

6-21-2022 Lab 22 - Broken OWASP Setup Installation

Tuesday, June 21, 2022 9:59 AM

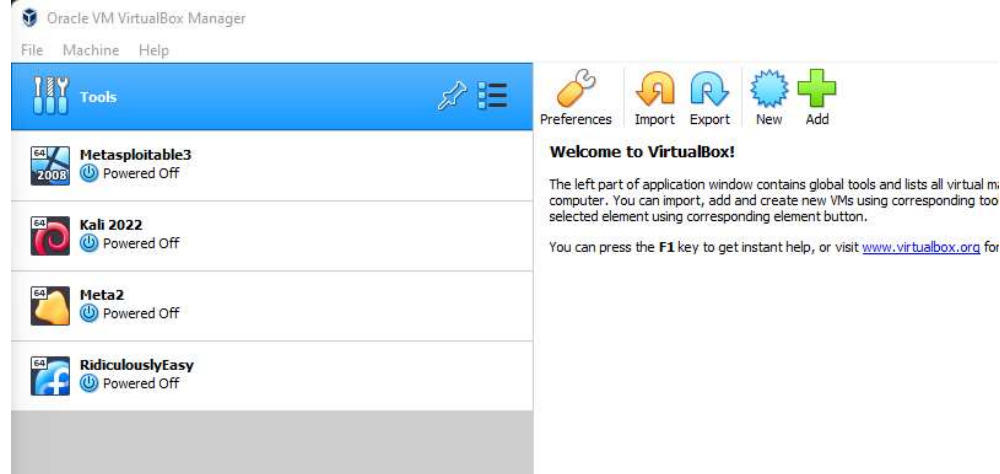
Download and unzip the link below.*(You can use 7zip or WinRAR)*

<https://sourceforge.net/projects/owaspbwa/files/>

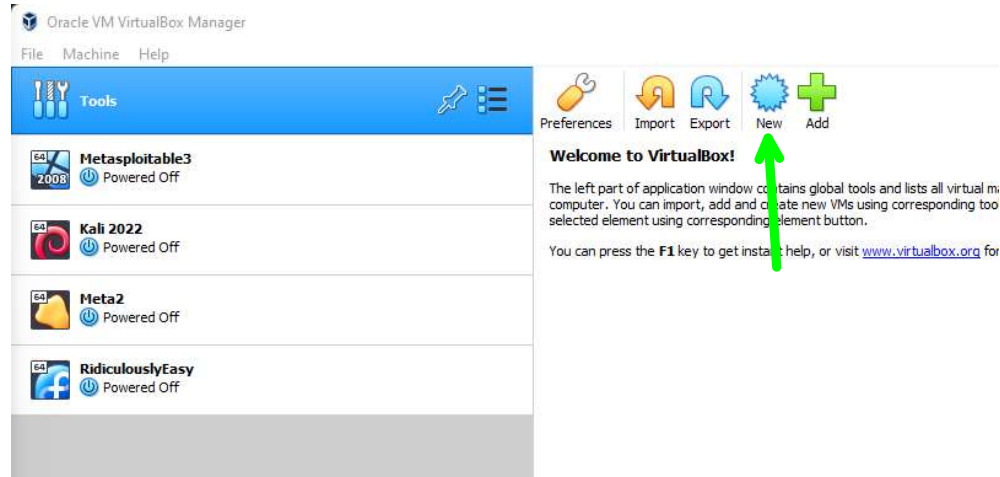
You can download 7zip using the following link

7zip: <https://www.7-zip.org/download.html> WinRAR: [WinRAR archiver, a powerful tool to process RAR and ZIP files \(rarlab.com\)](http://www.rarlab.com)

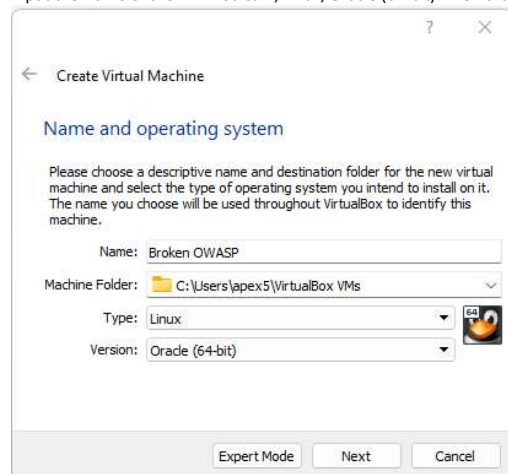
Open Virtualbox



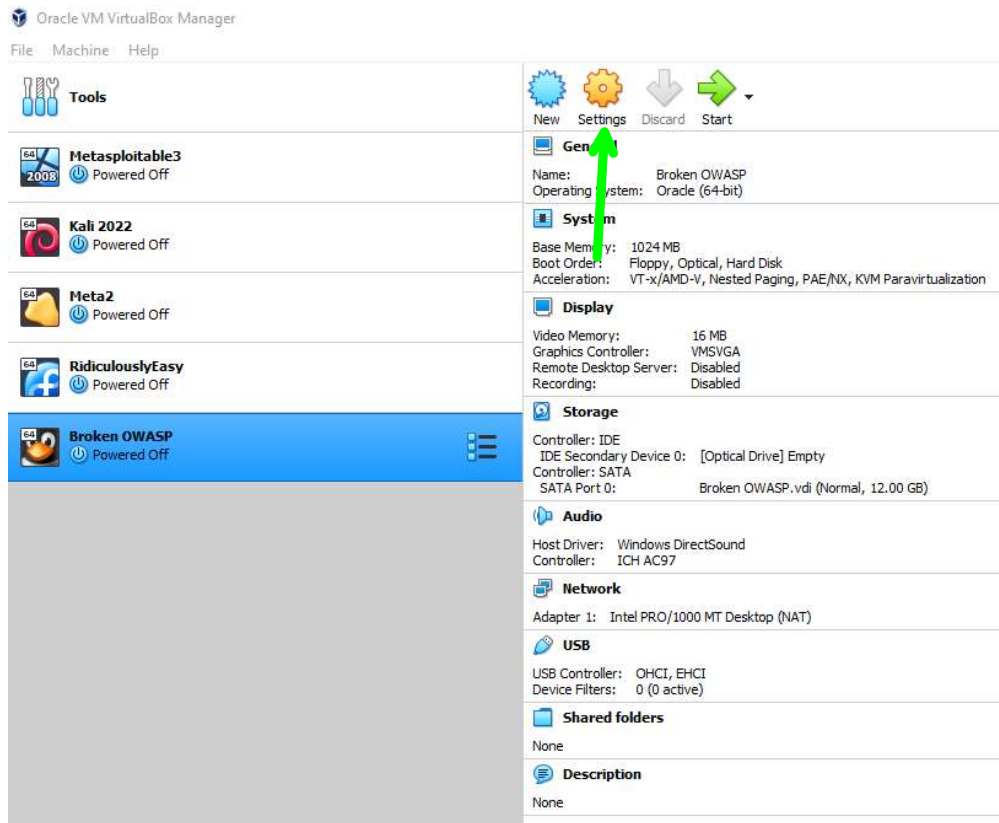
Click New



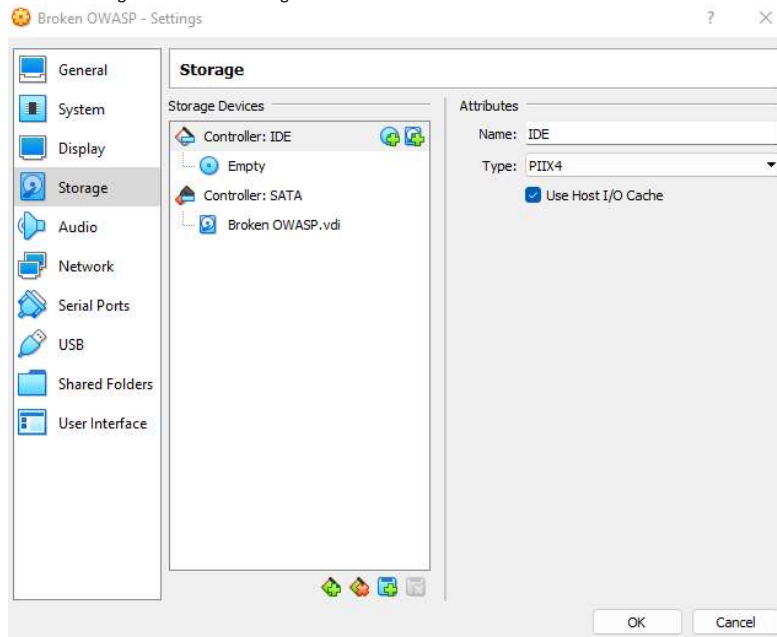
Input the Name of the VM*You can , Linux, Oracle (64-bit). Then click next to completion.



