

## Task 9

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

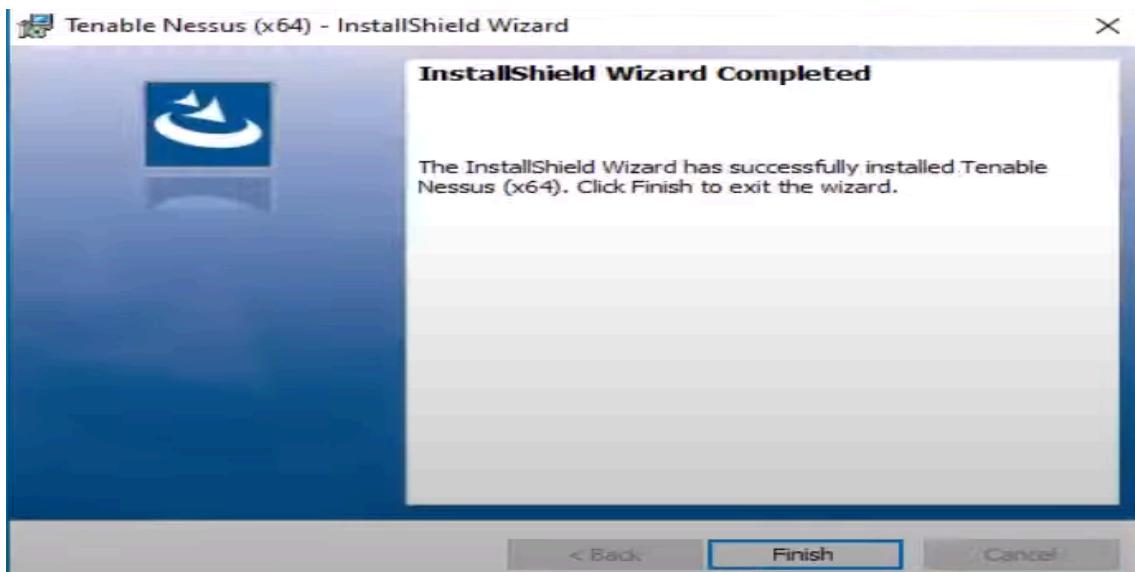
- a) Host Discovery Scan
- b) Basic Network Scan

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

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

The screenshot shows a web browser window with the URL [tenable.com/downloads/nessus?loginAttempted=true](https://www.tenable.com/downloads/nessus?loginAttempted=true) in the address bar. The page is titled "Tenable Nessus". On the left, there's a sidebar with links like "Tenable Nessus", "Tenable Nessus Agent", "Tenable Nessus Network Monitor", etc. The main content area has two sections: "1 Download and Install Nessus" and "2 Start and Setup Nessus". Under "1 Download and Install Nessus", there are dropdown menus for "Version" (set to "Nessus - 10.7.2") and "Platform" (set to "Windows - x86\_64"). Below these are buttons for "Download" (with a "Checksum" link), "Download by curl", "Docker", and "Virtual Machines". To the right, there's a "Summary" section with release details: "Release Date: Apr 2, 2024", "Release Notes: Tenable Nessus 10.7.2 Release Notes", and "Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above), RPM-GPG-KEY-Tenable-2048 (10.3 & below)".

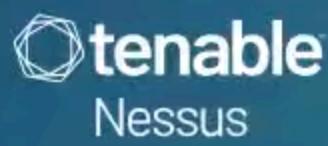
Step2 : Once you have download and have an msi file just double click and download the default and finish it



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



Initializing

Please wait while Nessus is initializing.

© 2023 Tenable®, Inc.

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”



## Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

- Set up a purchased instance of Nessus
- Start a trial of Nessus Expert
- Start a trial of Nessus Professional
- Register for Nessus Essentials
- Link Nessus to another Tenable product

Back

Continue

© 2023 Tenable™, Inc.

