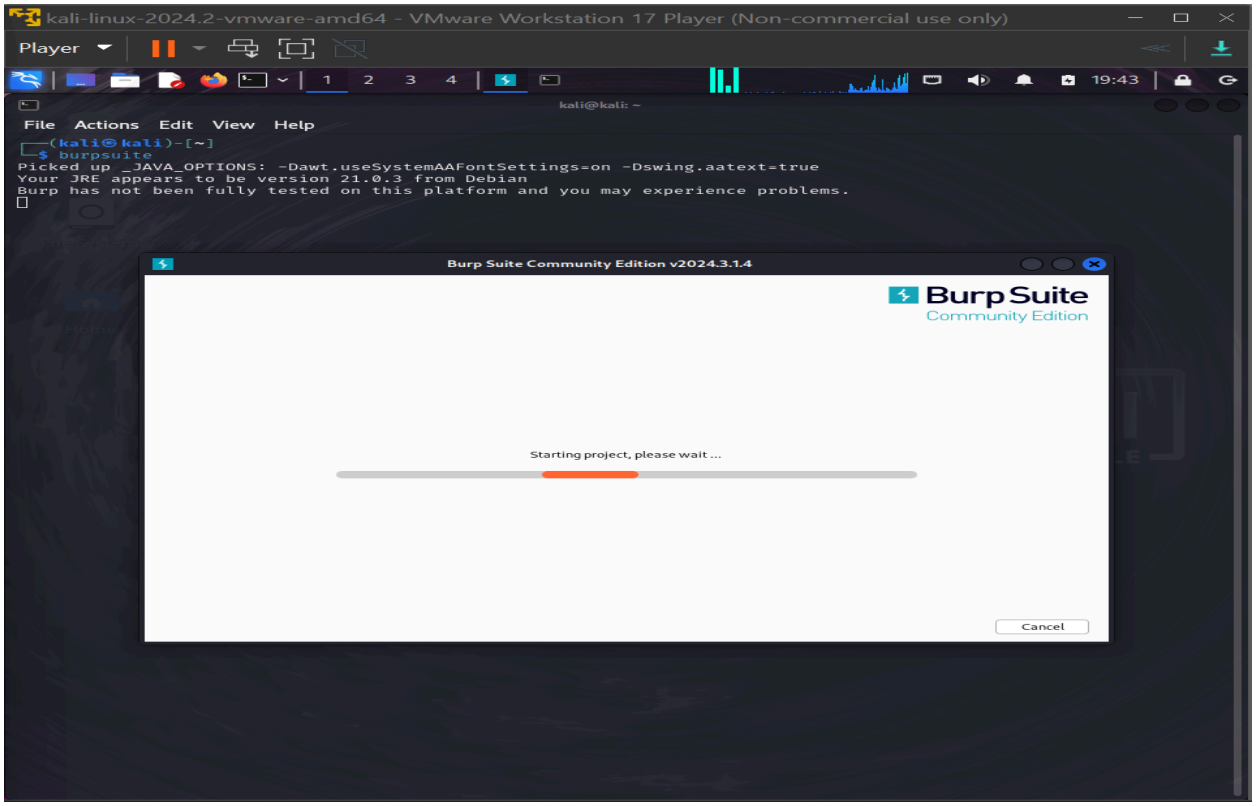
USING BURP SUITE TO INTERCEPT CLIENT SIDE REQUEST.

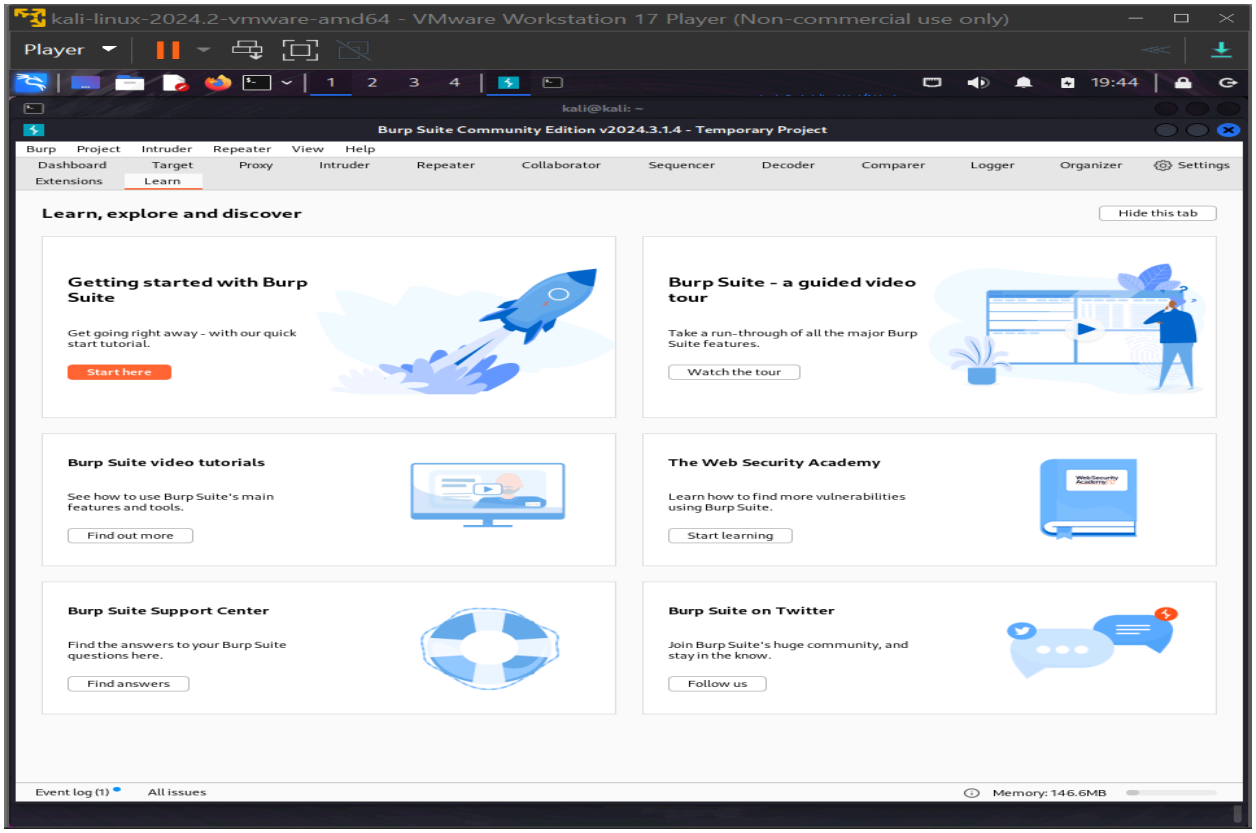
TOOLS : Kali Linux [BURP SUITE]
Project-Site : http://testasp.vulnweb.com