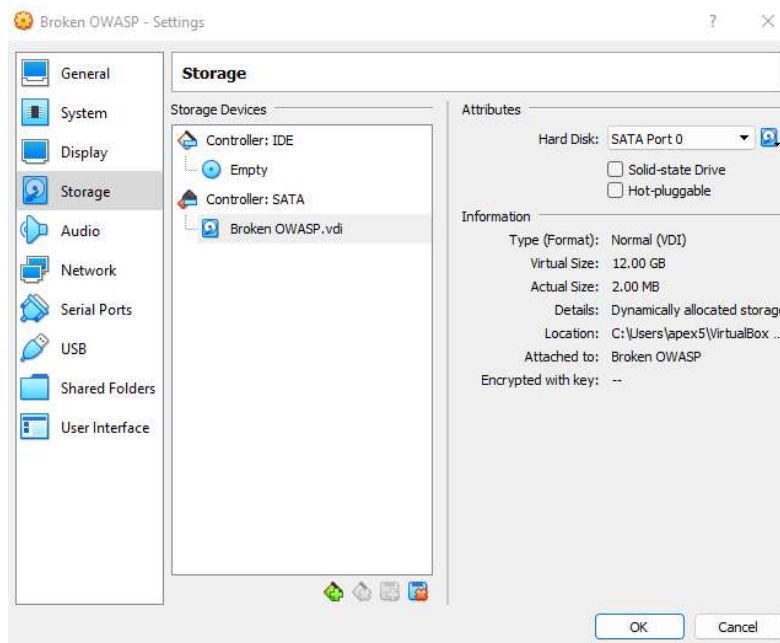
Open Settings for the New VM



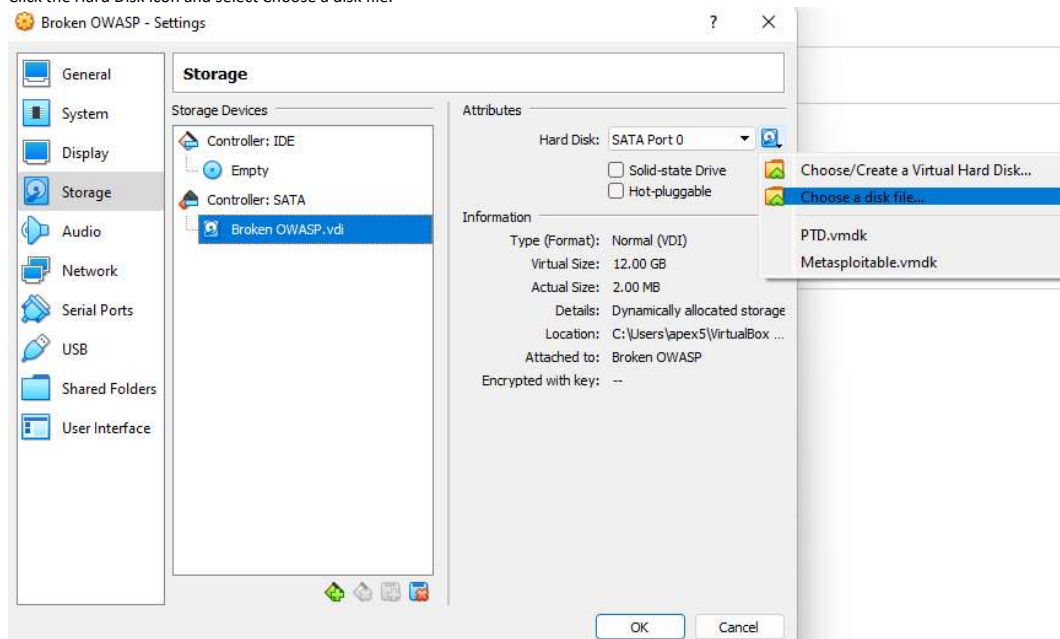
Click the Storage Tab in the Left Navigation Menu.



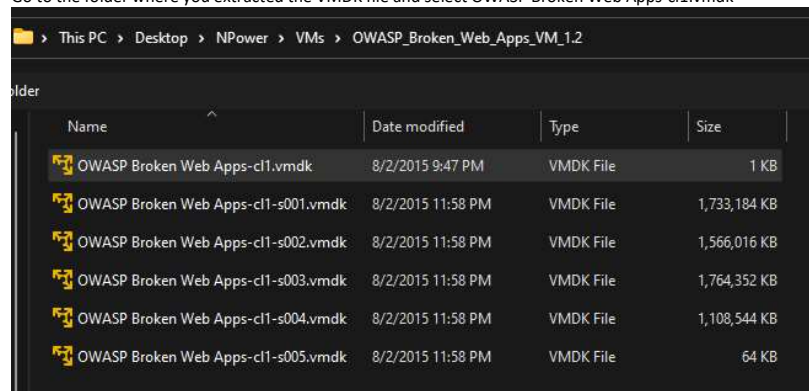
Click the Broken OWASP VDI



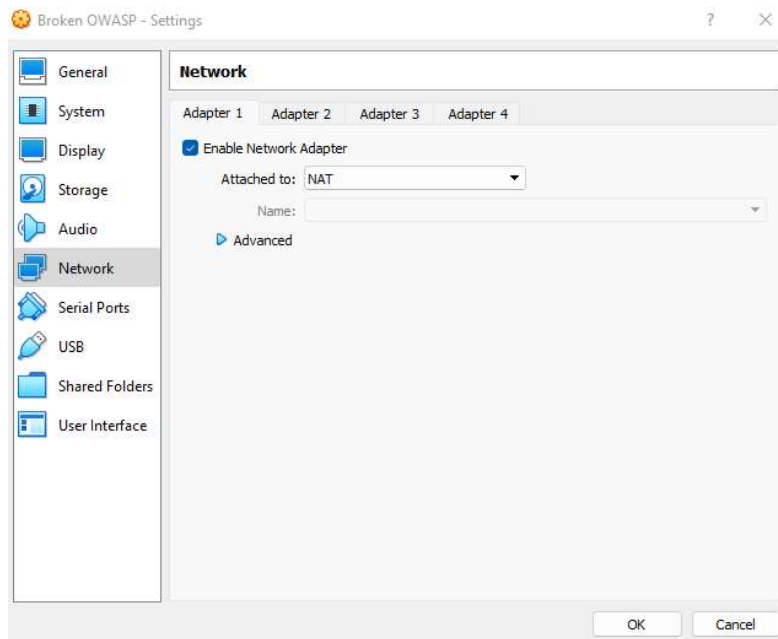
Click the Hard Disk icon and select Choose a disk file.



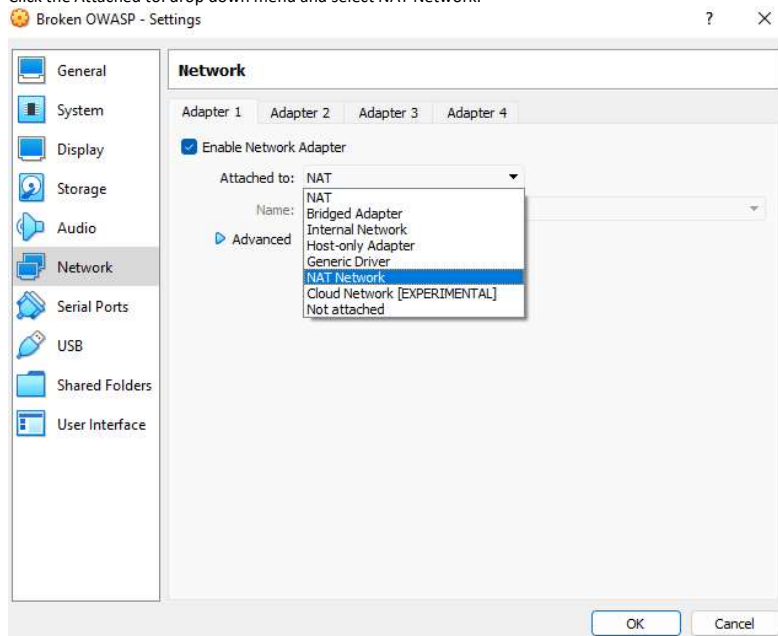
Go to the folder where you extracted the VMDK file and select OWASP Broken Web Apps-cl1.vmdk