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

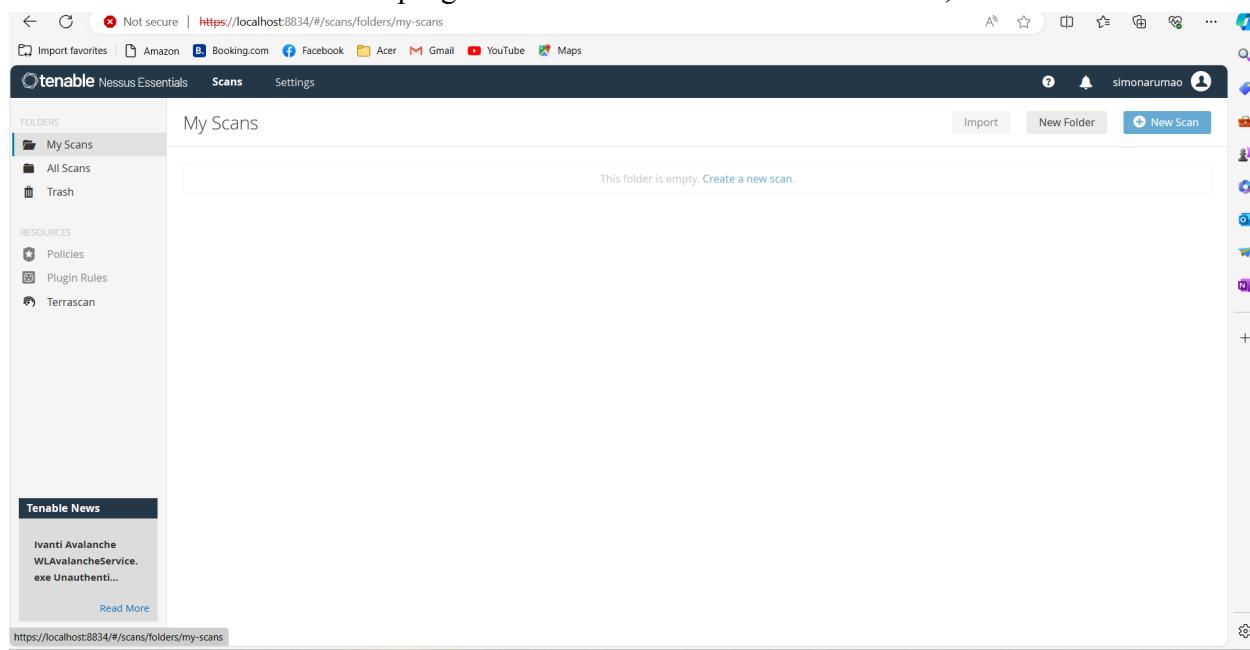
Step 7 : Then will see the license information just click on continue

Step 8 : Then will get an option to get sign in into the scanner using username and password

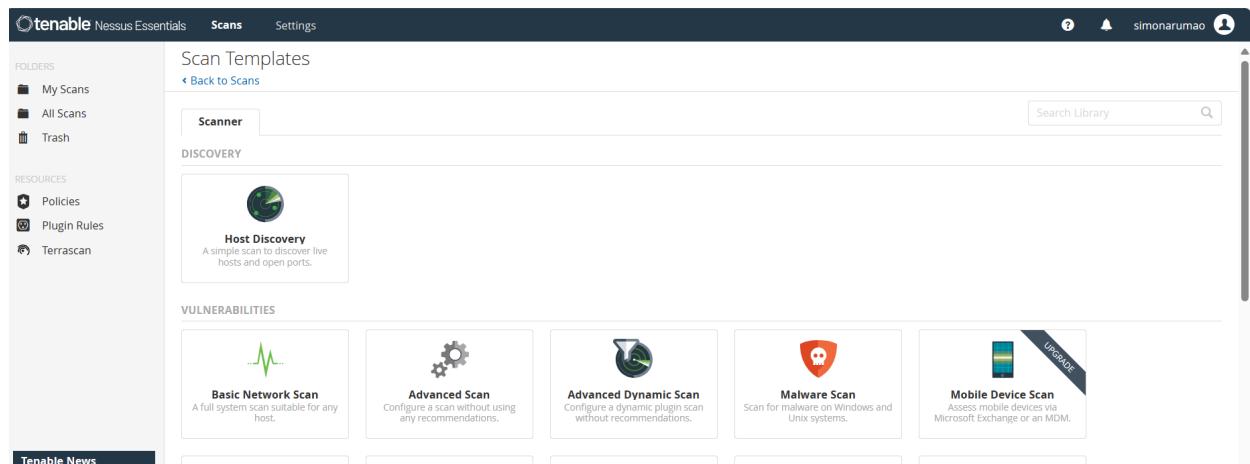
Step 9 : Now it keep on initializing and we will enter into the nessus tool, but here the nessus tool will take some time to get all the plugins, on the top right corner there is a circle if that stops means all plugins are installed and now we are ready to test the vulnerability