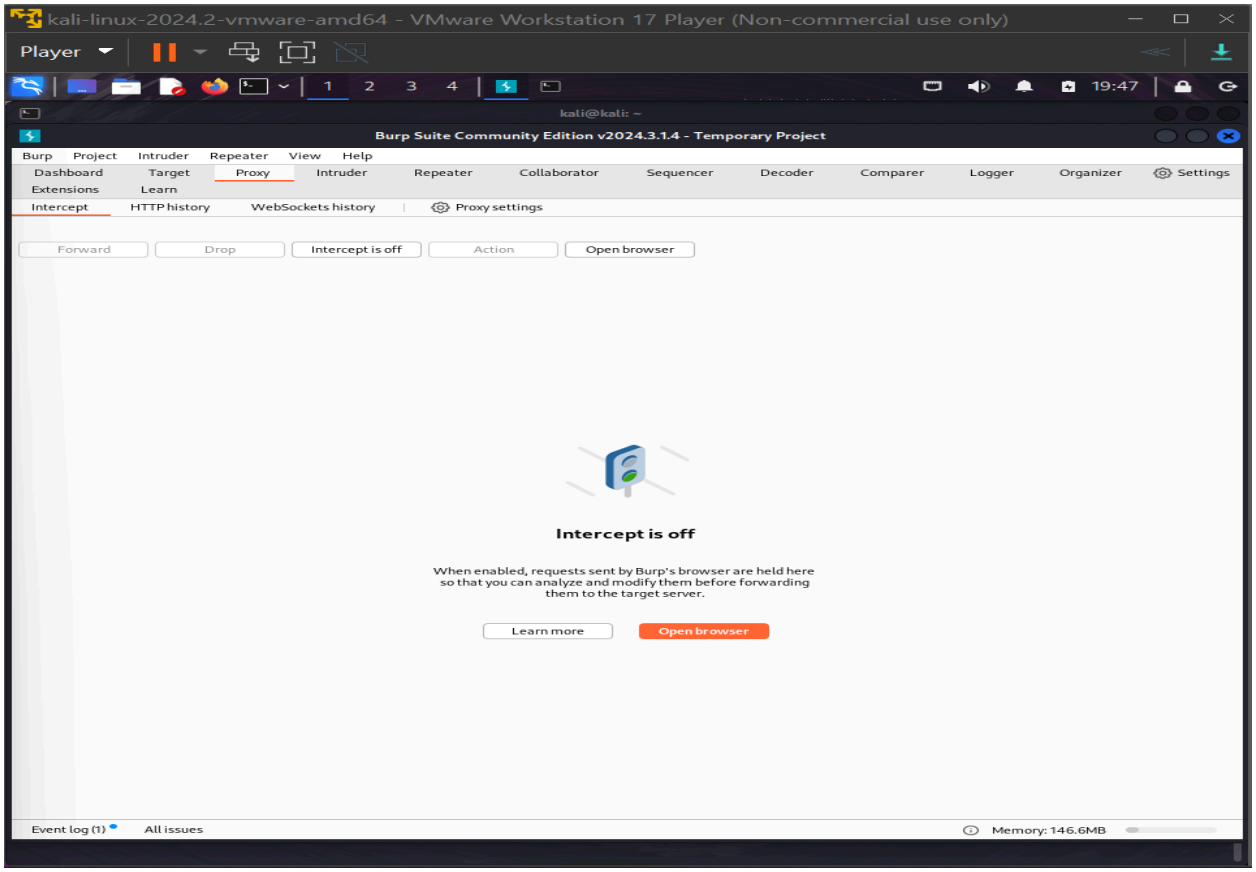
Burp suite is a popular web application security testing tool used by penetration testers and security professionals, it provides a range of features for web application security assessment like proxy, scanner, intruder, repeater, decoder, comparer. In this lab we will be focusing on the local proxy 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.

