INTERCEPTING CLIENT-SIDE REQUESTS

Tool: Burp Suite

Burp Suite is a popular web vulnerability scanner and security testing tool developed by PortSwigger. It is primarily used by security professionals and developers to find and exploit vulnerabilities in web applications.

There are two main versions of Burp Suite:

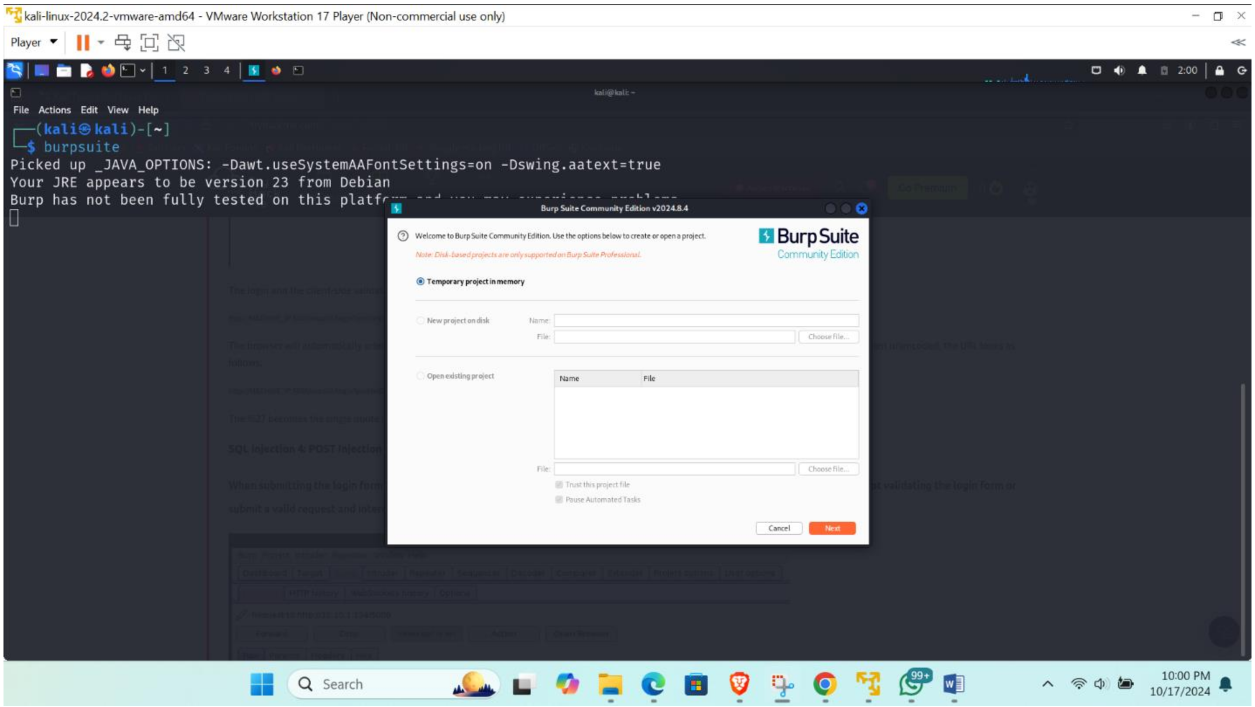
- **Community Edition:** Free but has limited features.

- **Professional Edition:** Paid, with advanced features like automated vulnerability scanning and other premium tools.

Task 1

Run "burpsuite" command in Kali terminal screen as "kali" user. Accept and update as required.

Once Burp is opened, choose "Temporary Project" from the list of options and click next.



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23 from Debian
Burp has not fully tested on this platform and you may experience problems.
```

Burp Suite Community Edition v2024.8.4

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project in memory

○ New project on disk — Name: — File: — Choose file...