## 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

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, basichost, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'New Scan / Host Discovery' with a 'Back to Scan Templates' link. It has tabs for 'Settings' (selected) and 'Plugins'. Under 'Settings', there's a 'BASIC' section with 'General', 'Schedule', 'Notifications', 'DISCOVERY' (selected), 'REPORT', and 'ADVANCED' options. In the 'DISCOVERY' section, the 'Name' field is empty, 'Description' is empty, 'Folder' is set to 'My Scans', and the 'Targets' field contains 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'. Below the targets field are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

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)

This screenshot shows the same 'New Scan / Host Discovery' configuration page as the previous one, but with changes made to the 'Name' and 'Targets' fields. The 'Name' field now contains 'host discovery'. The 'Targets' field now contains '10.0.0.1'. The rest of the configuration remains the same, including the 'Folder' set to 'My Scans'.

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

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . .
Link-local IPv6 Address . . . . : fe80::4689:d9ea:841a:68f8%9
IPv4 Address . . . . . : 10.0.0.6
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1

```

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

The screenshot shows the Tenable Nessus Essentials web interface. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans', 'basichost', 'All Scans', and 'Trash'. Under 'RESOURCES', there are 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is also present. The main content area has tabs for 'Scans' and 'Settings'. The 'Scans' tab is active, showing a 'REPORT' configuration screen. The 'Output' section contains several checkboxes:

- Allow users to edit scan results: When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name: Uses the host name rather than IP address for report output.
- Display hosts that respond to ping: Reports hosts that successfully respond to a ping.
- Display unreachable hosts: When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters: When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

At the bottom of the form are 'Save' and 'Cancel' buttons.

