Task 9

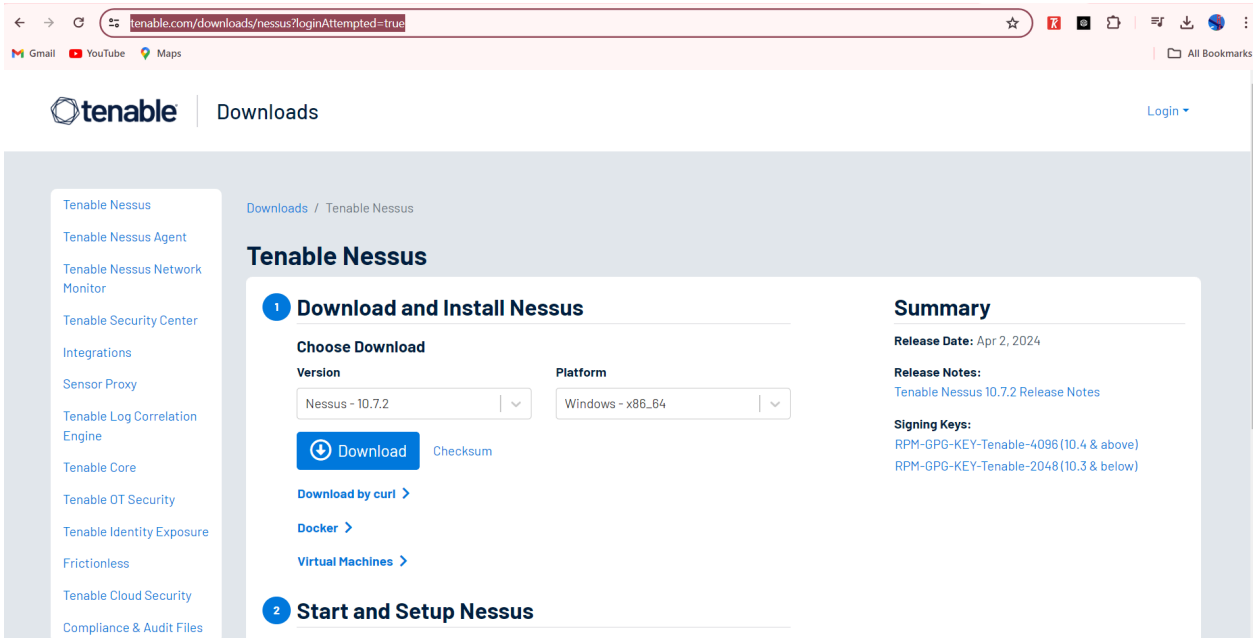
A. Perform different scans on your network using the Nessus tool and generate a report.

a) Host Discovery Scan

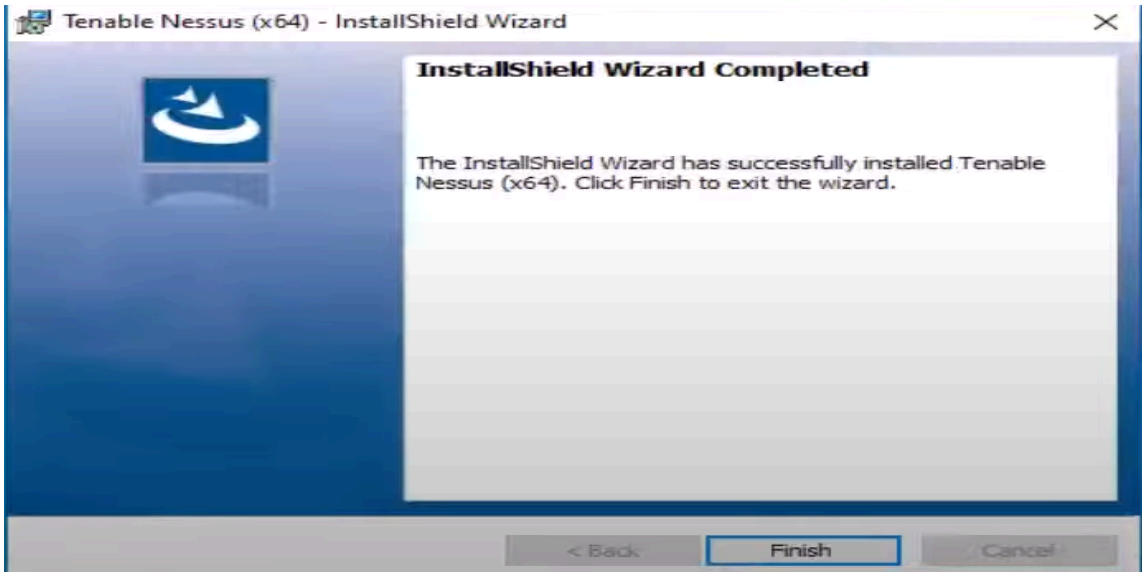
b) Basic Network Scan

Step 1 : Go to the Google chrome and download the Nessus tool

https://www.tenable.com/downloads/nessus?loginAttempted=true : link to download

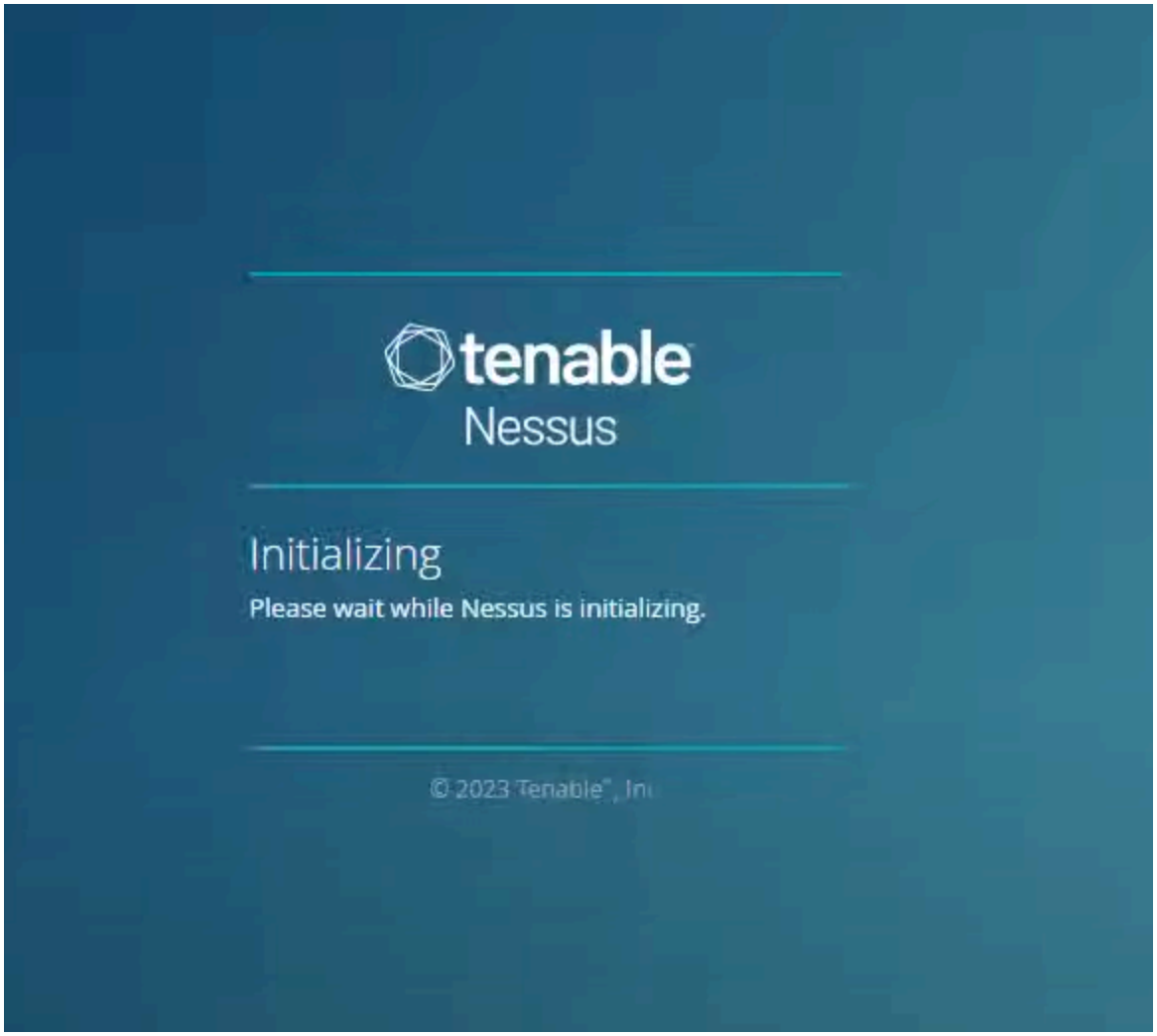


Step2 : Once you have download and have an msi file just double click and download the default and finish it

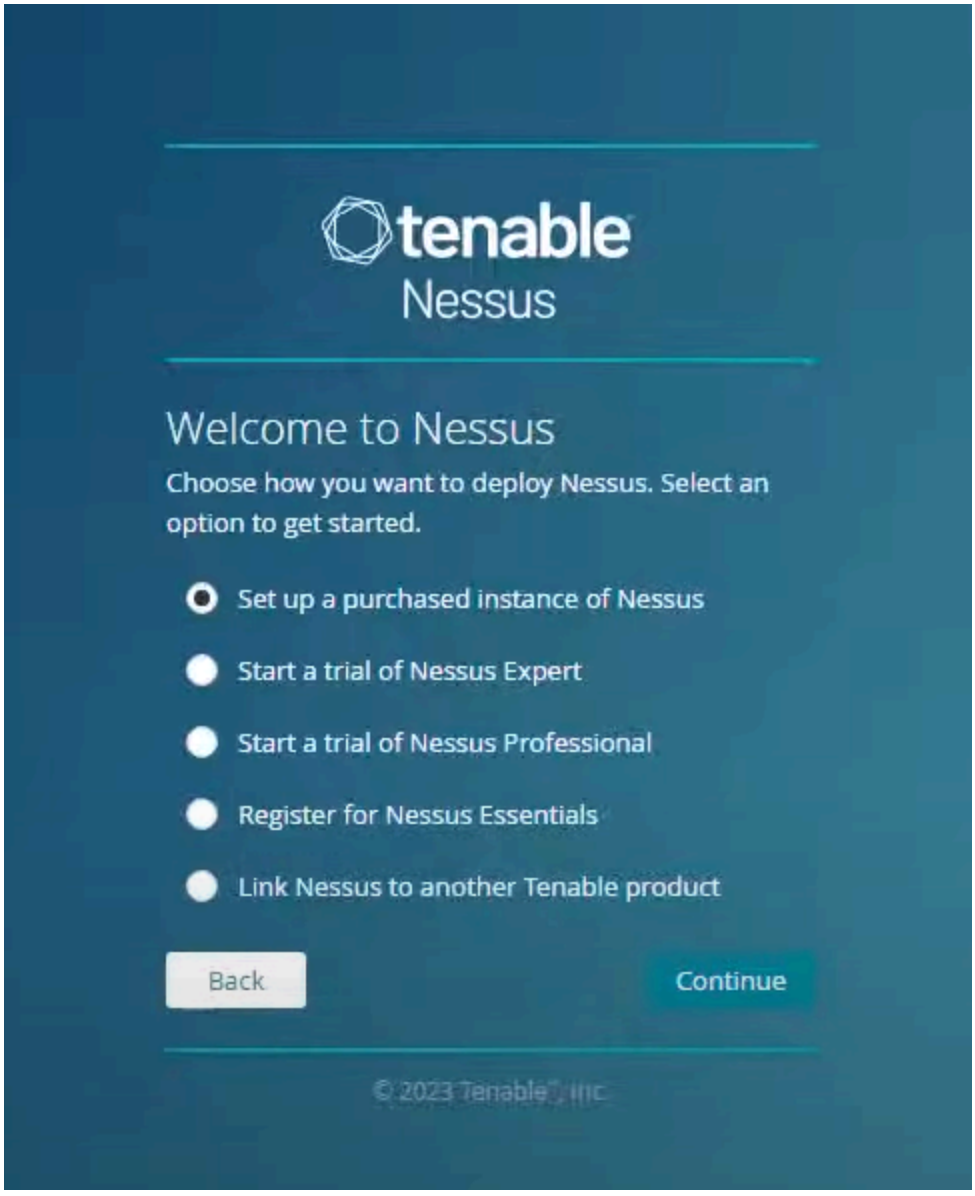


Step 3 : Once we click on finish we will a interface of nessus, in which we have connect to ssl button click on it then first we will get a error which connection is not secure, so just click on advance connection and continue to localhost

Step 4 : Then the nessus tool will go to the initializing we will let it initialize on its own



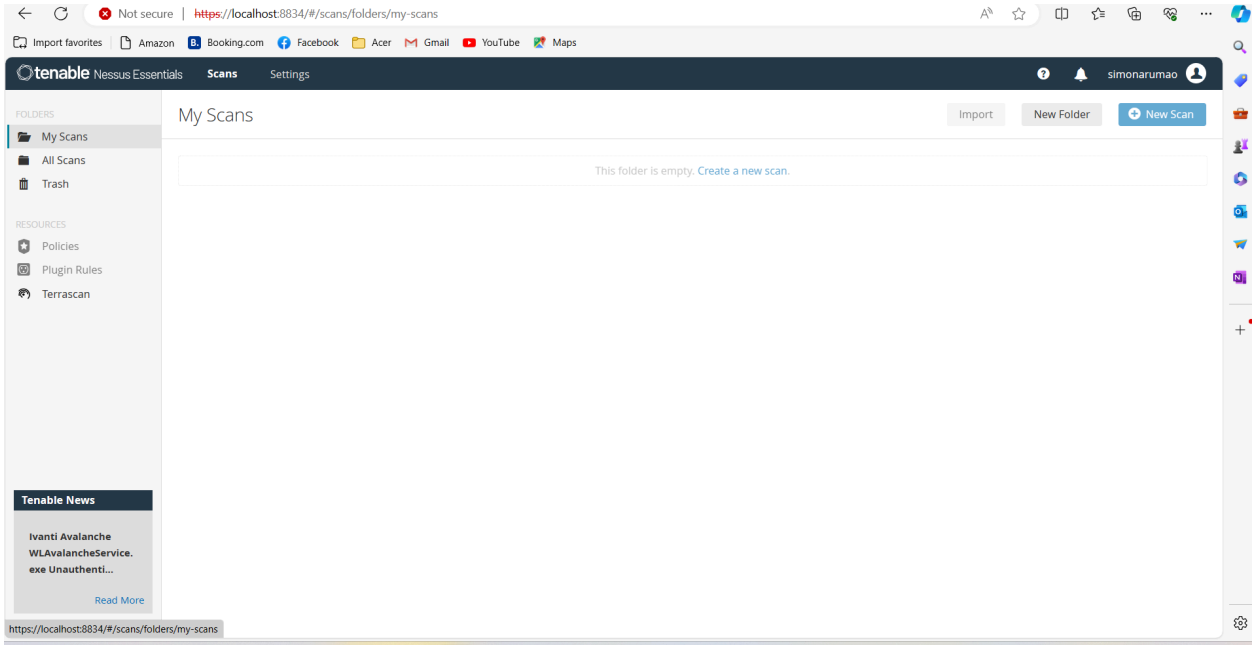
Step 5 : Then we will get a option to deploy nessus and most of them are the enterprise versions so will start with “register for nessus essentials”



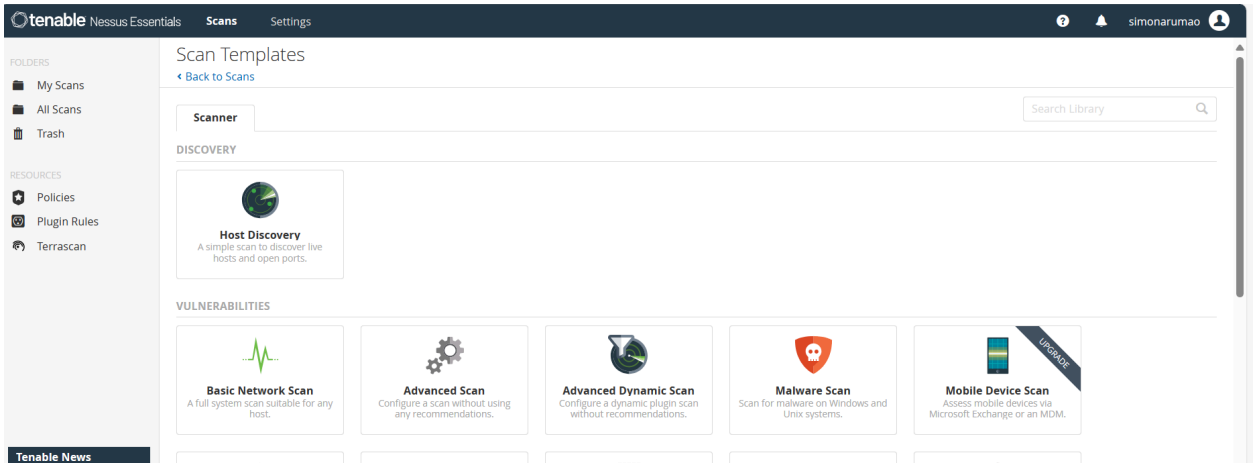
Step 6 : Then we get the option to register yourself, here the issue you might encounter is you will try to put your email address but that won't work as it requires work email so will put an email for the temp mail(a temporary mail website) and register with username and password
Step 7 : Then will see the license information just click on continue
Step 8 : Then will get an option to get sign in into the scanner using username and password
Step 9 : Now it keep on initializing and we will enter into the nessus tool, but here the nessus tool will take some time to get all the plugins, on the top right corner there is a circle if that stops means all plugins are installed and now we are ready to test the vulnerability

1) HOST DISCOVERY SCAN

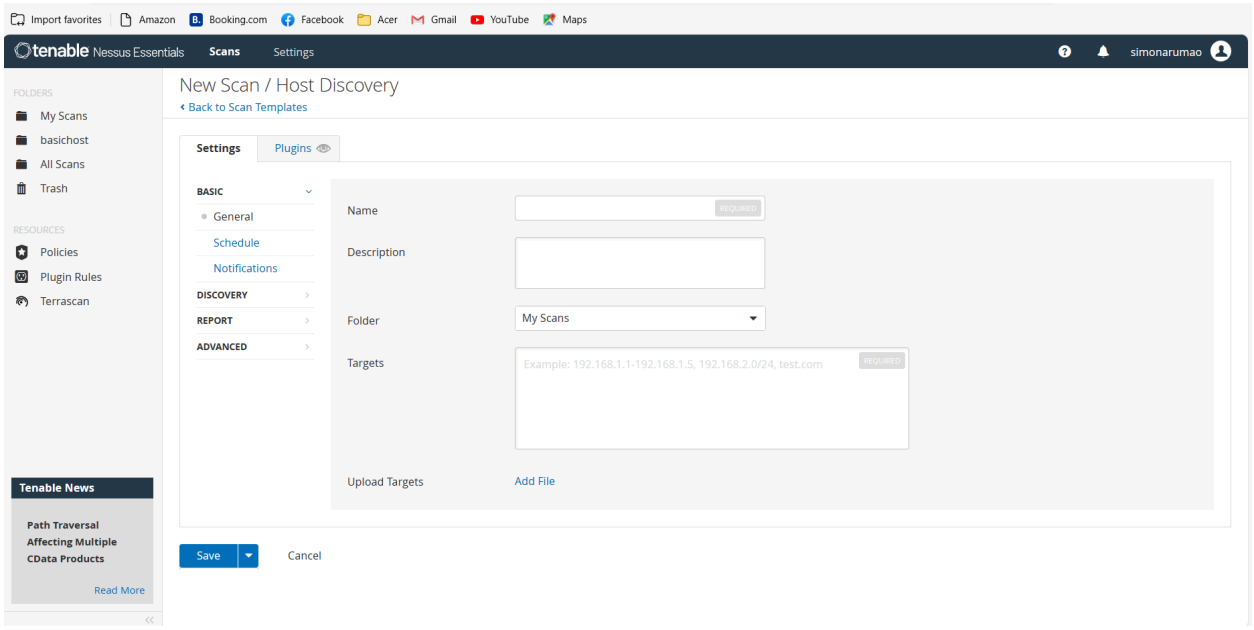
Step 10 : Now we will start the scan for host discovery, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



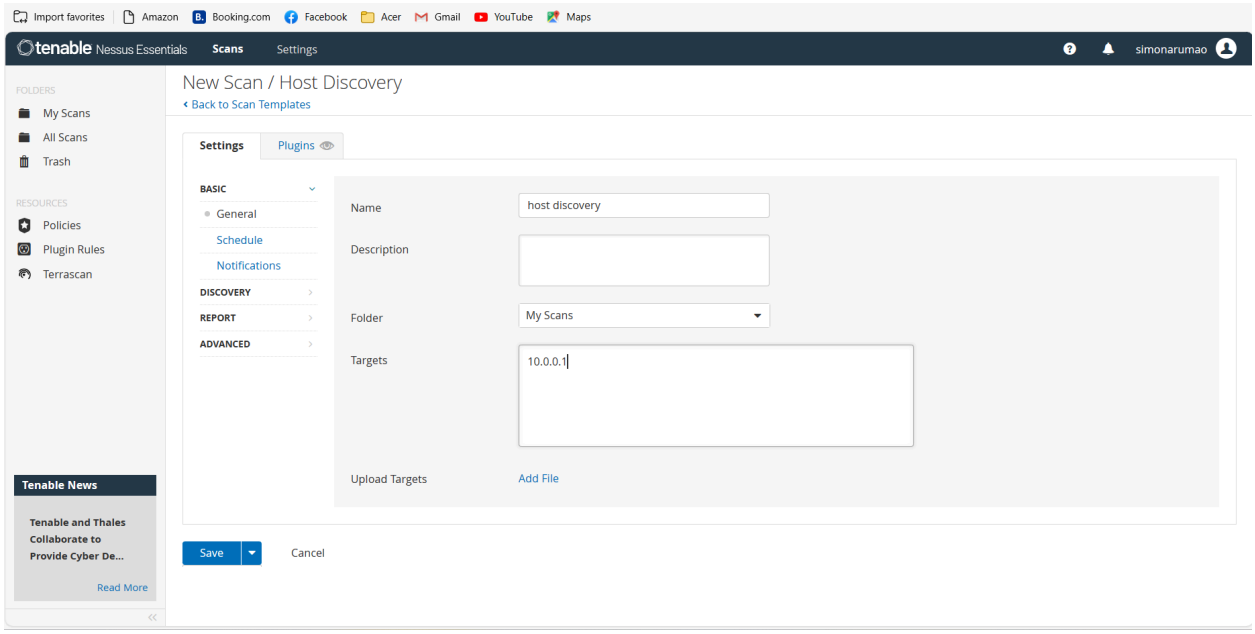
Step 11 : When you click on new scan we can see various templates in that scan, the first template is itself about the host discovery, click on that template



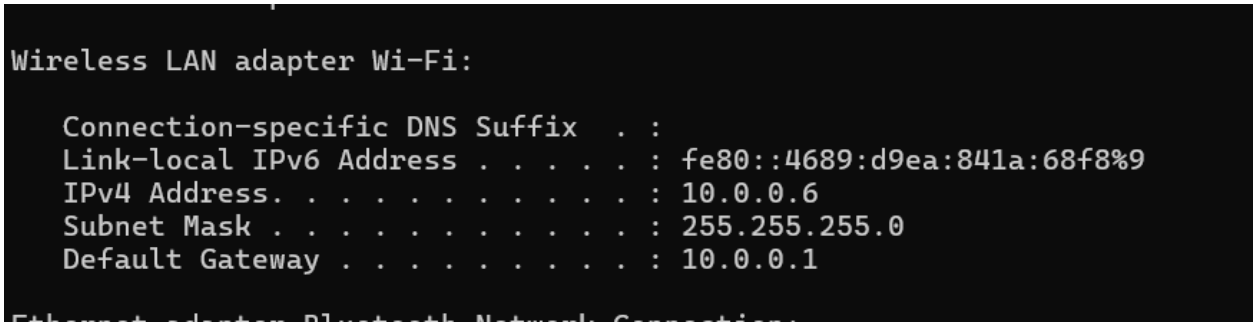
Step 12: Then a form like scan template will open in this we will fill the basic details