○ Open existing project

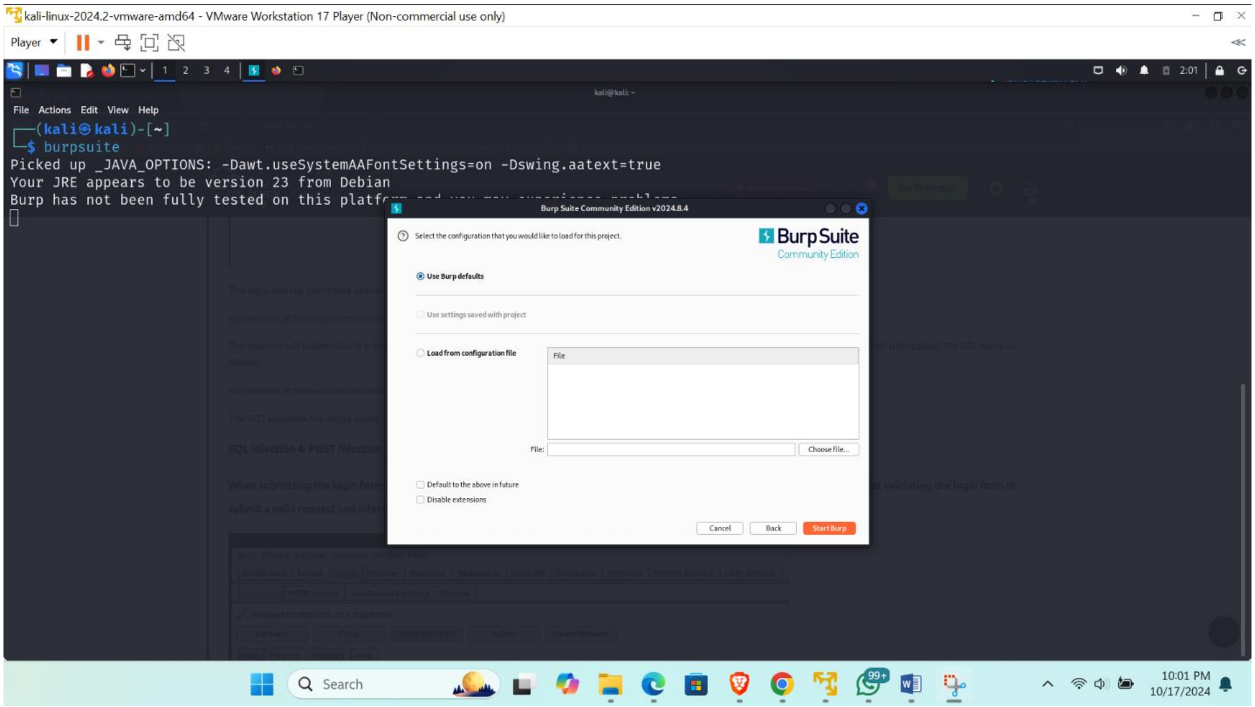
Name	File

File: — Choose file...

☑ Trust this project file

☑ Pause Automated Tasks

In the next screen, choose the option to setup Burp using Burp defaults, and then press “Start Burp”.



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

```
┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23 from Debian
Burp has not been fully tested on this platf
```

Burp Suite Community Edition v2024.8.4

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

○ Load from configuration file

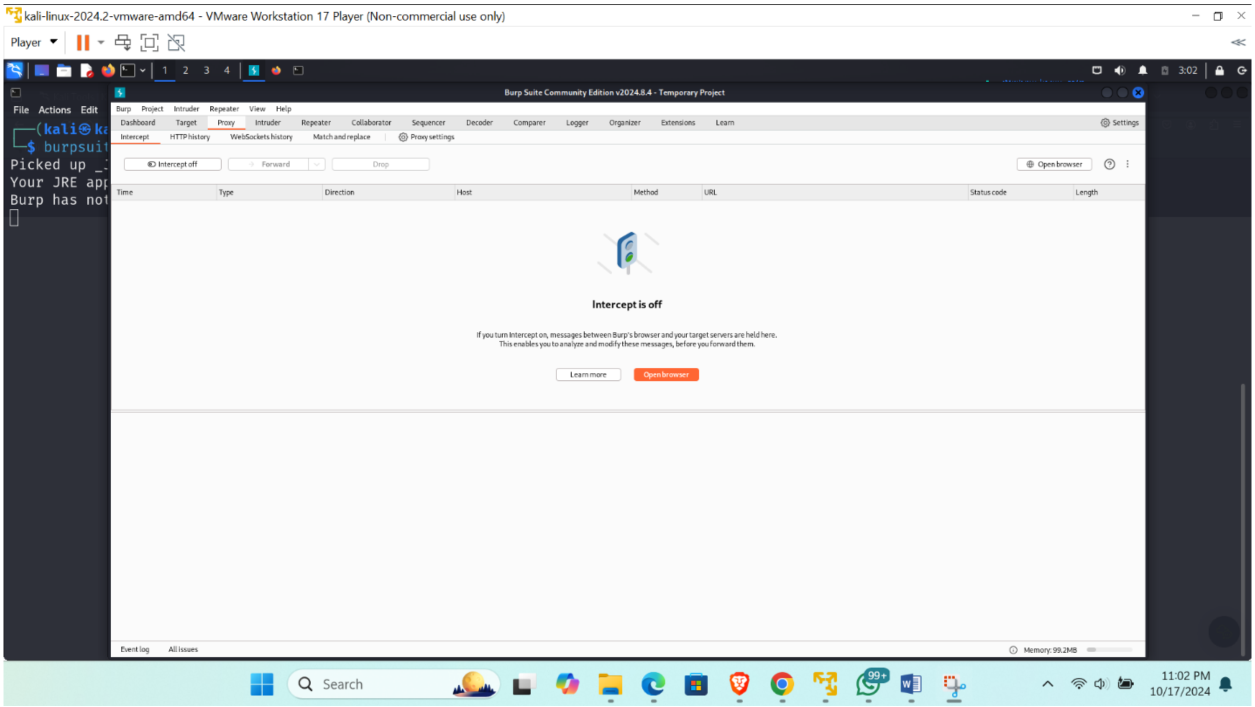
File:

□ Default to the above in future

□ Disable extensions

Task 2

Once Burp Suite is opened, you will see a lot of tabs and other information, but choose **proxy and click on intercept and then off the intercept mode.**



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Burp Suite Community Edition v2024.8.4 - Temporary Project

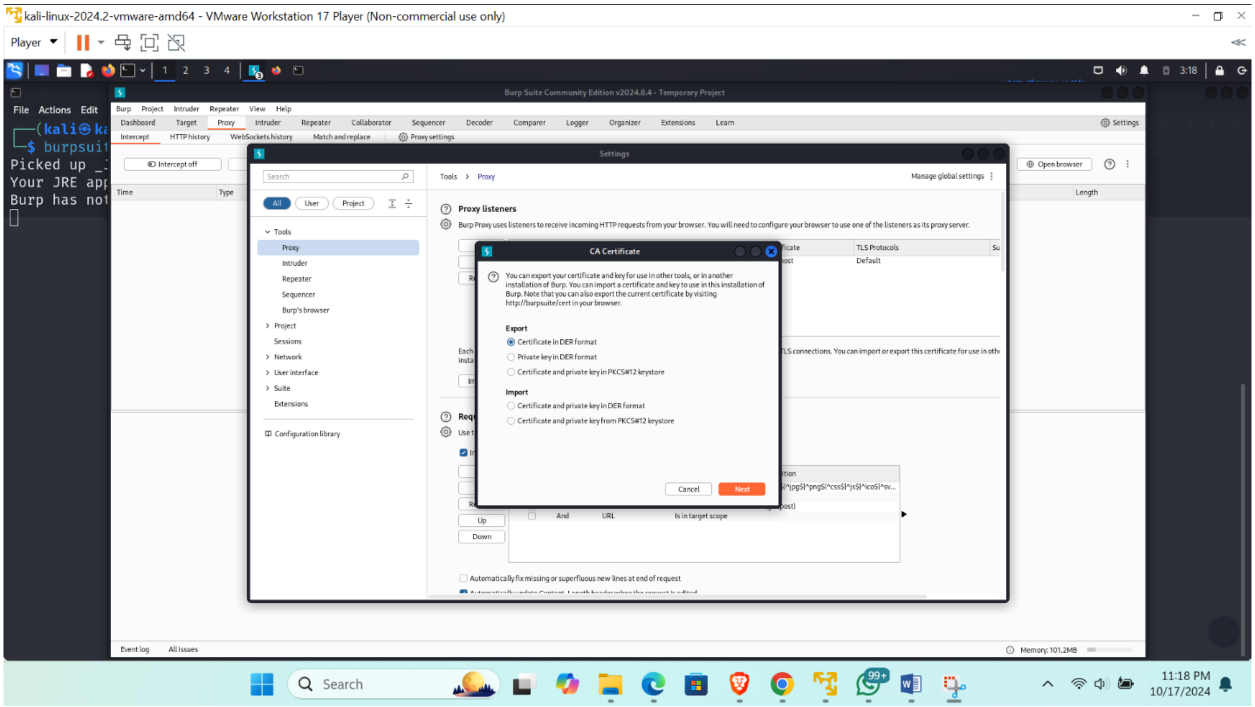
Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Player
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 Match and replace Proxy settings
Intercept off
Forward
Drop
Open browser
Time Type Direction Host Method URL Status code Length
Learn more
Open browser
Event log All issues
Memory: 99.2MB
Search
11:02 PM
10/17/2024

Task 3

We will begin by learning how to use Burp with Firefox. Navigate to the proxy tab, and then to the options tab. Then, click on “Import/export CA Certificate”. This is the certificate which will allow our browser to trust Burp Suite.



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Burp Suite Community Edition v2024.8.4 - Temporary Project

Settings

Tools > Proxy

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.

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

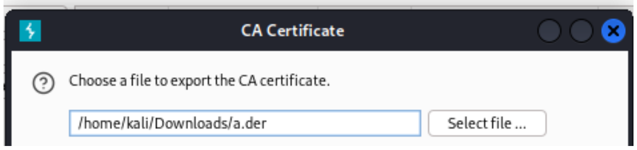
○ Certificate and private key in PKCS#12 keystore

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12 keystore

Then, browse to a location on your Kali VM where you want to save the file. It is important that, when you are saving the file, you save it with a .der extension, otherwise the file won’t import correctly into Firefox.