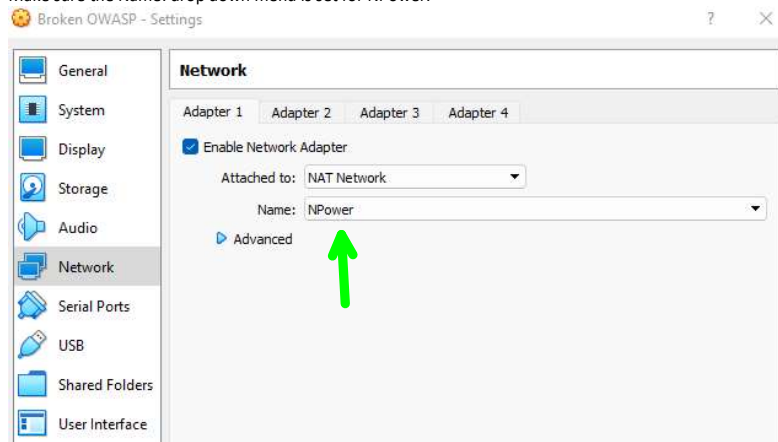
Click the Network tab in the left navigation menu.



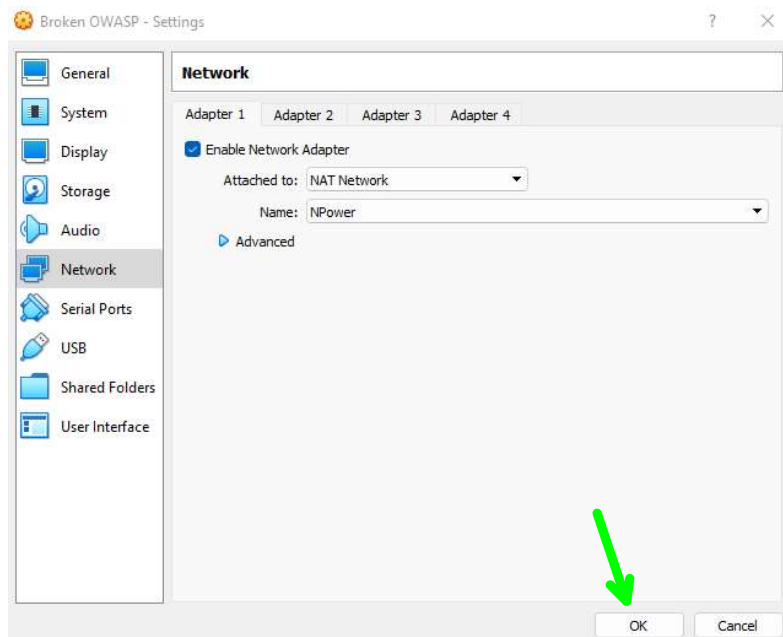
Click the Attached to: drop down menu and select NAT Network.



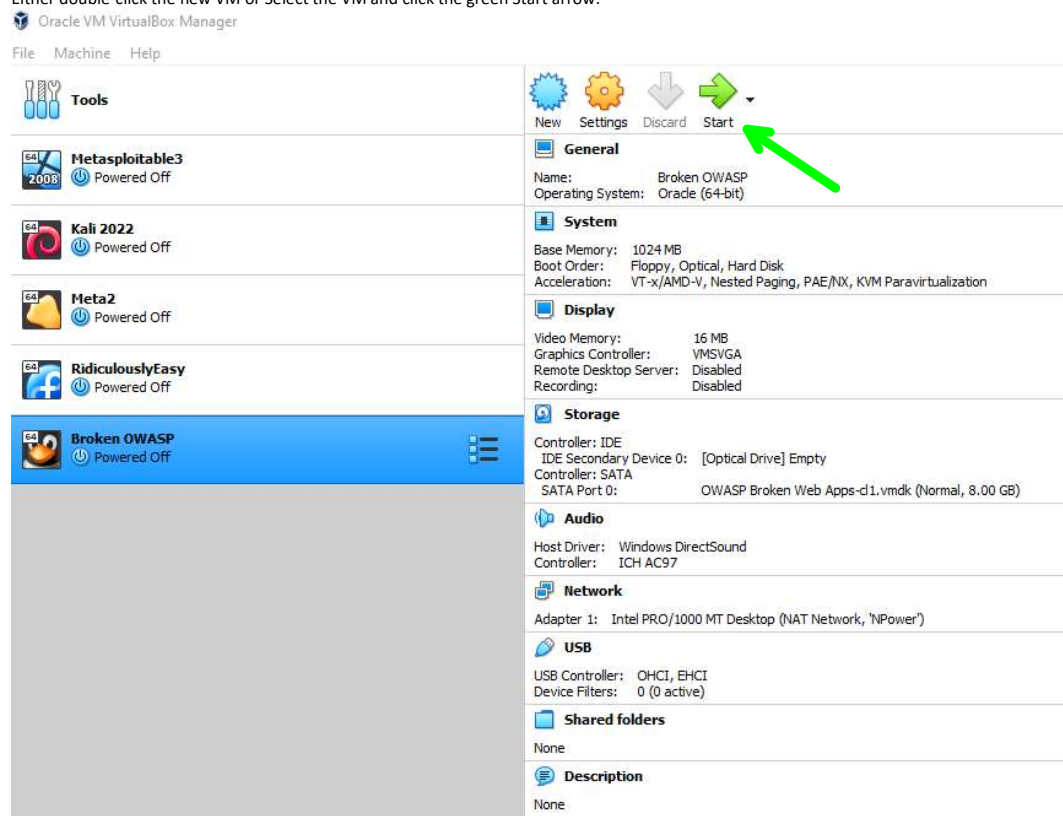
Make sure the Name: drop down menu is set for NPower.



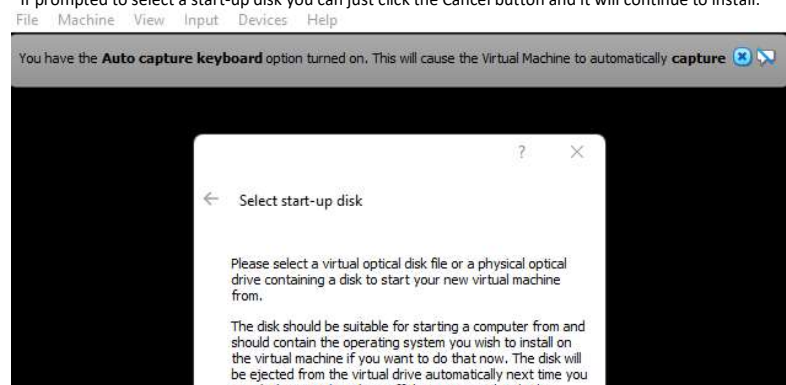
Click OK.

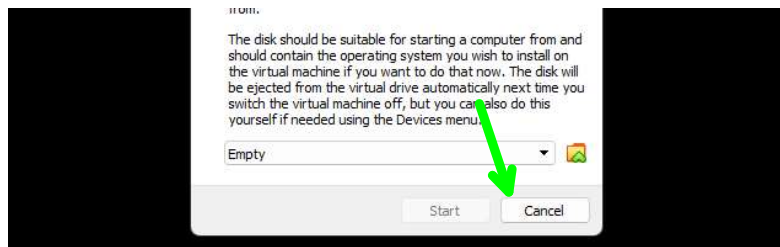


Either double-click the new VM or Select the VM and click the green Start arrow.