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

Not secure | <https://localhost:8834/#/scans/folders>

Import favorites | [Amazon](#) [Booking.com](#) [Facebook](#) [Acer](#) [Gmail](#) [YouTube](#) [Maps](#)

Tenable Nessus Essentials [Scans](#) [Settings](#) simonarumao

My Scans

Search Scans  1 Scan

Name	Schedule	Last Scanned	Launch
Host Discovery Local Network	On Demand	N/A	<a href="#">▶</a> <a href="#">X</a>

FOLDERS: My Scans, basichost, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Terrascan

Tenable News: Ivanti Avalanche, VLAvalancheService.exe Unauthenti... [Read More](#)

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

Import favorites | [Amazon](#) [Booking.com](#) [Facebook](#) [Acer](#) [Gmail](#) [YouTube](#) [Maps](#)

Tenable Nessus Essentials [Scans](#) [Settings](#) simonarumao

Host Discovery Local Network simona [Configure](#)

Hosts 6 Vulnerabilities 2 History 1

Filter  Search Hosts [X](#) 6 Hosts

Host	FQDN	Ports	%
10.0.0.7			100%
10.0.0.6			100%
10.0.0.4			100%
10.0.0.3			100%
10.0.0.2		135, 139, 445, 49664, 49665, 49666, 49667, 49668...	100%
10.0.0.1	www.routerlogin.com		100%

Scan Details

Policy: Host Discovery  
Status: Running (green circle)  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 12:08 AM

Vulnerabilities

Critical (red), High (orange), Medium (yellow), Low (light blue), Info (blue)

Tenable News: Microsoft Azure Synapse Analytics - Privilege Escalation [Read More](#)

Host Discovery Local Network simona

Configure Audit Trail Launch Report Export

Scan Details

Policy	Host Discovery
Status	Completed
Severity Base	CVSS v3.0
Scanner	Local Scanner
Start	Today at 12:08 AM
End	Today at 12:13 AM
Elapsed	5 minutes

Vulnerabilities

Critical  
High  
Medium  
Low  
Info

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

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:

✓ Insert page break between vulnerability results

Generate Report Cancel Save as default

10.0.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	2

Vulnerabilities Total: 2

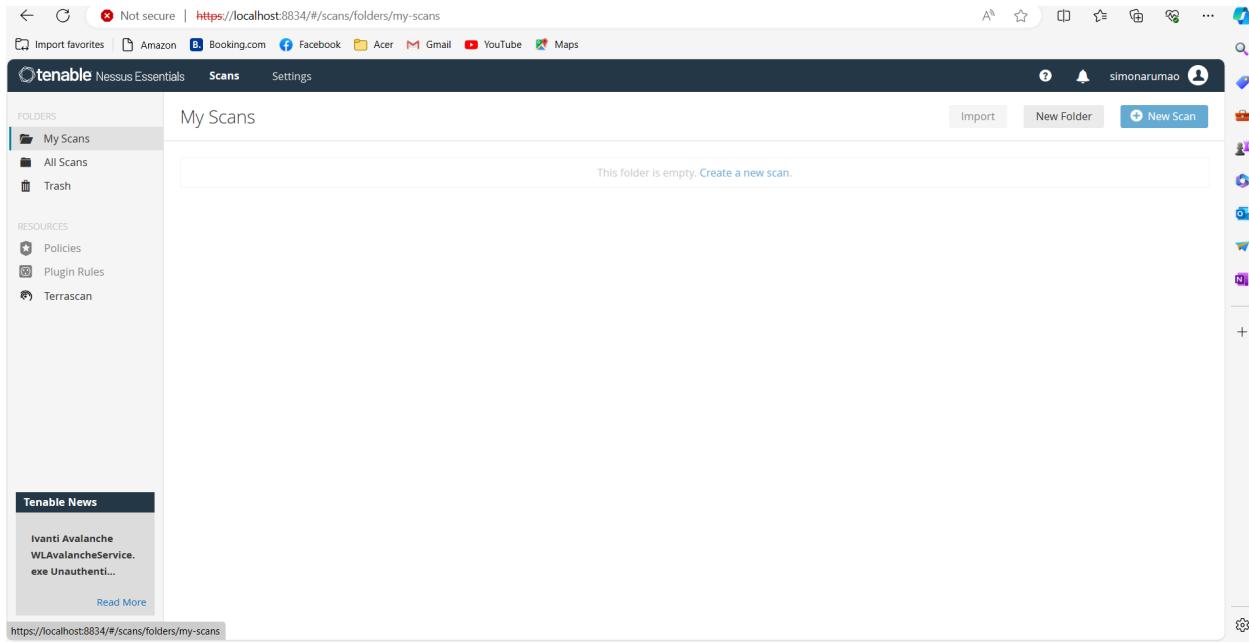
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10180	Ping the remote host

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

Powered by Adobe Acrobat

## 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 .



Not secure | <https://localhost:8834/#/scans/folders/my-scans>