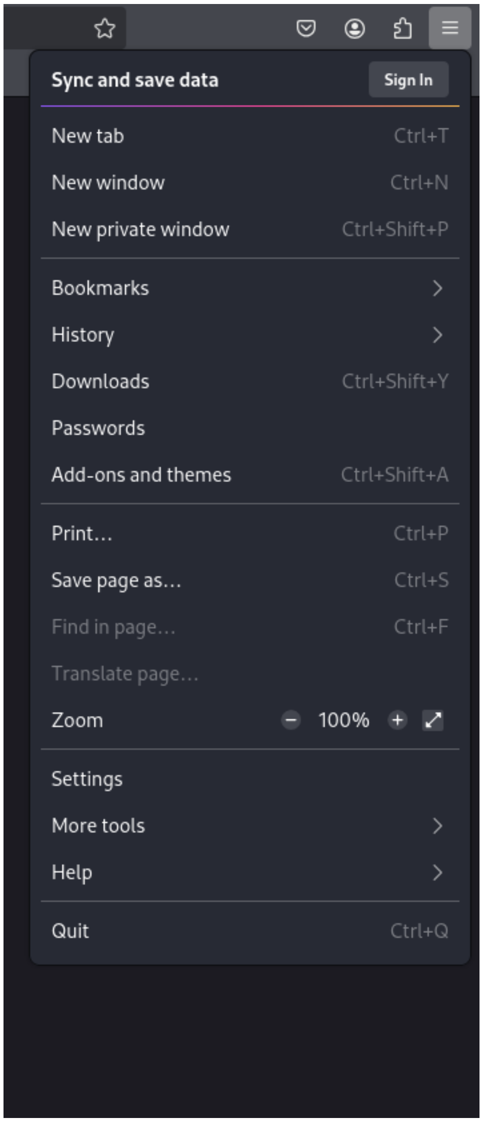
CA Certificate

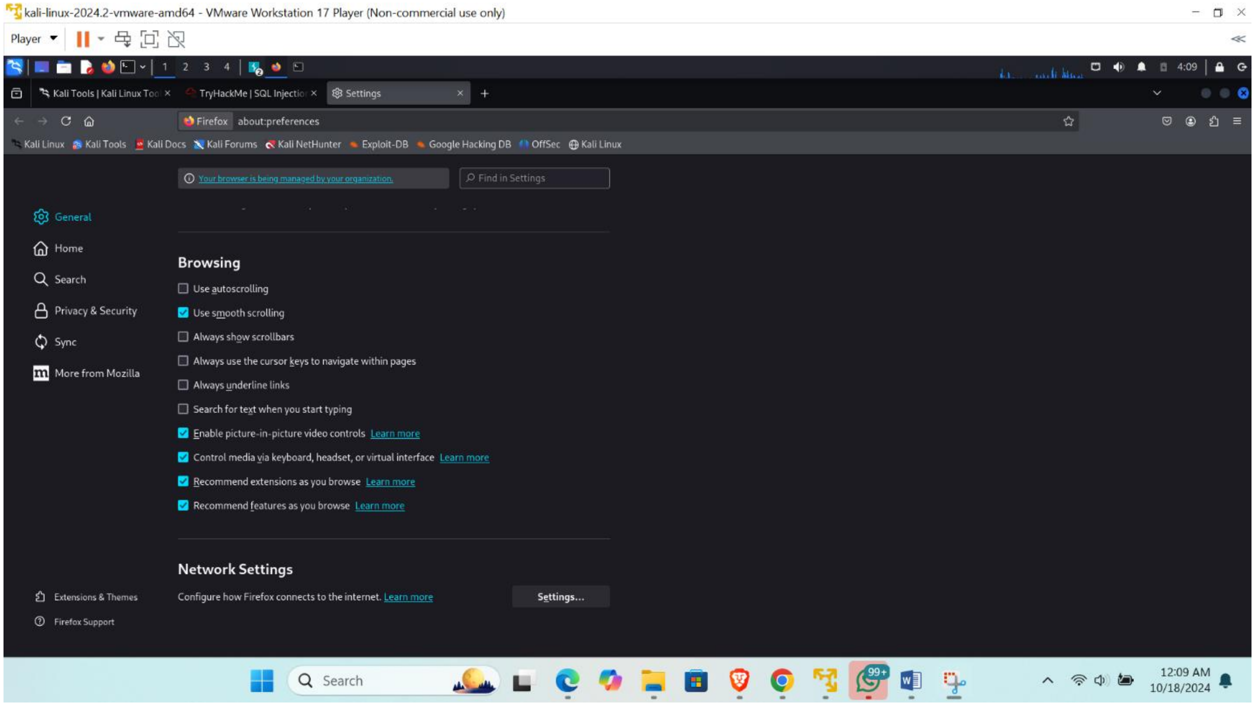
Choose a file to export the CA certificate.

/home/kali/Downloads/a.der

Task 4

Once this is done, open Web Browser (Firefox) in Kali and navigate to the options. Find “proxy” in Preferences’ search box. Click on the button called “Settings” under Network Settings.





