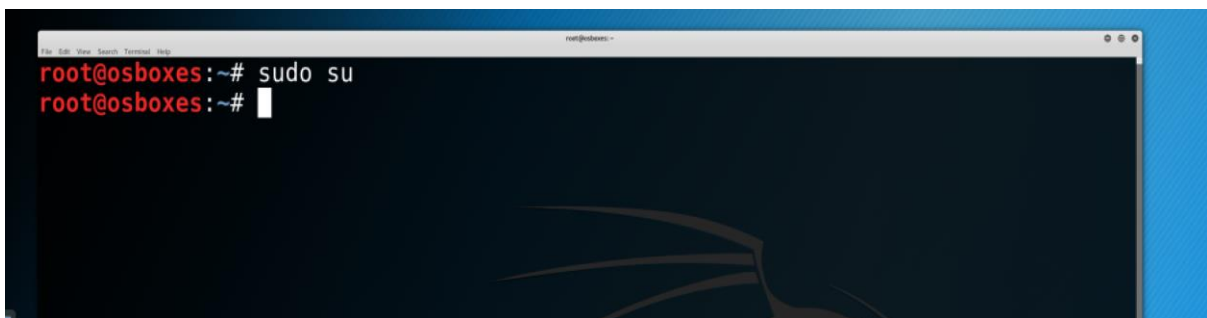


WEEK 8 - ACTIVITY - WEB SECURITY AND ETHICAL HACKING WITH BURP SUITE

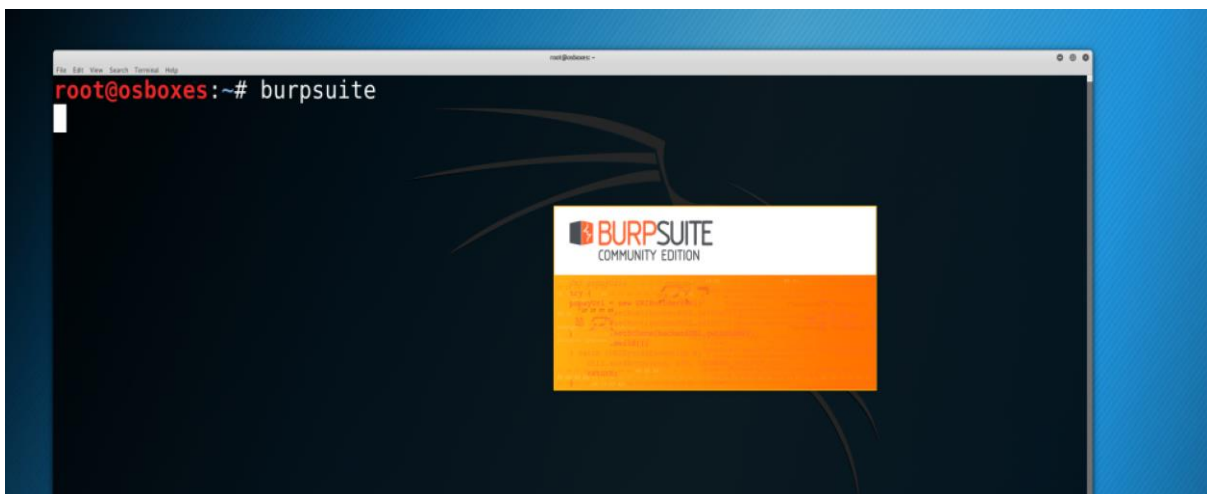
1. Open Kali Linux terminal and type `sudo su`

The screenshot shows the user entering the command `sudo su` in a Linux terminal. This command switches the current user to the **root (administrator)** account, granting full administrative privileges. The change in the command prompt to `root@osboxes:~#` confirms that the user has successfully gained root access.