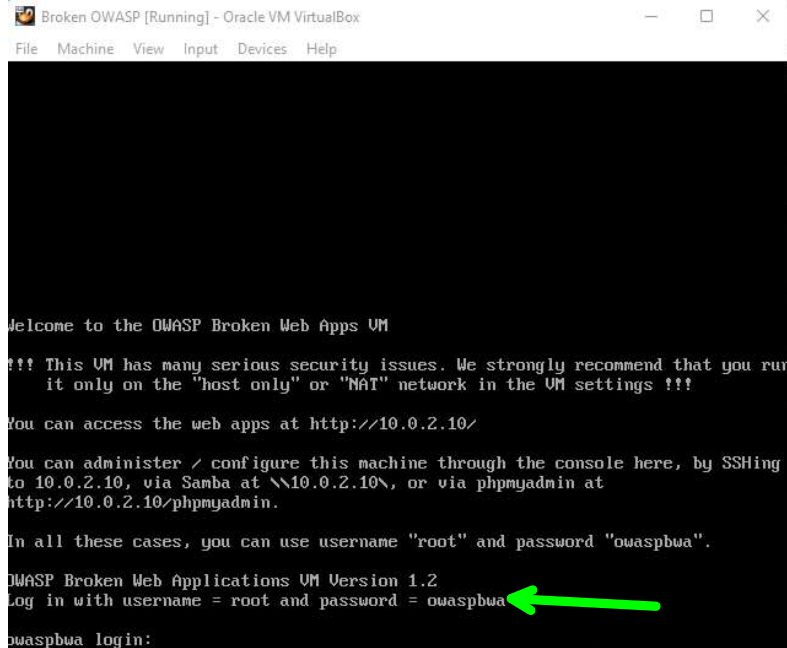


If prompted to select a start-up disk you can just click the Cancel button and it will continue to install.

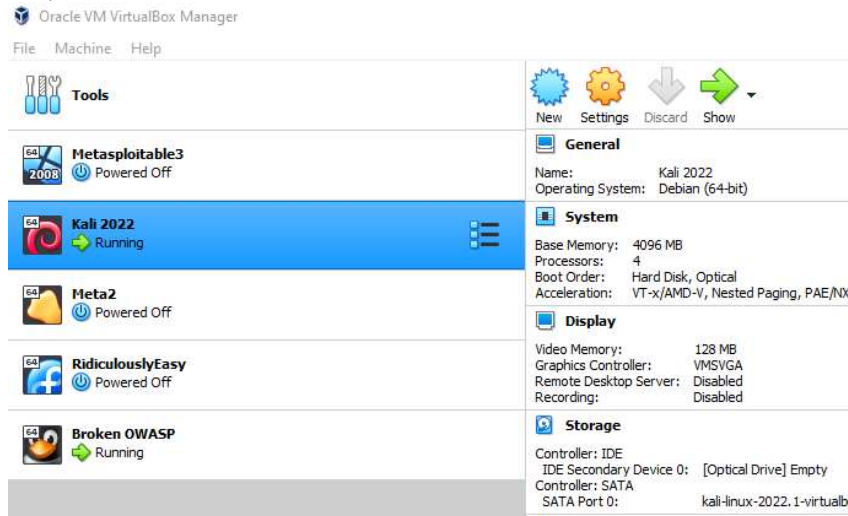




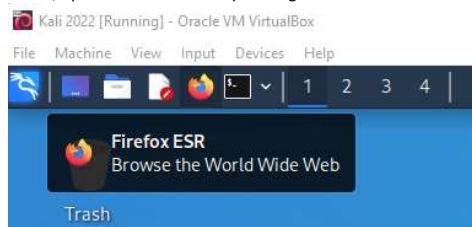
You will be prompted for a username and password. *The username is root and the password is owaspbwa. It is displayed on the screen*



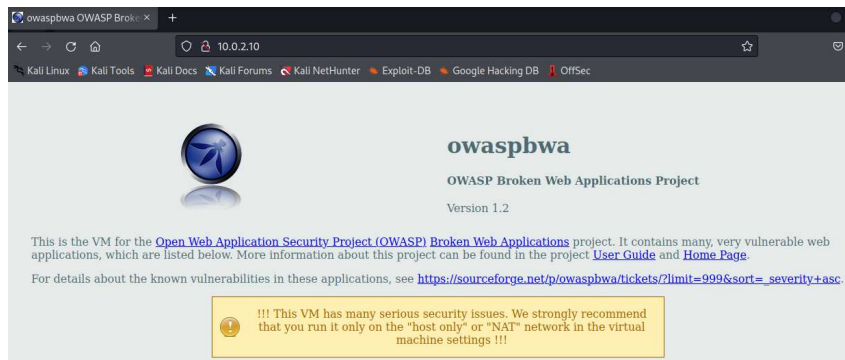
Start your Kali VM.



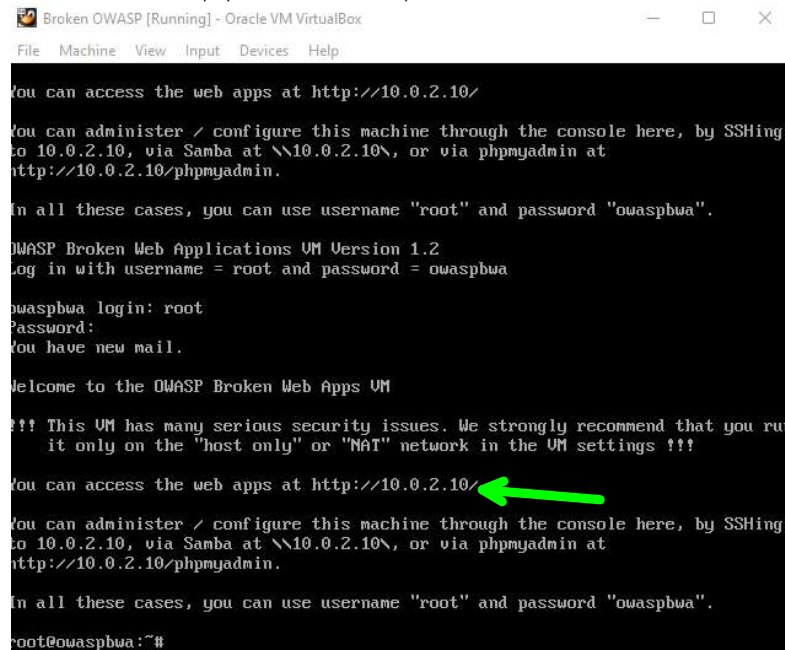
In Kali, open Firefox browser by clicking the Firefox ESR button located in the upper right.



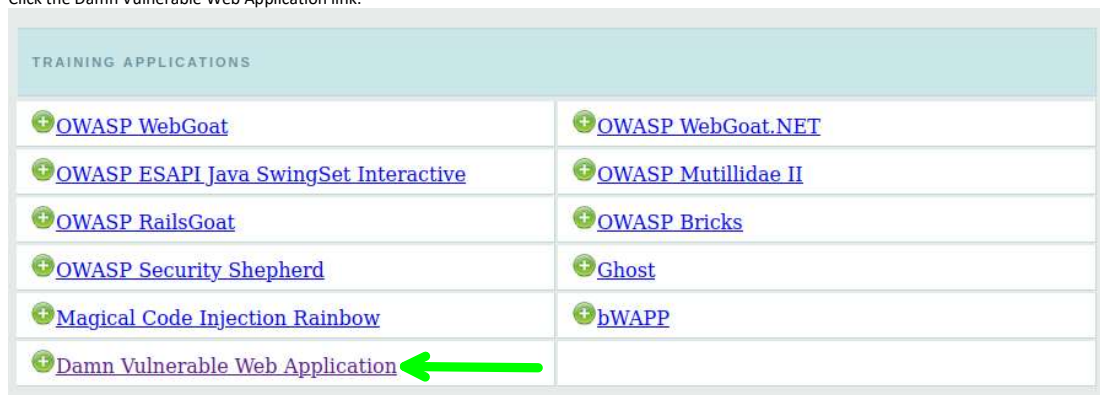
In the search bar of the browser, input the IP address of the Broken OWASP VM.



The IP address will be displayed on the Broken Owasp VM Window



Click the Damn Vulnerable Web Application link.



Use username admin and password admin to login.