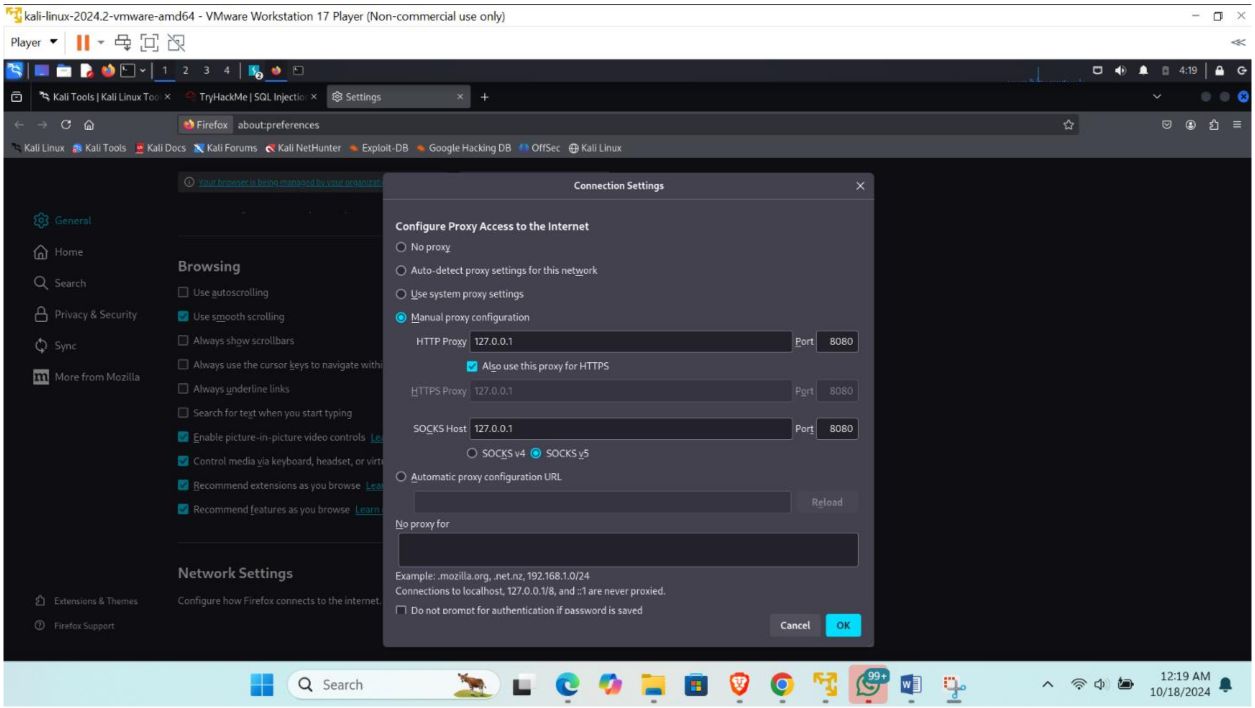
Browsing

- ☐ Use autoscrolling
- ☑ Use smooth scrolling
- ☐ Always show scrollbars
- ☐ Always use the cursor keys to navigate within pages
- ☐ Always underline links
- ☐ 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…

Then, click Manual Proxy Configuration and enter the following details:



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 127.0.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

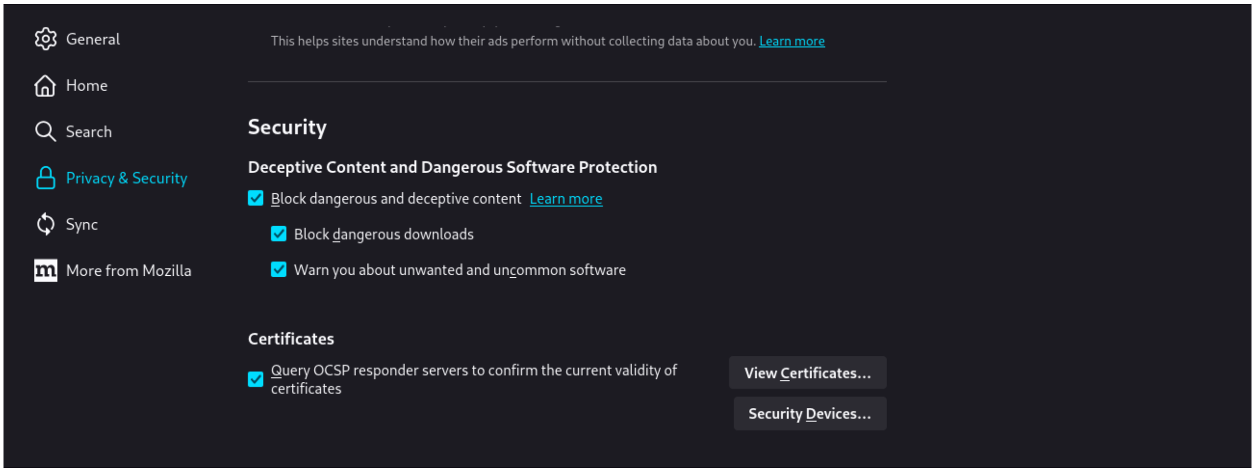
Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

Cancel OK

Task 5

Once this is done, navigate to the Privacy & Security tab and then to the Certificates section. This is where we will import the certificate from Burp we saved earlier. To do this, press on “View Certificates” and click on “Import”.