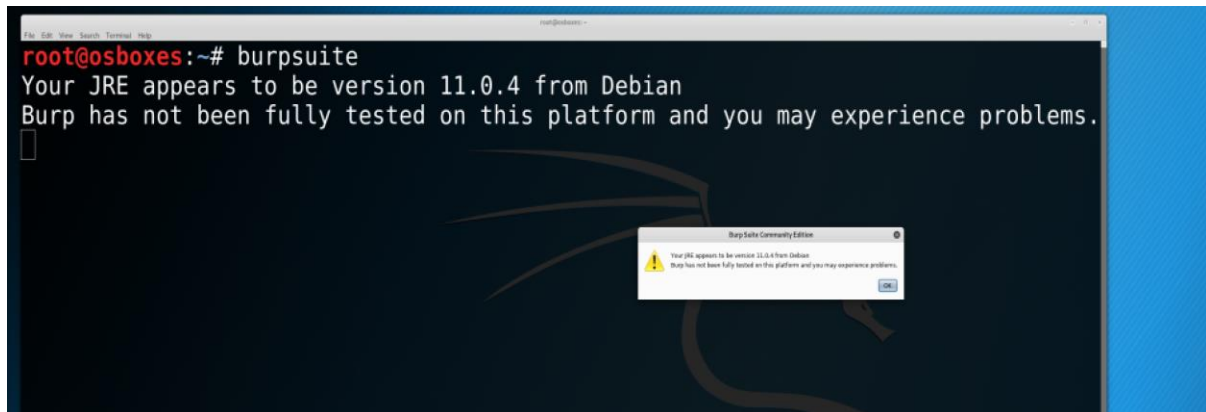


2. Type `burpsuite` on your kali Linux terminal

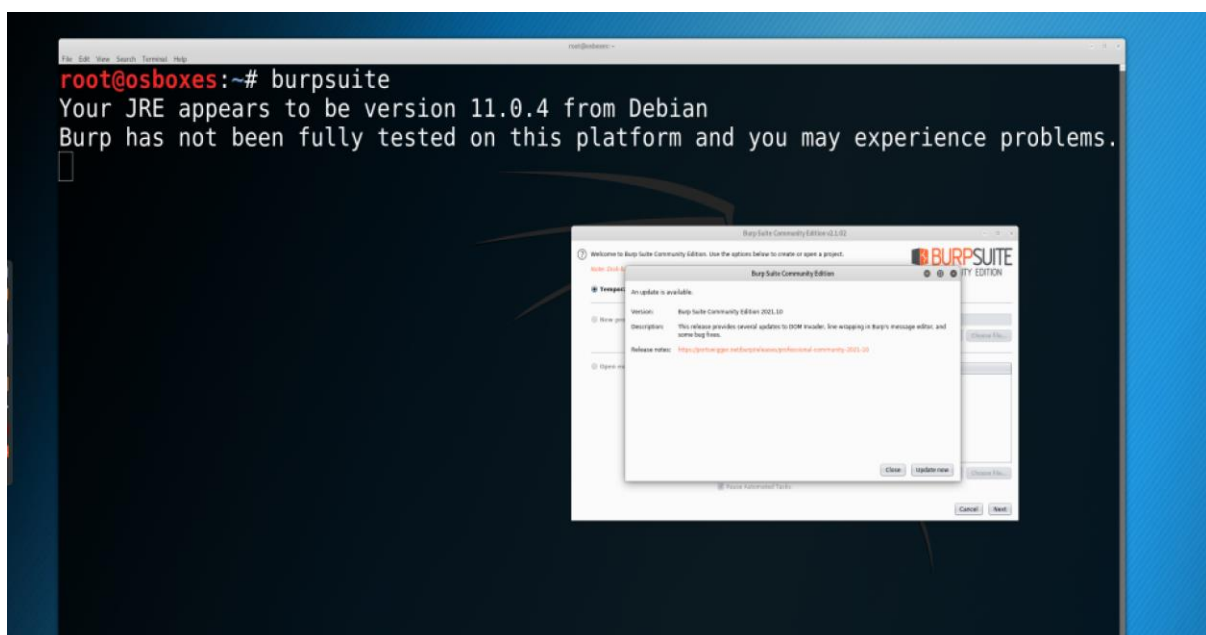
The screenshot shows the user typing the `burpsuite` command in the Kali Linux terminal to launch **Burp Suite Community Edition**. The Burp Suite startup screen appears, indicating that the application is loading successfully. Burp Suite is a web application security testing tool used to intercept, inspect, and analyse HTTP/HTTPS traffic during penetration testing.



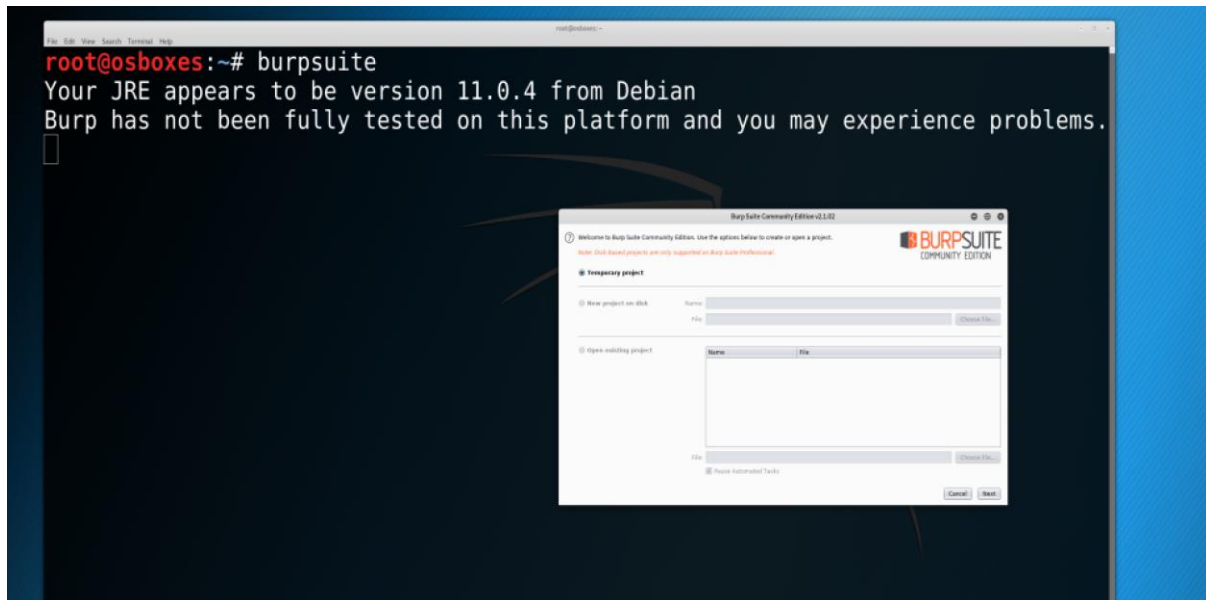
- The screenshot shows Burp Suite launching after the **burpsuite** command is executed. A warning message appears stating that the installed **Java Runtime Environment (JRE) version 11.0.4** from Debian has not been fully tested with Burp Suite, so compatibility issues may occur. This is a warning only, and the user can click **OK** to continue launching Burp Suite.



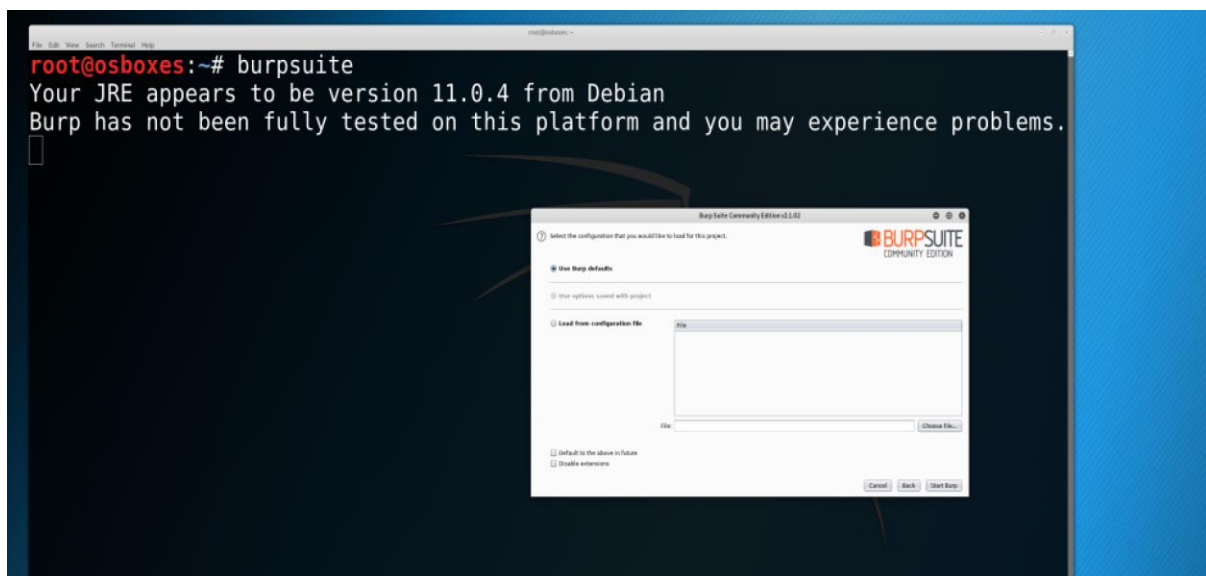
- The screenshot shows Burp Suite displaying an **update notification** after launching. For this setup, no update is required, so the user should click **Close** to dismiss the update window and continue using the current version of Burp Suite. If you have already updated Burp Suite previously, you may not receive this update notification, and you can proceed directly to the next step.