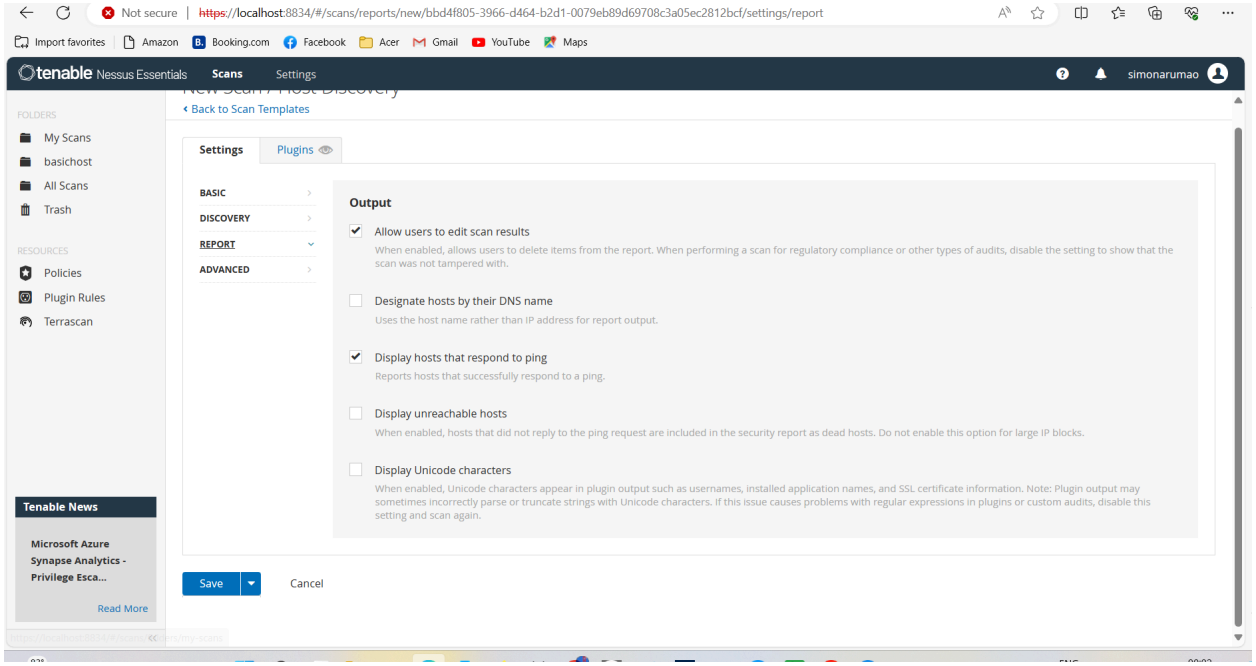
Step 13 : In this templates first we will give our scan a name, then in the field of targets we will put our network ip address(like router ip address)



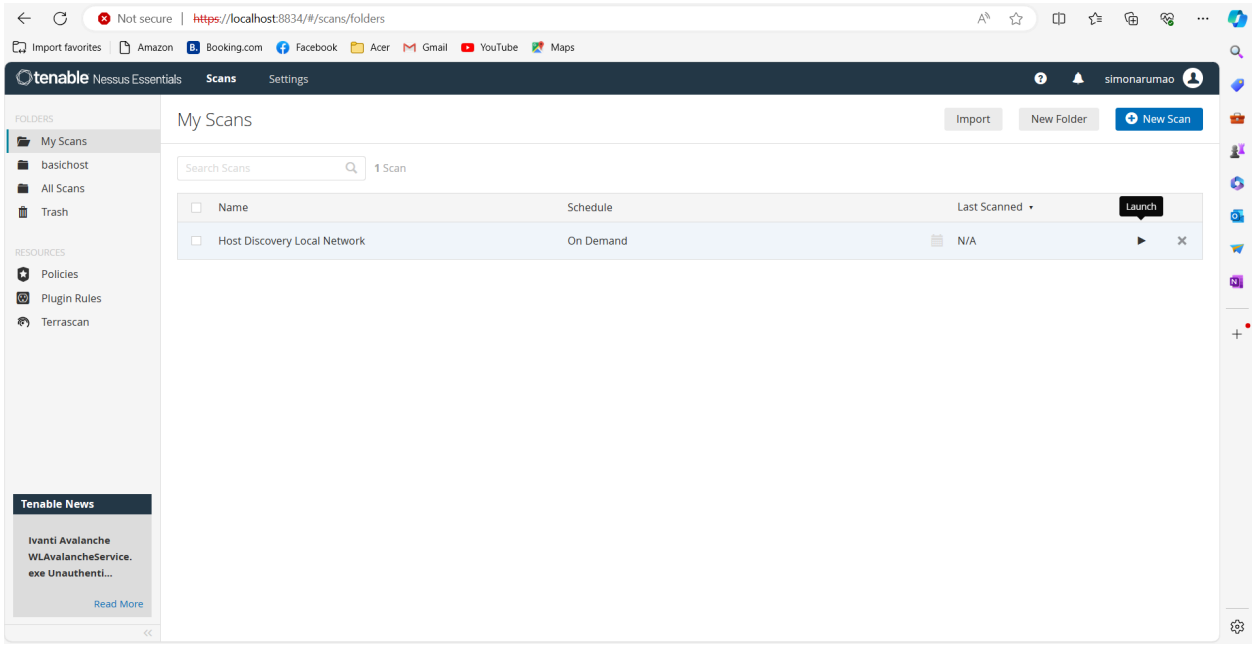
Step 14 : To get router ip address, go command prompt and type ipconfig and see the wifi section and you will router address under the name of default gateway



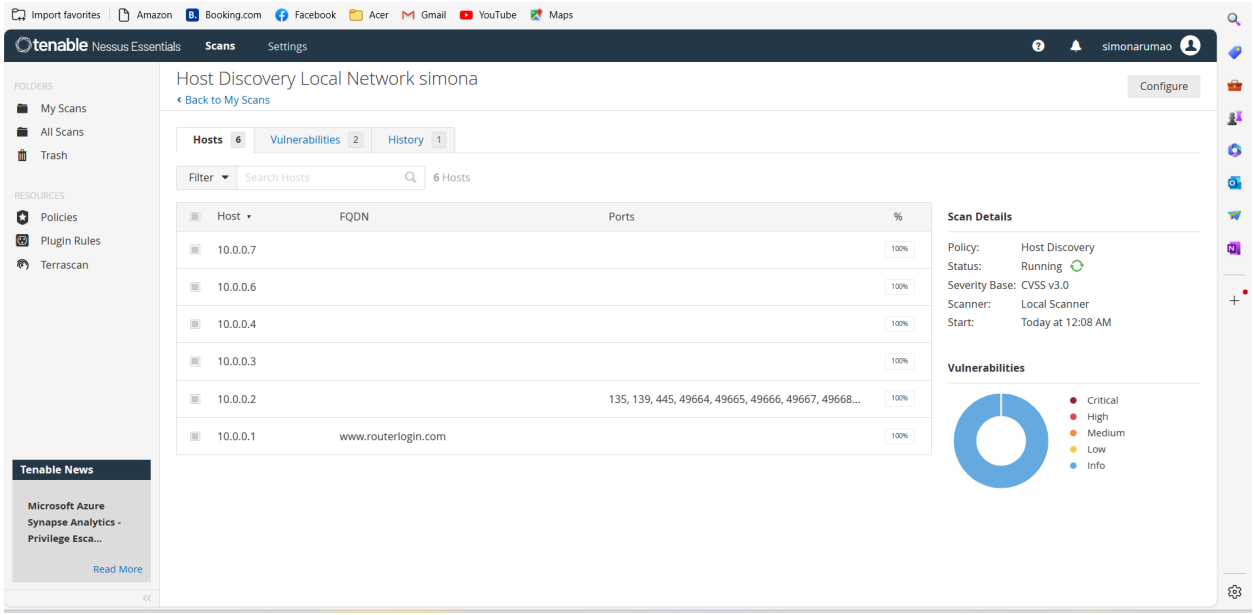
Step 15: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default

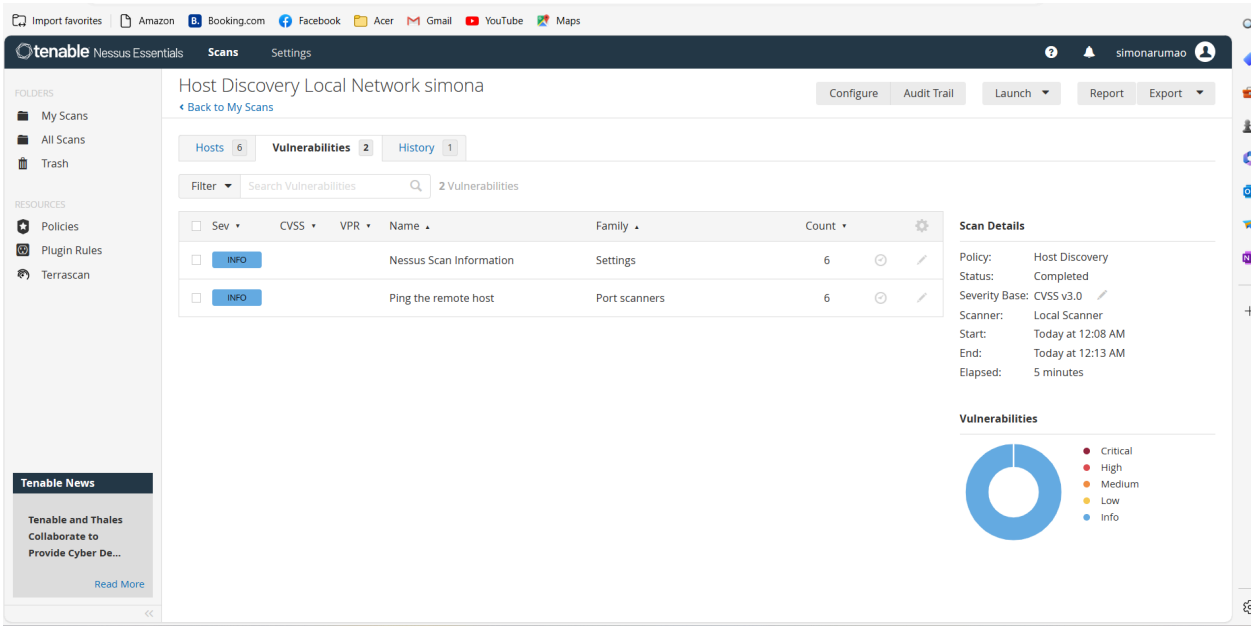


Step 16 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

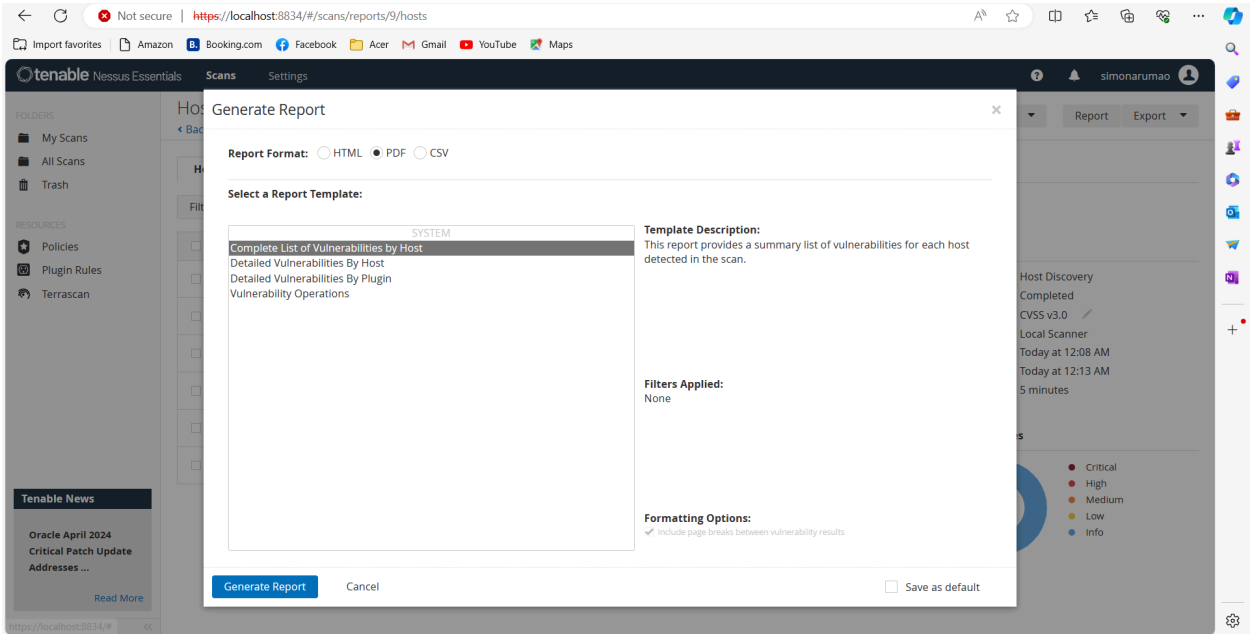


Step 17:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities





Step 18 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



10.0.0.1

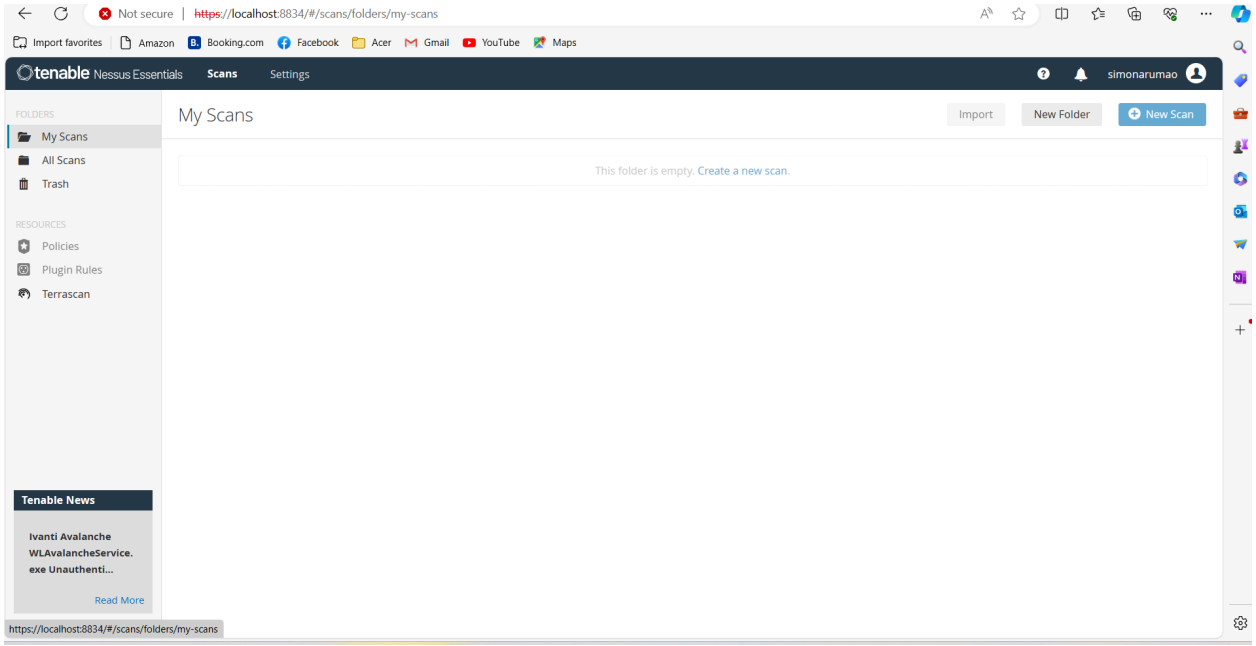
Vulnerabilities Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

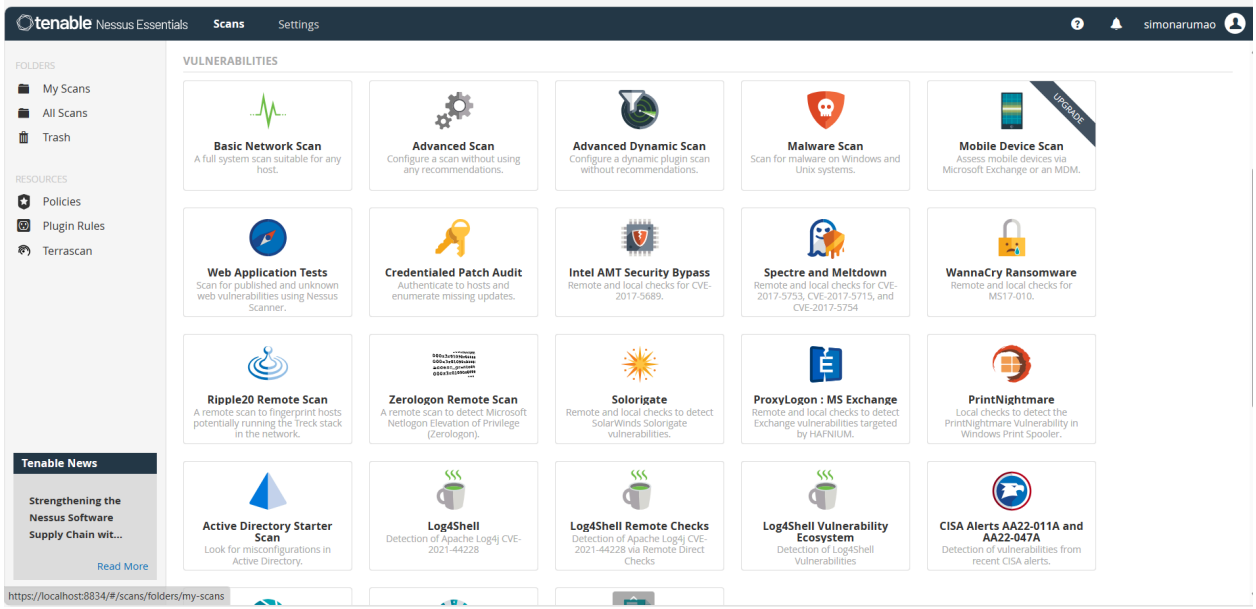
* indicates the v3.0 score was not available; the v2.0 score is shown

2) BASIC NETWORK SCAN

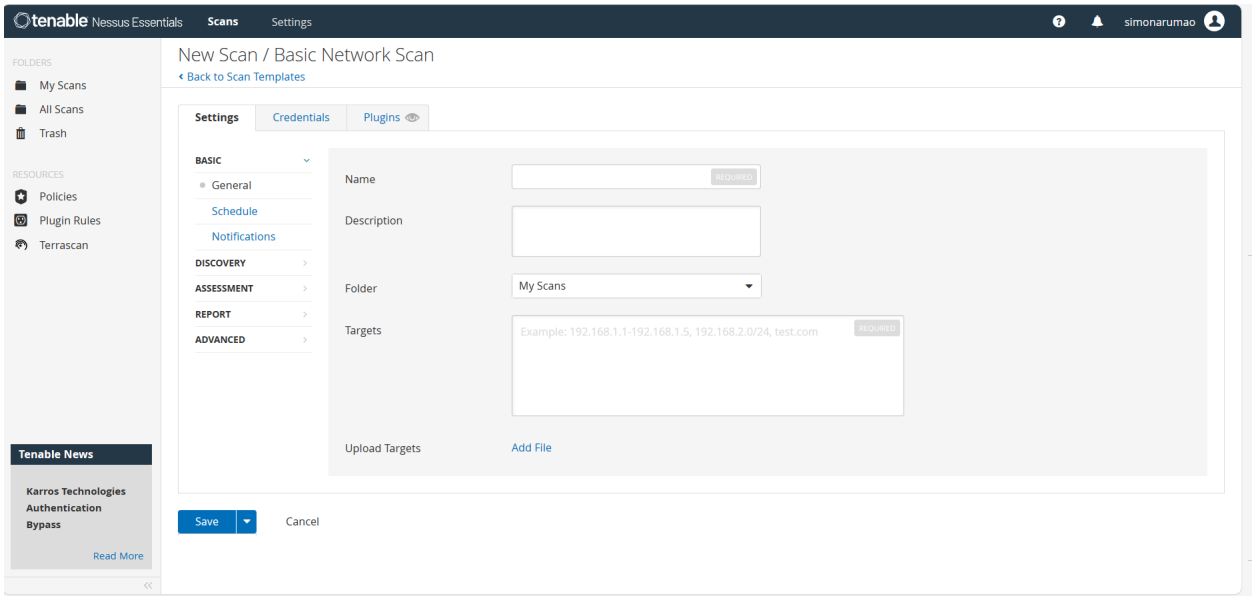
Step 1 : Now we will start the scan for basic network scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



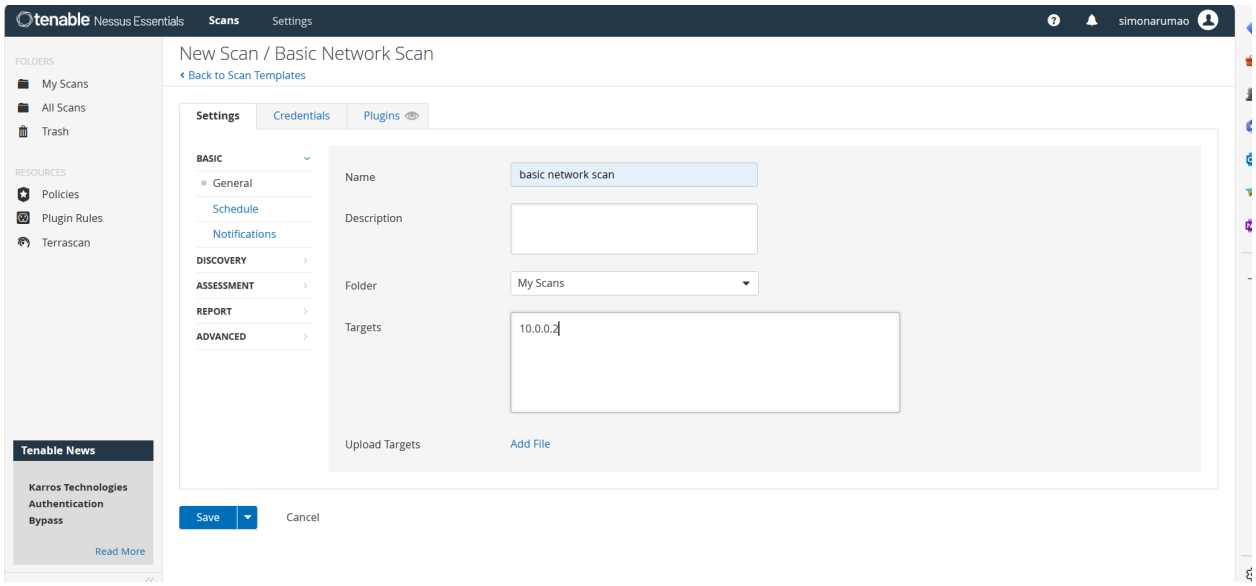
Step 2 : When you click on new scan we can see various templates in that scan, the first template is in the vulnerabilities itself is about the basic network, click on that template



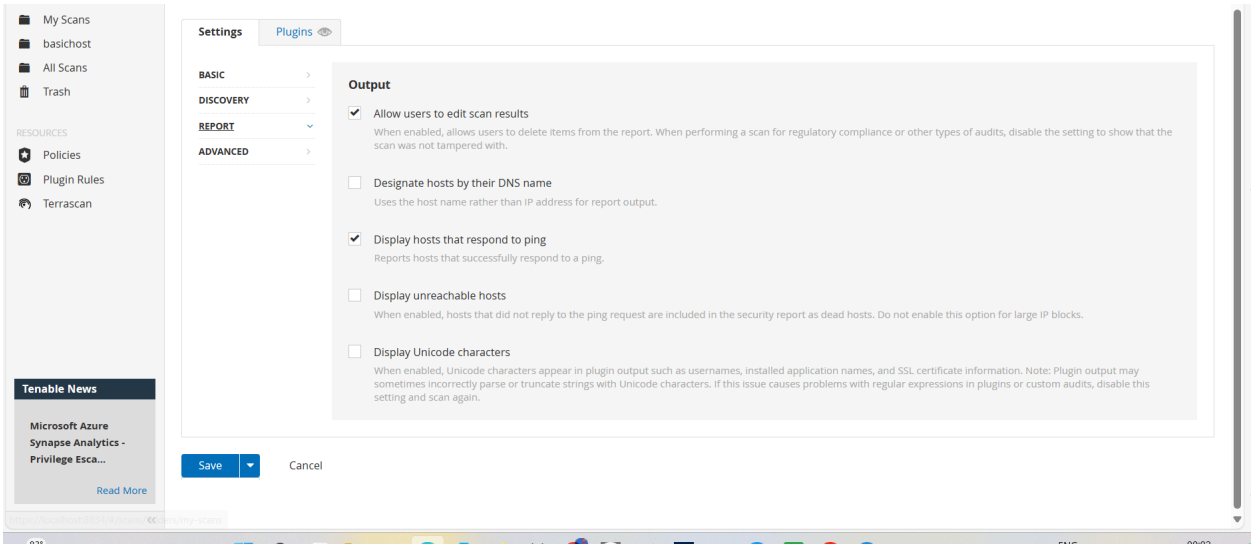
Step 3: Then a form like scan template will open in this we will fill the basic details