This helps sites understand how their ads perform without collecting data about you. Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

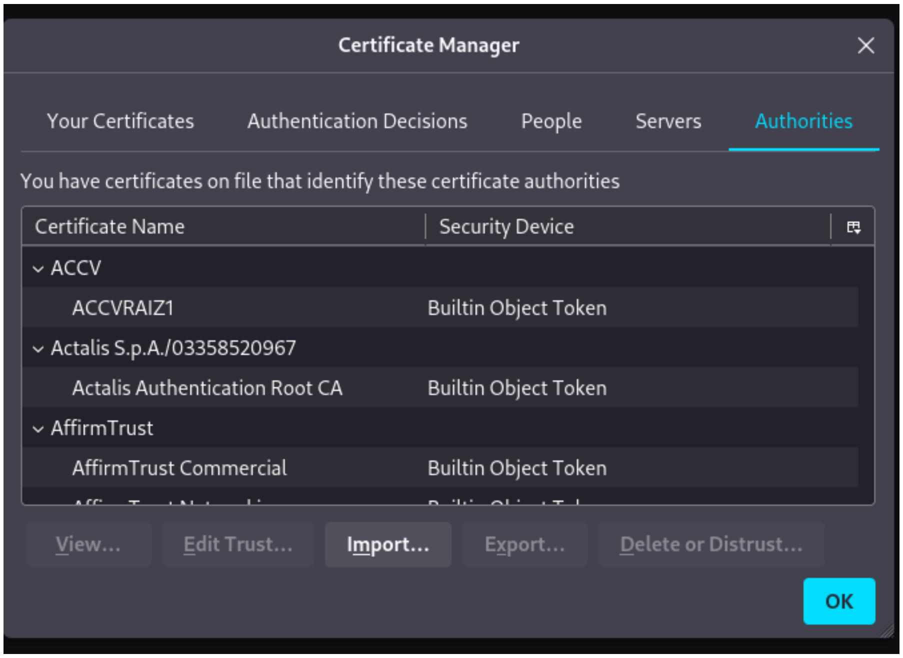
☑ Warn you about unwanted and uncommon software

Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

View Certificates…

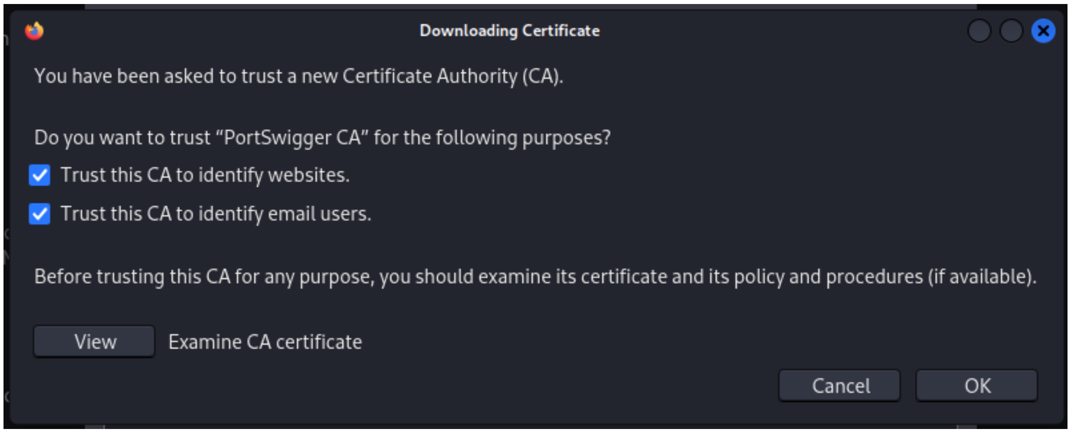
Security Devices…



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token
AffirmTrust	
AffirmTrust Commercial	Builtin Object Token

Navigate to the .der file that we saved earlier. Once selected, a box will pop up asking if you would like Burp Suite to be able to intercept emails and connections to websites. Select both options and click “Ok”.



You have been asked to trust a new Certificate Authority (CA).