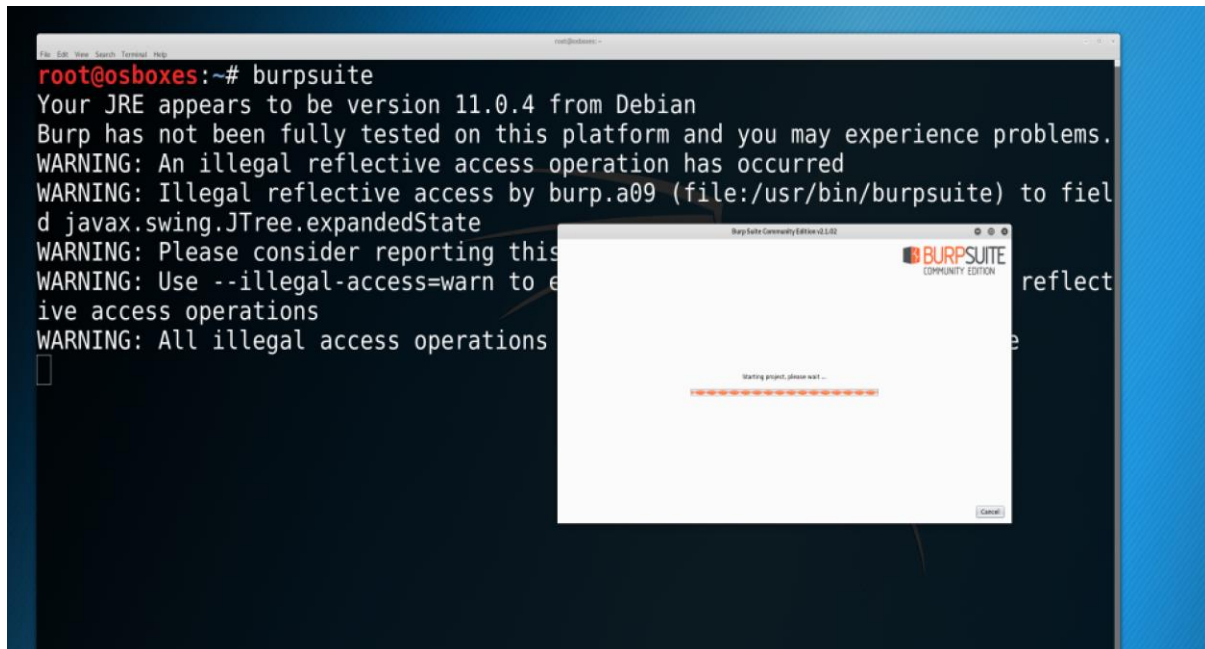
5. The screenshot shows the **Burp Suite Community Edition** project setup screen. The **Temporary project** option is selected by default, allowing Burp Suite to create a temporary workspace for the current session without saving project data. Leave this option selected and click **Next** to continue with the setup.



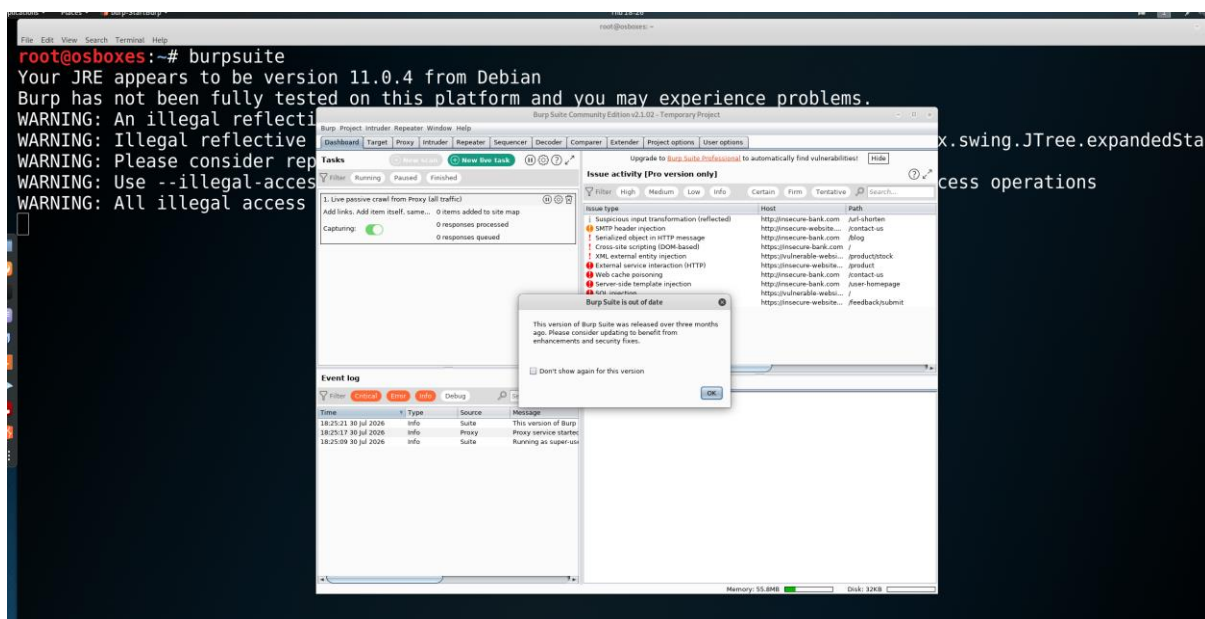
6. The screenshot shows the **Burp Suite configuration** screen. Leave the default option, **Use Burp defaults**, selected to load the standard configuration settings. Then click **Start Burp** (or **Start Burp Suite**, depending on the version) to launch Burp Suite and begin using the application.