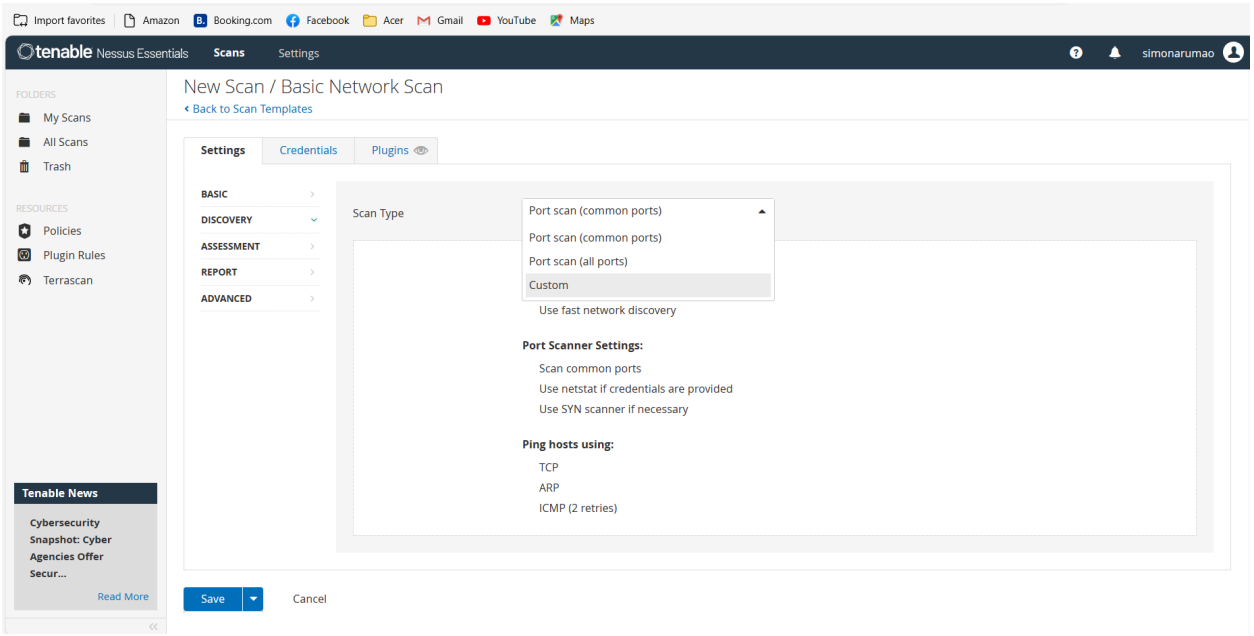
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put our any host ip address



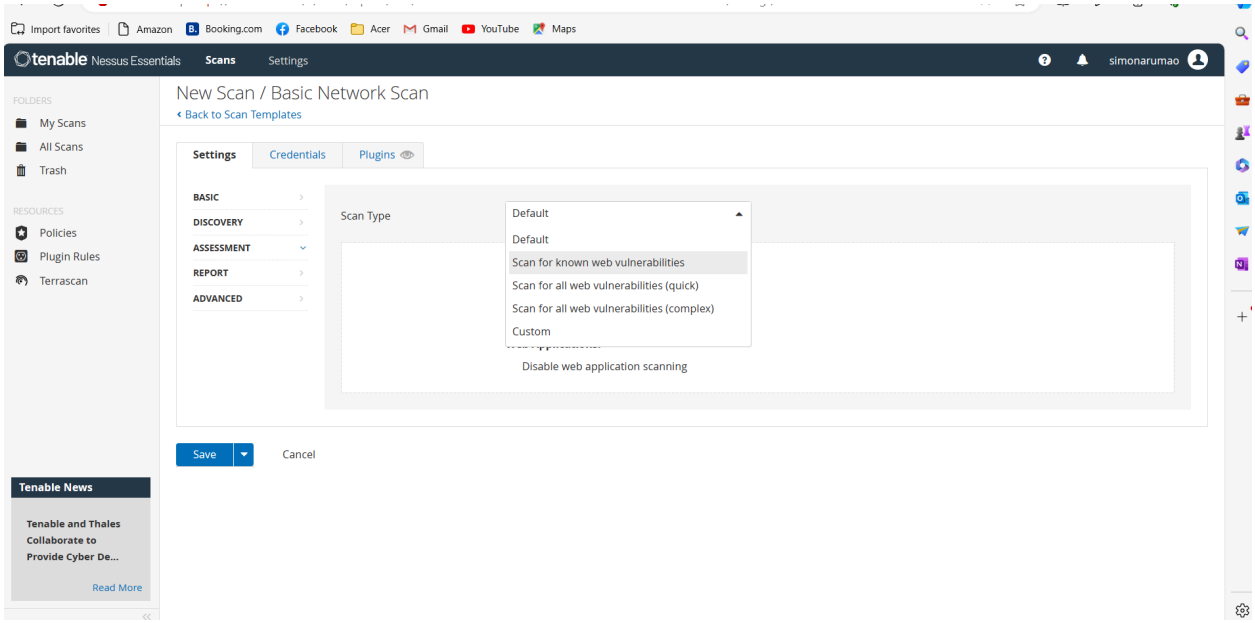
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



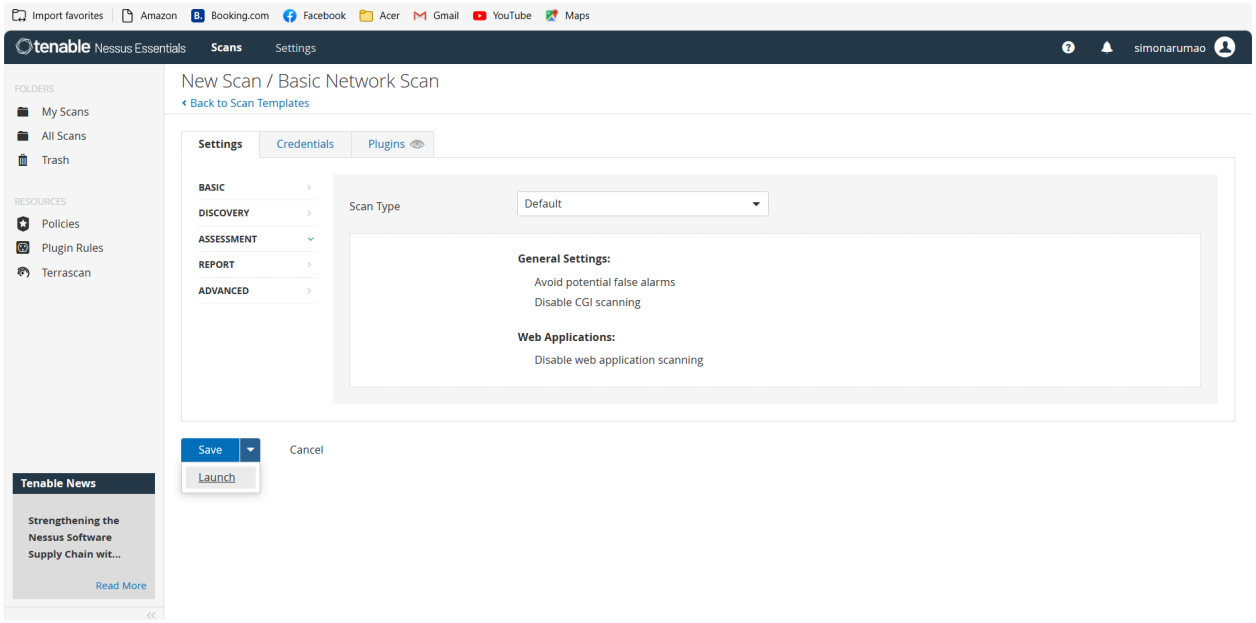
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



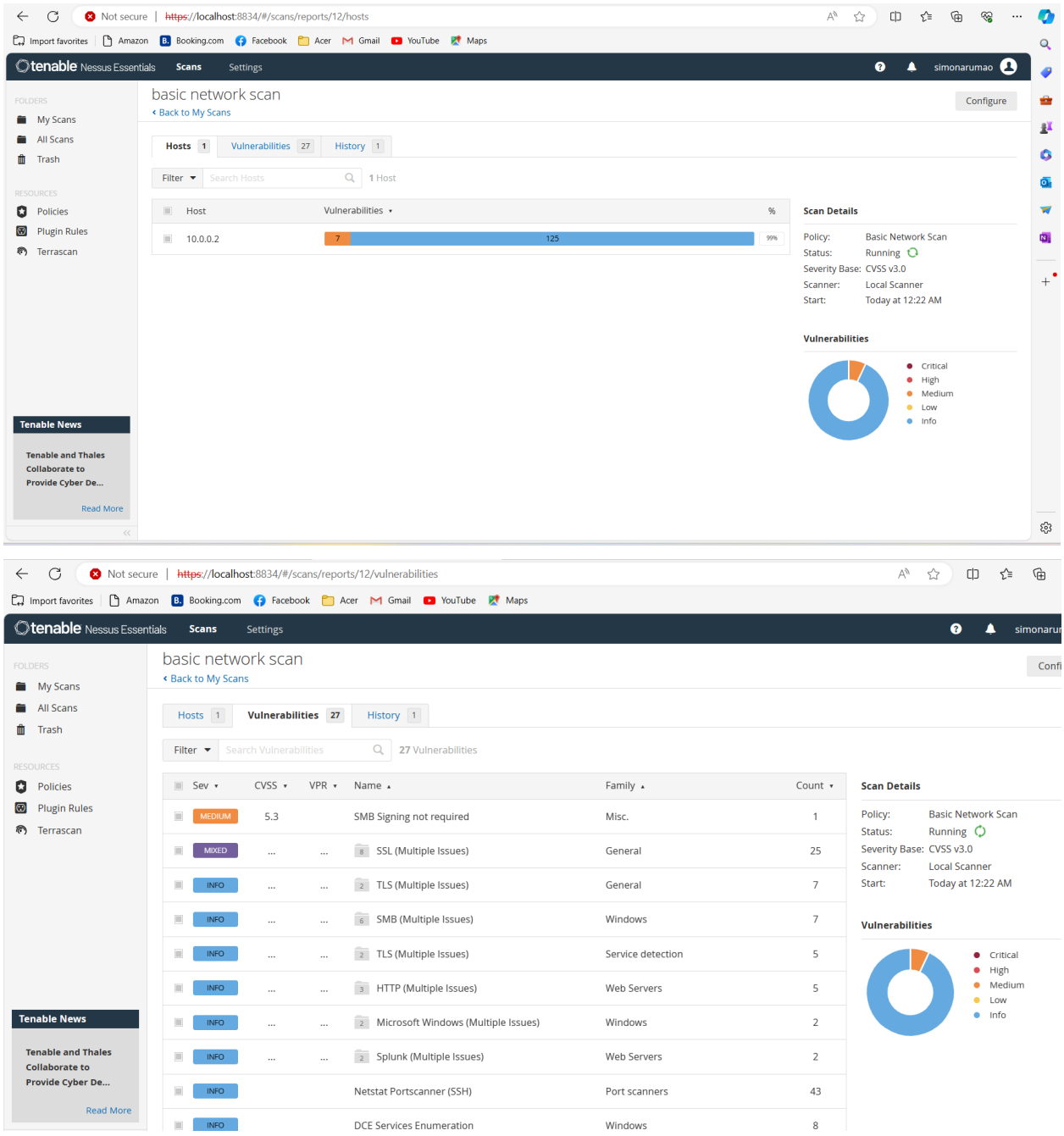
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans



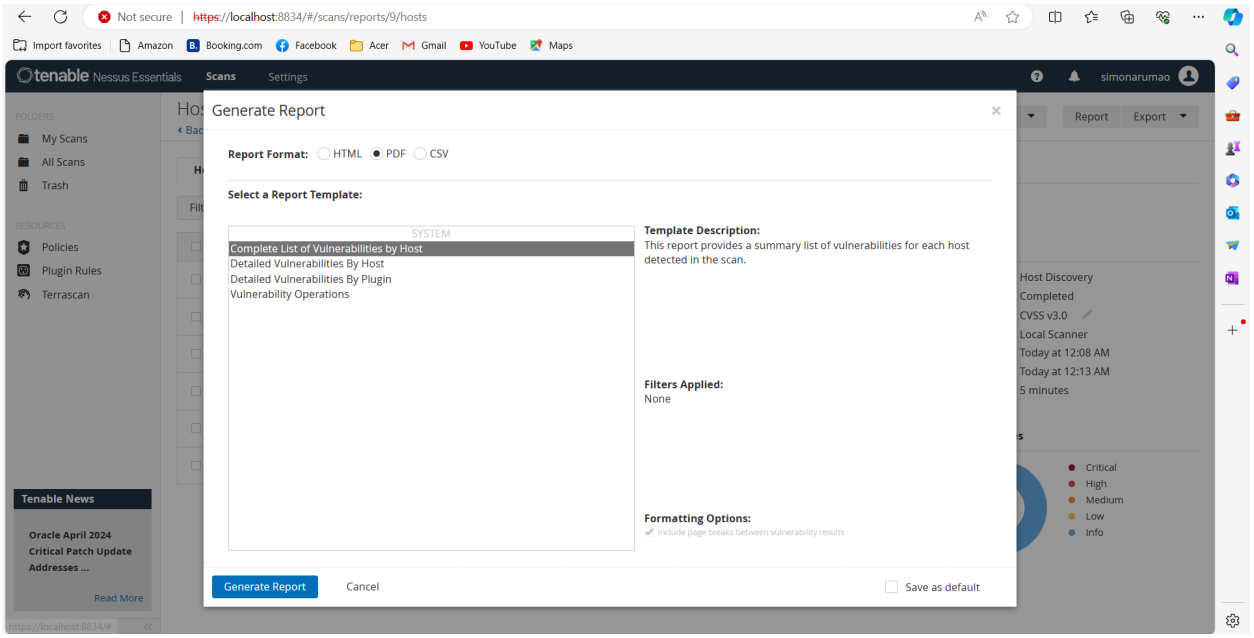
Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

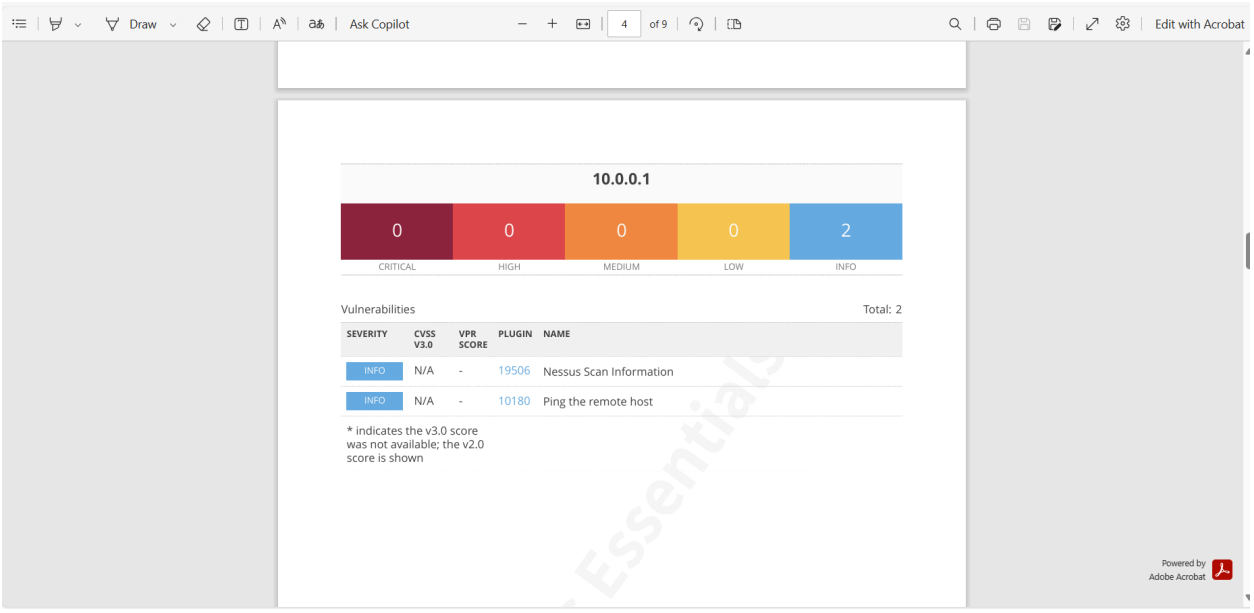


Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities



Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us

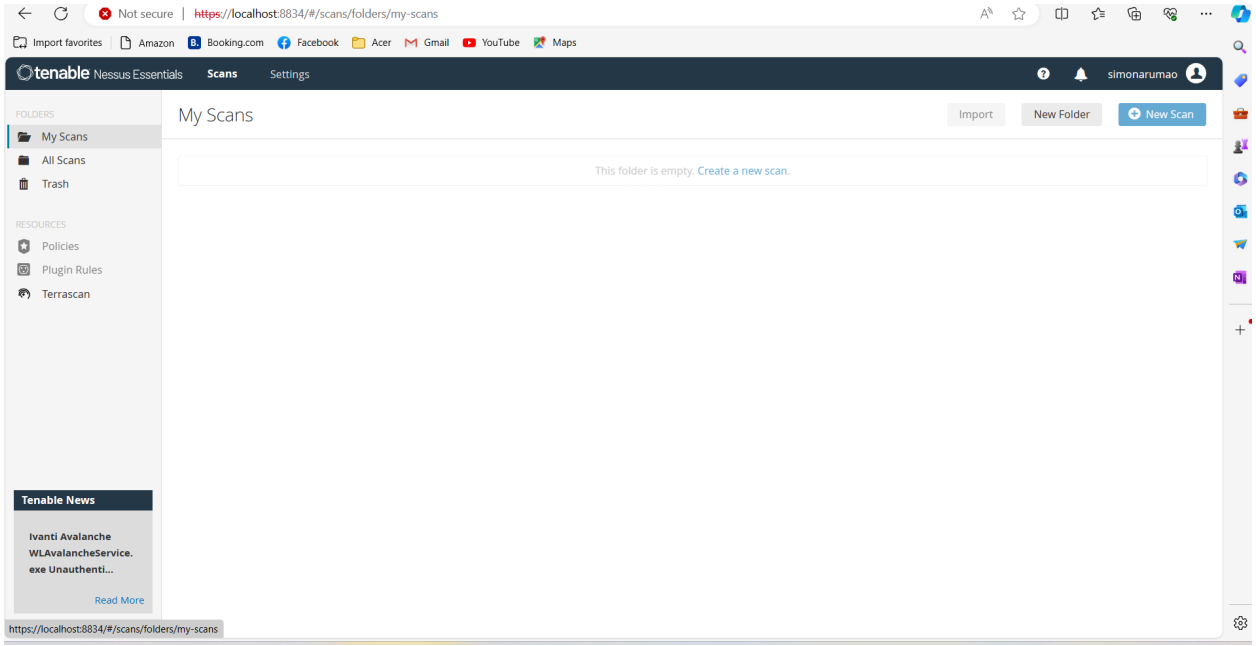

Not secure | https://localhost:8834/#/scans/reports/9/hosts
Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
Report
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Host Discovery
Completed
CVSS v3.0
Local Scanner
Today at 12:08 AM
Today at 12:13 AM
5 minutes
Critical
High
Medium
Low
Info


Draw
Ask Copilot
4
of 9
Edit with Acrobat
10.0.0.1
0
0
0
0
2
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 2
SEVERITY
CVSS V3.0
VPR SCORE
PLUGIN
NAME
INFO
N/A
-
19506
Nessus Scan Information
INFO
N/A
-
10180
Ping the remote host
* indicates the v3.0 score was not available; the v2.0 score is shown
Powered by Adobe Acrobat

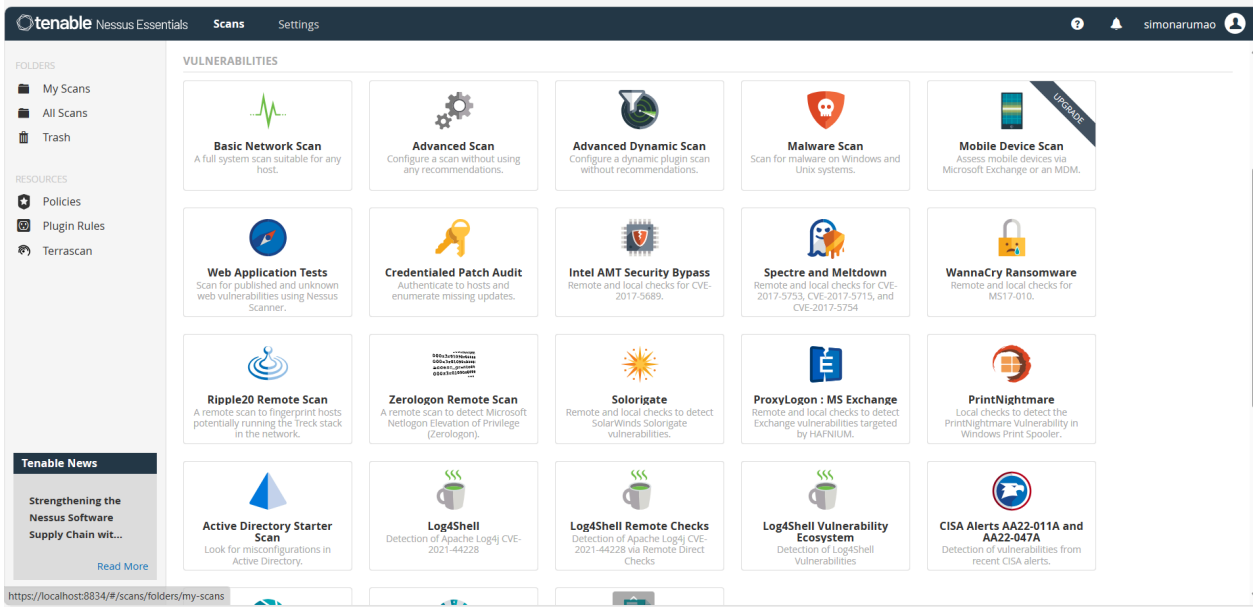
B. Perform Web Application Tests Scan in the Nessus tool on the below targets:
a) http://testasp.vulnweb.com/
b) https://www.shoppersstop.com/

Web application test on testasp

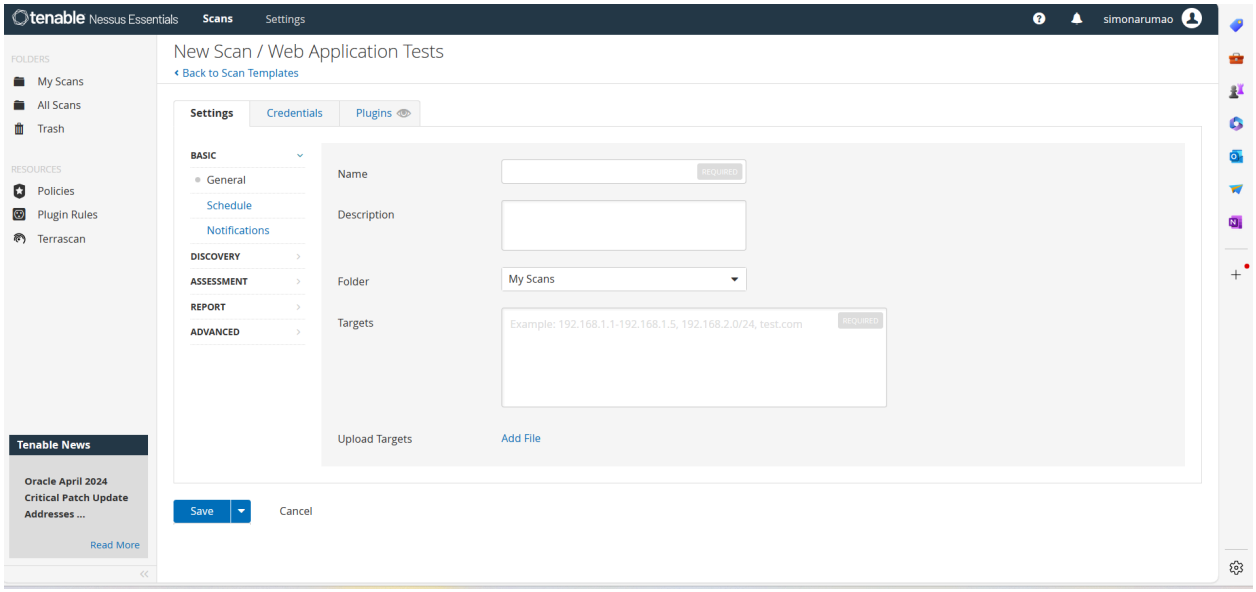
Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



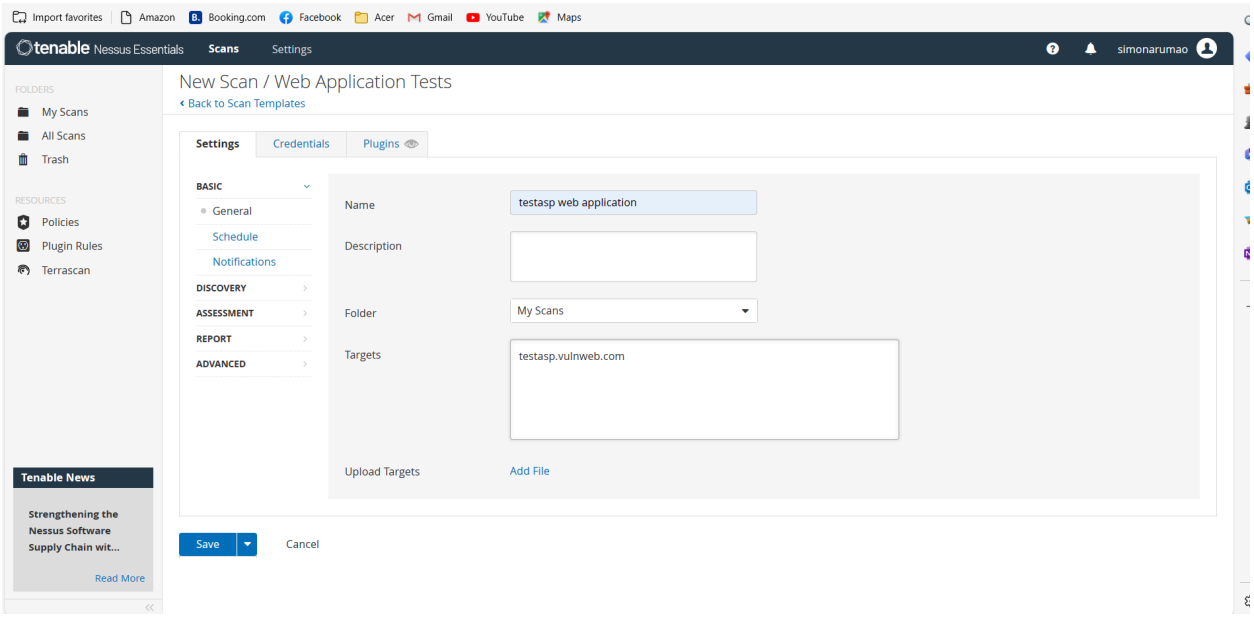
Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