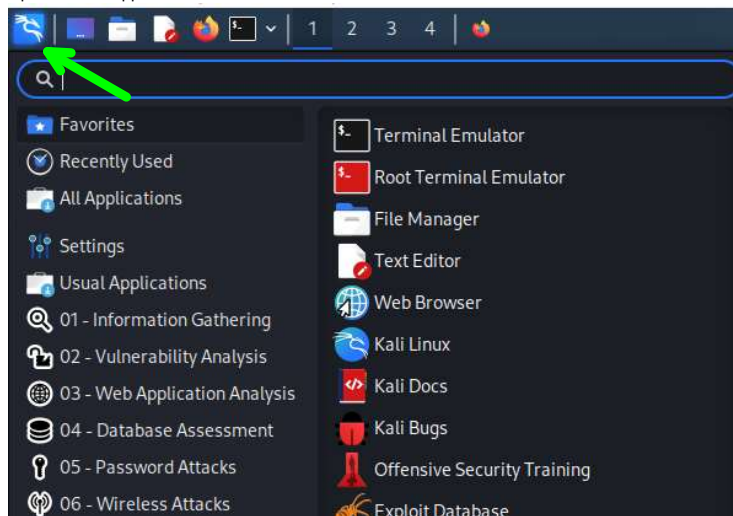
Username

Password

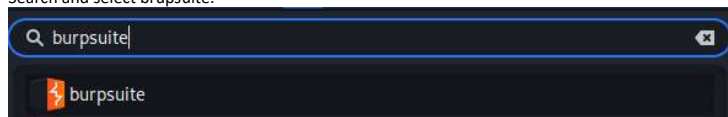
Login

You have logged out

Open the Kali Application Menu



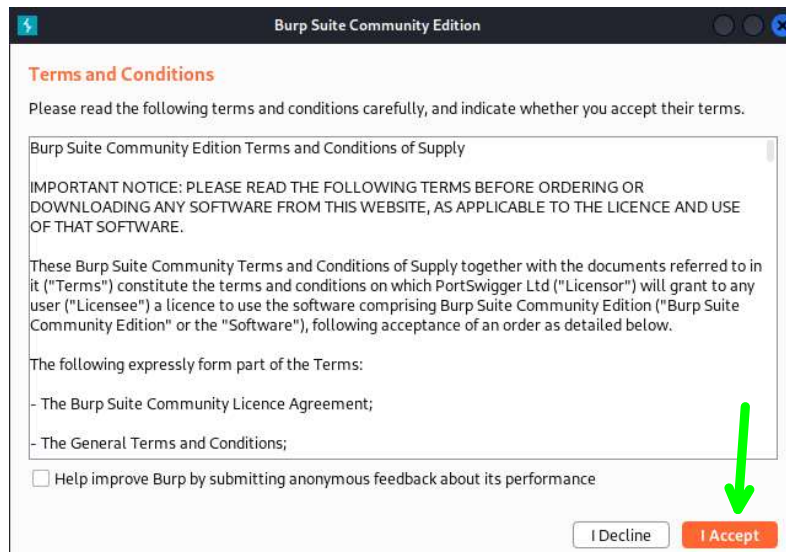
Search and select burpsuite.



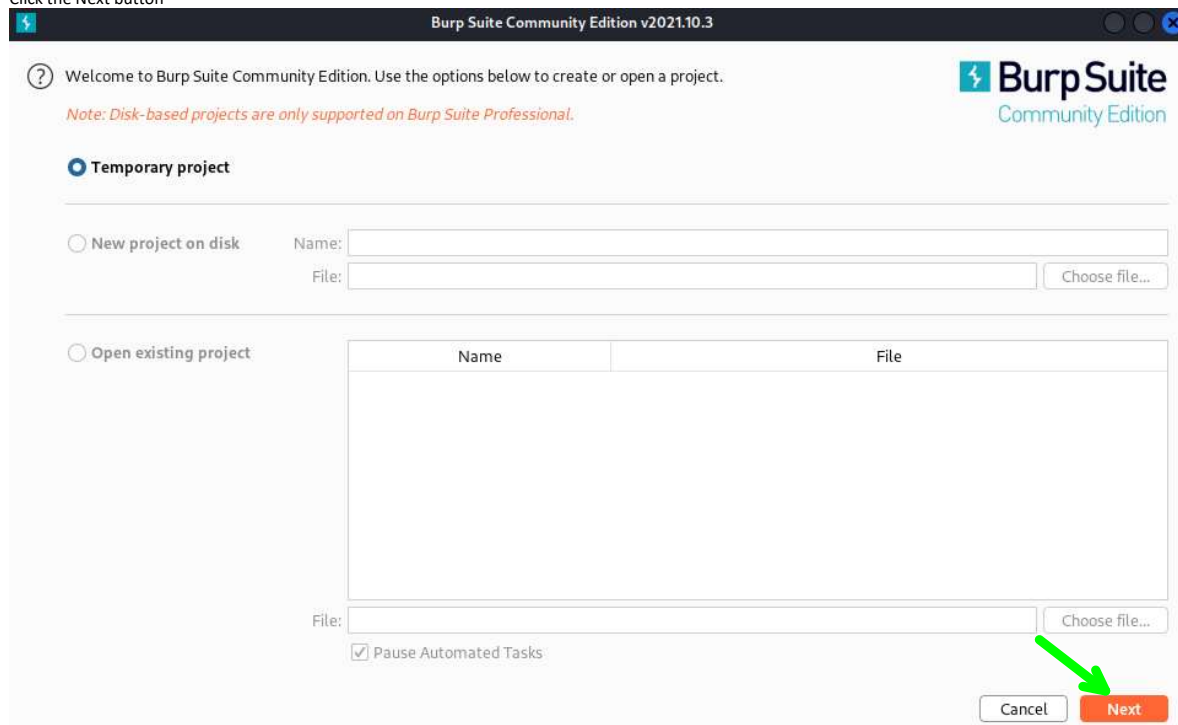
If you received this message, you can check the Don't show again for this JRE box and click OK