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

Tenable Nessus Essentials **Scans** Settings

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News

Ivanti Avalanche  
WLAValancheService.exe Unauthenti...  
[Read More](#)

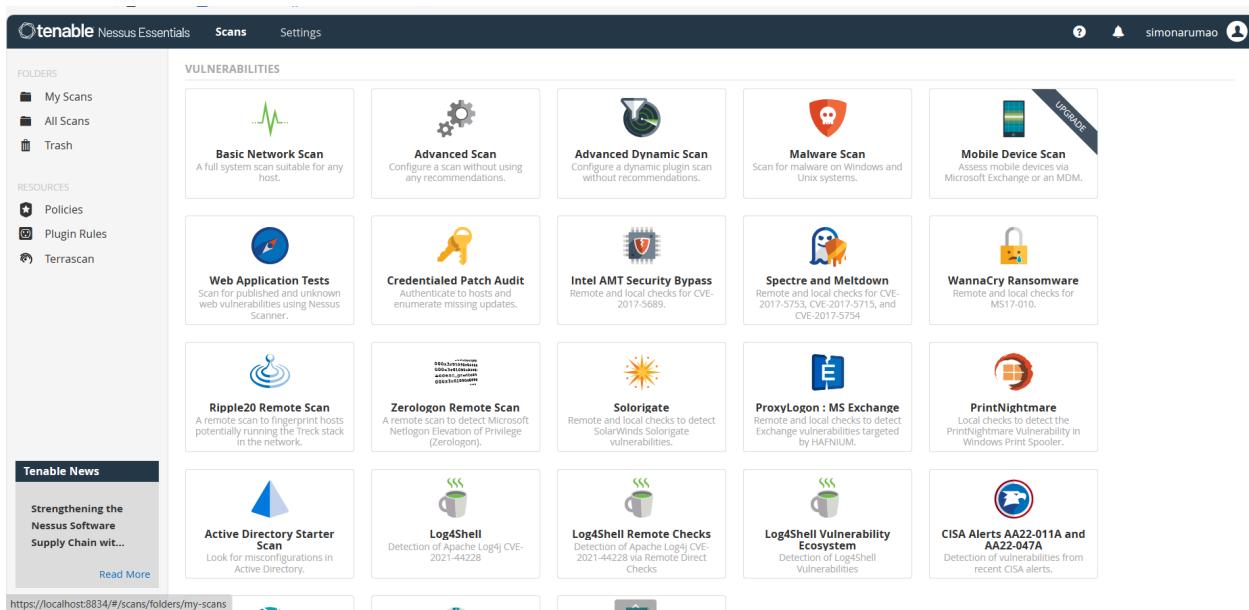
My Scans

This folder is empty. [Create a new scan.](#)

Import New Folder + New Scan

https://localhost:8834/#/scans/folders/my-scans

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



VULNERABILITIES

Basic Network Scan A full system scan suitable for any host.

Advanced Scan Configure a scan without using any recommendations.

Advanced Dynamic Scan Configure a dynamic plugin scan without recommendations.

Malware Scan Scan for malware on Windows and Unix systems.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. **UPGRADE**

Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialled Patch Audit Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware Remote and local checks for MS17-010.

Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solarigate Remote and local checks to detect SolarWinds Solarigate vulnerabilities.

ProxyLogon + MS Exchange Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan Look for misconfigurations in Active Directory.

Log4Shell Detection of Apache Log4j CVE-2021-44228.

Log4Shell Remote Checks Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks.

Log4Shell Vulnerability Ecosystem Detection of Log4Shell Vulnerabilities

CISA Alerts AA22-011A and AA22-047A Detection of vulnerabilities from recent CISA alerts.

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News

Strengthening the Nessus Software Supply Chain wit...  
[Read More](#)

https://localhost:8834/#/scans/folders/my-scans

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

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area has tabs for 'Settings', 'Credentials', and 'Plugins'. Under 'Settings', the 'BASIC' tab is selected, showing fields for 'Name' (empty), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (a text input field containing 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). Below these are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

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