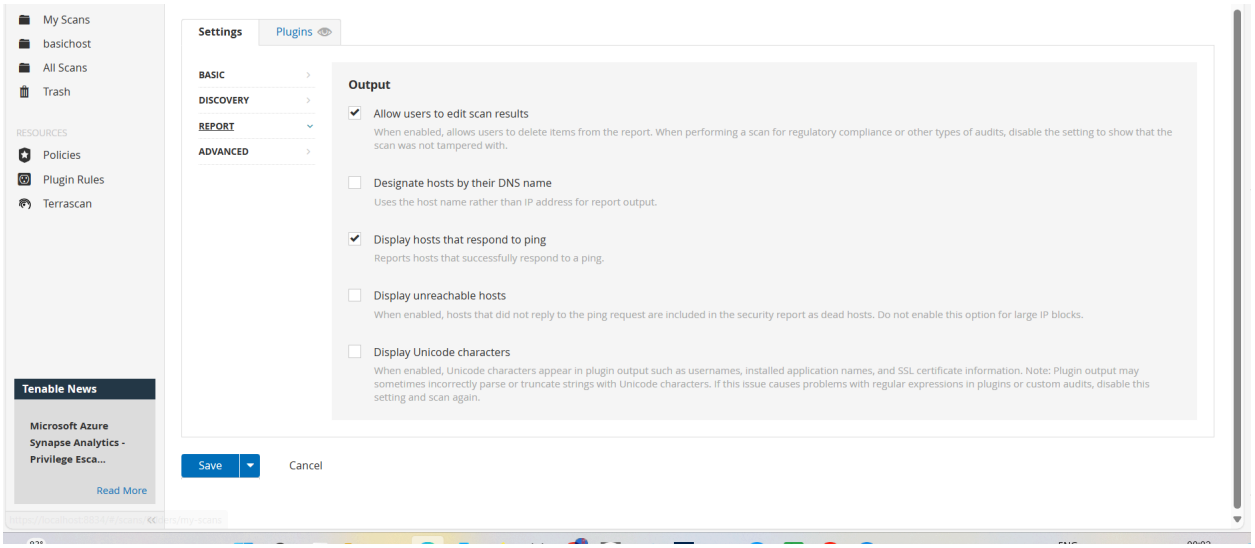
Step 3: Then a form like scan template will open in this we will fill the basic details



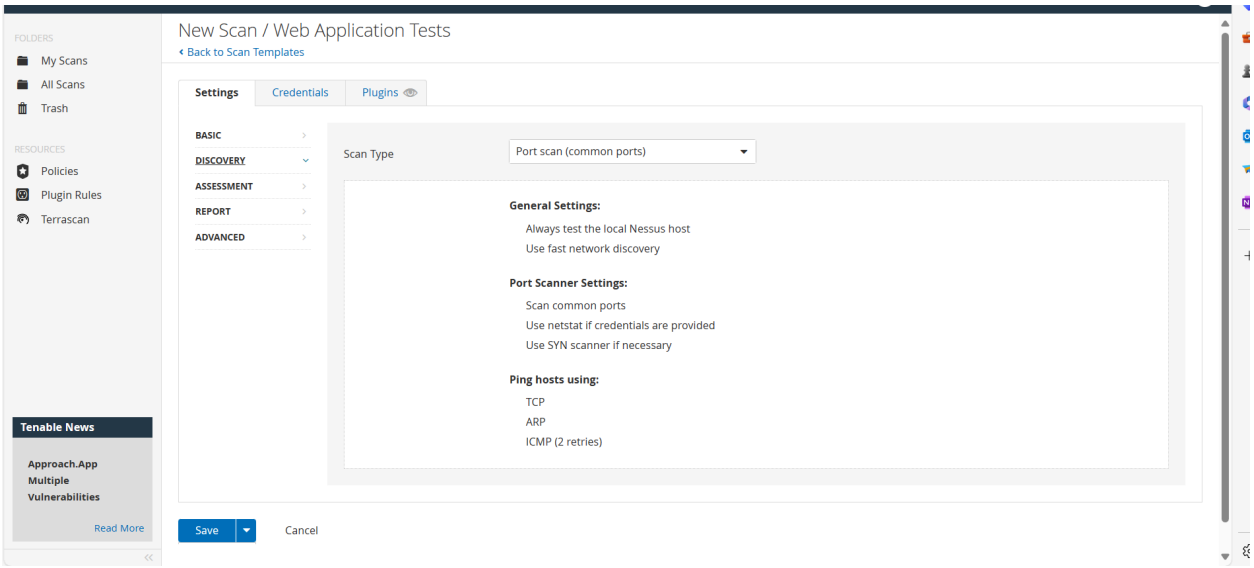
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name



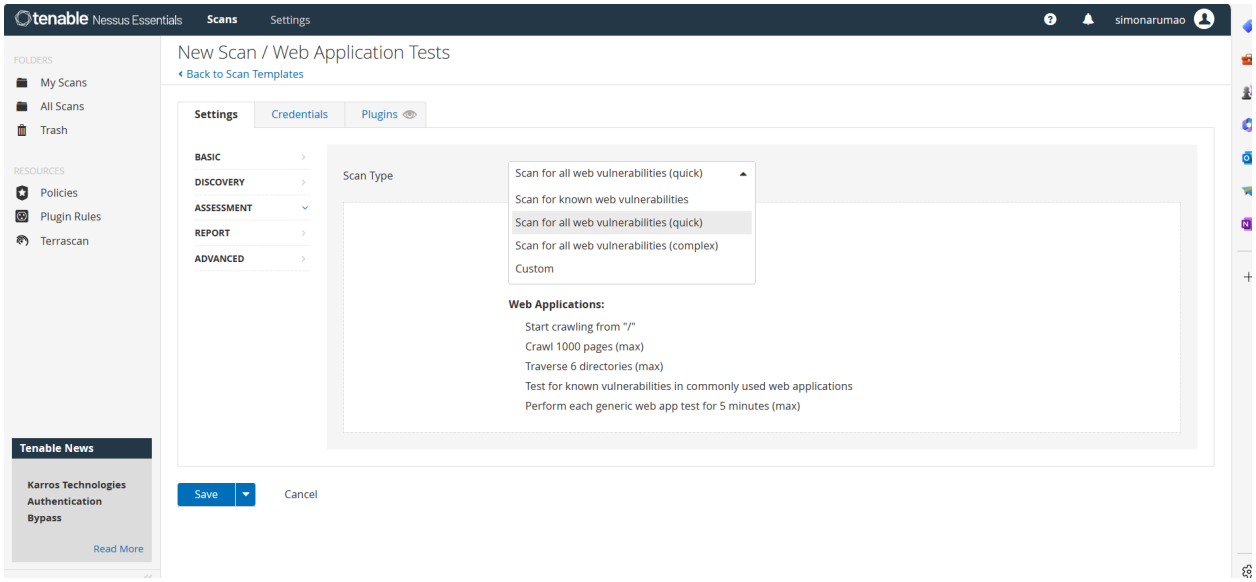
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



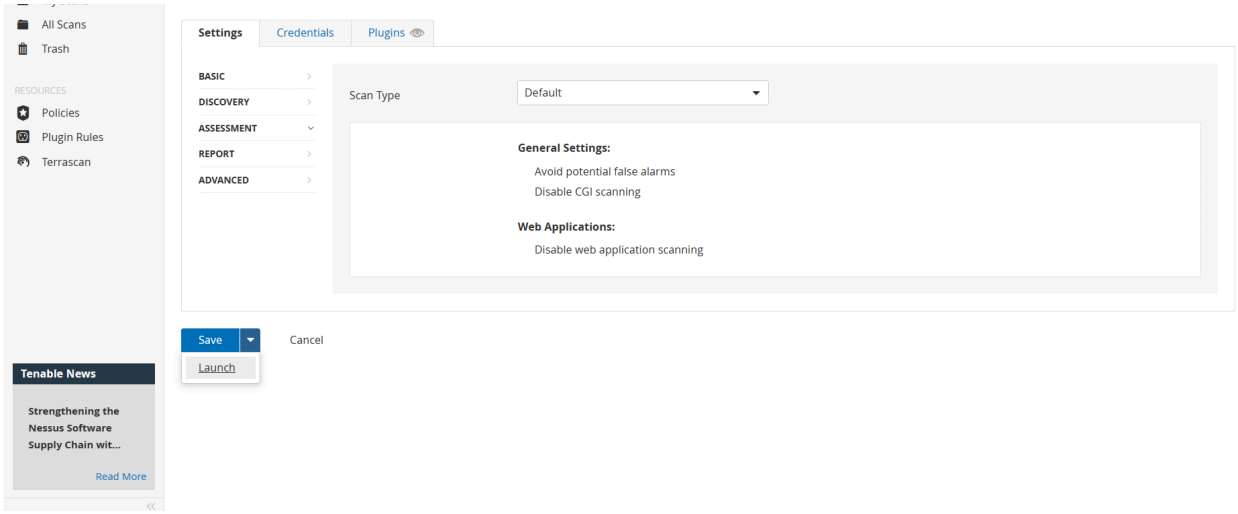
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



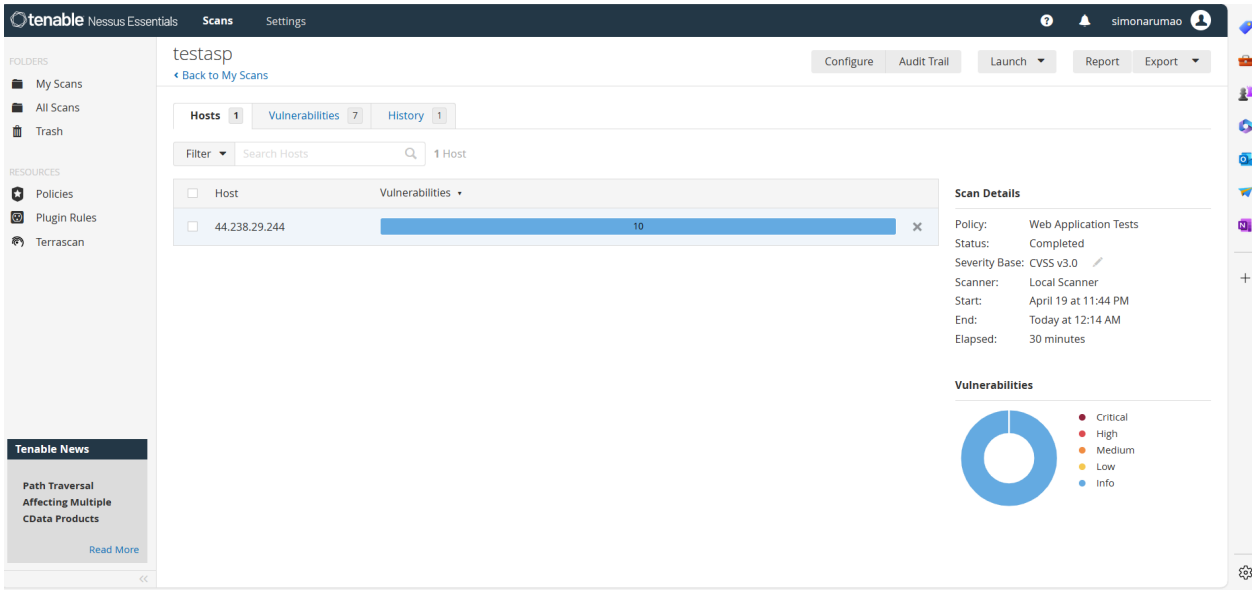
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

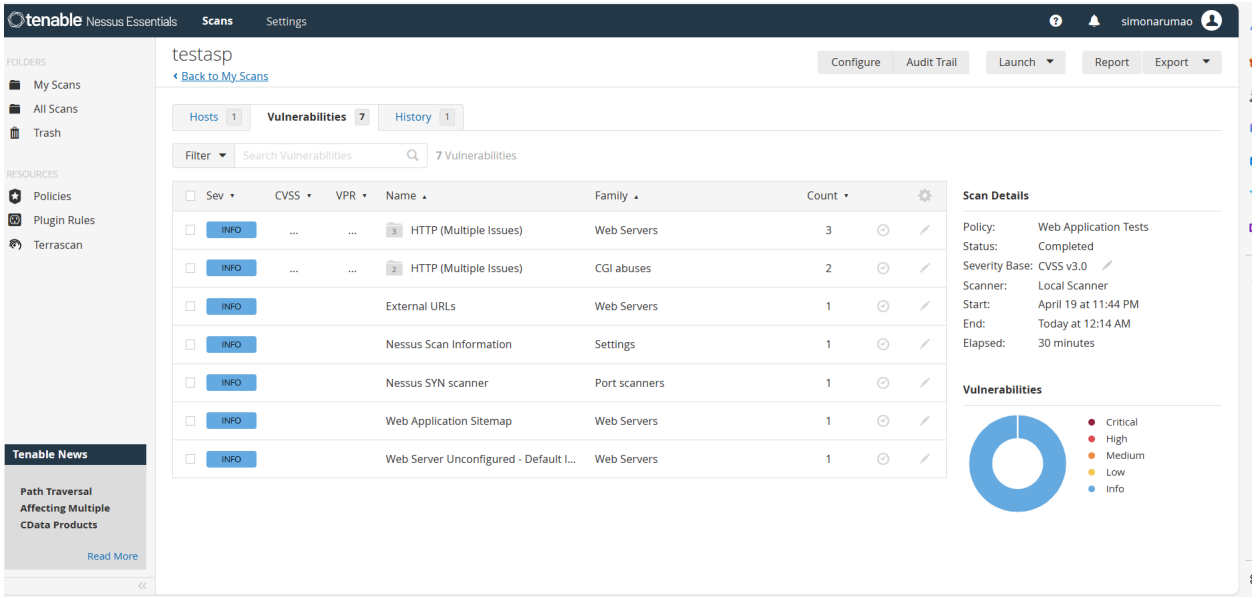


Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan

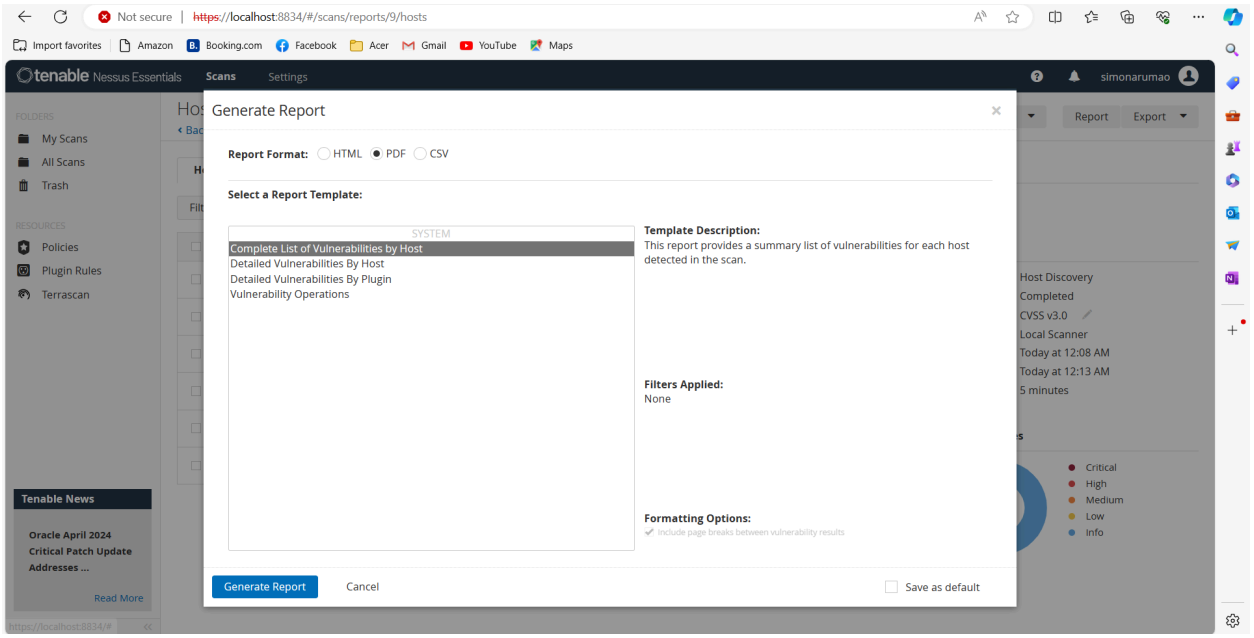


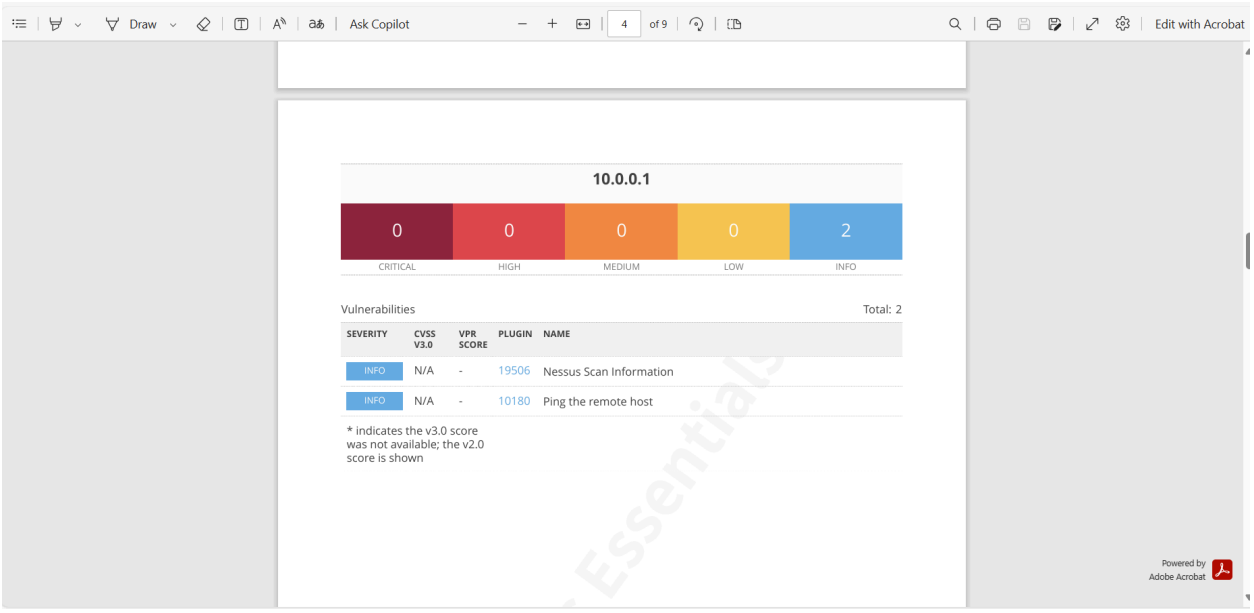
Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities





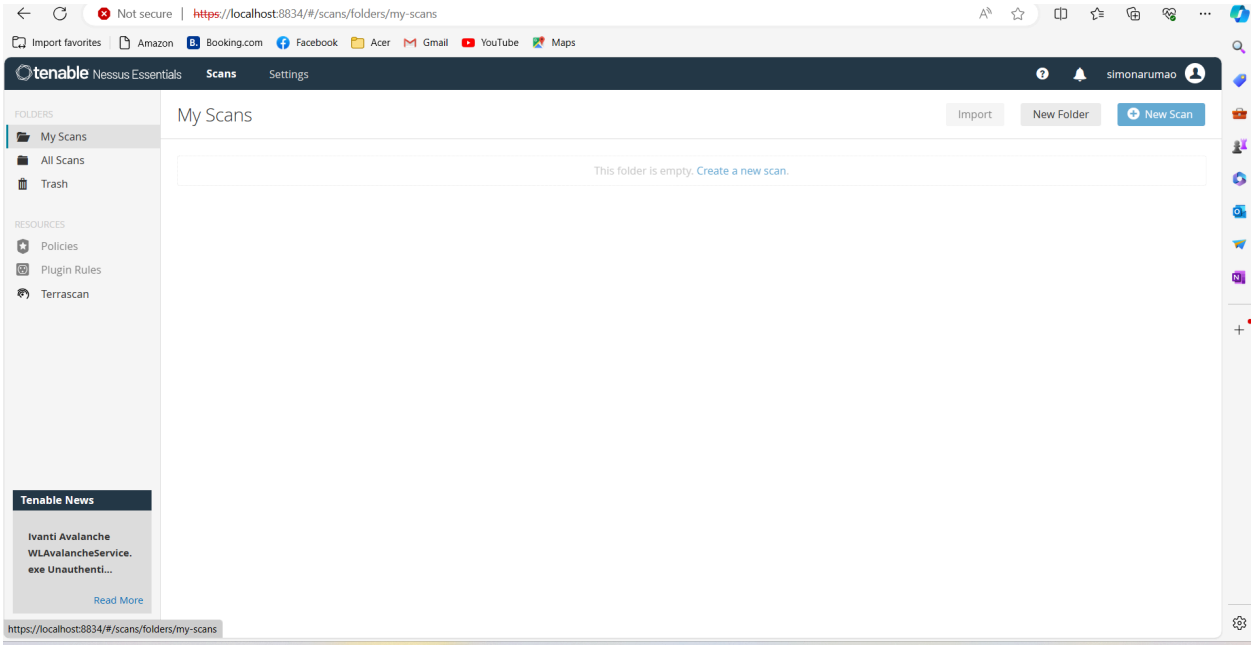
Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us


Not secure | https://localhost:8834/#/scans/reports/9/hosts
Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
Report
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Host Discovery
Completed
CVSS v3.0
Local Scanner
Today at 12:08 AM
Today at 12:13 AM
5 minutes
Critical
High
Medium
Low
Info

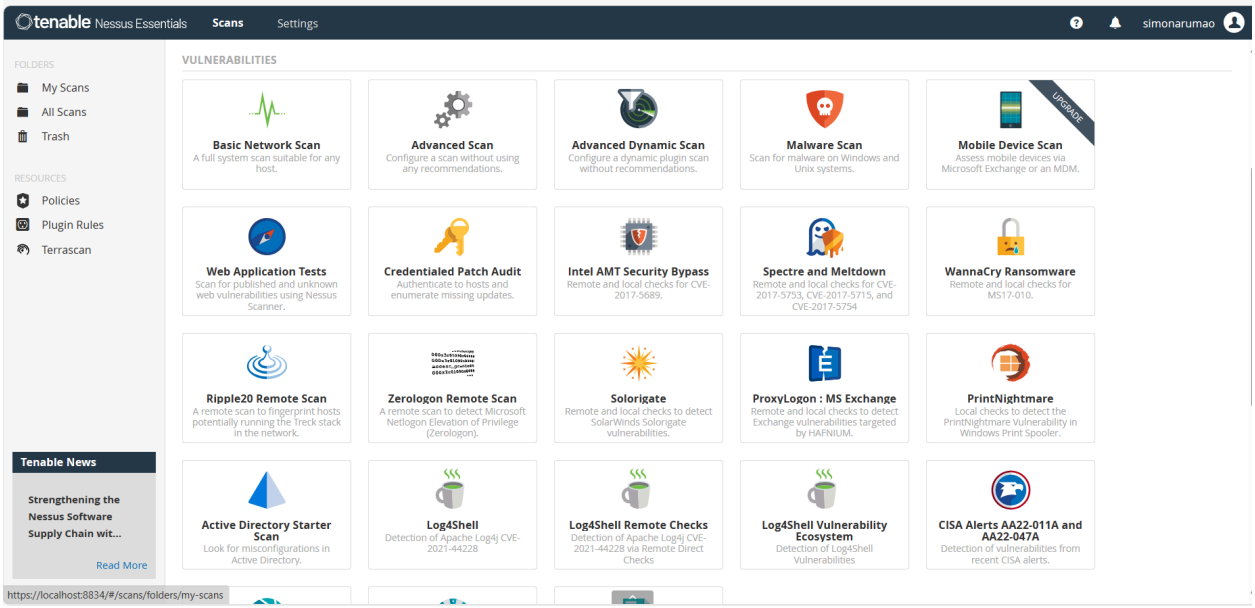

Draw
Ask Copilot
4
of 9
Edit with Acrobat
10.0.0.1
0
0
0
0
2
CRITICAL
HIGH
MEDIUM
LOW
INFO
Vulnerabilities
Total: 2
SEVERITY
CVSS V3.0
VPR SCORE
PLUGIN
NAME
INFO
N/A
-
19506
Nessus Scan Information
INFO
N/A
-
10180
Ping the remote host
* indicates the v3.0 score was not available; the v2.0 score is shown
Powered by Adobe Acrobat

Web application test on ShopperStop

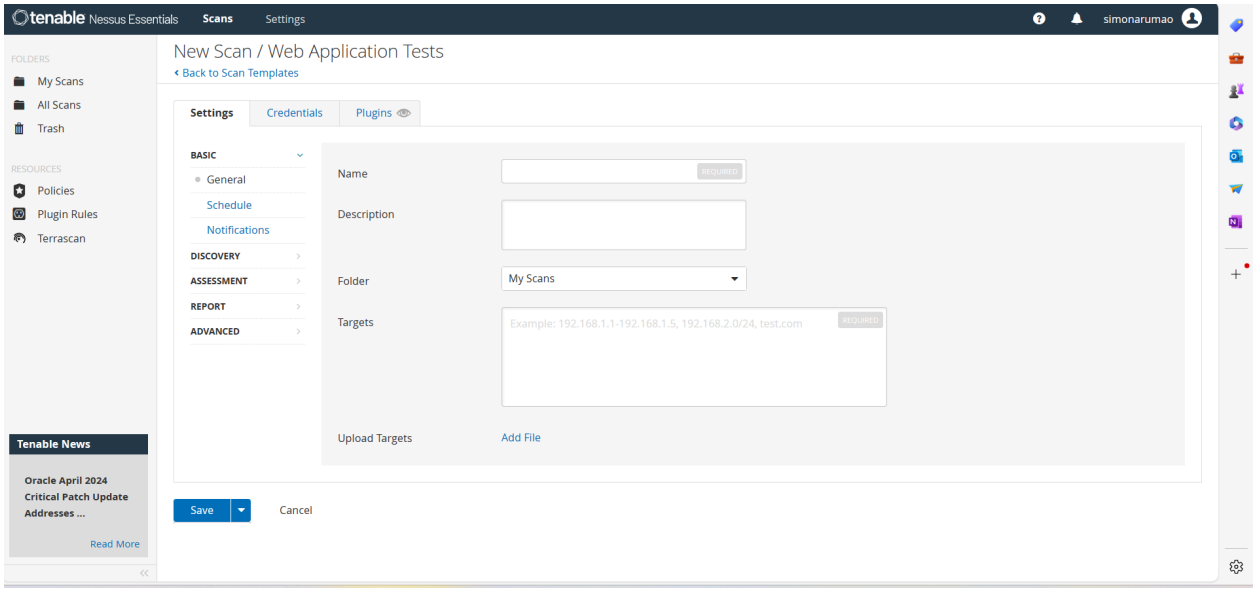
Step 1 : Now we will start the scan for web application test scan, in the interface we can see all the scans on the dashboard and on the top right corner there is the button new scan , click on new scan .