Do you want to trust “PortSwigger CA” for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

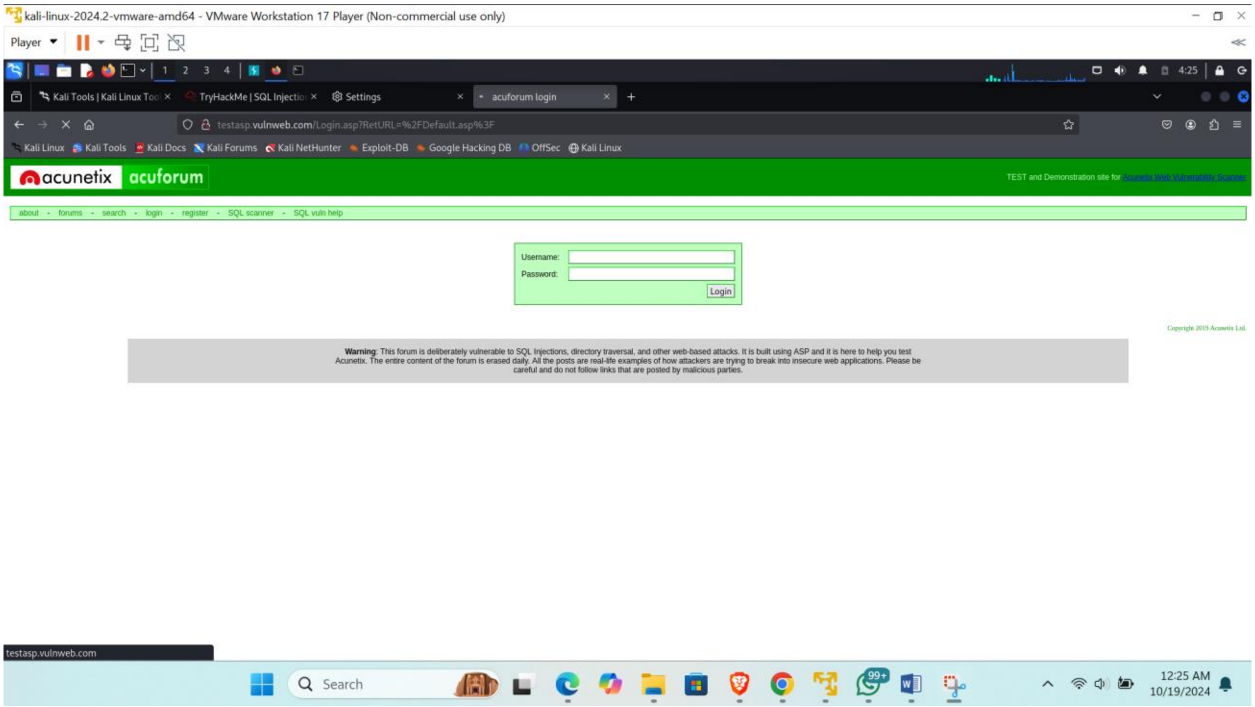
Examine CA certificate

Task 6

Once the web browser opens, navigate to the following site:

http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F

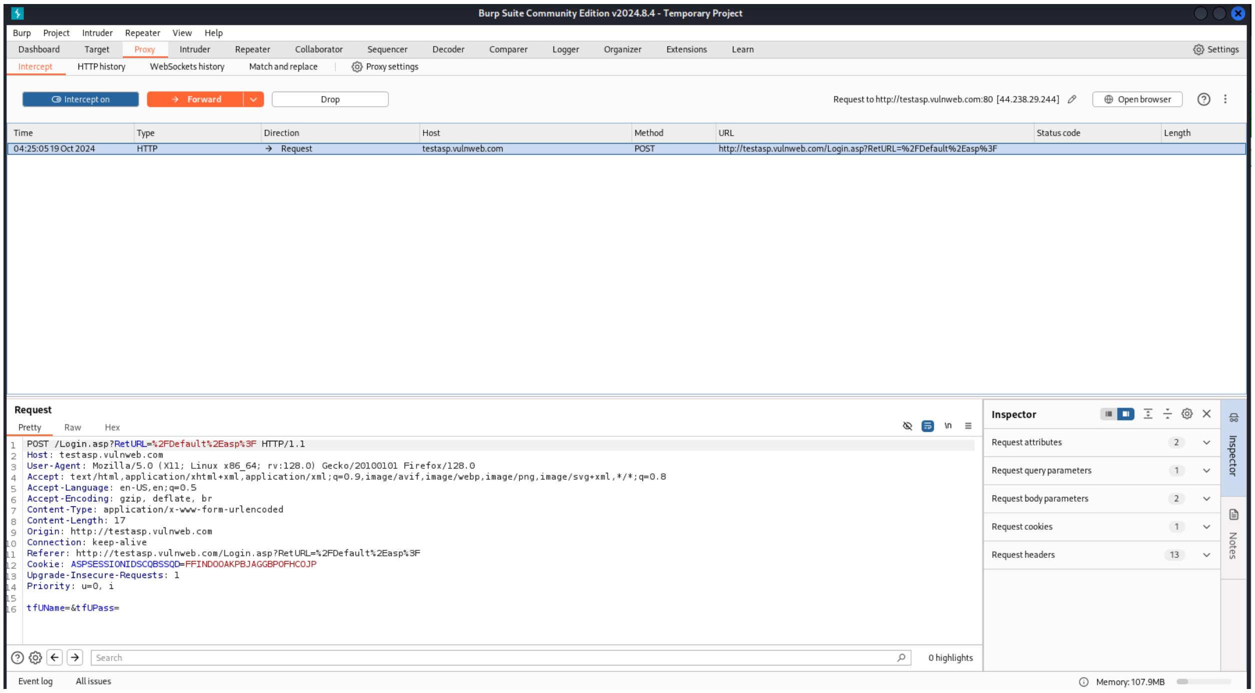
Once there, go back to Burp and turn ON intercept mode. Then, enter any username and password combination into the site and click “Login”. As you will see, the page will remain in a loading state. This is because Burp has now intercepted the request we sent to the server, and is holding it for us to manipulate.