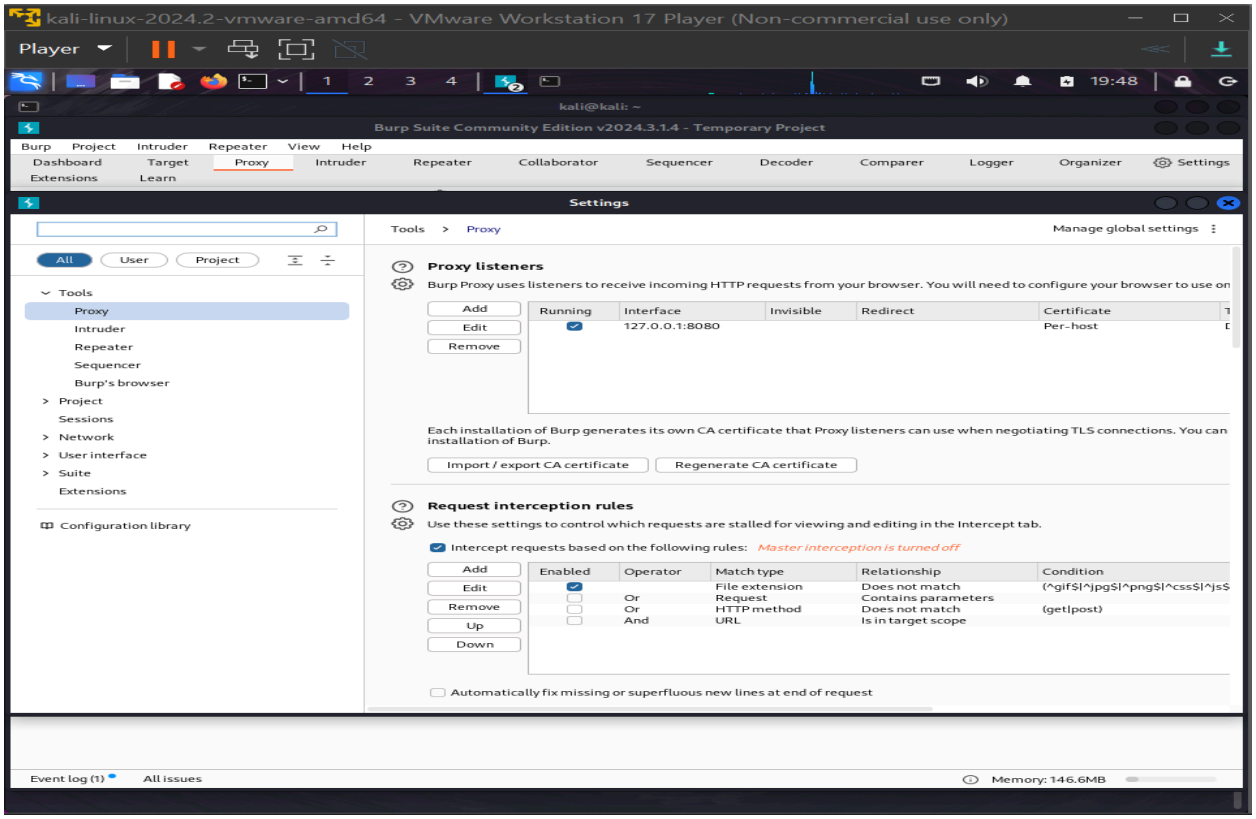
Input from kali : BURPSUITE

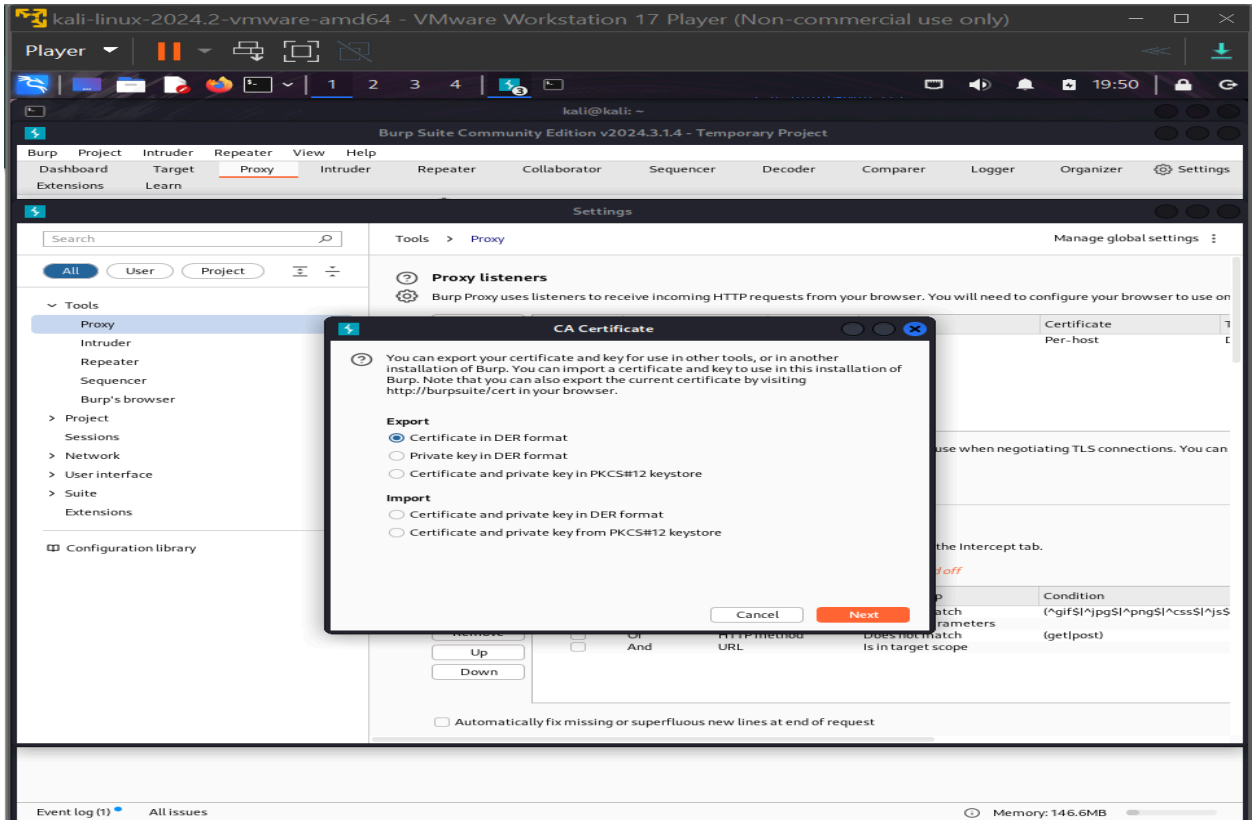


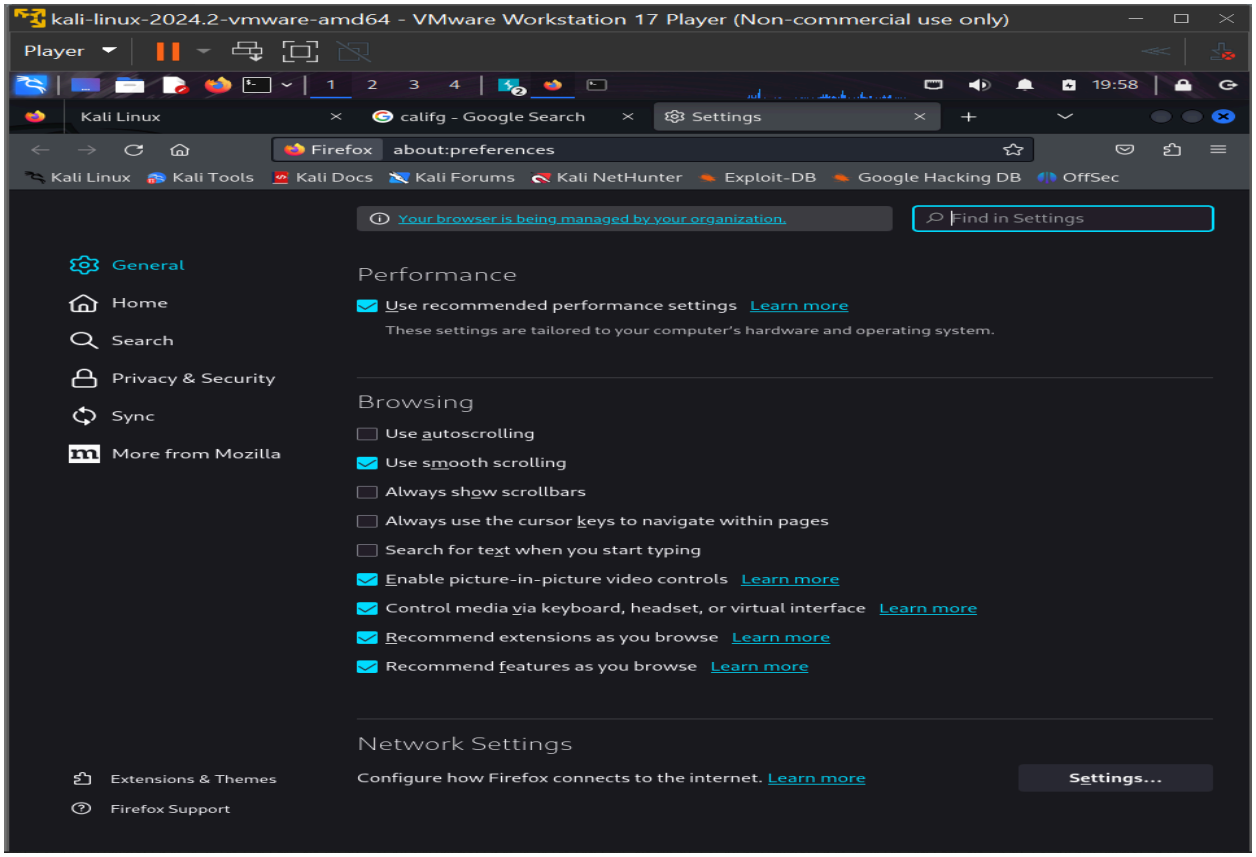

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:43
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 21.0.3 from Debian
Burp has not been fully tested on this platform and you may experience problems.
Burp Suite Community Edition v2024.3.1.4
Burp Suite
Community Edition
Starting project, please wait ...
Cancel