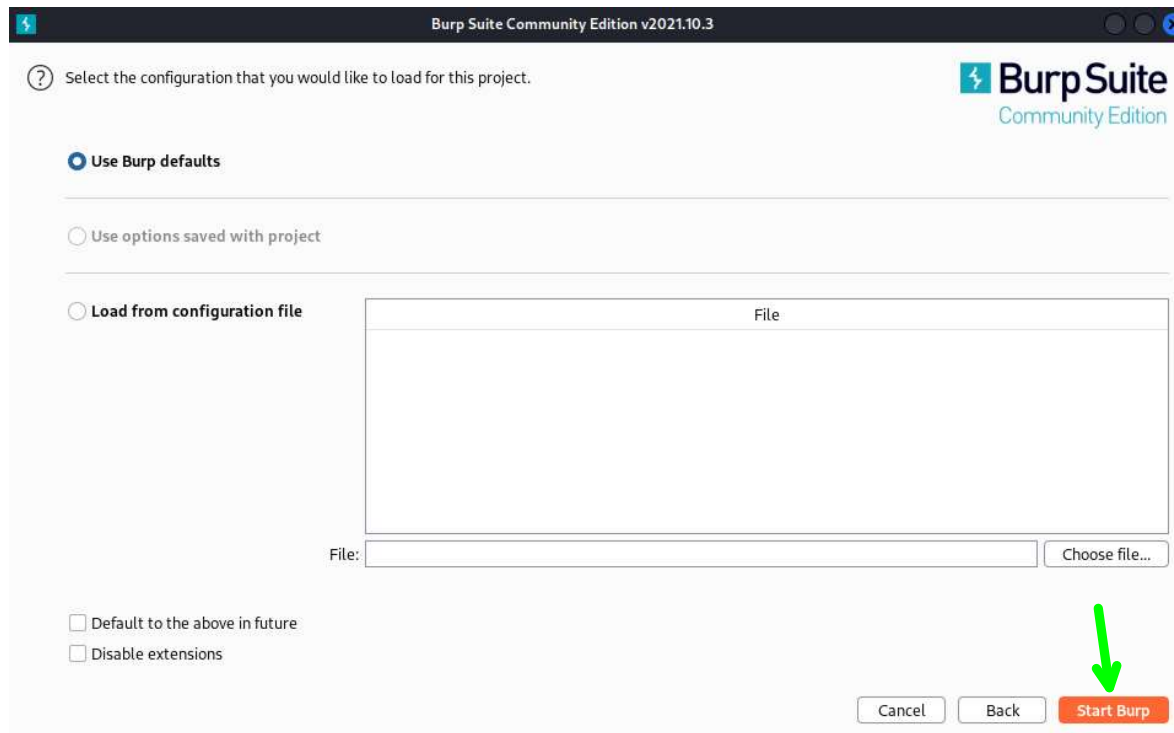
Click the I Accept button



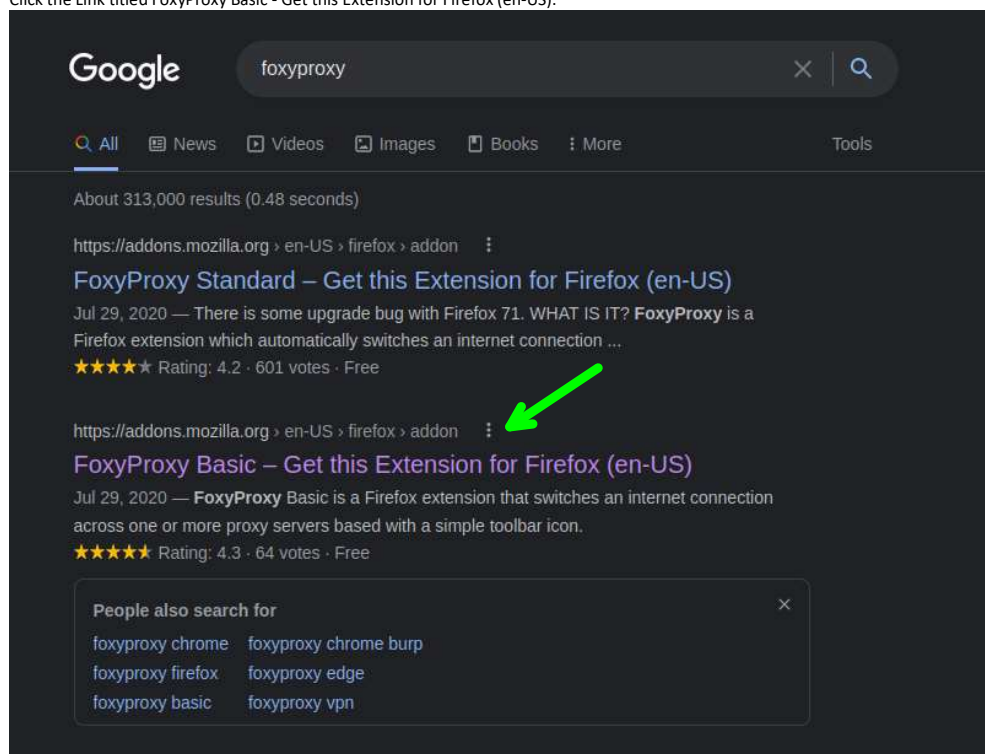
Click the Next button



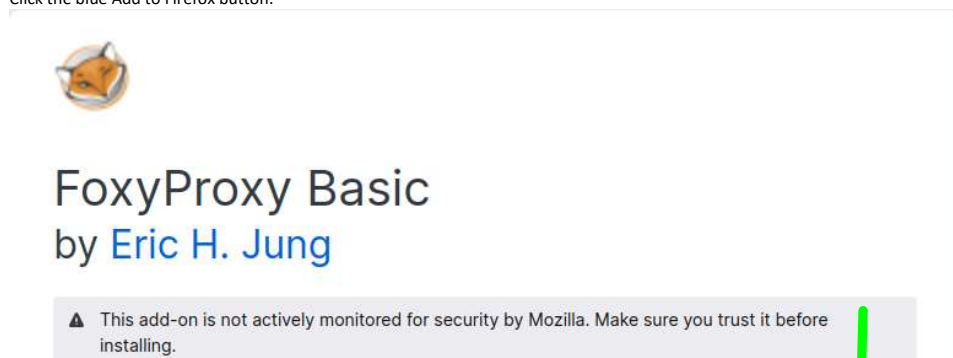
Click the Start Burp button



Click the Link titled FoxyProxy Basic - Get this Extension for Firefox (en-US).



Click the blue Add to Firefox button.



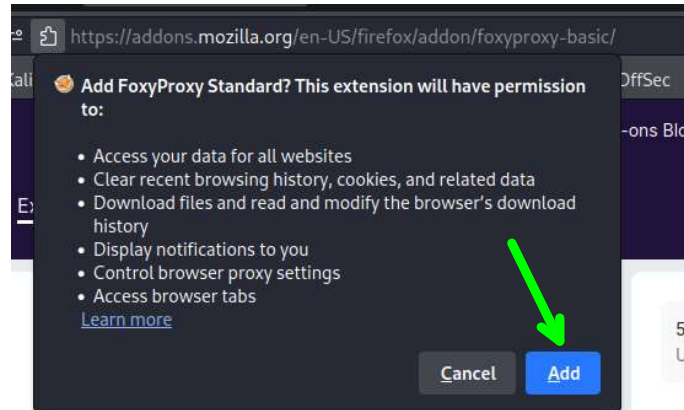
⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

[Learn more](#)

FoxyProxy Basic is a simple on/off proxy switcher. More advanced features and configuration options are offered by FoxyProxy Standard.

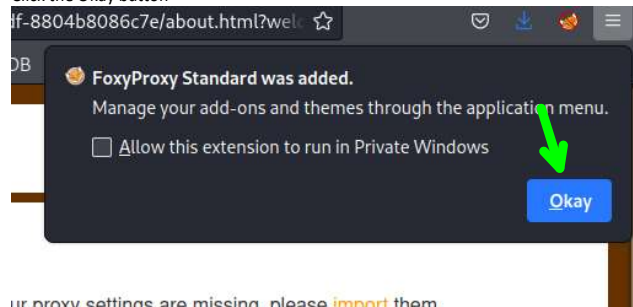
Add to Firefox

Click the blue Add button.



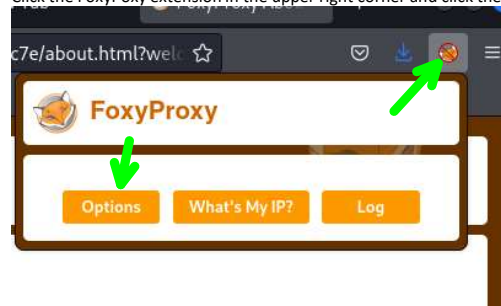
sic

Click the Okay button

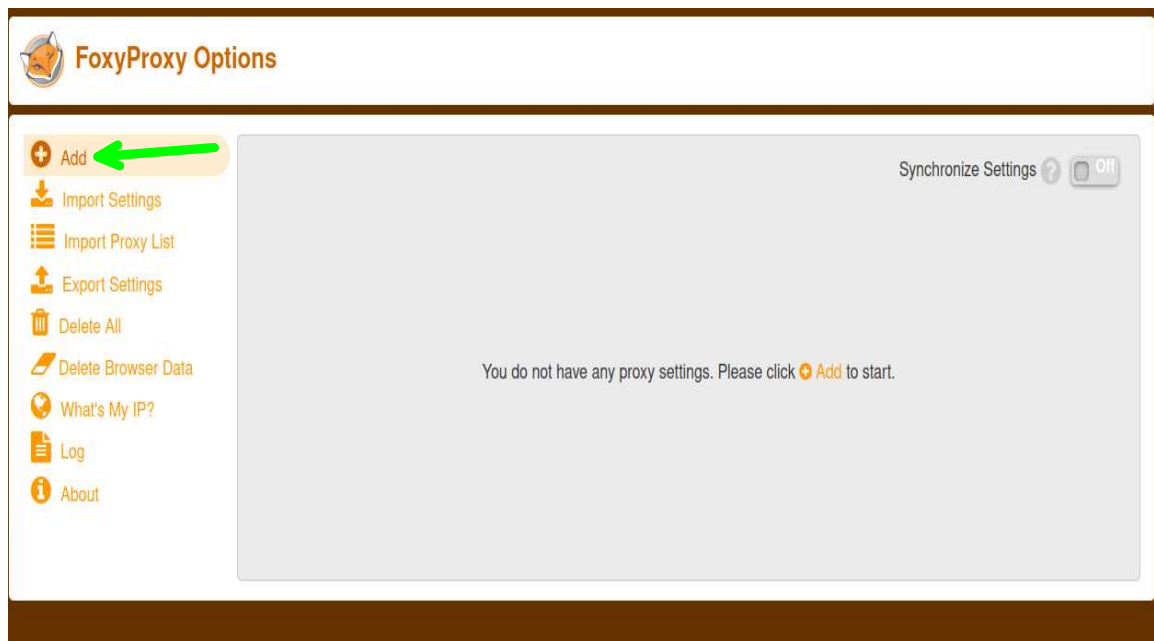


ur proxy settings are missing, please **import** them.

Click the FoxyProxy extension in the upper right corner and click the Options button.

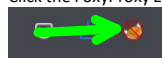


Click the Add tab in the left navigation menu.

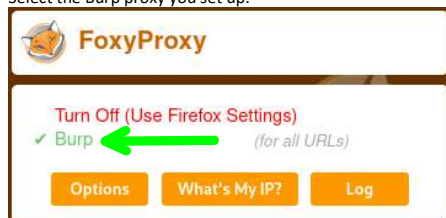


Input Burp for the Title Leave Proxy Type as HTTP, Input 127.0.0.1 as the Proxy IP Address and change the Port to 8080. Then click the blue Save button.