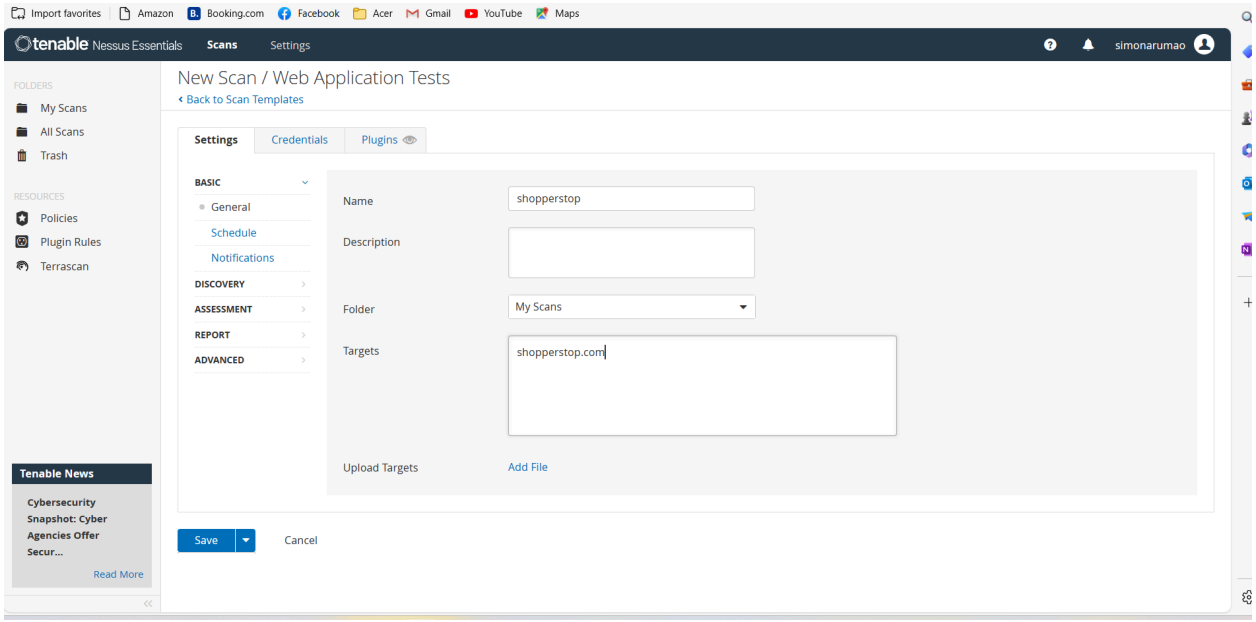
Step 2 : When you click on new scan we can see various templates in that scan, we can see the web application tests template, click on that template



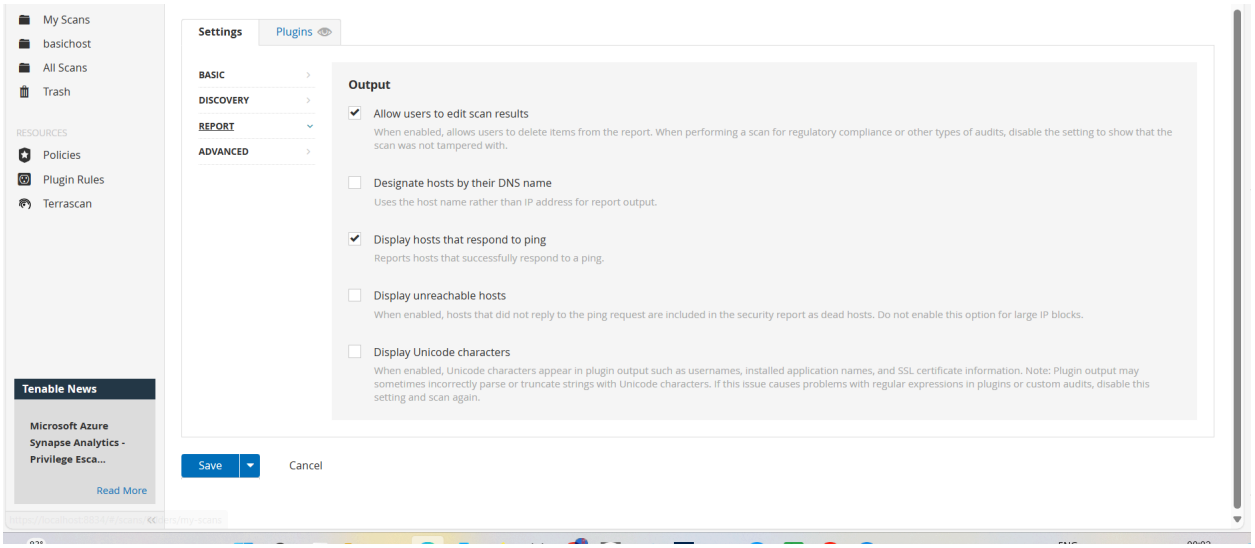
Step 3: Then a form like scan template will open in this we will fill the basic details



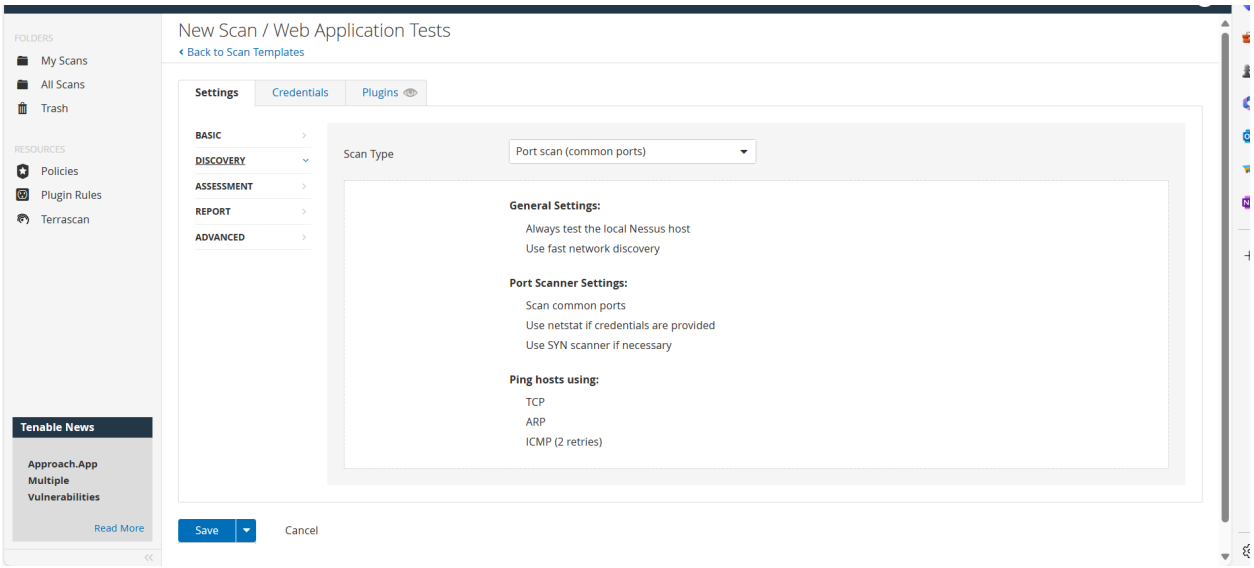
Step 4 : In this templates first we will give our scan a name, then in the field of targets we will put the website ip address or the domain name



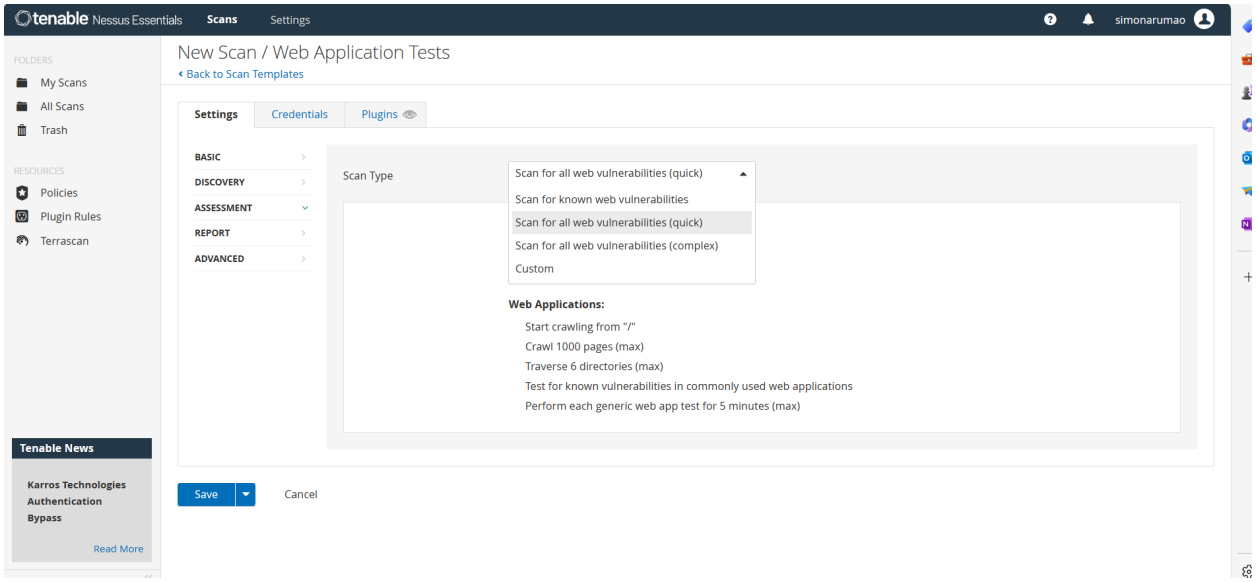
Step 5: In the side panel we can also see the reports section that is how we want the report format to be we will keep this setting default



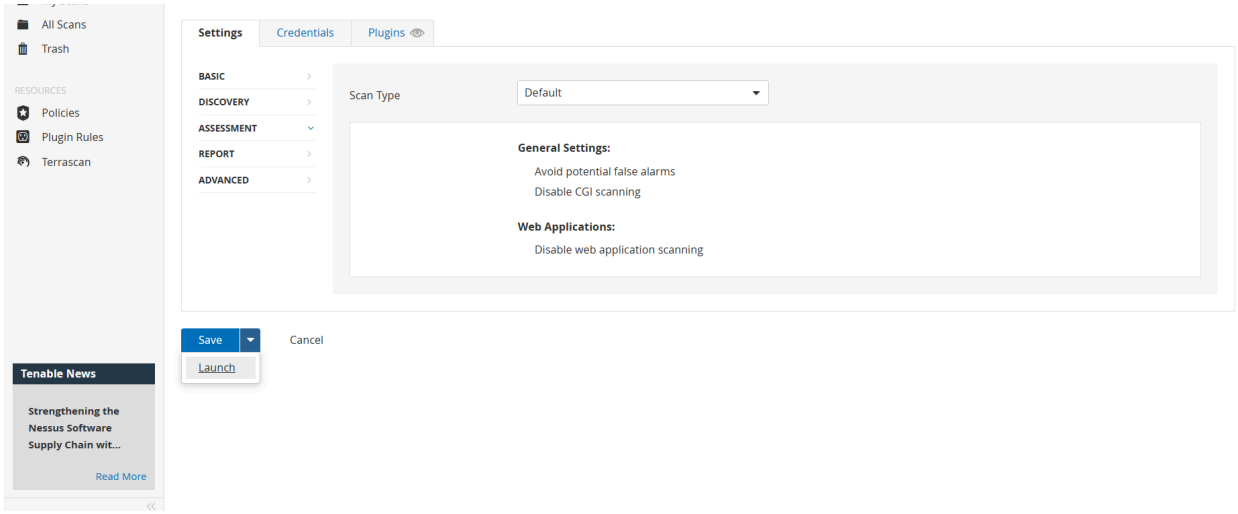
Step 6 : In the basic network scan we have more options like discovery in which we can choose the scan type whether we want it on common ports or entire ports



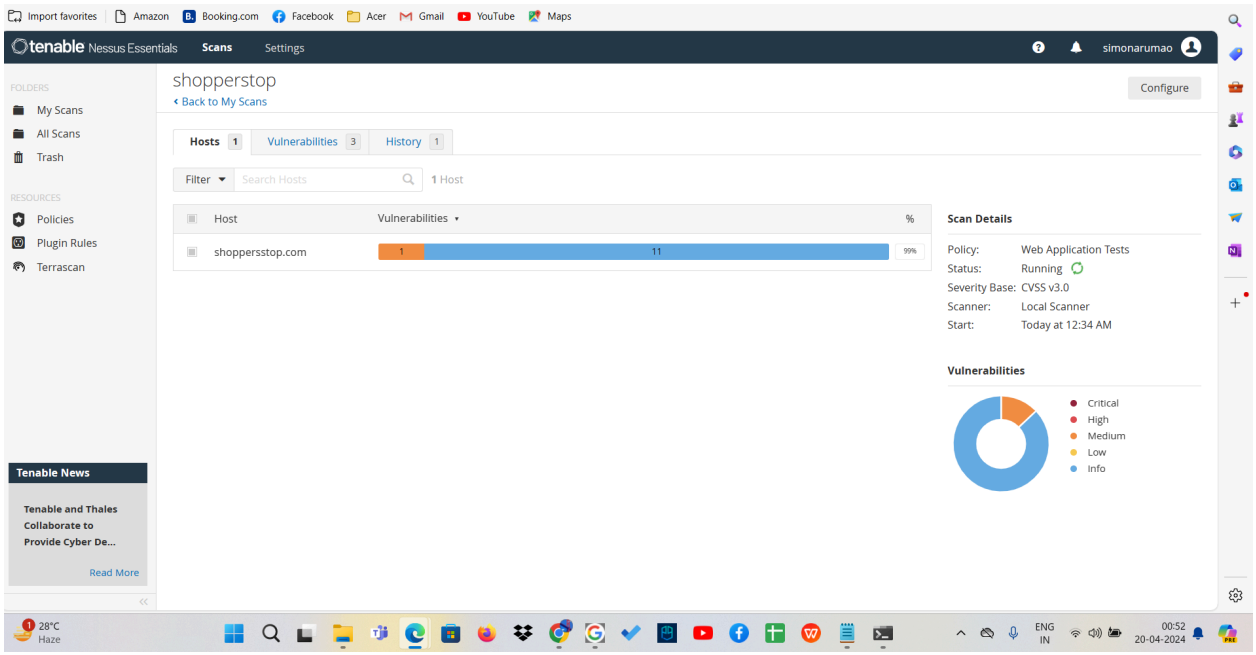
Step 7 : In the assessment tab we can choose whether we want a quick scan or more advance scan like complex scans

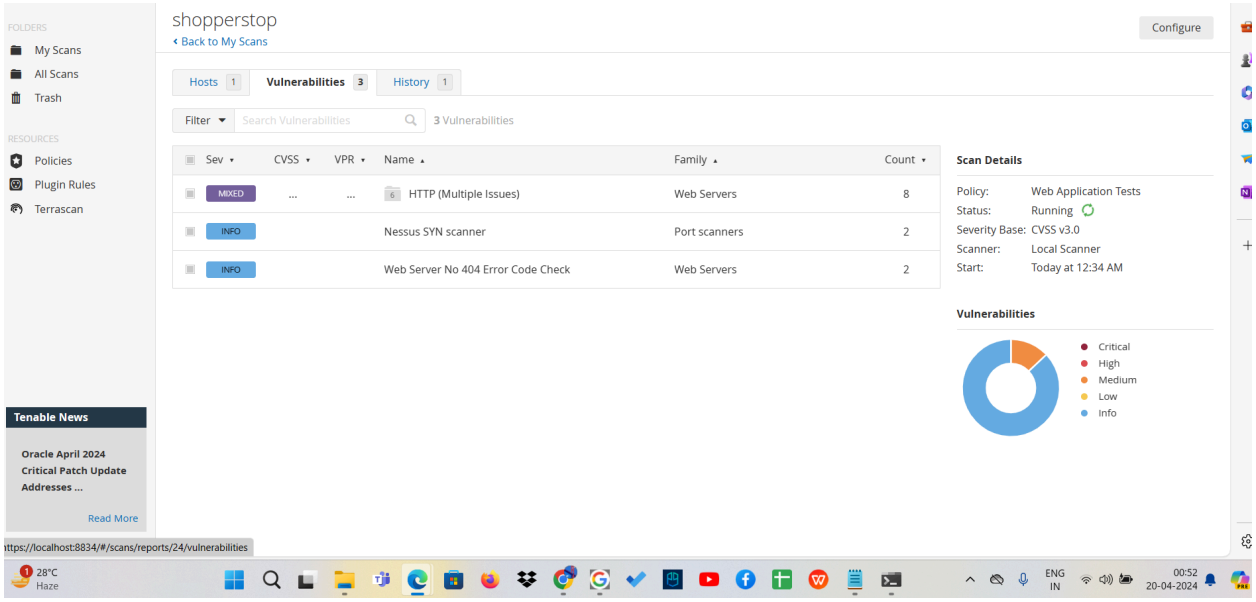


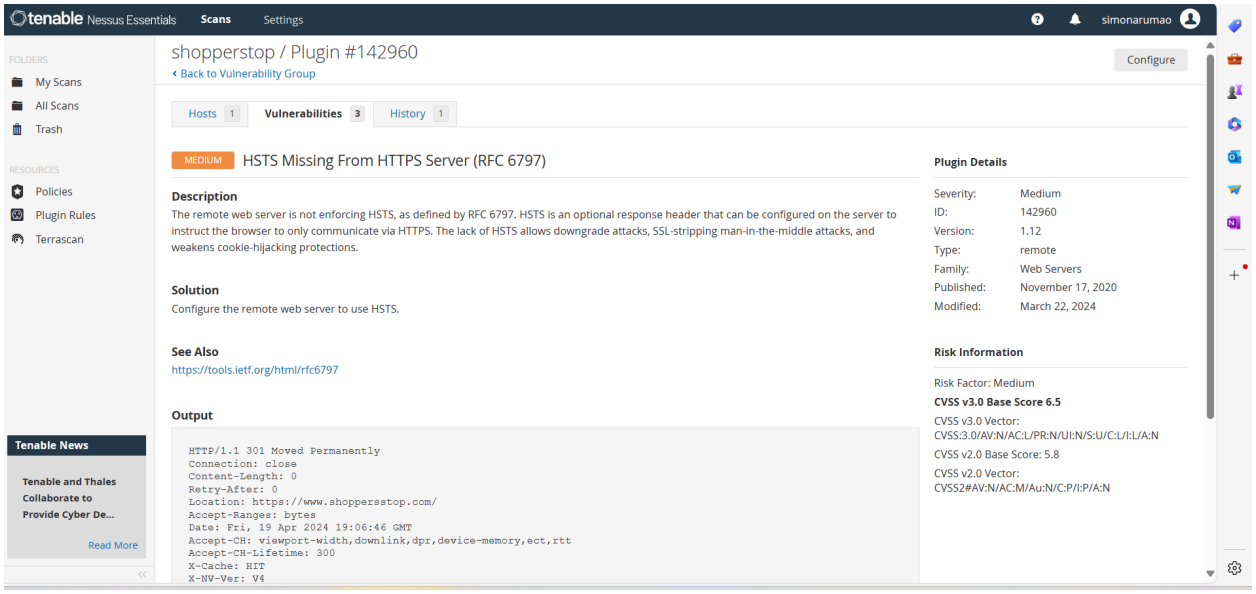
Step 8 : Then click on save and on the dashboard in the scan there is small play button click on that to launch the scan



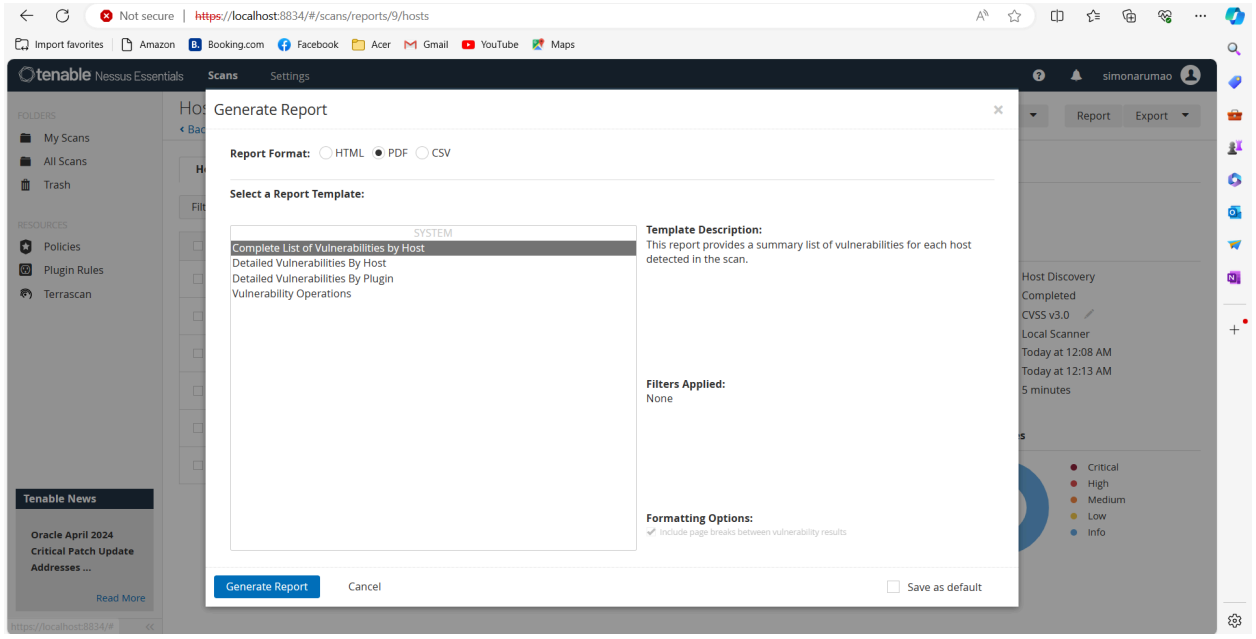
Step 9:Once we launch it will start scanning and we can see all the host on our network, in the vulnerabilities tab , we can see all the vulnerabilities


Import favorites
Amazon
Booking.com
Facebook
Acer
Gmail
YouTube
Maps
tenable Nessus Essentials
Scans
Settings
simonarumao
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
shopperstop
Back to My Scans
Configure
Hosts 1
Vulnerabilities 3
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
%
shoppersstop.com
1
11
99%
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Tenable and Thales Collaborate to Provide Cyber De...
Read More
28°C
Haze
ENG
IN
00:52
20-04-2024


FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
shopperstop
Back to My Scans
Configure
Hosts 1
Vulnerabilities 3
History 1
Filter
Search Vulnerabilities
3 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED
HTTP (Multiple Issues)
Web Servers
8
INFO
Nessus SYN scanner
Port scanners
2
INFO
Web Server No 404 Error Code Check
Web Servers
2
Scan Details
Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:34 AM
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Oracle April 2024 Critical Patch Update Addresses ...
Read More
https://localhost:8834/#/scans/reports/24/vulnerabilities
28°C
Haze
ENG
IN
00:52
20-04-2024