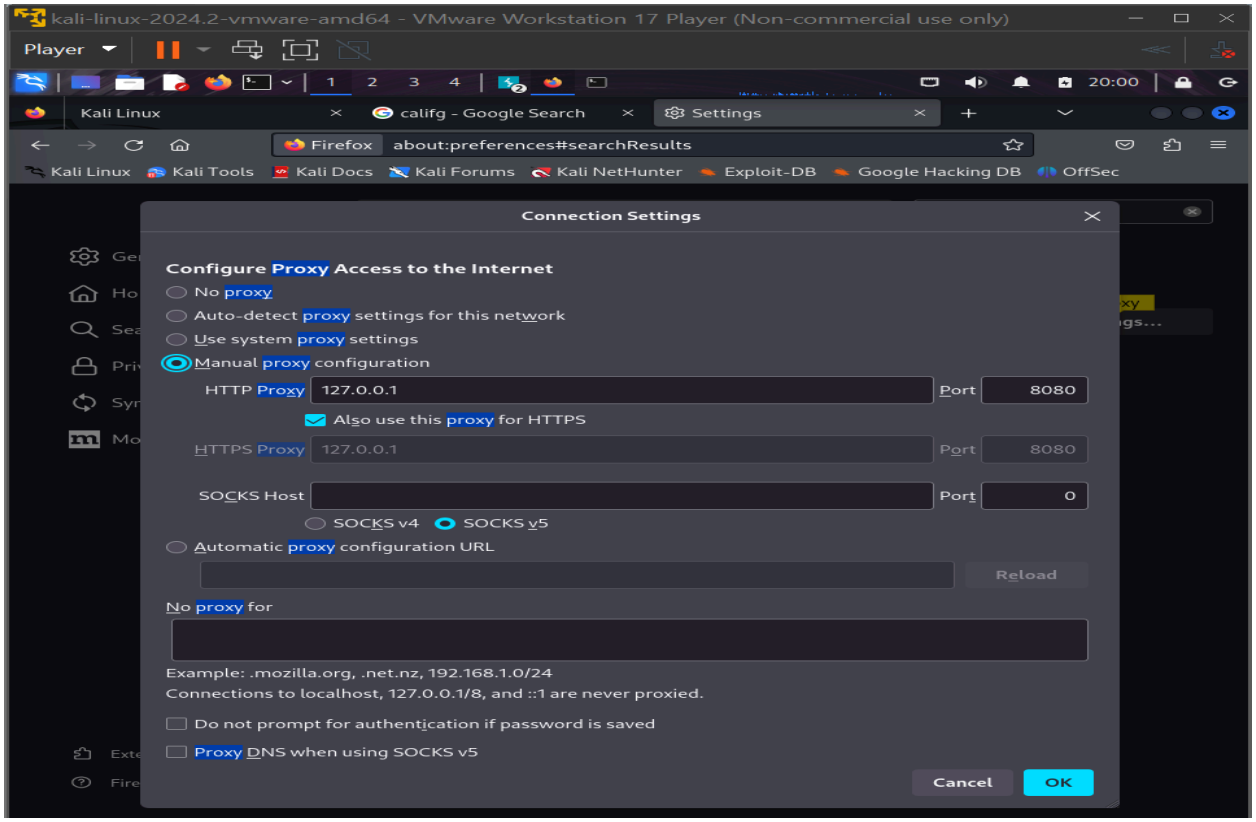

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:44
kali@kali: ~
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Learn, explore and discover
Hide this tab
Getting started with Burp Suite
Get going right away - with our quick start tutorial.
Start here
Burp Suite - a guided video tour
Take a run-through of all the major Burp Suite features.
Watch the tour
Burp Suite video tutorials
See how to use Burp Suite's main features and tools.
Find out more
The Web Security Academy
Learn how to find more vulnerabilities using Burp Suite.
Start learning
Burp Suite Support Center
Find the answers to your Burp Suite questions here.
Find answers
Burp Suite on Twitter
Join Burp Suite's huge community, and stay in the know.
Follow us
Event log (1)
All issues
Memory: 146.6MB

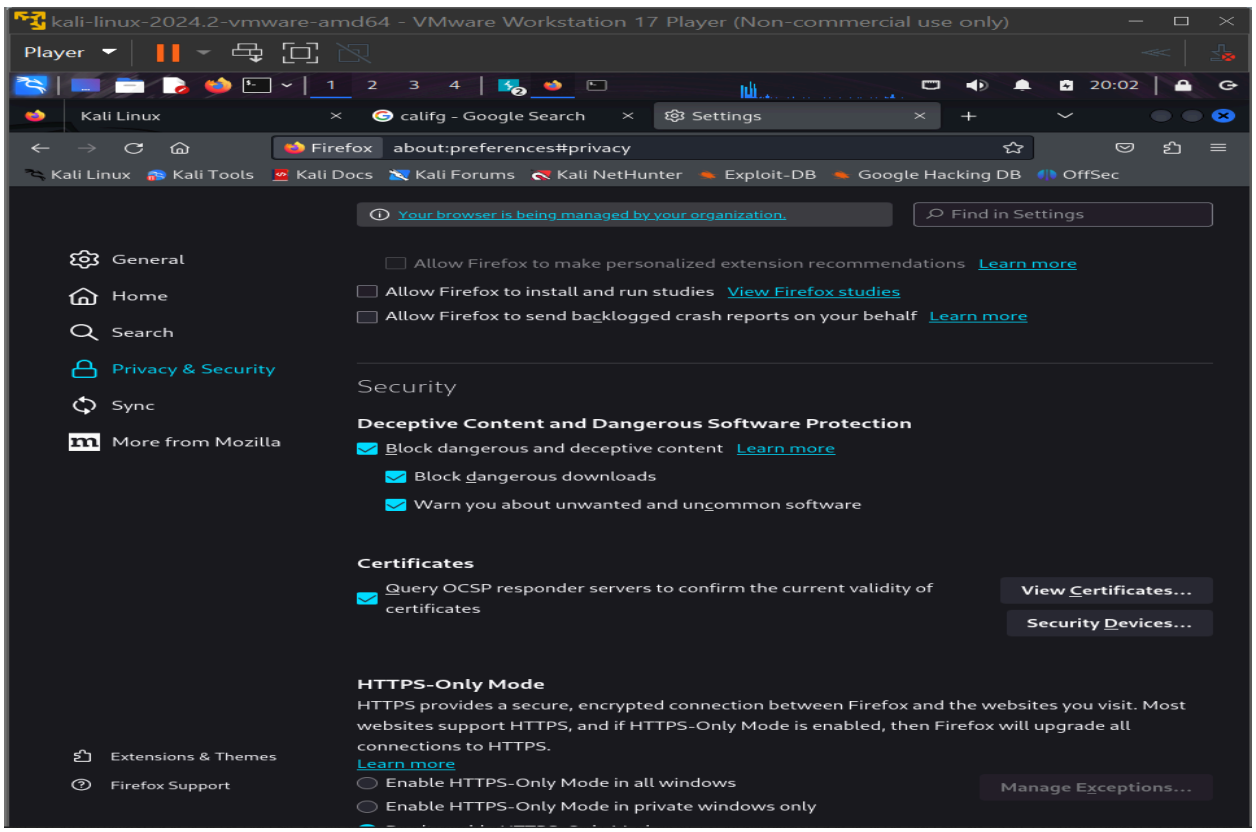

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:47
kali@kali: ~
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
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
Event log (1) All issues
Memory: 146.6MB