This screenshot shows the same configuration page as above, but with specific values entered. The 'Name' field contains 'basic network scan', and the 'Targets' field contains '10.0.0.2'. The rest of the fields ('Description', 'Folder', 'Upload Targets', 'Add File', 'Save', and 'Cancel') remain the same.

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

**Output**

- Allow users to edit scan results
 

When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
- Designate hosts by their DNS name
 

Uses the host name rather than IP address for report output.
- Display hosts that respond to ping
 

Reports hosts that successfully respond to a ping.
- Display unreachable hosts
 

When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
- Display Unicode characters
 

When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

**Save** **Cancel**

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

**Scan Type**

- Port scan (common ports)
- Port scan (common ports)
- Port scan (all ports)
- Custom**

**Port Scanner Settings:**

- Scan common ports
- Use netstat if credentials are provided
- Use SYN scanner if necessary

**Ping hosts using:**

- TCP
- ARP
- ICMP (2 retries)

**Save** **Cancel**

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

New Scan / Basic Network Scan

Scan Type

- Default
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick)
- Scan for all web vulnerabilities (complex)
- Custom

Disable web application scanning

Save Cancel

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

New Scan / Basic Network Scan

Scan Type

General Settings:

- Avoid potential false alarms
- Disable CGI scanning

Web Applications:

- Disable web application scanning

Save Launch Cancel

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

Not secure | <https://localhost:8834/#/scans/reports/12/hosts>

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

**Tenable Nessus Essentials** Scans Settings

basic network scan

Hosts 1 Vulnerabilities 27 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
10.0.0.2	7	125 99%

Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:22 AM

Vulnerabilities

Critical  
High  
Medium  
Low  
Info

Not secure | <https://localhost:8834/#/scans/reports/12/vulnerabilities>

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

**Tenable Nessus Essentials** Scans Settings

basic network scan