Step 10 : Once the scan is performed we will get an option to generate report, if we click on it, it will an execute report format and click on generare format, it will generate an report for us



10.0.0.1

Vulnerabilities Total: 2

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

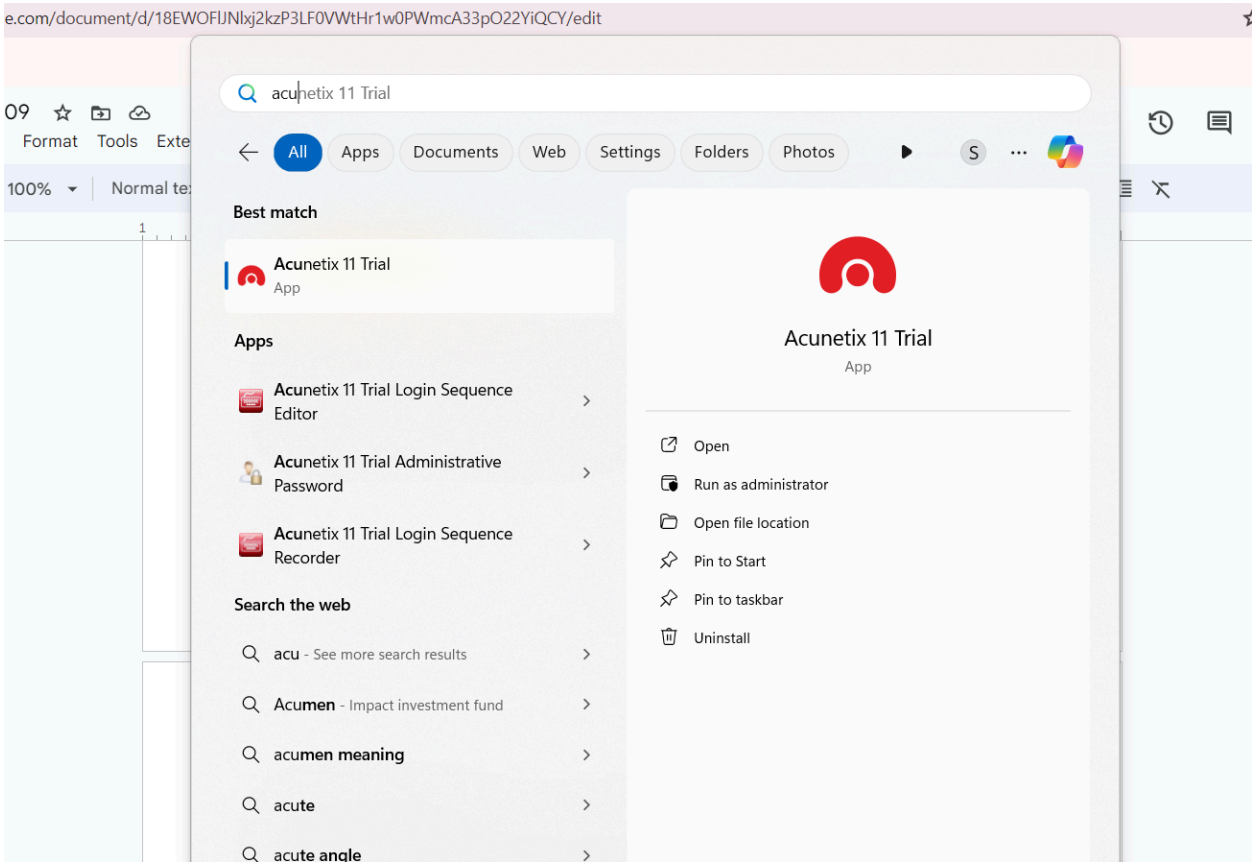
* indicates the v3.0 score was not available; the v2.0 score is shown

C. Scan the below-mentioned targets Using the Acunetix Vulnerability scanner:
a) https://www.ebay.com/
b) https://shopping.rediff.com/

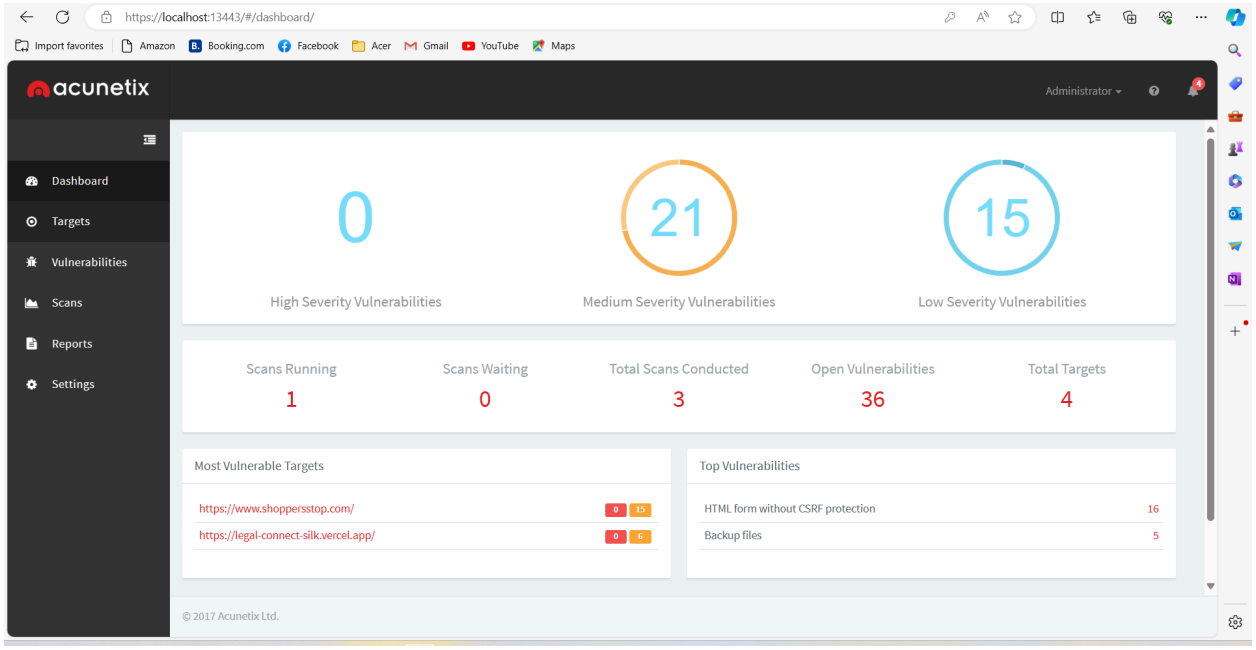
Website 1 : https://shopping.rediff.com/

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

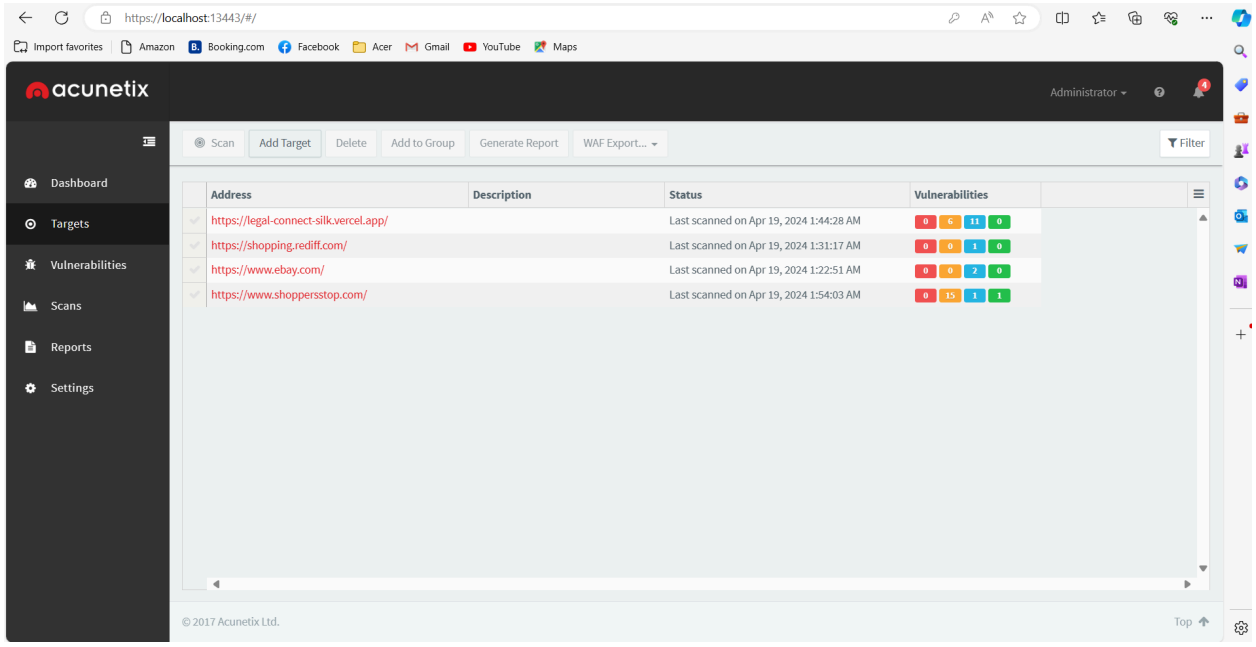
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



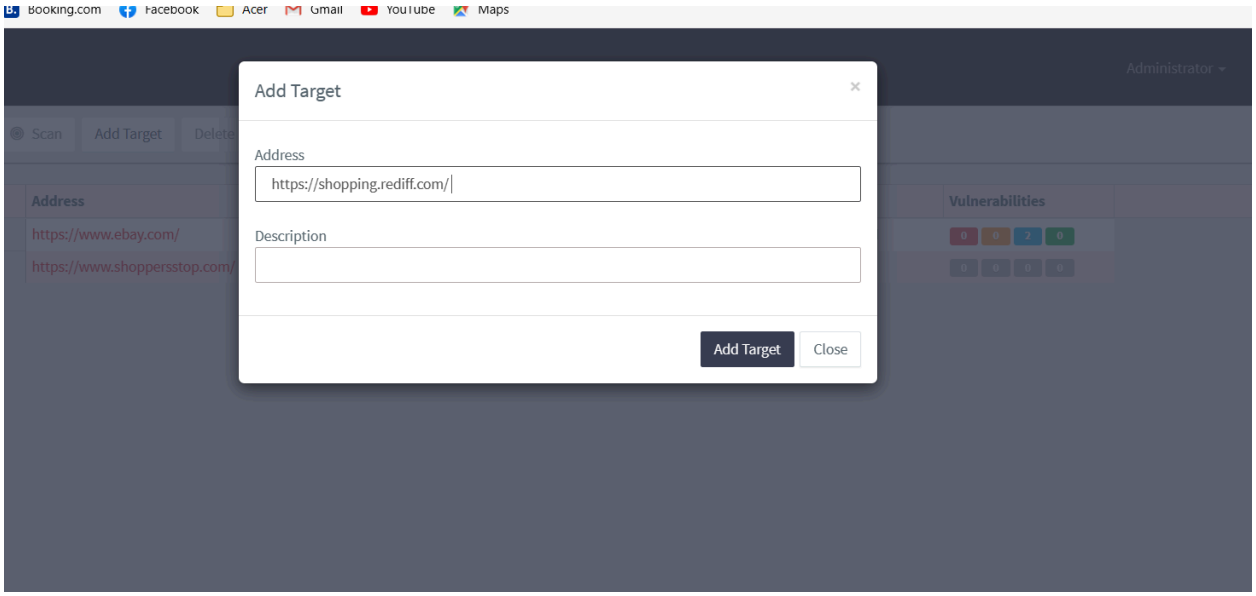
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



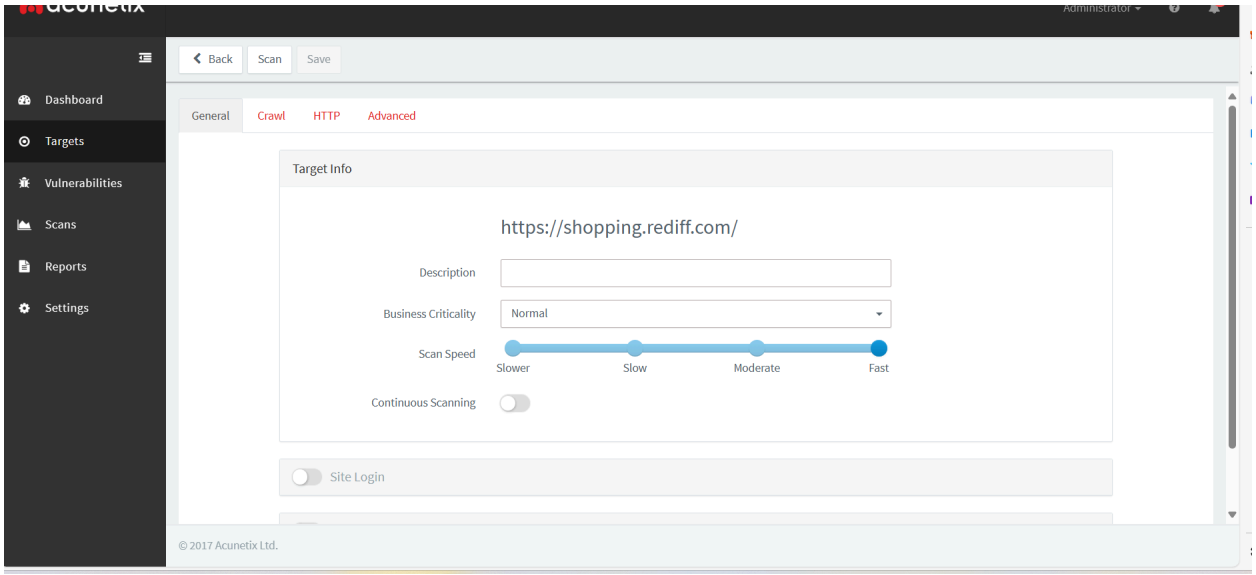
Step 4 : Go to the targets open and click on add target , In top there is a add target button

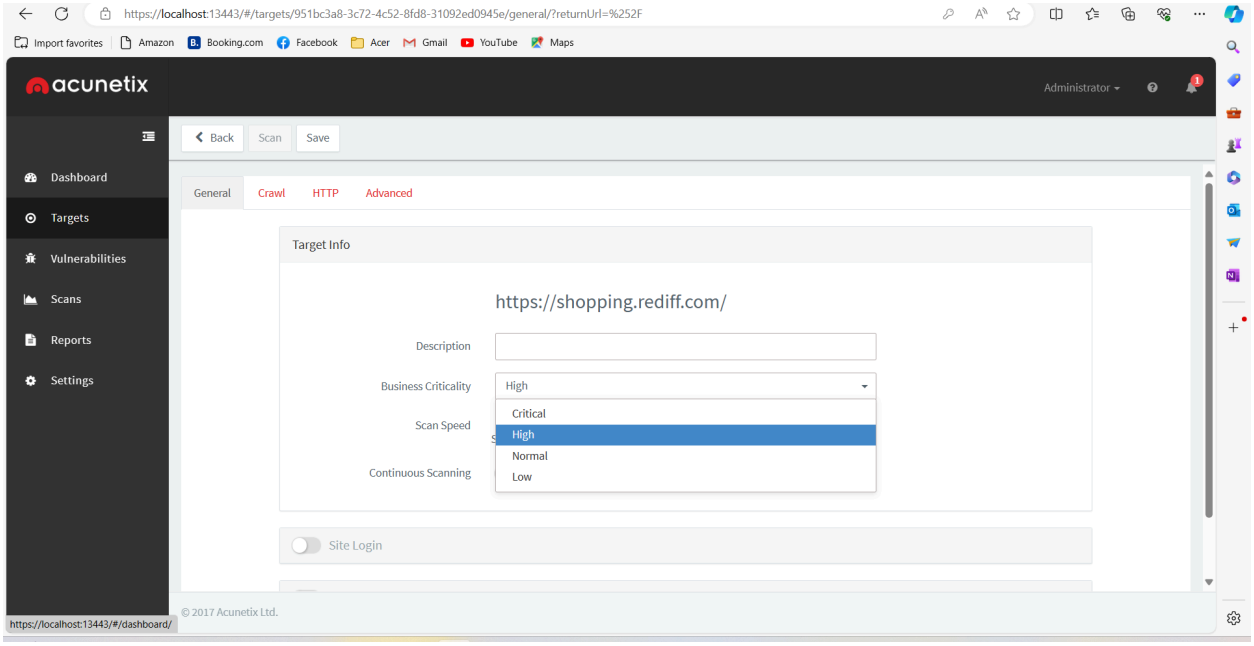


Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target

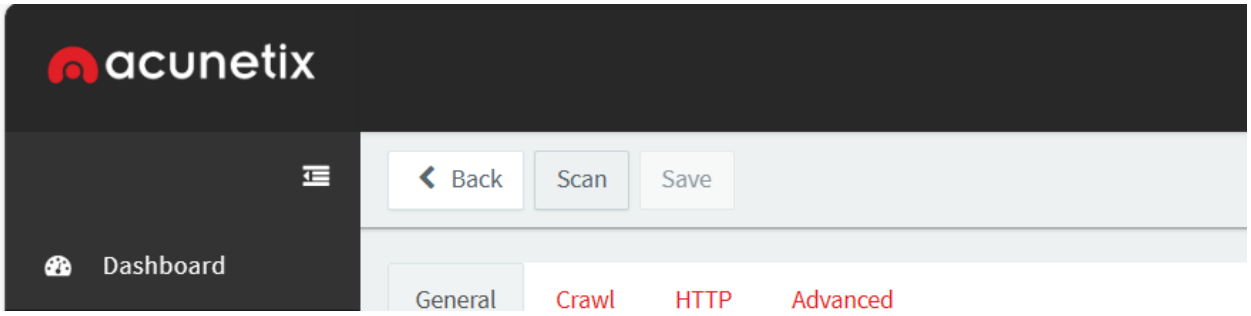


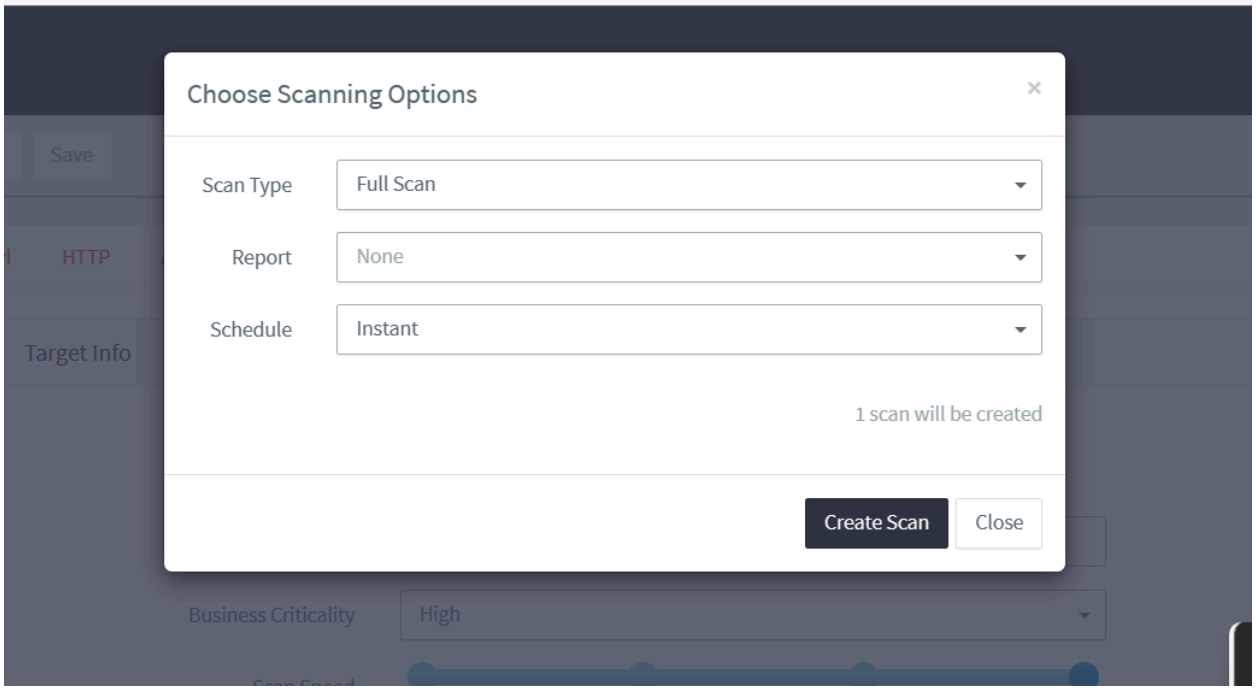
Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button



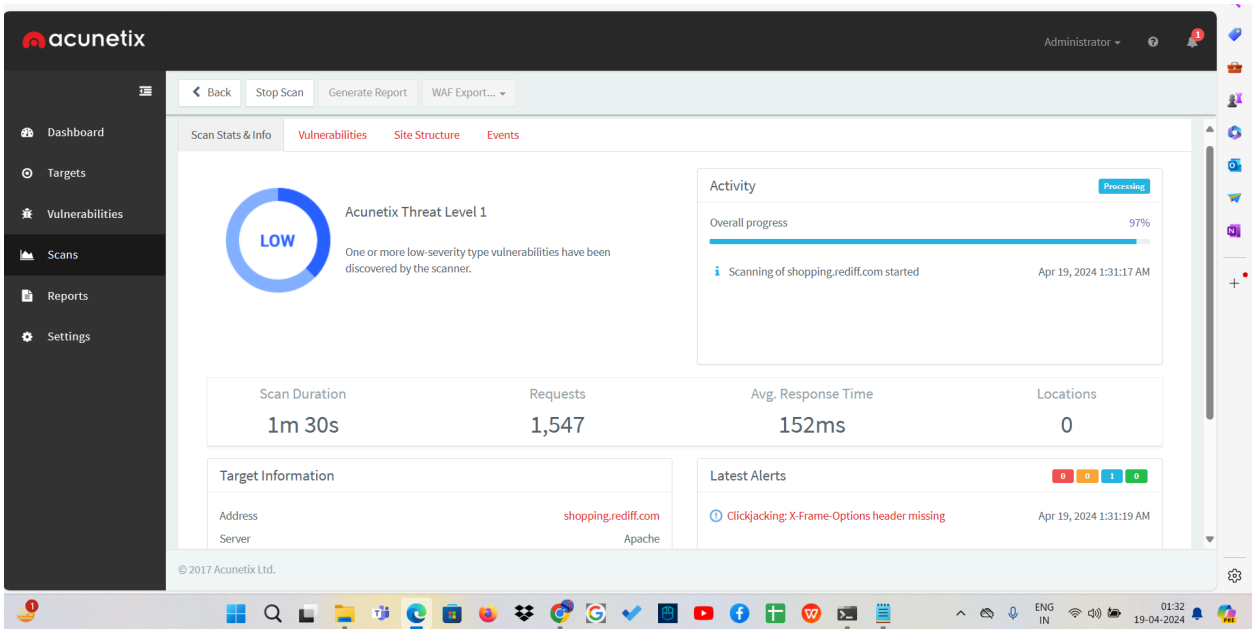


Step 7: Then click on the scan button on the top to start scanning the web application