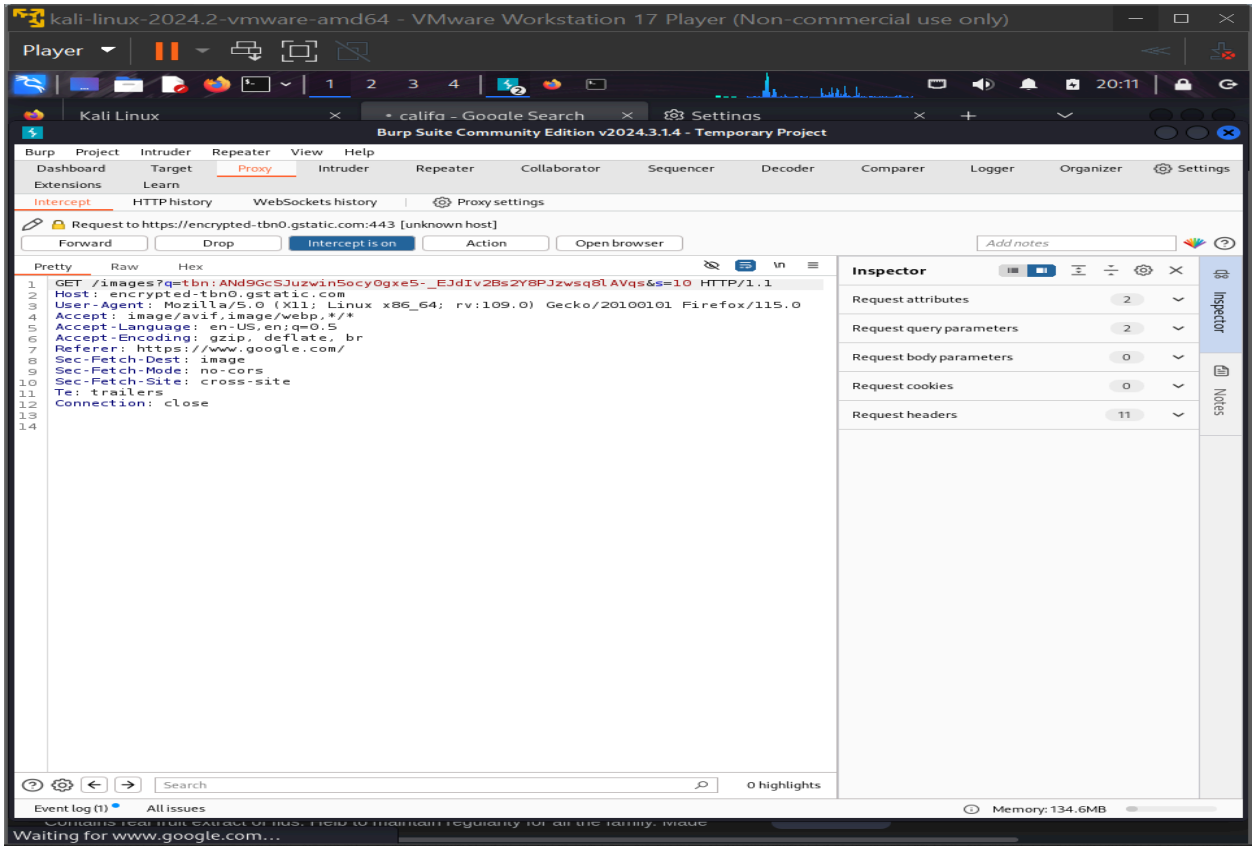

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:48
kali@kali: ~
Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Settings
Tools > Proxy
Manage global settings
All User Project
Tools
Proxy
Intruder
Repeater
Sequencer
Burp's browser
Project
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 on
Add
Edit
Remove
Running Interface Invisible Redirect Certificate
127.0.0.1:8080 Per-host
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can
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$
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: 146.6MB


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:50
kali@kali: ~
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 Settings
Extensions Learn
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 on
Certificate
Per-host
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
use when negotiating TLS connections. You can
the Intercept tab.
Condition
(^gif$|^jpg$|^png$|^css$|^js$
(get|post)
Is in target scope
Up
Down
Automatically fix missing or superfluous new lines at end of request
Event log (1)
All issues
Memory: 146.6MB