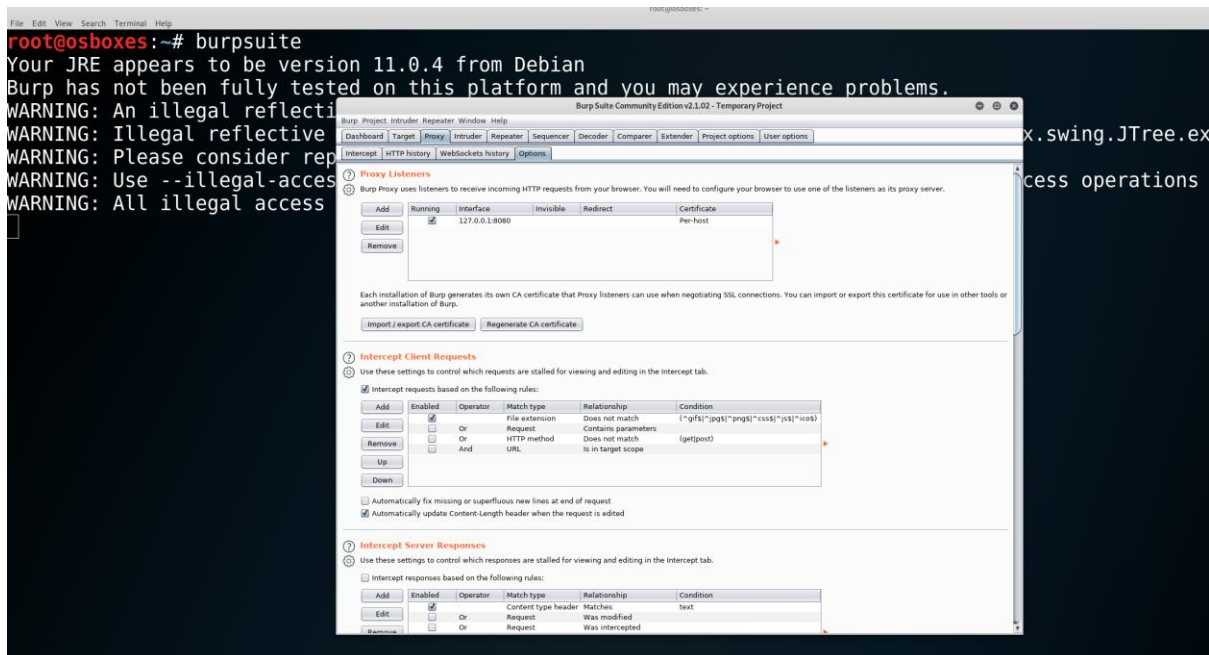
7. The screenshot shows **Burp Suite loading** after the configuration has been completed. The progress bar indicates that the application is starting the temporary project and initializing its components. The warning messages displayed in the terminal are common Java-related notifications and do not prevent Burp Suite from launching successfully.



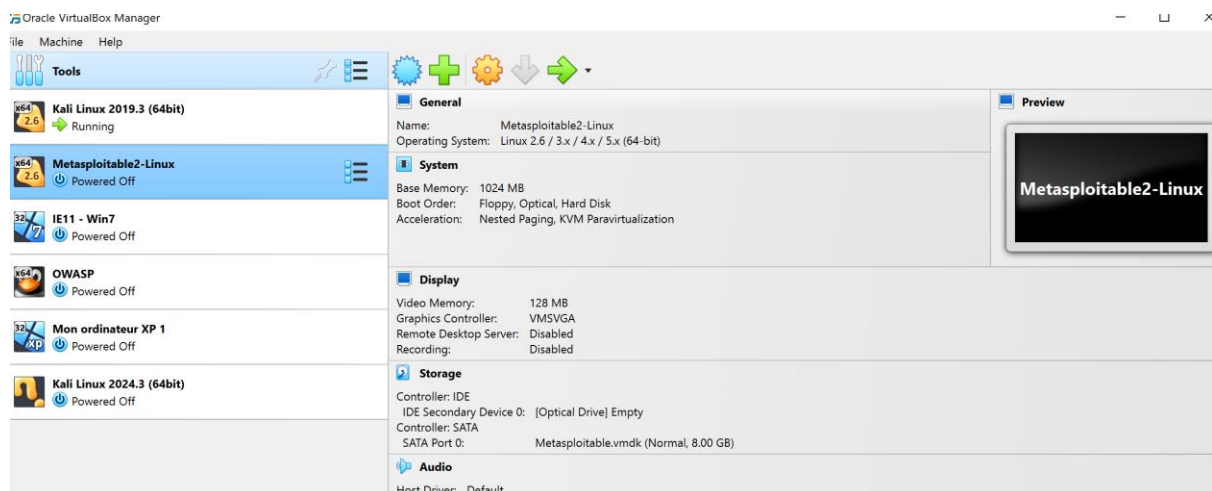
8. The screenshot shows **Burp Suite Community Edition** successfully launched and ready for use. An **out-of-date version** notification is displayed, informing the user that a newer version is available. For this setup, click **OK** to dismiss the message and continue. If you have already updated Burp Suite, you may not see this notification.



9. The screenshot shows the **Proxy → Options** tab in Burp Suite. Verify that the **Proxy Listener** is enabled and configured to listen on **127.0.0.1:8080** (localhost). This loopback address ensures that Burp Suite can intercept web traffic from the browser configured to use this local proxy.



10. The screenshot shows **Oracle VirtualBox Manager** with the **Metasploitable 2 Linux** virtual machine selected. To continue the lab, start the **Metasploitable2-Linux** virtual machine by selecting it and clicking the **Start** button. This launches the vulnerable target system that will be used for web application security testing with Burp Suite.



11. The screenshot shows the **Metasploitable 2** login screen. Log in using the default credentials, **username: msfadmin** and **password: msfadmin**. After entering the credentials, press **Enter** to access the vulnerable virtual machine and continue with the lab.