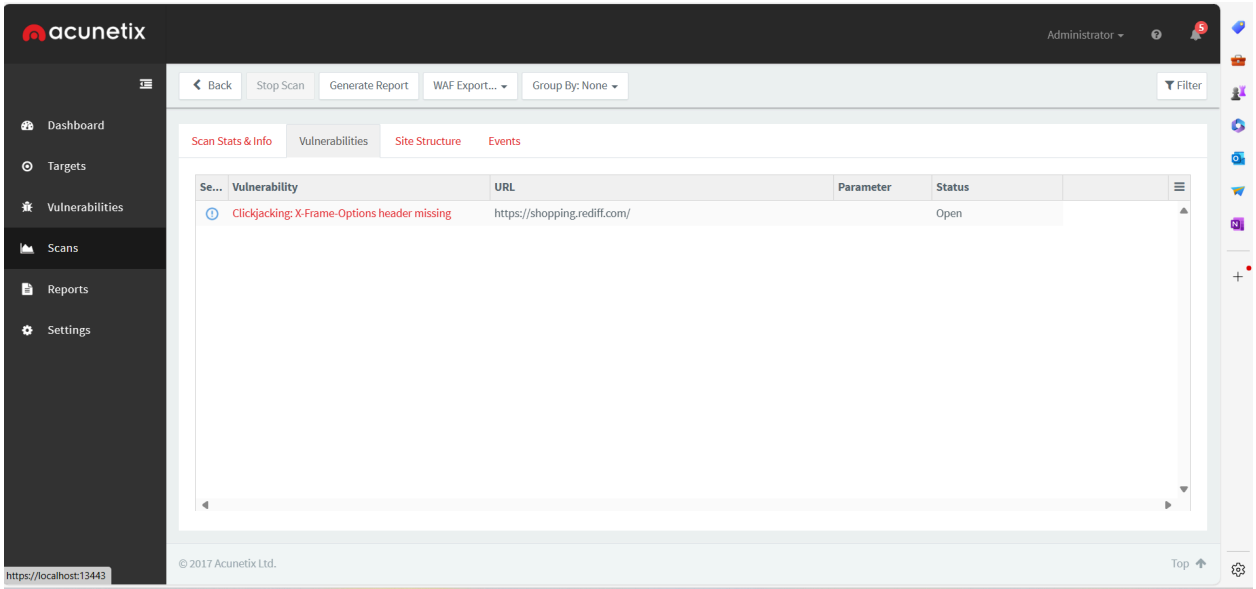


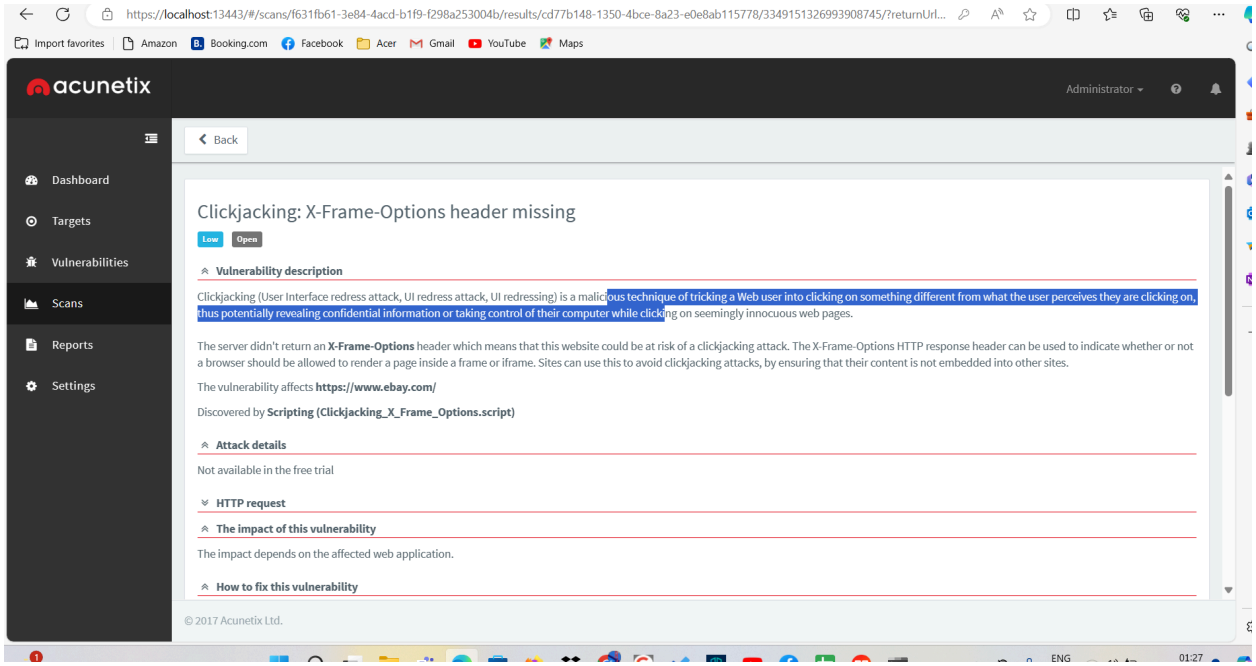


Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

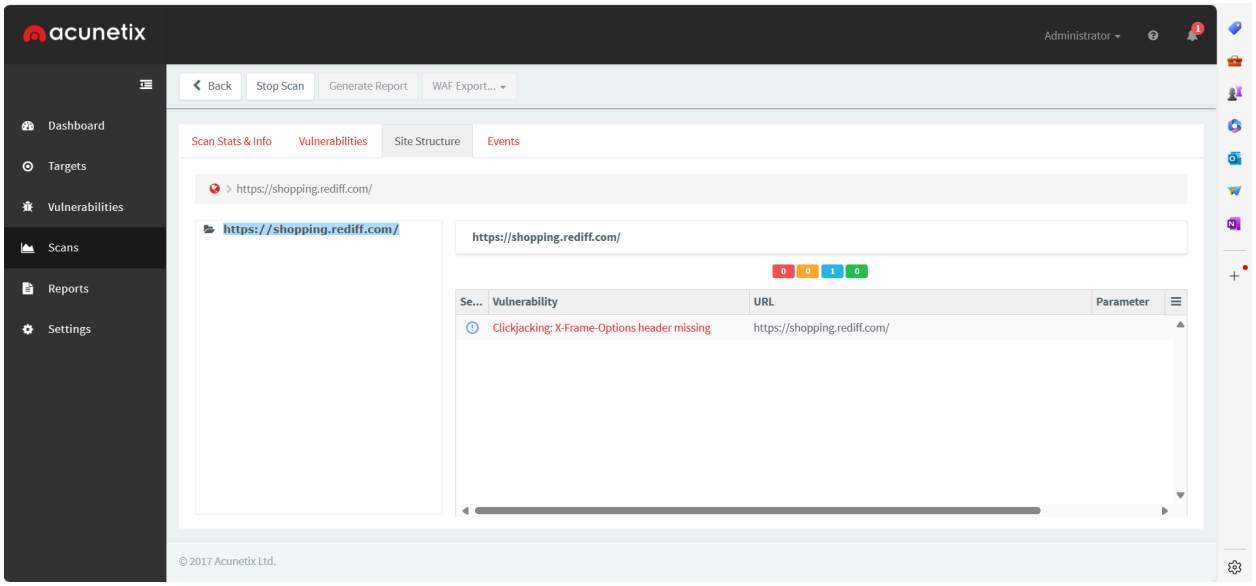


Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

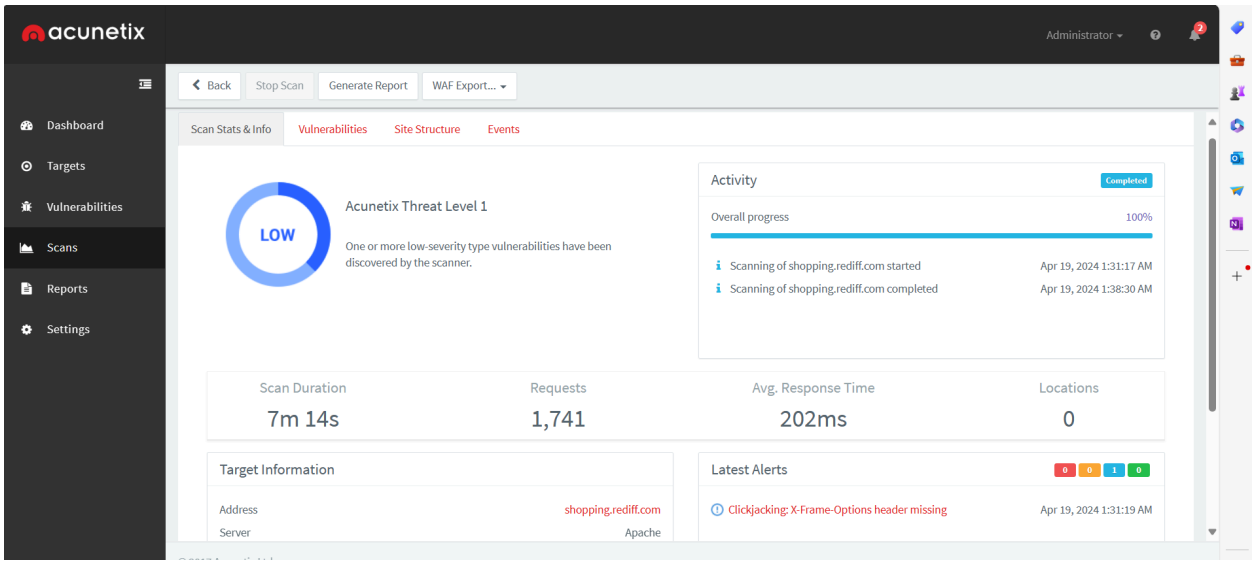


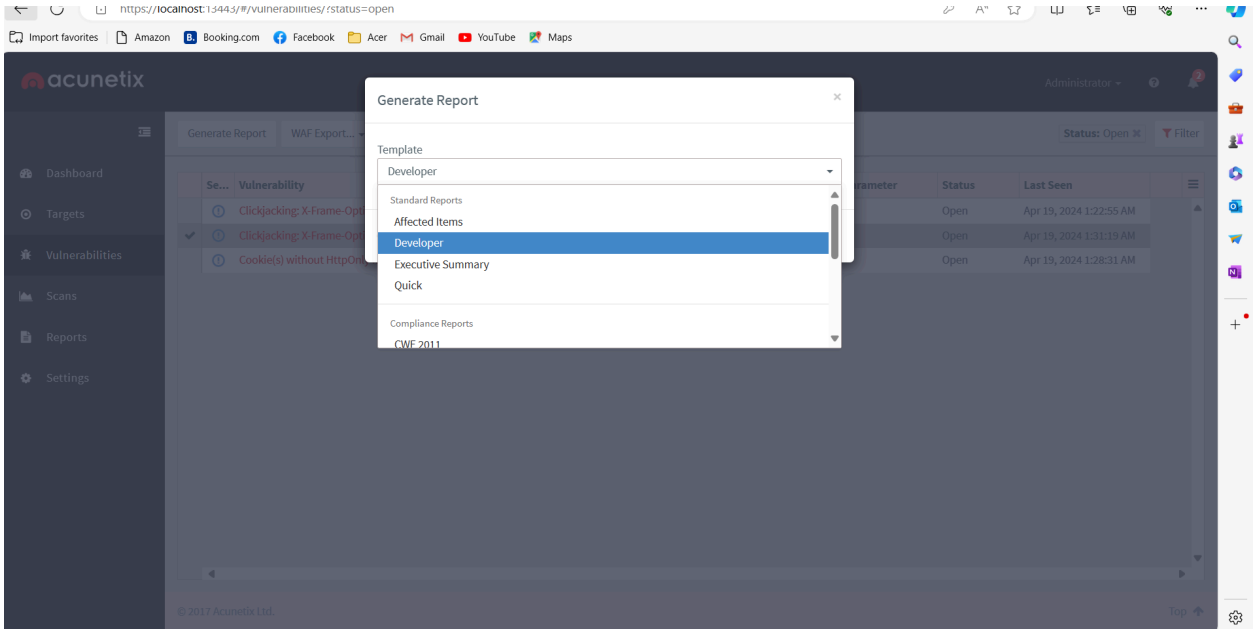


Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible



Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report


acunetix
Administrator
Back
Stop Scan
Generate Report
WAF Export...
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Scan Stats & Info
Vulnerabilities
Site Structure
Events
LOW
Acunetix Threat Level 1
One or more low-severity type vulnerabilities have been discovered by the scanner.
Activity
Completed
Overall progress
100%
Scanning of shopping.rediff.com started
Apr 19, 2024 1:31:17 AM
Scanning of shopping.rediff.com completed
Apr 19, 2024 1:38:30 AM
Scan Duration
7m 14s
Requests
1,741
Avg. Response Time
202ms
Locations
0
Target Information
Address
shopping.rediff.com
Server
Apache
Latest Alerts
Clickjacking: X-Frame-Options header missing
Apr 19, 2024 1:31:19 AM


https://localhost:13443/#/vulnerabilities/?status=open
Import favorites
Amazon
Booking.com
Facebook
Acer
Gmail
YouTube
Maps
acunetix
Generate Report
Template
Developer
Standard Reports
Affected Items
Developer
Executive Summary
Quick
Compliance Reports
CWE 2011

Selected vulnerabilities

Scan details

Scan information	
Start url	https://shopping.rediff.com/
Host	https://shopping.rediff.com/

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

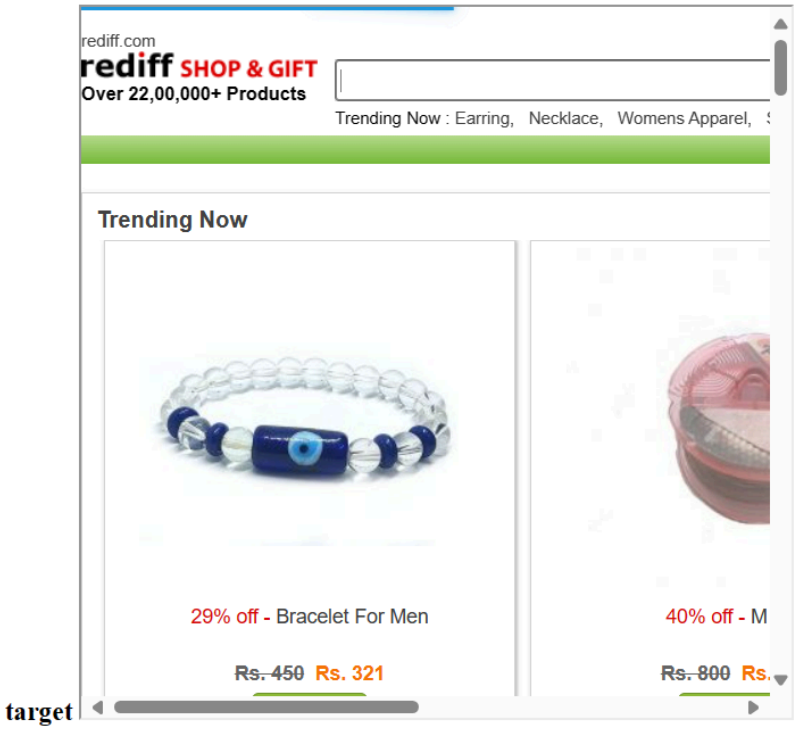
Alerts distribution

Total alerts found	1
High	0
Medium	0
Low	1
Informational	0

Step 12: In shoprediff website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe

clickjacking

iframe

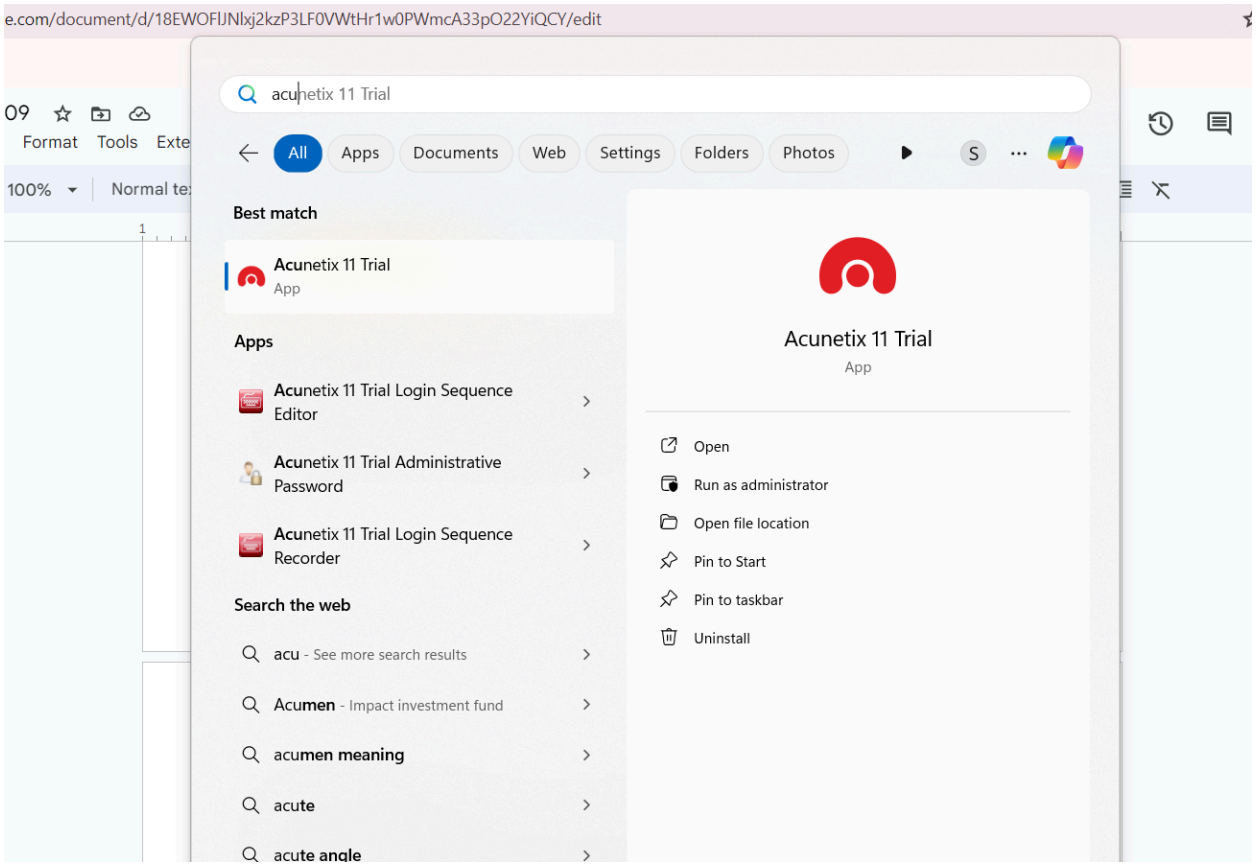


target

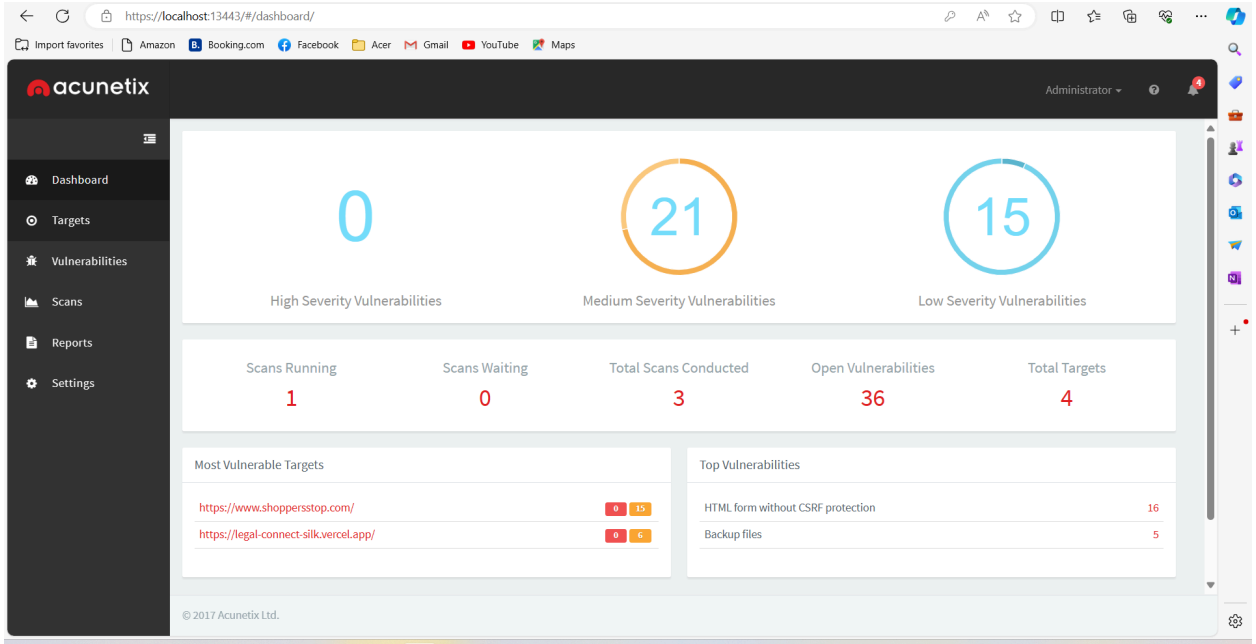
Website 2 : https://www.ebay.com/

Step 1: To perform the web application vulnerability scanning we are going to use the Acunetix vulnerability scanning tool, so firstly we need to download this tool to perform the scanning

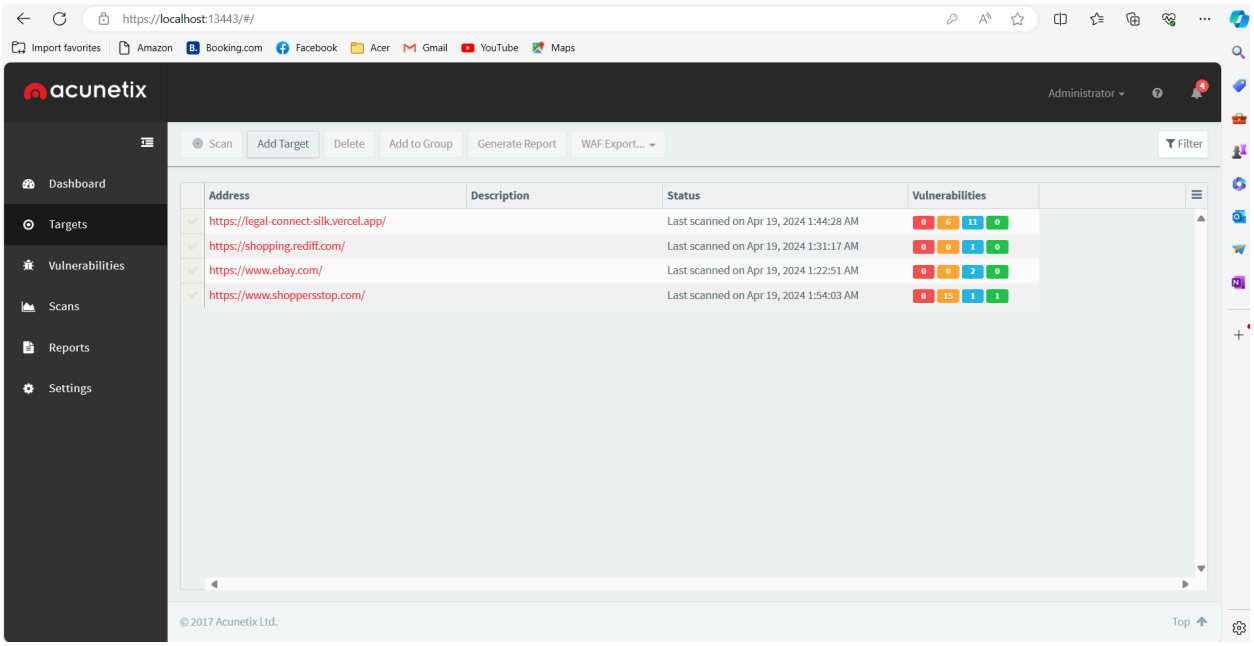
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



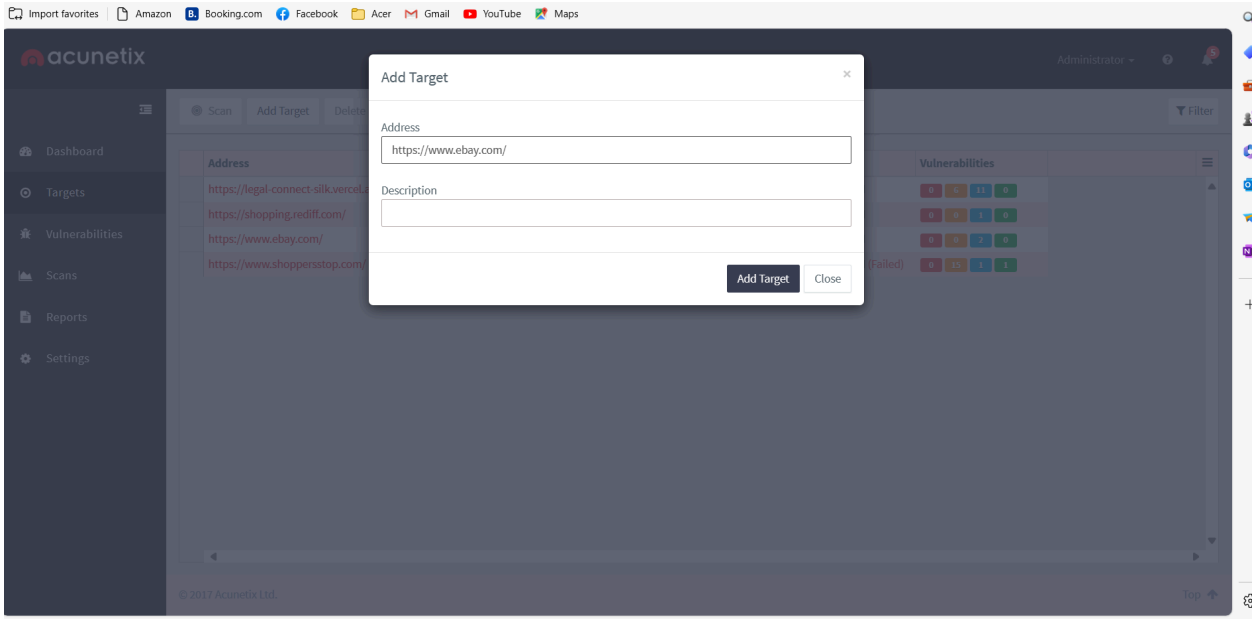
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