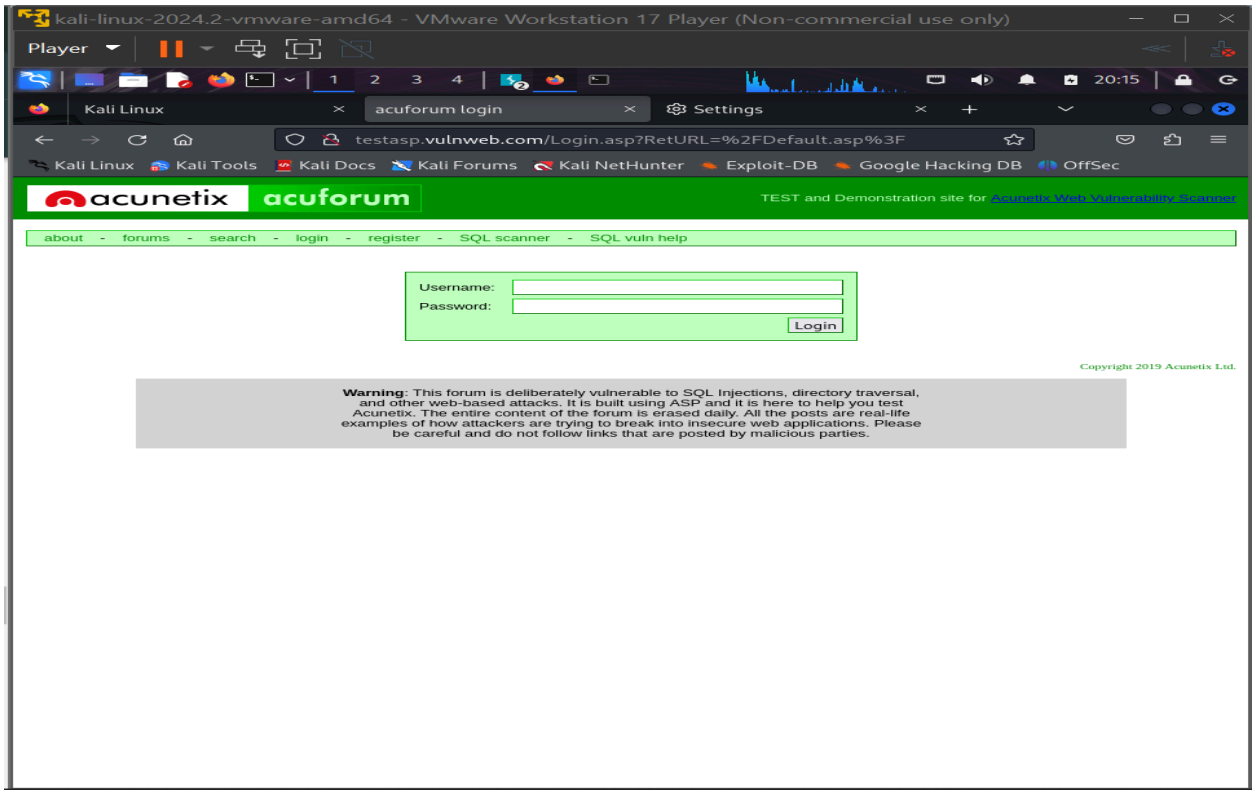

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:58
Kali Linux
califg - Google Search
Settings
Firefox about:preferences
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Performance
Use recommended performance settings Learn more
These settings are tailored to your computer's hardware and operating system.
Browsing
Use autoscrolling
Use smooth scrolling
Always show scrollbars
Always use the cursor keys to navigate within pages
Search for text when you start typing
Enable picture-in-picture video controls Learn more
Control media via keyboard, headset, or virtual interface Learn more
Recommend extensions as you browse Learn more
Recommend features as you browse Learn more
Network Settings
Configure how Firefox connects to the internet. Learn more
Settings...
Extensions & Themes
Firefox Support

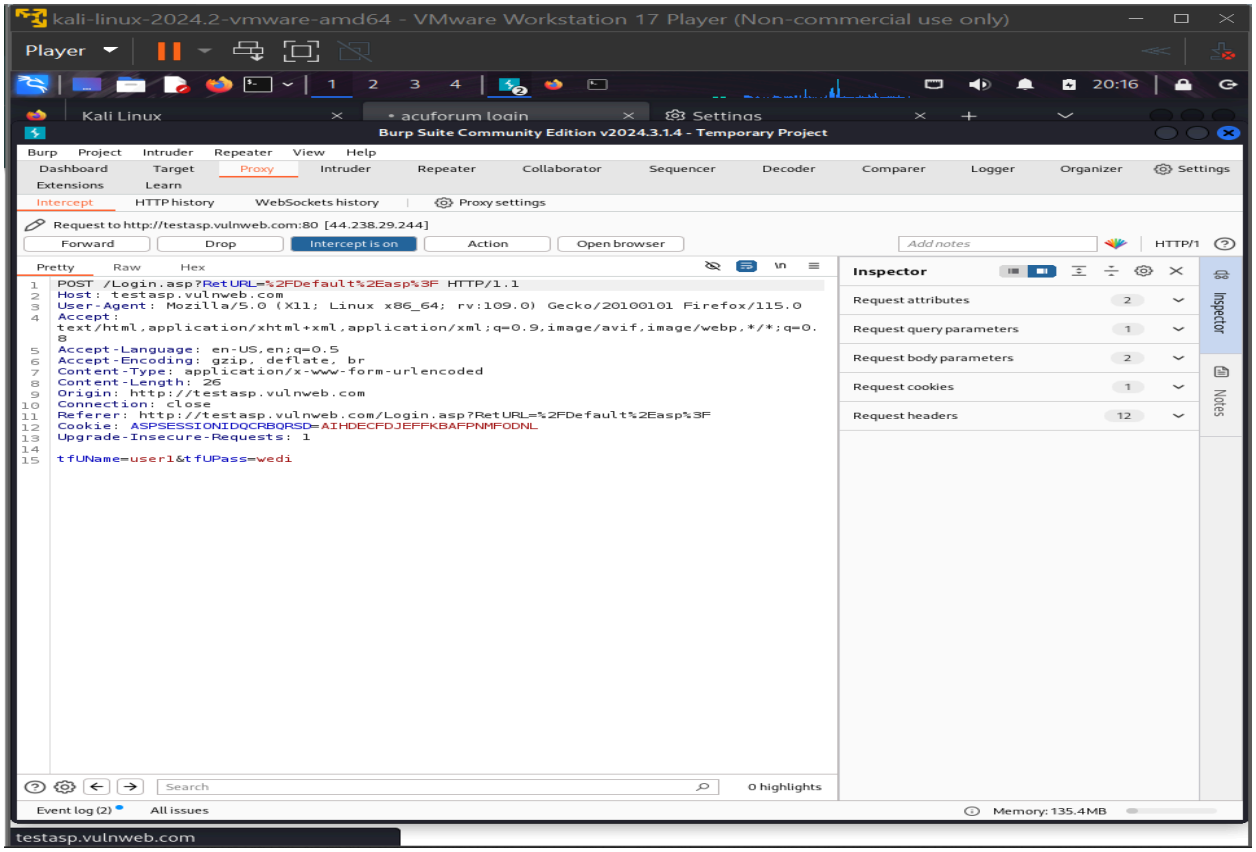

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
califg - Google Search
Settings
Firefox
about:preferences#searchResults
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Connection Settings
Configure 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
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.
Do not prompt for authentication if password is saved
Proxy DNS when using SOCKS v5
Cancel
OK