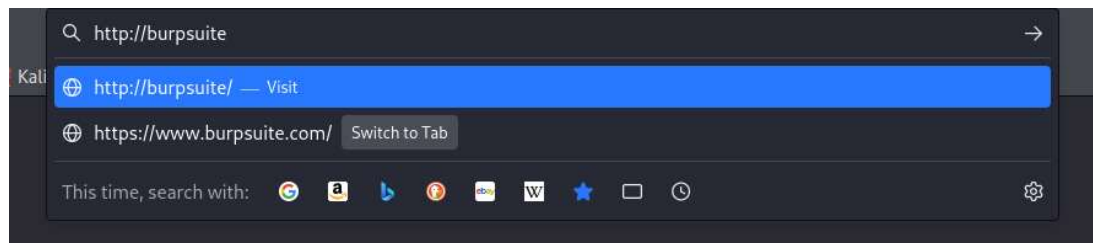
Click the FoxyProxy Extension in the upper right corner.



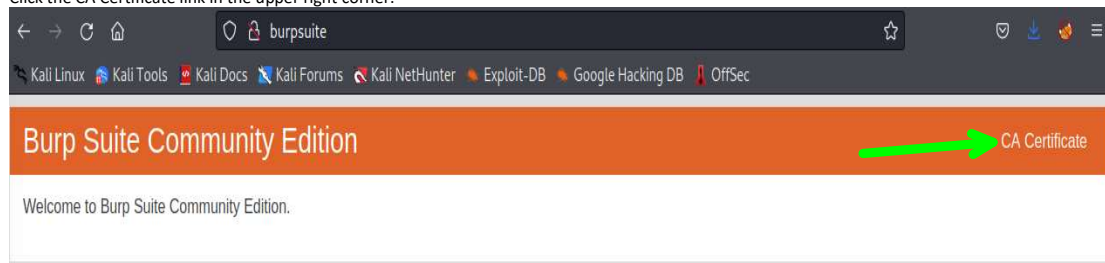
Select the Burp proxy you set up.



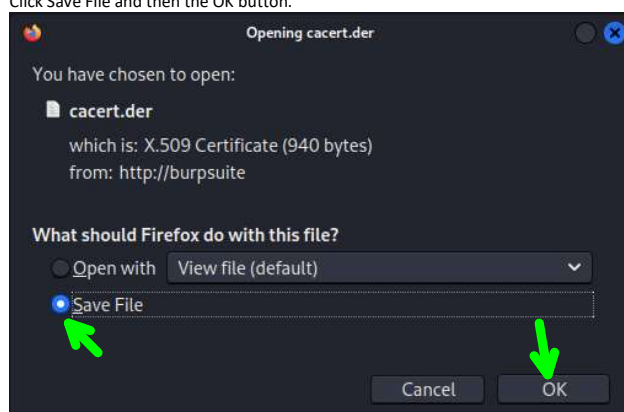
Input <http://burpsuite> in the search browser.



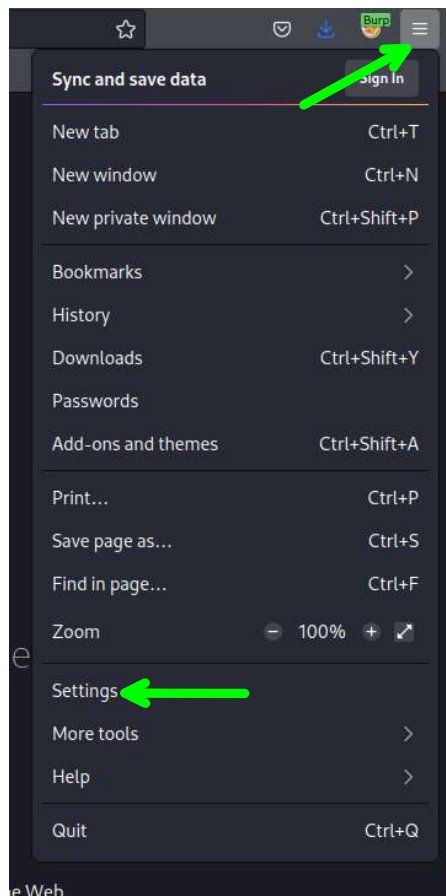
Click the CA Certificate link in the upper right corner.



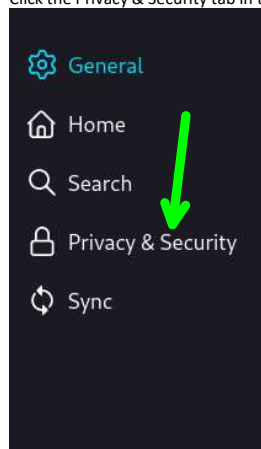
Click Save File and then the OK button.



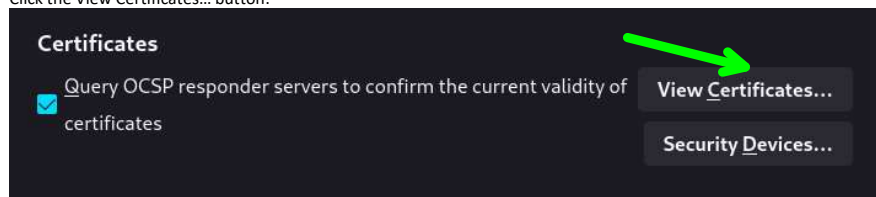
Click the three horizontal lines in the right upper corner (Hamburger Menu) and select Settings.



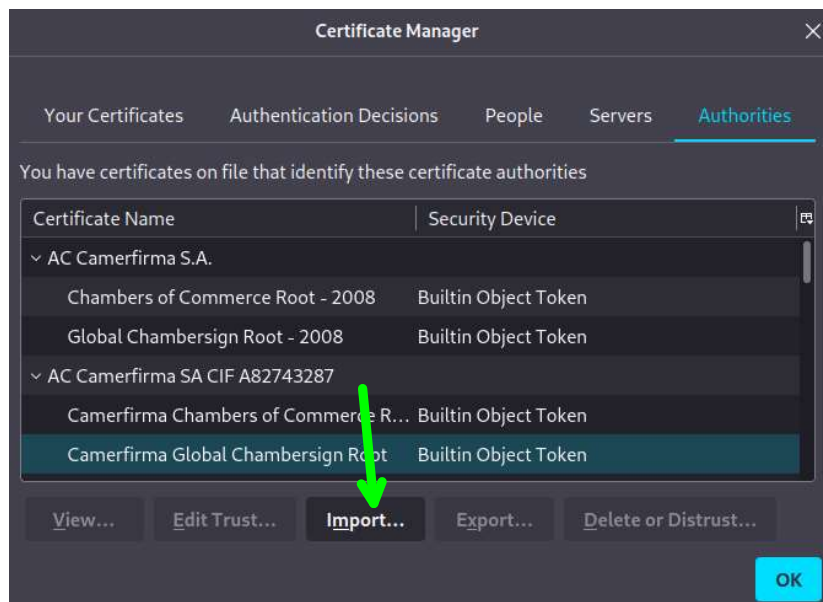
Click the Privacy & Security tab in the left navigation menu.



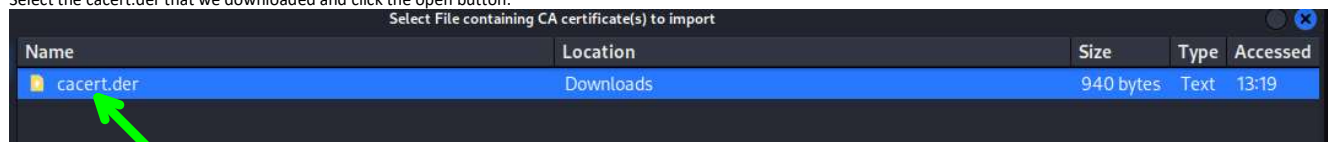
Click the View Certificates... button.



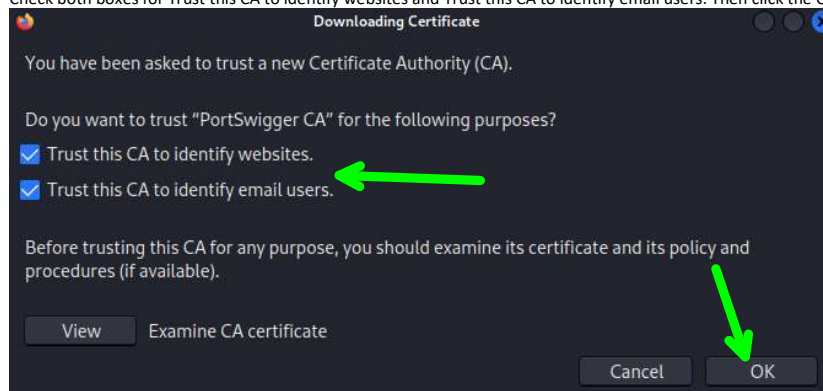
Click the Import... button.