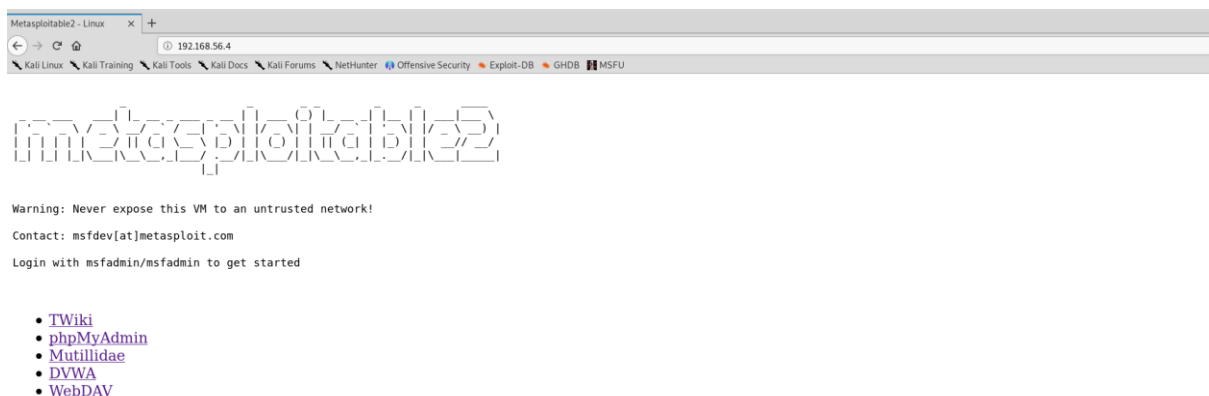
```
contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: _
```