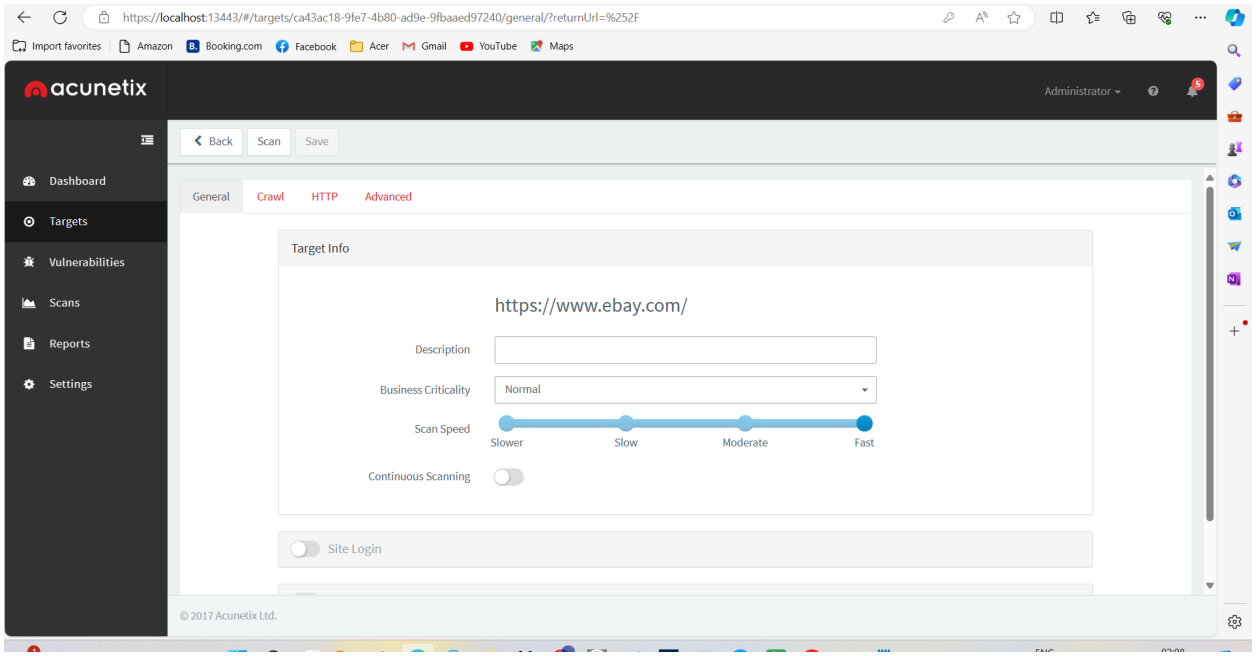
Step 4 : Go to the targets open and click on add target , In top there is a add target button

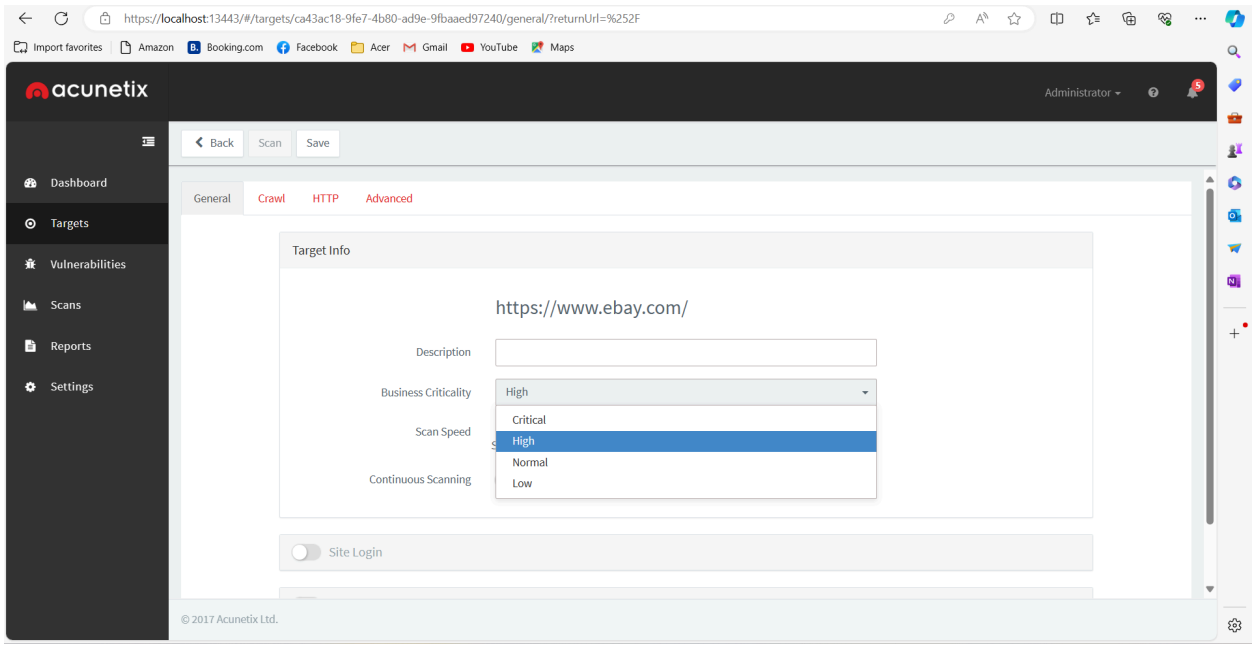


Step 5: Once you click on the add target button you have the option of adding a particular target link, we enter the link there and click on add target

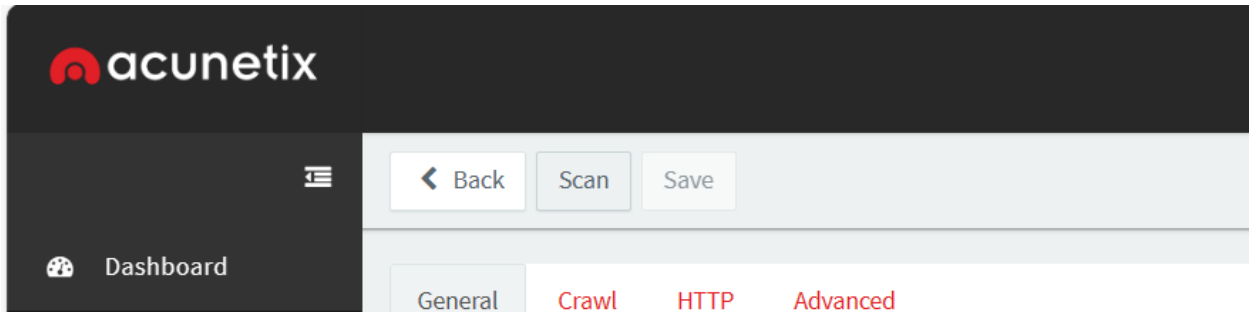


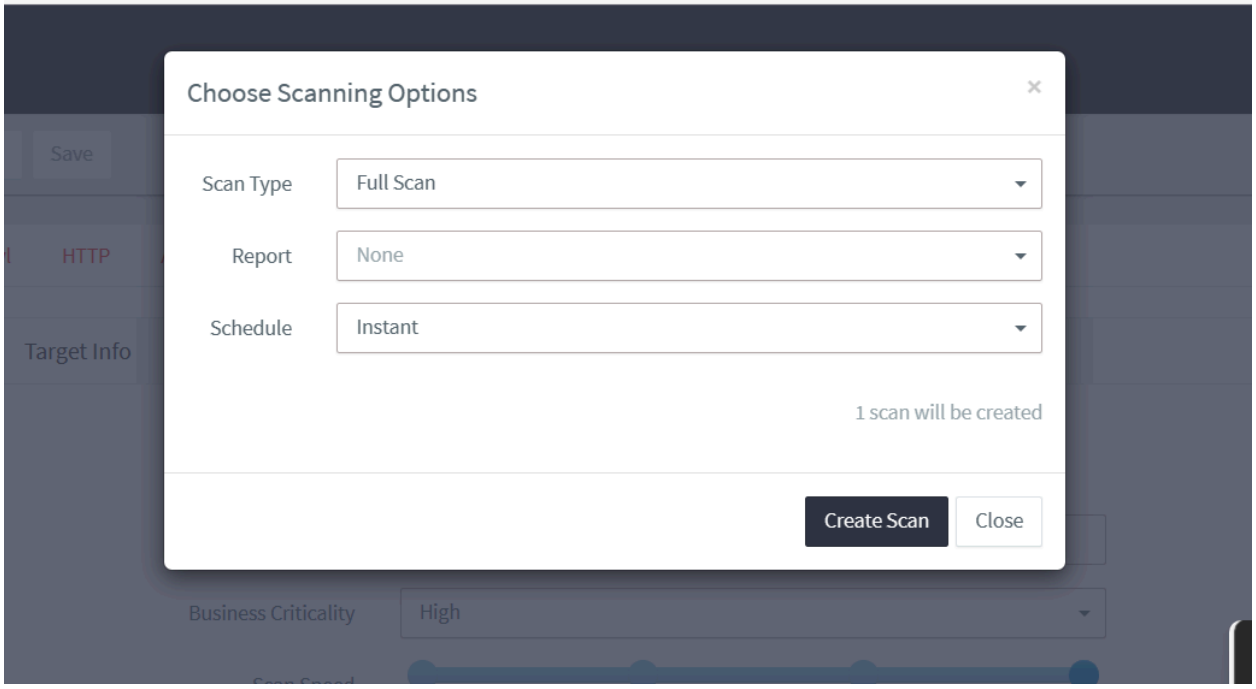
Step 6: Once you add target we get a interface where we set the business Criticality to high,low,medium,critical, once we add that we can click on save button



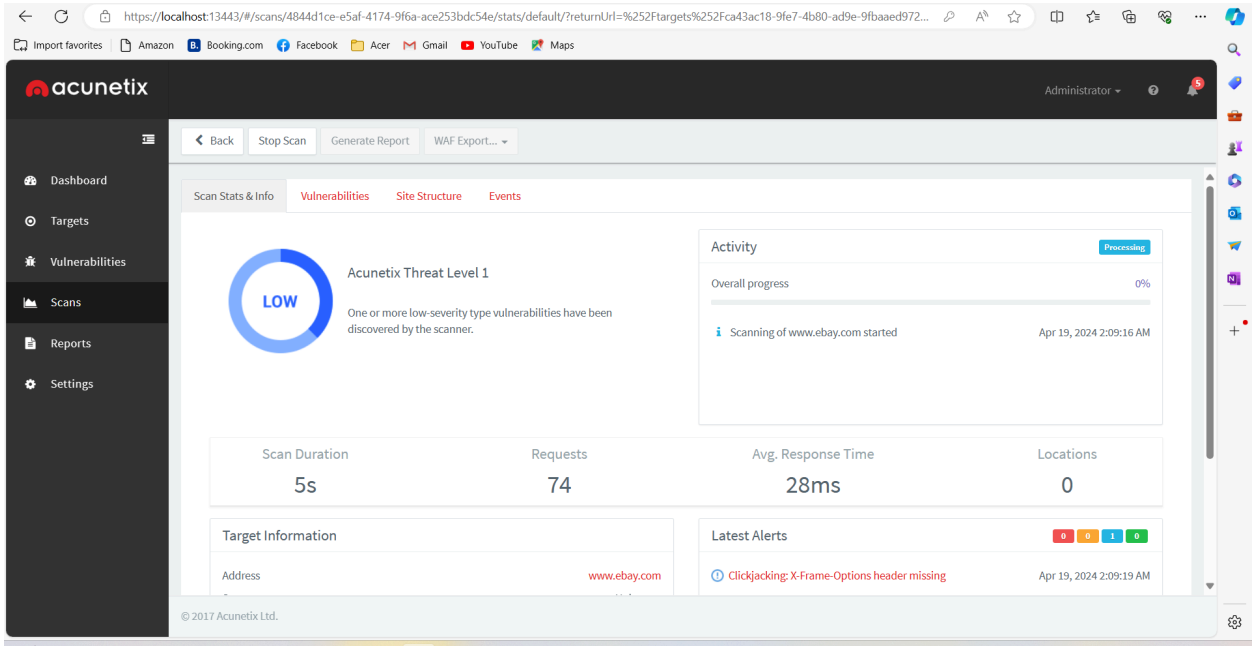


Step 7: Then click on the scan button on the top to start scanning the web application

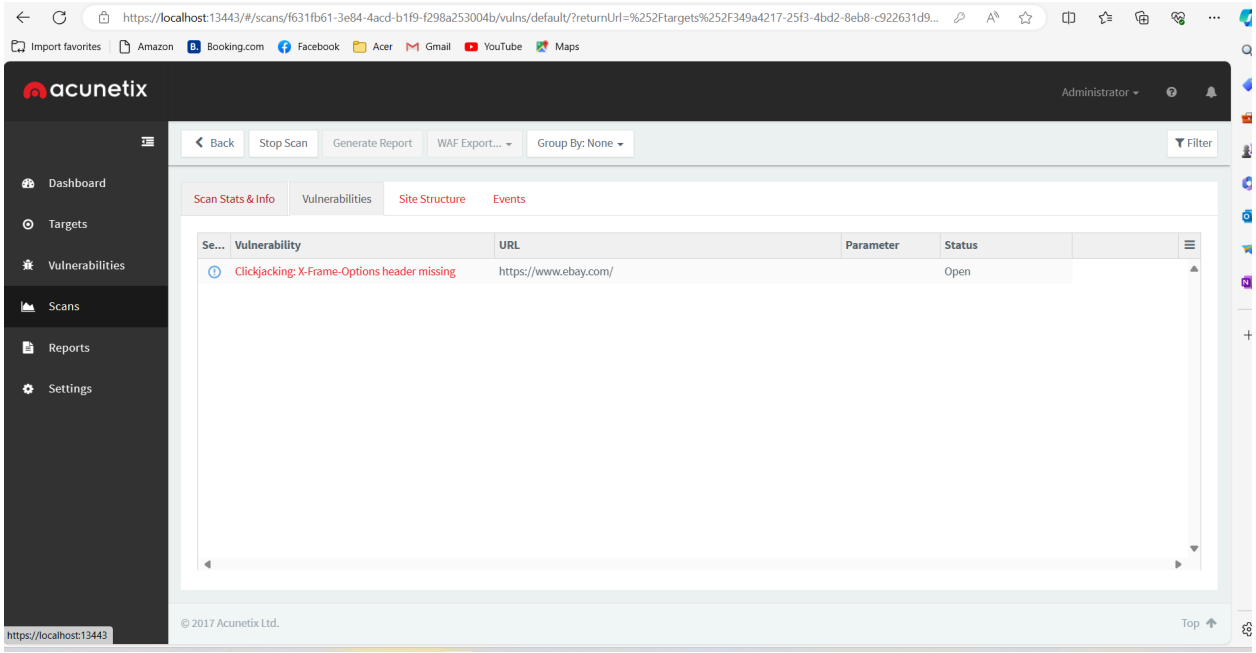


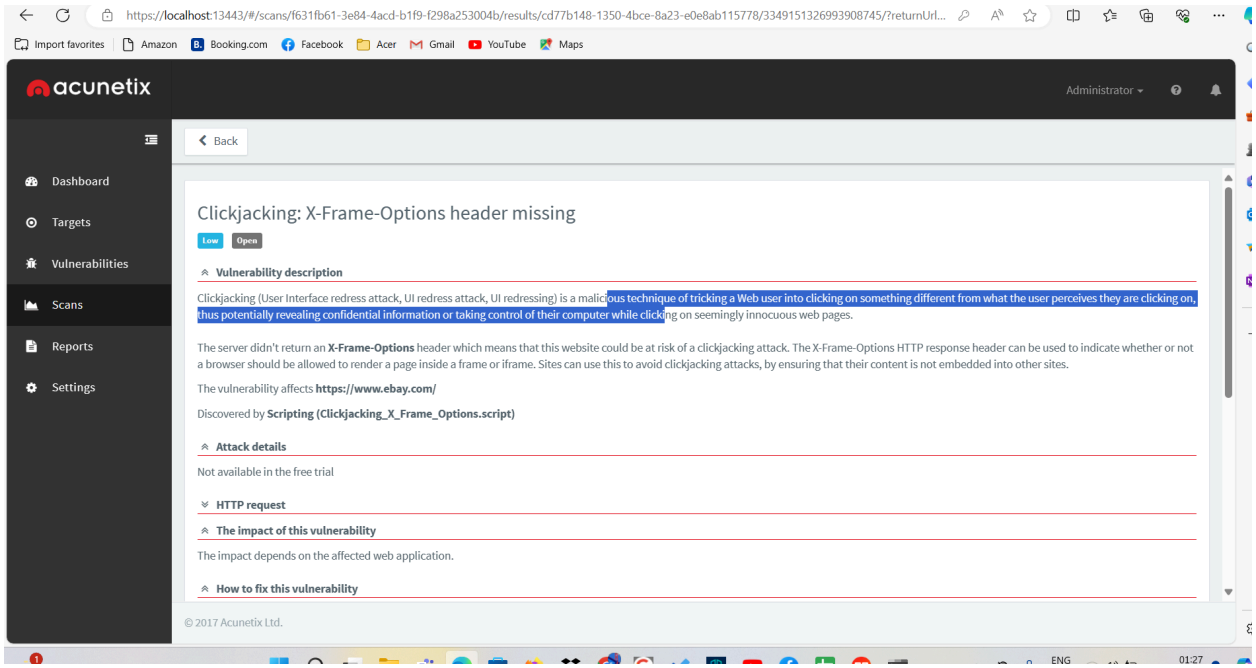


Step 8: Now the scanning will be started and we can see various like activity like how much scan is performed

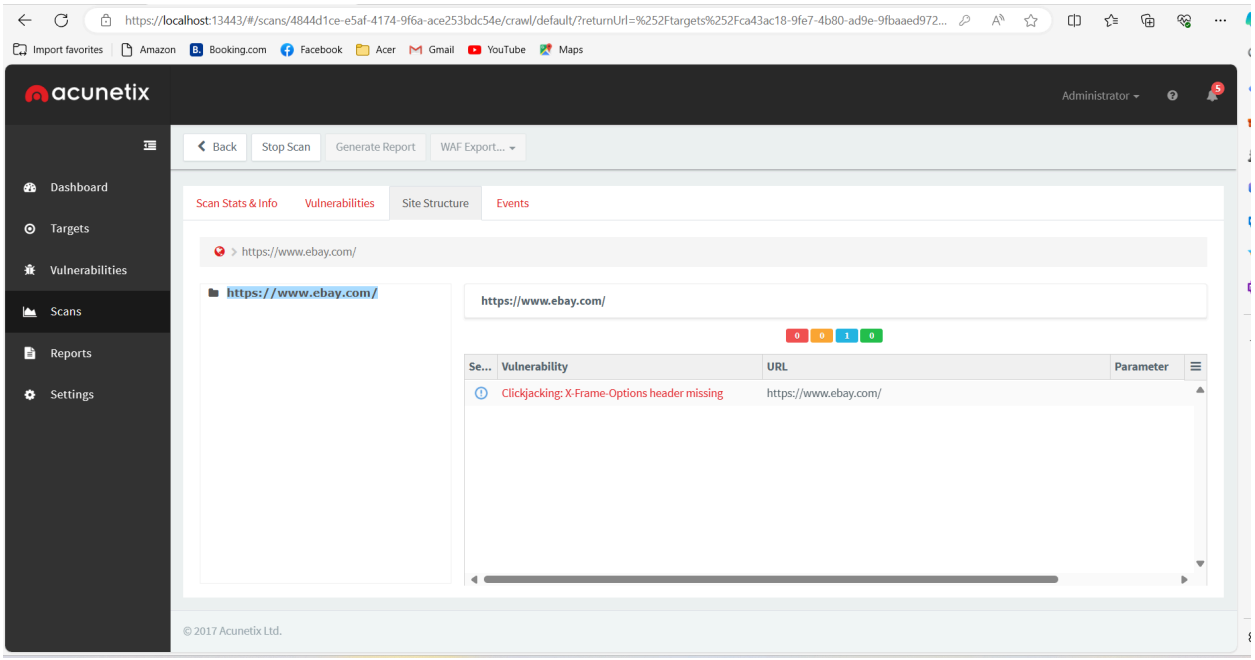


Step 9: There is a vulnerability tab, in that we can see all the vulnerabilities detected and if you click on that vulnerability you can see the detailed description about the vulnerability

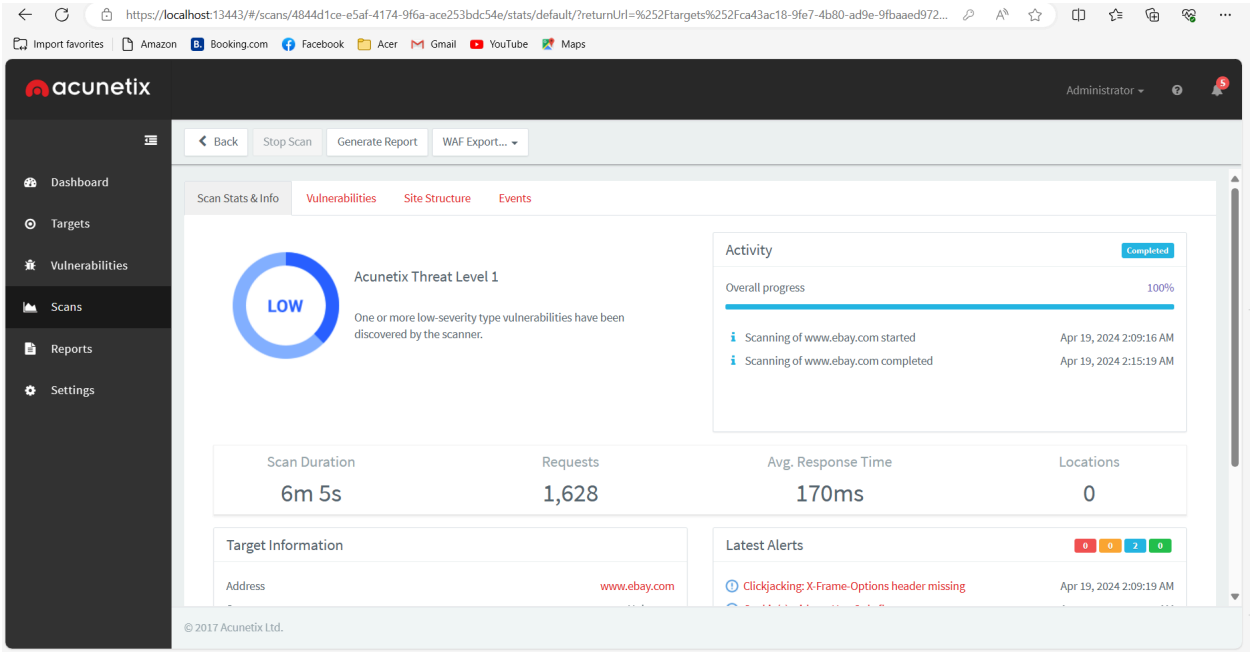


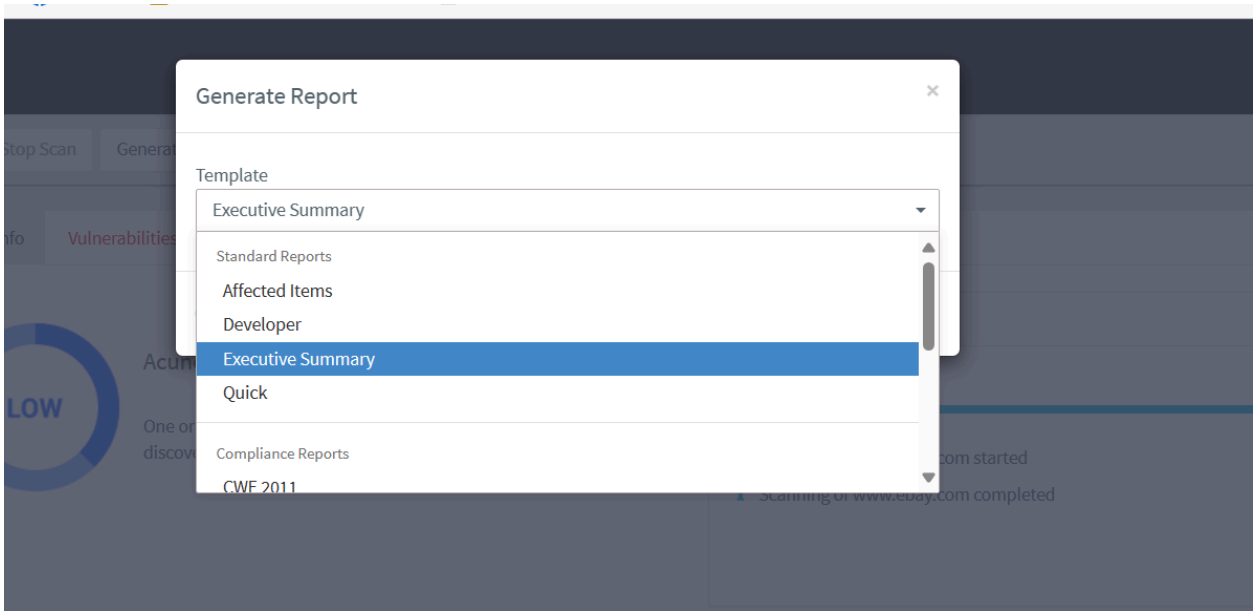


Step 10: There is one more tab in which we can see the site structure , how the site is been structure is completely visible



Step 11: Once the scan is completed , we can click on generate report tab and select the template that we want for report generation and then click on generate report





Scan of https://www.ebay.com/

Scan details

Scan information	
Start time	19/04/2024, 02:09:15
Start url	https://www.ebay.com/
Host	https://www.ebay.com/
Scan time	6 minutes, 5 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	2
High	0
Medium	0
Low	2
Informational	0

Step 12: In ebay website we found that it was vulnerable to clickjacking attack, so we tried to see if it was actually vulnerable to clickjacking attack and as the result it was vulnerable , because we could have the ebay website in the iframe

File | C:/Users/simon/Downloads/click.html

Import favorites | Amazon | Booking.com | Facebook | Acer | Gmail | YouTube | Maps

clickjacking

iframe

target