Select the cacert.der that we downloaded and click the open button.



Check both boxes for Trust this CA to identify websites and Trust this CA to identify email users. Then click the OK button.



Reload the Damn Vulnerable Web App page and you should see a response in burp suite.



Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to https://cdn.syndication.twimg.com:443 [72.21.91.70]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Hex

```

1 GET /timeline/profile?callback=_twtr.callbacks.tl_i0_profile_zaproxy_new&dnt=false&domain=owasp.org&lang=en&min_position=1537823718117888000&screen_name=zaproxy&suppress_response_codes=true&t=1839813&tz=GMT-0400&with_replies=false HTTP/1.1
2 Host: cdn.syndication.twimg.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Sec-Fetch-Dest: script
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Site: cross-site
10 If-Modified-Since: Tue, 21 Jun 2022 17:18:21 GMT
11 Te: trailers
12 Connection: close
  
```

Click the OWASP ZAP Zed Attack Proxy

Google owasp zap

All Videos Images News Shopping More Tools

About 587,000 results (0.40 seconds)

Ad • https://www.soos.io/

Automate ZAP Scanning - Advanced ZAP DAST Tooling

Integrations with leading tools. Simplify testing for free today! Shift DAST Left. **OWASP** Dynamic Application Security Testing - No Limit Web App Scanner. GitHub Integration.

Free Trial

Start with SOOS today! No CC required, cancel any time.

Pricing

A plan for your whole team. Unlimited projects. No scan limits.

About SOOS

Meet the SOOSTers. Try Us out!

Soos Blog

We've Got You Covered. Learn More!

https://owasp.org › www-project-zap

OWASP ZAP Zed Attack Proxy

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by a dedicated international team of ...

Click Download now

OWASP ZAP

For more details about ZAP see the main ZAP website at zapproxy.org.



[Home](#) [ZAP in Ten](#) [Documentation](#) [Get Involved](#) [Support](#)

[Download](#)



OWASP Zed Attack Proxy (ZAP)

The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.



[Quick Start Guide](#)

[Download now](#)



Tweets by @zapproxy



Zed Attack Proxy

@zapproxy

ZAP needs your help! zapproxy.org/blog/2022-06-1...



Help Needed: Fund ZAP Development

Has ZAP helped you? Now it is your turn to help ZAP



Tweets by @zapproxybot



zapbot

@zapproxybot

Where is @zapproxy installed? zapproxy.org/faq/where-is-z...



14h

Click Download now again.

OWASP ZAP

For more details about ZAP see the main ZAP website at zapproxy.org.



[Home](#) [ZAP in Ten](#) [Documentation](#) [Get Involved](#) [Support](#)

[Download](#)



OWASP Zed Attack Proxy (ZAP)

The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.



[Quick Start Guide](#)

[Download now](#)



Click the Download button for the Linux Installer.

ZAP 2.11.1

Windows (64) Installer

183 MB

[Download](#)

Windows (32) Installer

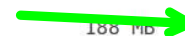
183 MB

[Download](#)

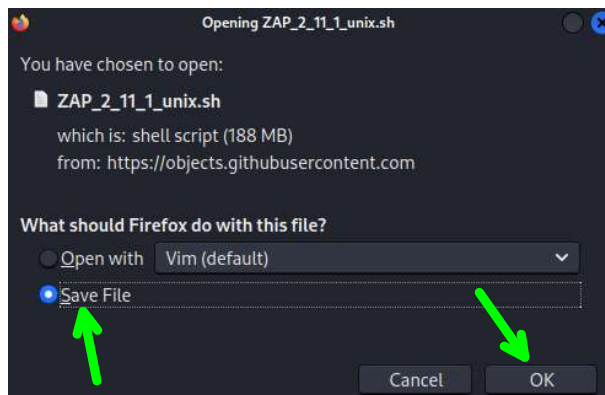
Linux Installer

188 MB

[Download](#)



Click Save File and OK.



Open a Terminal by clicking the terminal button in the upper right.



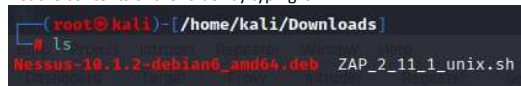
Sudo su for root privileges.



Change the directory to the Downloads directory.



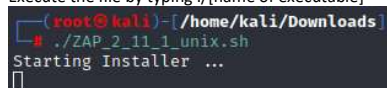
List the contents of the folder by typing ls.



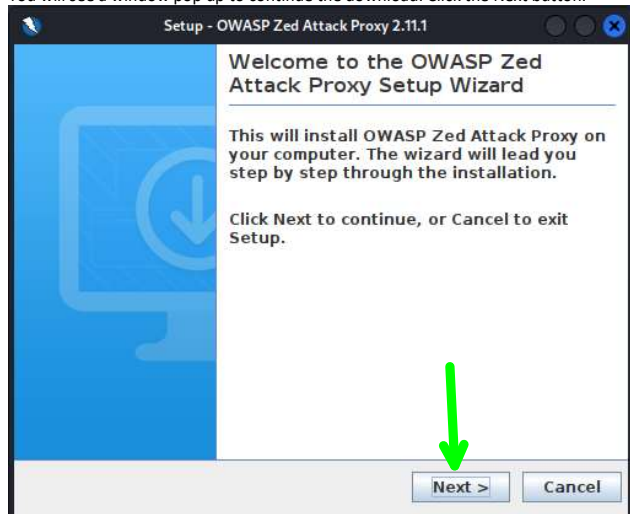
Add the executable permissions to ZAP_2_11_1_unix.sh file by typing chmod +x [name of file.]



Execute the file by typing ./[name of executable]



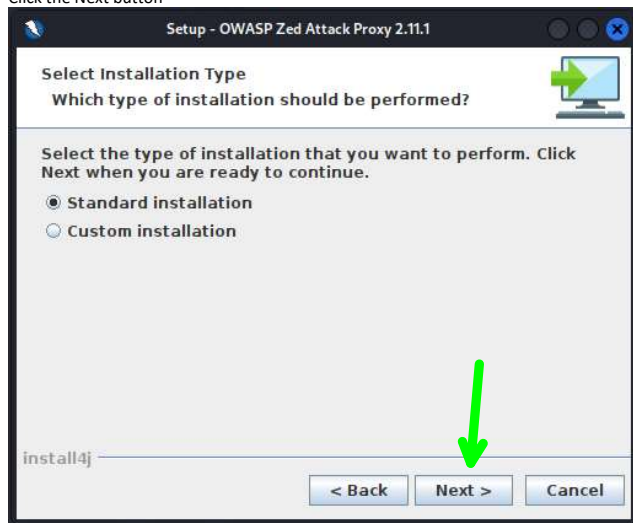
You will see a window pop up to continue the download. Click the Next button.



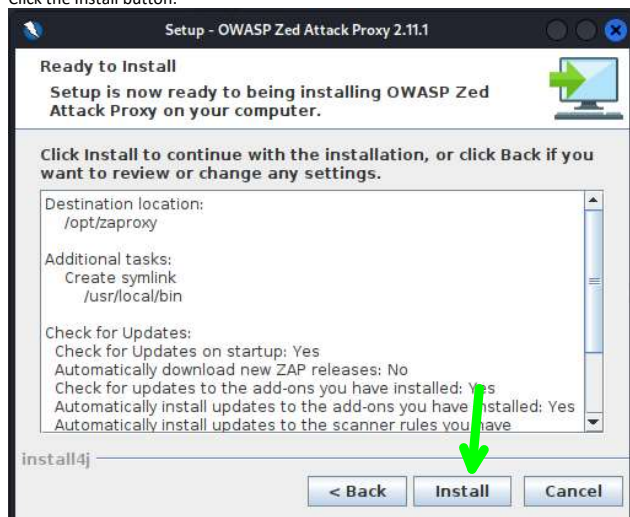
Click the I accept the agreement and click the Next button.



Click the Next button



Click the Install button.



Click the Finish button.