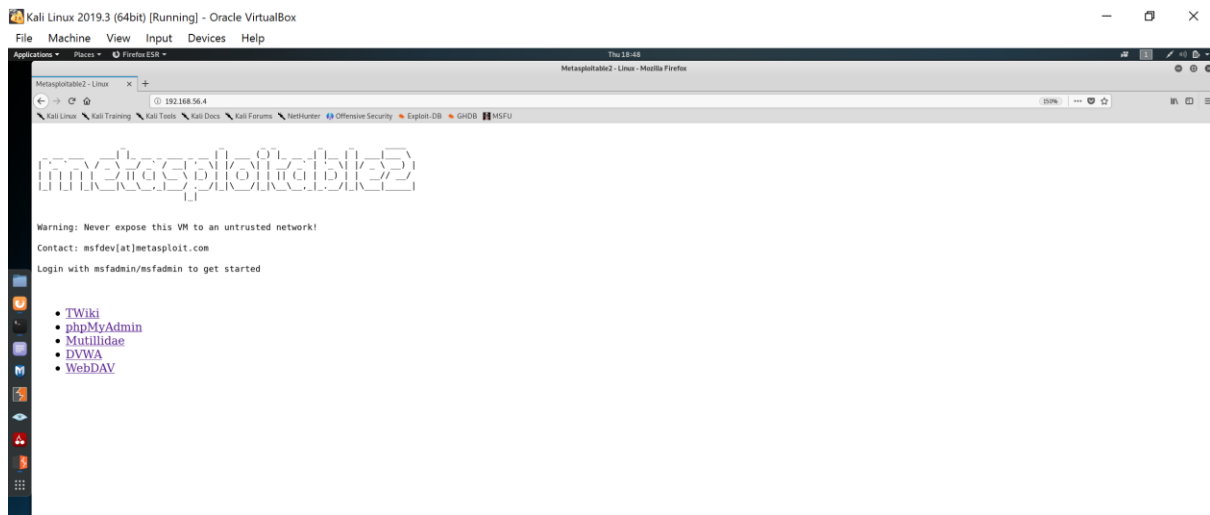
12. The screenshot shows the **ifconfig** command being executed on the **Metasploitable 2** virtual machine to display its network configuration. The **IP address** is listed under the **eth0** interface as **192.168.56.4**. Note this IP address, as it will be used to access the Metasploitable 2 web services and perform the security testing exercises.

```
Metasploitable [Running] - Oracle VirtualBox
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:19:7e:45
          inet addr:192.168.56.4  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe19:7e45/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

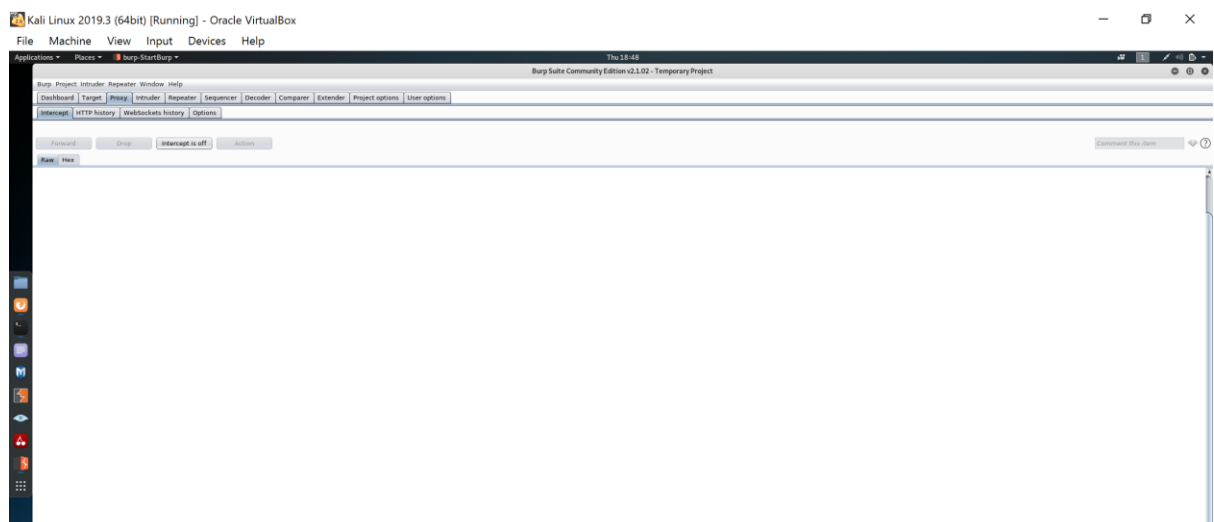
13. The screenshot shows **Firefox** on the Kali Linux virtual machine accessing the **Metasploitable 2** web server using its IP address (**192.168.56.4**). The Metasploitable home page is displayed, listing several vulnerable web applications. Click **DVWA (Damn Vulnerable Web Application)** to open the application and begin the web security testing exercises.



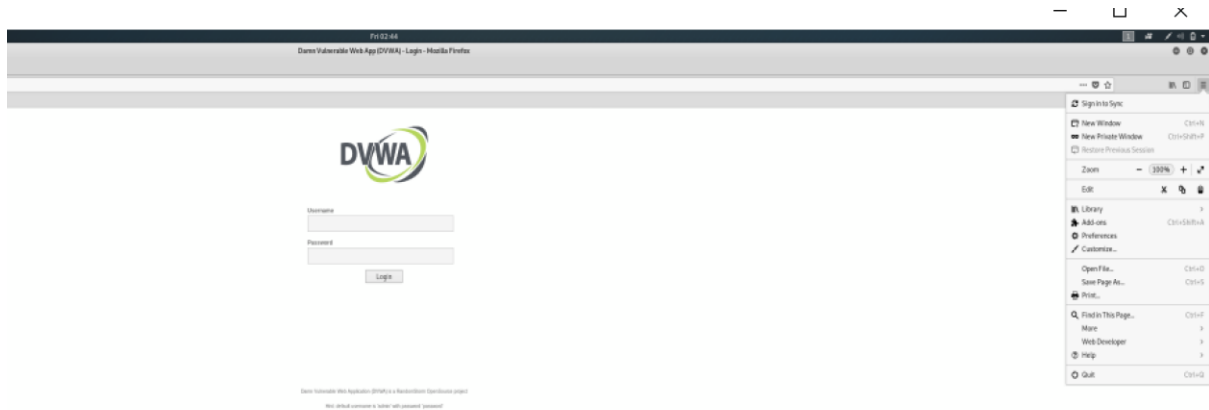
14. The screenshot shows the **DVWA (Damn Vulnerable Web Application)** login page displayed in Firefox after selecting **DVWA** from the Metasploitable 2 home page. This confirms that the application is accessible and ready for use. You can now log in using the default DVWA credentials to begin the web application security testing exercises.



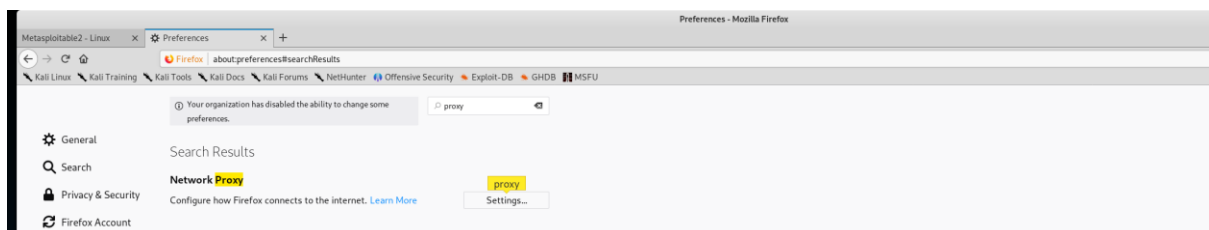
15. The screenshot shows the **Proxy → Intercept** tab in Burp Suite. Ensure that the **Intercept** feature is **turned off**, indicated by the **"Intercept is off"** button. With interception disabled, web traffic will pass through Burp Suite without being paused, allowing you to browse the DVWA application normally while still capturing requests in the HTTP history.