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
acuforum login
testasp.vulnweb.com/Login.asp?RetURL=%2FDefault.asp%3F
acunetix acuforum
about - forums - search - login - register - SQL scanner - SQL vuln help
Login
testasp.vulnweb.com

Username:
Password:

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.

Go back to Burp and you will find the intercepted request, along with the username and password data that we entered. To navigate through the different requests Burp is intercepting, simply press the “Forward” button to send the request to the server and view the next request.


Burp Suite Community Edition v2024.8.4 - 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 Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Request
Pretty Raw Hex
Inspector
Search
0 highlights
Event log All issues
Memory: 107.9MB

Request to http://testasp.vulnweb.com:80 [44.238.29.244]

Time	Type	Direction	Host	Method	URL	Status code	Length
04:25:05 19 Oct 2024	HTTP	→ Request	testasp.vulnweb.com	POST	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F		

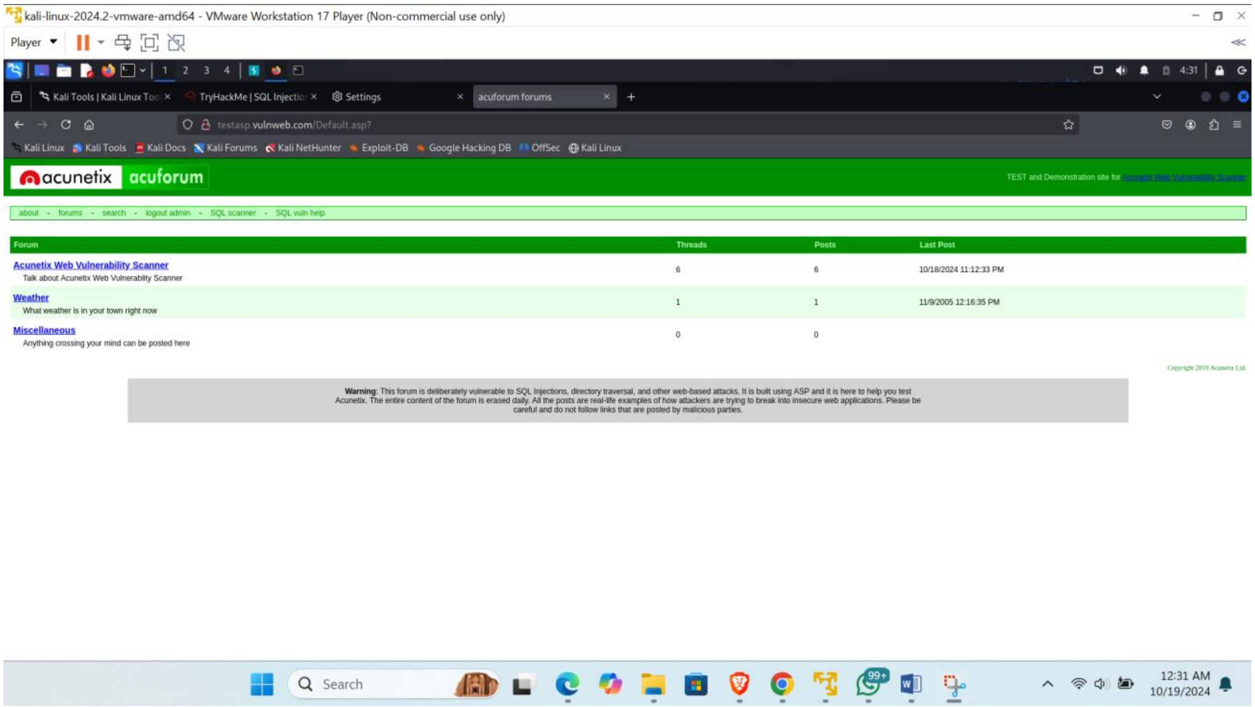
```
POST /Login.asp?RetURL=%2FDefault%2Easp%3F HTTP/1.1
Host: testasp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Origin: http://testasp.vulnweb.com
Connection: keep-alive
Referer: http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Cookie: ASPSESSIONIDSCQBSSQD=FFINDOOAKPBJAGGBPOFHCOJP
Upgrade-Insecure-Requests: 1
Priority: u=0, i

tfUName=&tfUPass=
```

Inspector	
Request attributes	2
Request query parameters	1
Request body parameters	2
Request cookies	1
Request headers	13

Task 7

You can also alter any text portion of web traffic when Burb interception mode is ON. Try to change “tfUName=admin” and “tfUPass=none” and press the “Forward” button. Those are valid credentials for the green-colored page, and you will be granted access to the next page.



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Kali Tools | Kali Linux Too
TryHackMe | SQL Injectio
Settings
acuforum forums
testasp.vulnweb.com/Default.asp?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Kali Linux
acunetix
acuforum
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout admin - SQL scanner - SQL vuln help
Search
12:31 AM
10/19/2024

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	6	6	10/18/2024 11:12:33 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.