Hosts 1 Vulnerabilities 27 History 1

Filter Search Vulnerabilities 27 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MEDIUM	5.3	...	SMB Signing not required	Misc.	1
MIXED	...	...	SSL (Multiple Issues)	General	25
INFO	...	...	TLS (Multiple Issues)	General	7
INFO	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	TLS (Multiple Issues)	Service detection	5
INFO	...	...	HTTP (Multiple Issues)	Web Servers	5
INFO	...	...	Microsoft Windows (Multiple Issues)	Windows	2
INFO	...	...	Splunk (Multiple Issues)	Web Servers	2
INFO	...	...	Netstat Portscanner (SSH)	Port scanners	43
INFO	...	...	DCE Services Enumeration	Windows	8

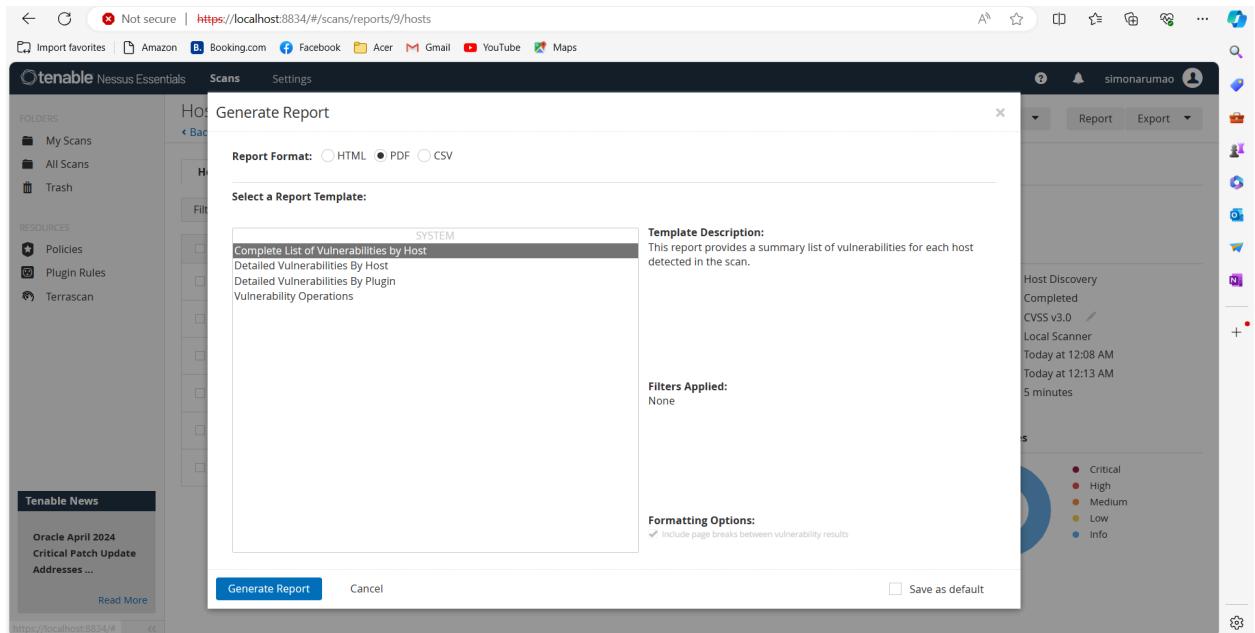
Scan Details

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 12:22 AM

Vulnerabilities

Critical  
High  
Medium  
Low  
Info

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



The screenshot shows a PDF document generated by Adobe Acrobat. The header includes standard toolbar icons like Draw, Ask Copilot, and a search bar. The main content is for host 10.0.0.1. At the top, there's a severity distribution chart with five bars: Critical (0), High (0), Medium (0), Low (0), and Info (2). Below the chart is a table of vulnerabilities:

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	Total: 2
INFO	N/A	-	19506	Nessus Scan Information	
INFO	N/A	-	10180	Ping the remote host	

A note at the bottom states: '\* indicates the v3.0 score was not available; the v2.0 score is shown.'

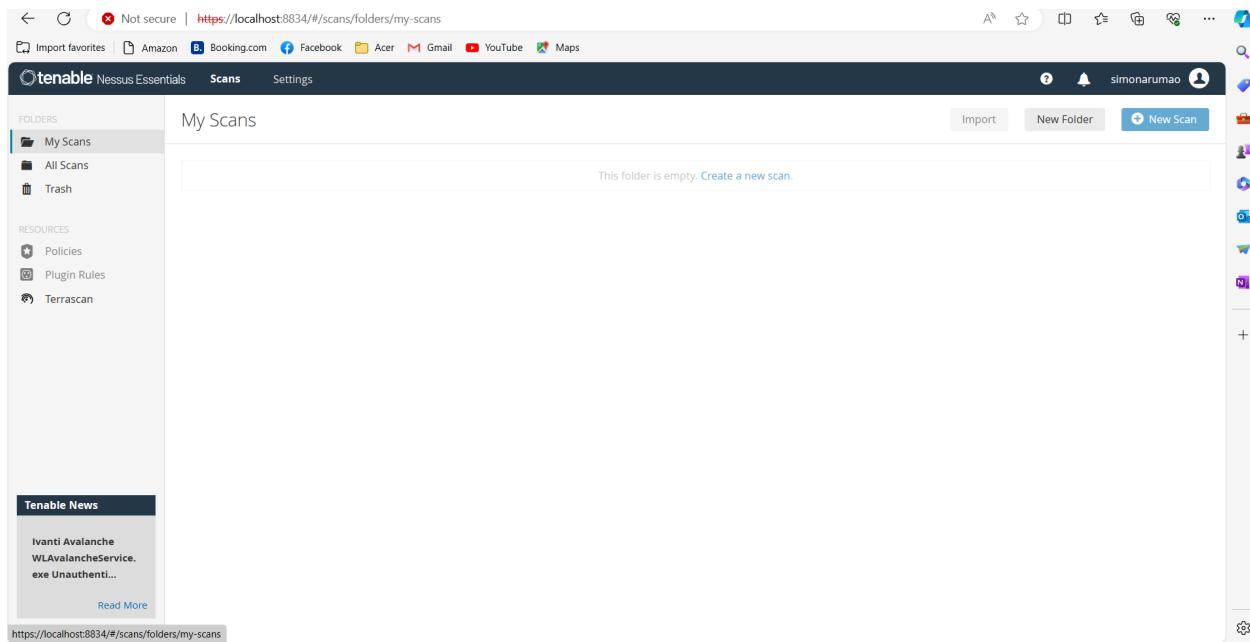
In the bottom right corner, it says 'Powered by Adobe Acrobat' with the Adobe logo.

## B. Perform Web Application Tests Scan in the Nessus tool on the below targets:

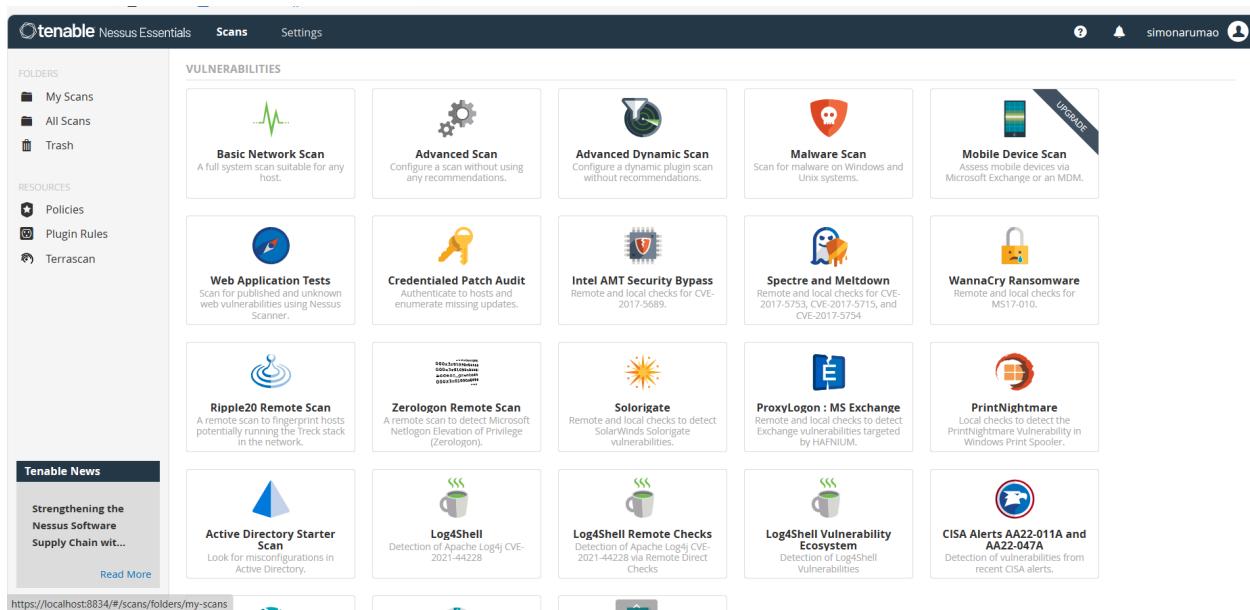
- a) <http://testasp.vulnweb.com/>
- b) <https://www.shoppersstop.com/>

### 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

New Scan / Web Application Tests

Back to Scan Templates

Settings    Credentials    Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name:

Description:

Folder: My Scans

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Upload Targets    Add File

Save    Cancel

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

New Scan / Web Application Tests

Back to Scan Templates

Settings    Credentials    Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: testasp web application