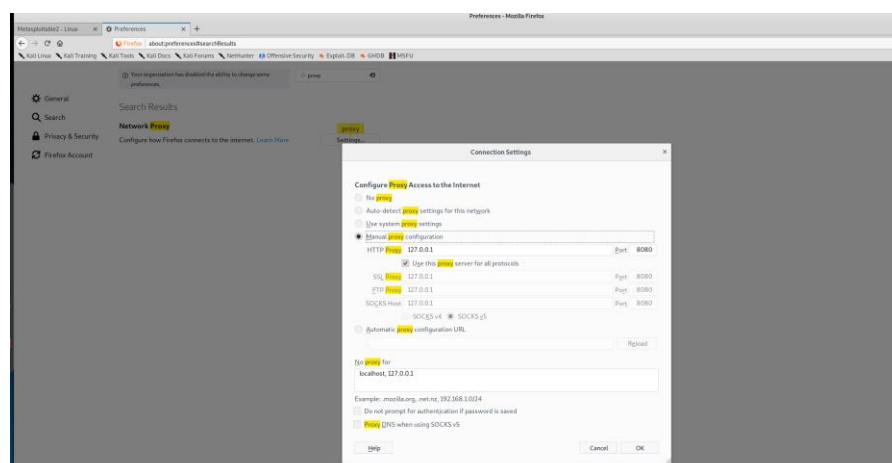
16. The screenshot shows the **Firefox** menu opened by clicking the **three-line menu** (hamburger menu) in the top-right corner of the browser. From the menu, select **Preferences** to open the browser settings, where you can configure the proxy settings required for Burp Suite to intercept web traffic.



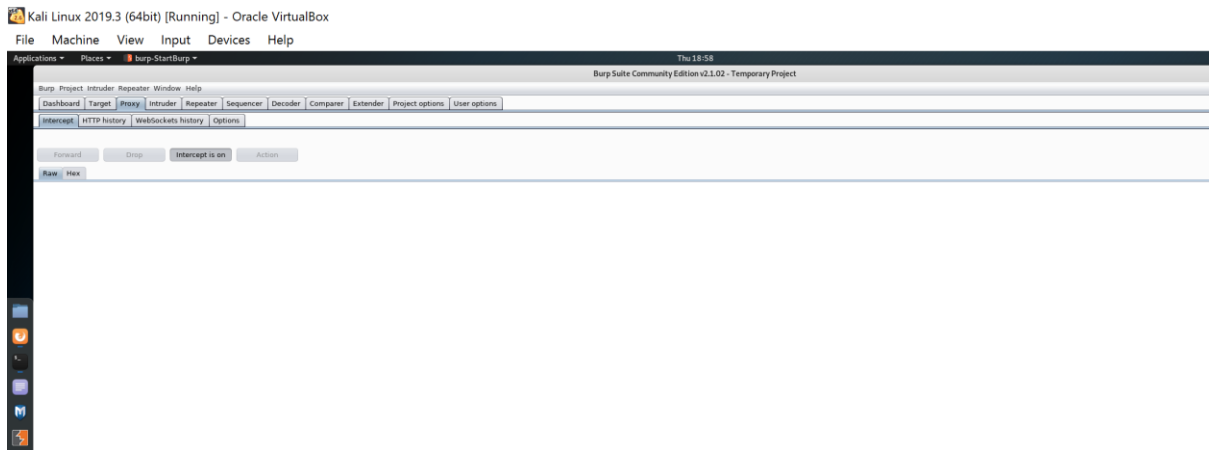
17. The screenshot shows you using the **Firefox Preferences** search bar to search for **proxy**. The search results display the **Network Proxy** section, where you should click **Settings** to open the browser's proxy configuration and configure Firefox to use Burp Suite as its proxy.



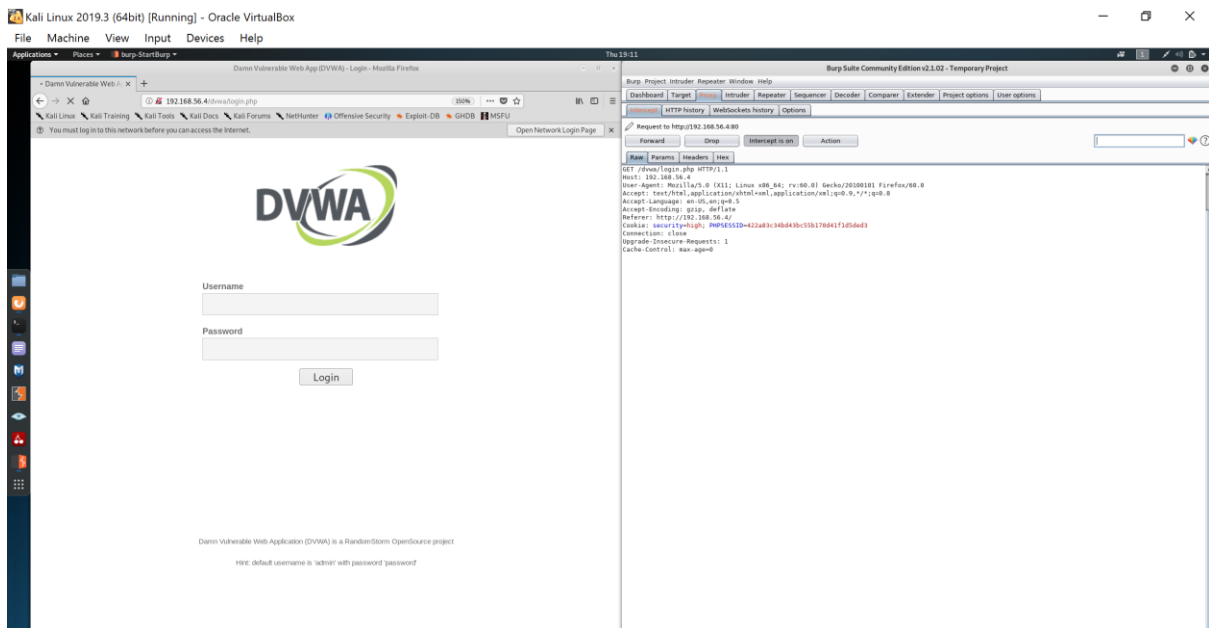
18. The screenshot shows you configuring **Firefox** to use **Burp Suite** as a manual proxy. Select **Manual proxy configuration**, enter **127.0.0.1** as the **HTTP Proxy** address, enter **8080** as the **Port**, and enable the option to **use this proxy server for all protocols** (including HTTPS and FTP). Finally, click **OK** to save the proxy settings.



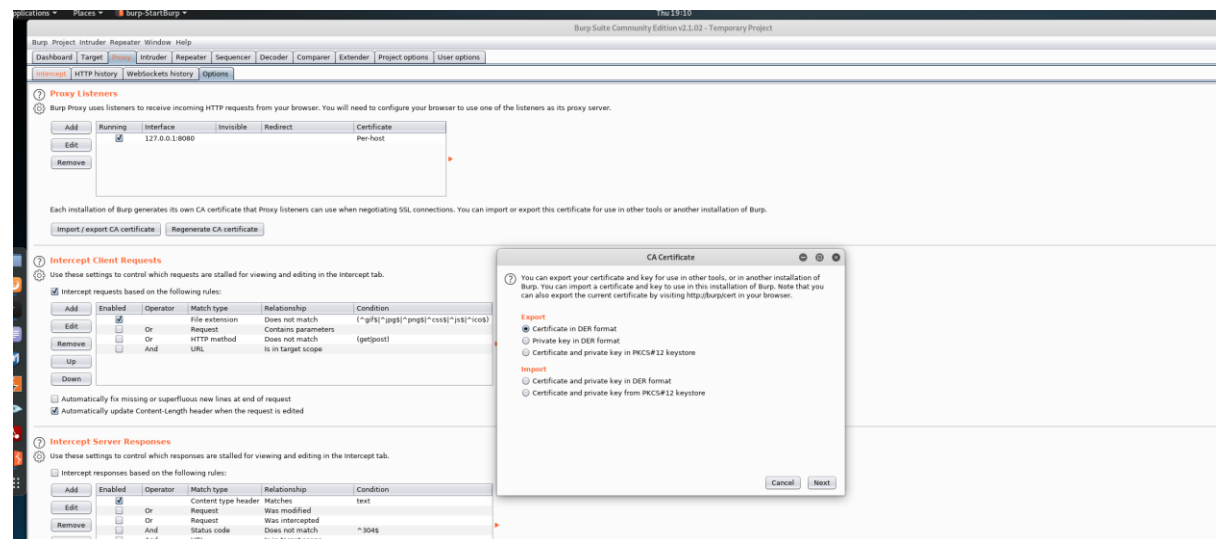
19. The screenshot shows you returning to the **Proxy → Intercept** tab in Burp Suite and enabling the **Intercept** feature. When the button displays "**Intercept is on**", Burp Suite will pause and capture incoming HTTP requests, allowing you to inspect and modify them before they are sent to the target web application.



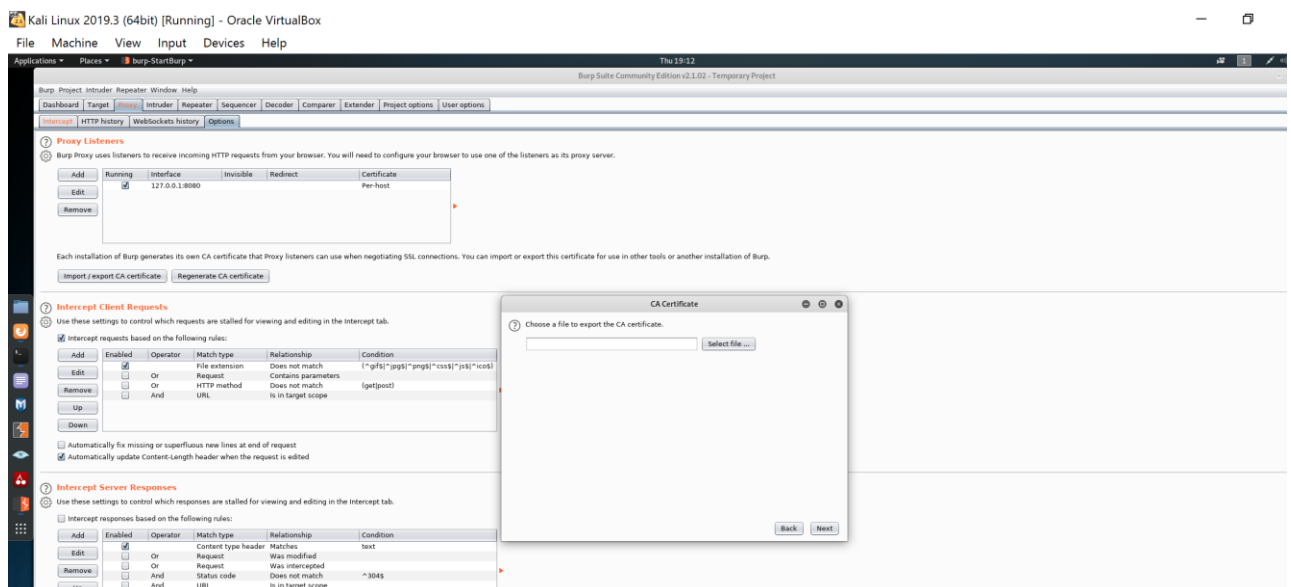
20. The screenshot shows you refreshing the **DVWA** page in Firefox while **Burp Suite Intercept** is turned on. Burp Suite captures the HTTP request before it reaches the web server, allowing you to inspect or modify the request. After reviewing the request details, click **Forward** to send it to the server and continue loading the web page.