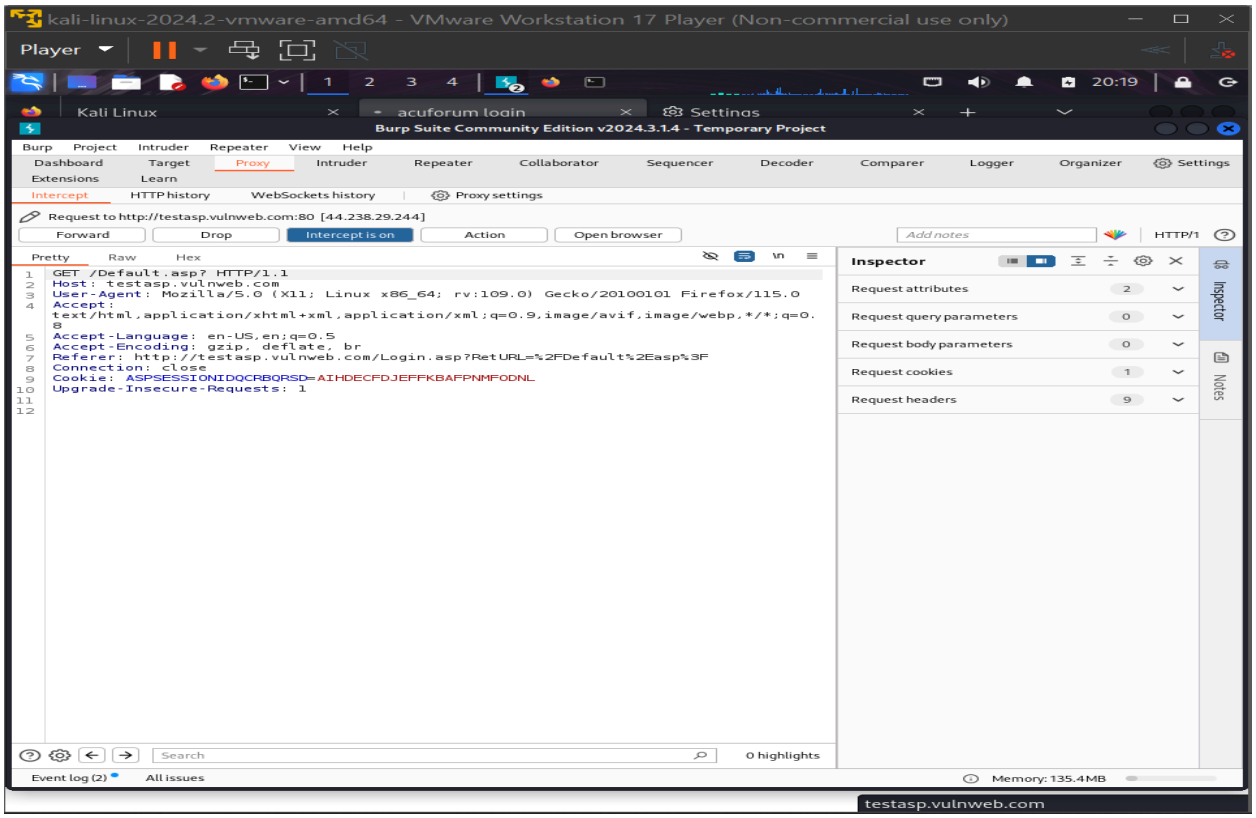

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
califg - Google Search
Settings
Firefox
about:preferences#privacy
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Your browser is being managed by your organization.
Find in Settings
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Allow Firefox to make personalized extension recommendations
Learn more
Allow Firefox to install and run studies
View Firefox studies
Allow Firefox to send backlogged crash reports on your behalf
Learn more
Security
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content
Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.
Learn more
Enable HTTPS-Only Mode in all windows
Enable HTTPS-Only Mode in private windows only
Manage Exceptions...
Extensions & Themes
Firefox Support

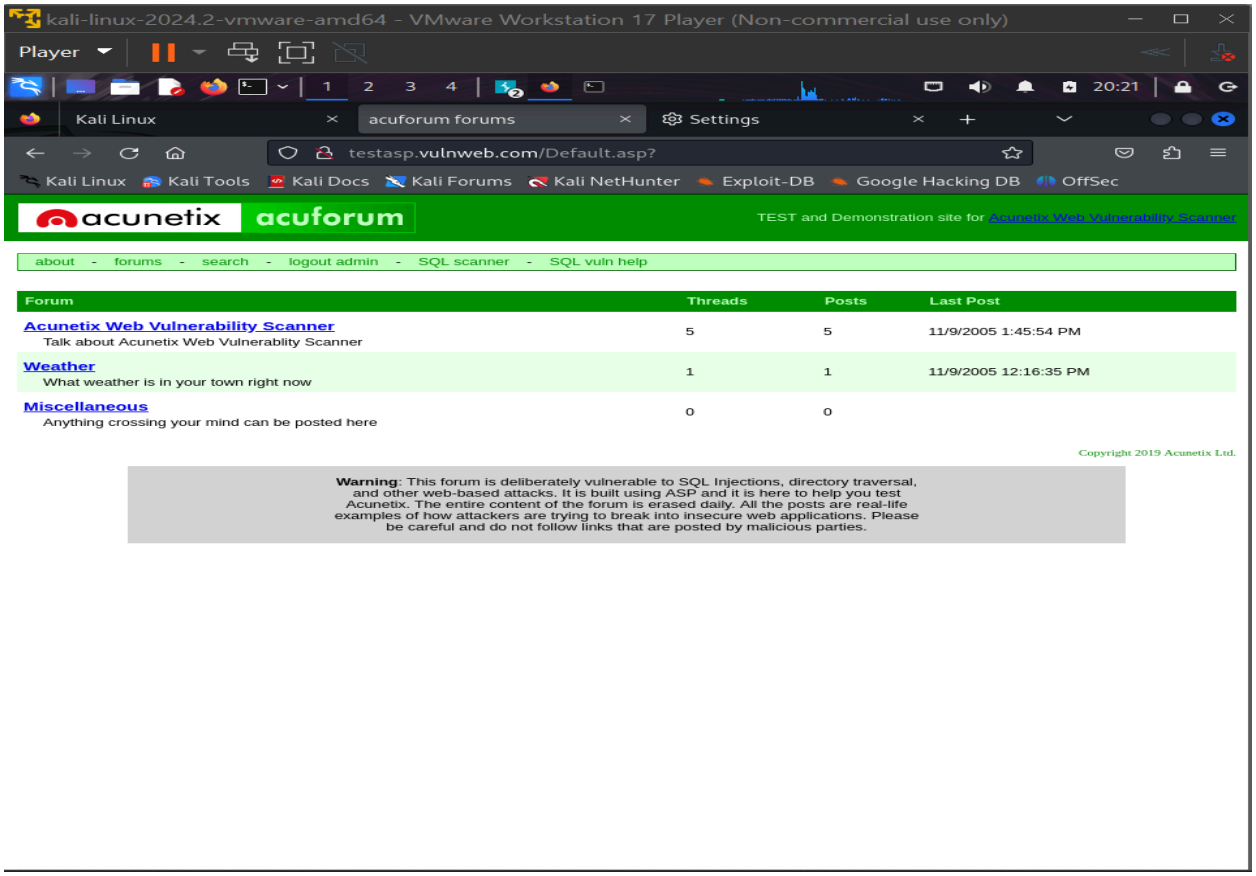


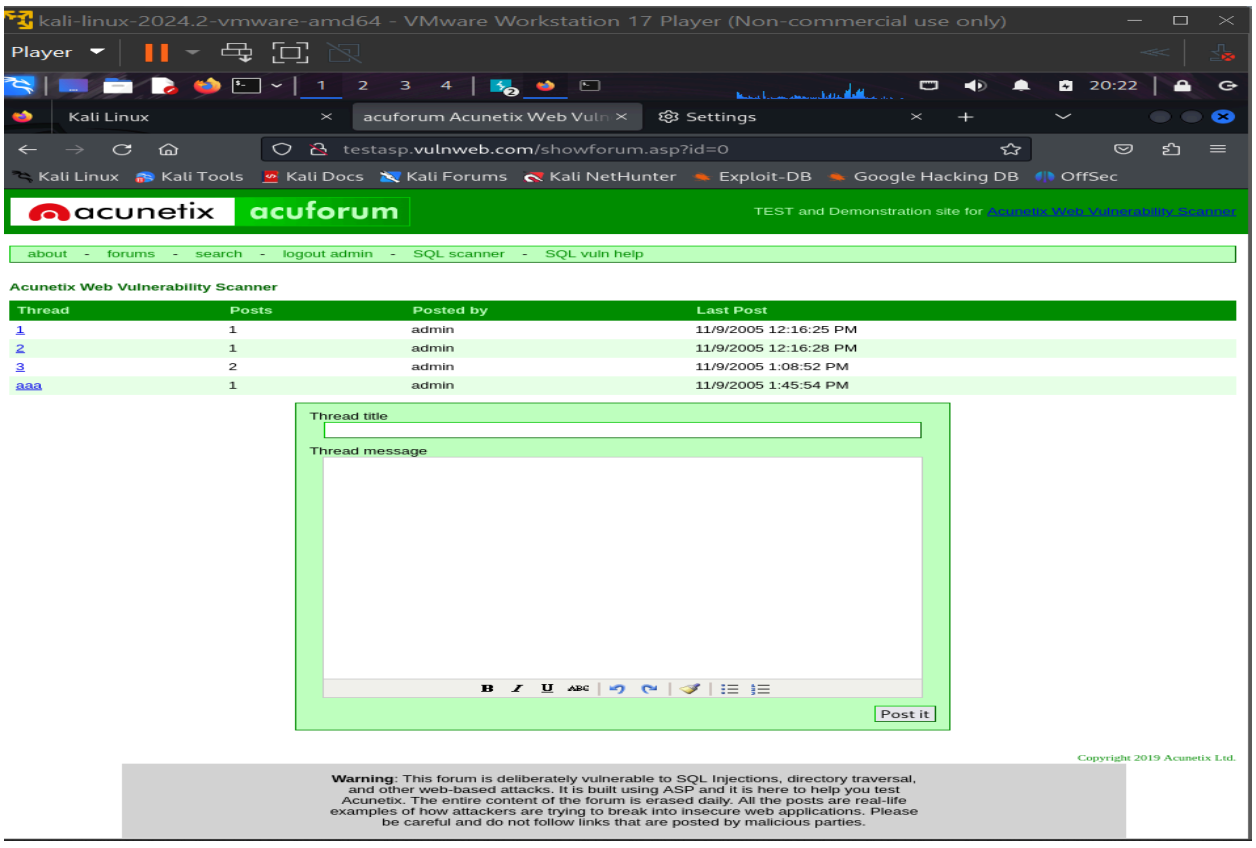
INPUT FROM : testasp.vulnweb.com




kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
acuforum login
Settings
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 Settings
Extensions Learn
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
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://testasp.vulnweb.com
Connection: close
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDQCRBQRSD=AIHDECFDJEFFKBAFPNMFODNL
Upgrade-Insecure-Requests: 1
tfUName=user1&tfUPass=wedi
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 2
Request cookies 1
Request headers 12
Search
0 highlights
Event log (2)
All issues
Memory: 135.4MB
testasp.vulnweb.com


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Linux
acuforum login
Settings
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 Settings
Extensions Learn
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
GET /Default.asp? HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Connection: close
Cookie: ASPSESSIONIDQCRBQRSD=AIHDECFDJEFFKBAFPNMFODNL
Upgrade-Insecure-Requests: 1
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 9
Search
0 highlights
Event log (2)
All issues
Memory: 135.4MB
testasp.vulnweb.com


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:21
Kali Linux
acuforum forums
Settings
testasp.vulnweb.com/Default.asp?
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
Forum Threads Posts Last Post
Acunetix Web Vulnerability Scanner
Talk about Acunetix Web Vulnerablity Scanner
5 5 11/9/2005 1:45:54 PM
Weather
What weather is in your town right now
1 1 11/9/2005 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.


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
20:22
Kali Linux
acuforum Acunetix Web Vuln
Settings
testasp.vulnweb.com/showforum.asp?id=0
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
Acunetix Web Vulnerability Scanner
Thread Posts Posted by Last Post
1 1 admin 11/9/2005 12:16:25 PM
2 1 admin 11/9/2005 12:16:28 PM
3 2 admin 11/9/2005 1:08:52 PM
aaa 1 admin 11/9/2005 1:45:54 PM
Thread title
Thread message
Post it
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.

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

Here we used burp suite to intercept client-side requests. We first navigated to our machine and we ran the burp suite command as kali user as seen in the first picture. We then updated the necessary drivers and accepted. Now we want to configure burp, when burp launched we choose TEMPORARY PROJECT then next, then we set burp to default then we started BURP.

Once the burp suite opens, we can see a lot of tabs and other information as seen in image3. We would be working on the proxy tab for this project, so we navigate to the proxy tab. We can see that the intercept is off but for burp to intercept traffic it has to be on. We want to use burp suite with firefox, now we navigate to the proxy and then the options tab. Then we click on IMPORT/EXPORT CA CERTIFICATE. This will allow our browser to trust the burp suite. Then we browsed to a location on our kali vm where we want the file saved. We also saved the file with a .der extension so that the file will be able to import. When we are done we would then open our built-in firefox in kali and then we navigate to the options, then we searched for proxy and clicked on the settings button under network settings, then we clicked on manual proxy configuration and entered the following details as seen in image8. Once we are done we then navigate to the privacy and security tab and then to the certificates section.this is where we want to import the certificates from burp that we downloaded earlier. We then click on view certificates and click on import, then we navigate to the .der file we downloaded and we then click on OK. Now firefox has been configured to work with burp. We then test it out by turning on intercept mode on burp suite and searching for something on firefox. In image 10 we can see that the request was intercepted and it was captured in burp suite for us to either manipulate or examine.

Now we want to use burp suite to intercept browser network traffic. We do this by navigating to our browser and to the site, we enter any username and password and we click login. **This is done when the**

interception is turned on. We can see that the page remains in loading state. This is because burp has intercepted the request we sent to the server, and it is holding it for us to inspect or manipulate. We then go back to burp and we would find the intercepted request, along with the username and password data that we have entered. To navigate through the intercepted request we simply click on forward, here we can see that the request has gone through and the website has loaded. We can also try to change the "tfUName to "admin" and "tfUPass to "none" and click login to gain access into the page. Here we just manipulated the page by intercepting the traffic and changing the login and password from burpsuite then we released it to send another request different from the initial one we entered in the site. We can see that we have been granted access to the next page in image 14 AND 15.