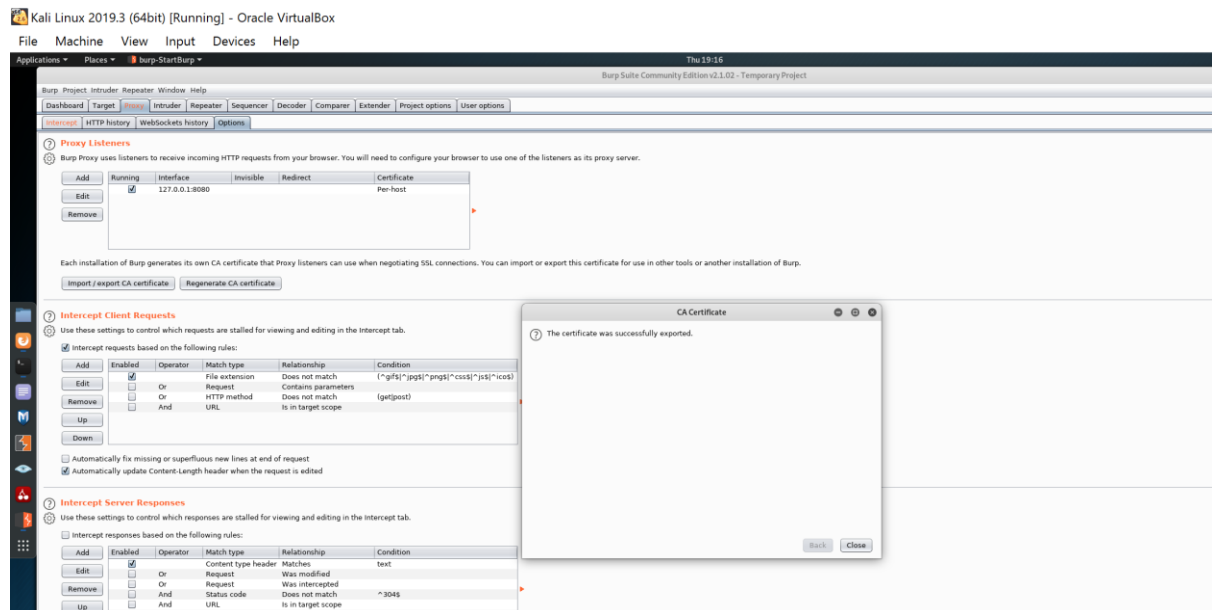
21. The screenshot shows the **Proxy → Options** tab in Burp Suite, where you can configure the proxy listener and manage Burp Suite's **CA certificate**. If you receive a certificate or HTTPS error in Firefox, ensure that the proxy listener is using the **127.0.0.1 (loopback)** address. Then use the **Import / Export CA Certificate** option to export Burp Suite's CA certificate and import it into Firefox. This allows the browser to trust Burp Suite's certificate and intercept HTTPS traffic without certificate warnings. Select **Certificate in DER format**



22. The screenshot shows the **Burp Suite CA Certificate** export dialog prompting you to choose a location to save the certificate. Click **Select File**, choose a folder where you want to save the certificate, provide a filename if required, and then click **Next** to export the certificate. This certificate will later be imported into Firefox so the browser can trust Burp Suite when intercepting HTTPS traffic.



23. The screenshot confirms that the **Burp Suite CA certificate** has been successfully exported and saved to the selected folder. This certificate is now ready to be imported into **Firefox**, allowing the browser to trust Burp Suite and intercept HTTPS traffic without certificate warnings.



24. The screenshot shows you searching for **certificate** in the **Firefox Preferences** page and opening the **Certificate Manager** by clicking **View Certificates**. From the **Authorities** tab, click **Import**, **All Files**, select the **Burp Suite CA certificate** that was previously exported, and import it. This allows Firefox to trust Burp Suite and intercept HTTPS traffic without displaying certificate warnings.