Description:

Folder: My Scans

Targets: testasp.vulnweb.com

Upload Targets    Add File

Save    Cancel

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

**Settings** Plugins

**BASIC** **DISCOVERY** **REPORT** **ADVANCED**

**Output**

Allow users to edit scan results  
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.

Designate hosts by their DNS name  
Uses the host name rather than IP address for report output.

Display hosts that respond to ping  
Reports hosts that successfully respond to a ping.

Display unreachable hosts  
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.

Display Unicode characters  
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save Cancel

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

New Scan / Web Application Tests [Back to Scan Templates](#)

**Settings** Credentials Plugins

**BASIC** **DISCOVERY** **ASSESSMENT** **REPORT** **ADVANCED**

Scan Type: Port scan (common ports)

**General Settings:**  
Always test the local Nessus host  
Use fast network discovery

**Port Scanner Settings:**  
Scan common ports  
Use netstat if credentials are provided  
Use SYN scanner if necessary

**Ping hosts using:**  
TCP  
ARP  
ICMP (2 retries)

Save Cancel

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

New Scan / Web Application Tests

Scan Type

- Scan for all web vulnerabilities (quick)
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick) **(selected)**
- Scan for all web vulnerabilities (complex)
- Custom

Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 5 minutes (max)

Save Cancel

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

Scan Type

Default

General Settings:

- Avoid potential false alarms
- Disable CGI scanning

Web Applications:

- Disable web application scanning

Save Launch Cancel

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

Screenshot of the Tenable Nessus Essentials interface showing a completed scan named "testasp".

**Scan Details:**

- Policy: Web Application Tests
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 19 at 11:44 PM
- End: Today at 12:14 AM
- Elapsed: 30 minutes

**Vulnerabilities:**



Critical	High	Medium	Low	Info
0	0	0	0	10

Screenshot of the Tenable Nessus Essentials interface showing a completed scan named "testasp".

**Scan Details:**

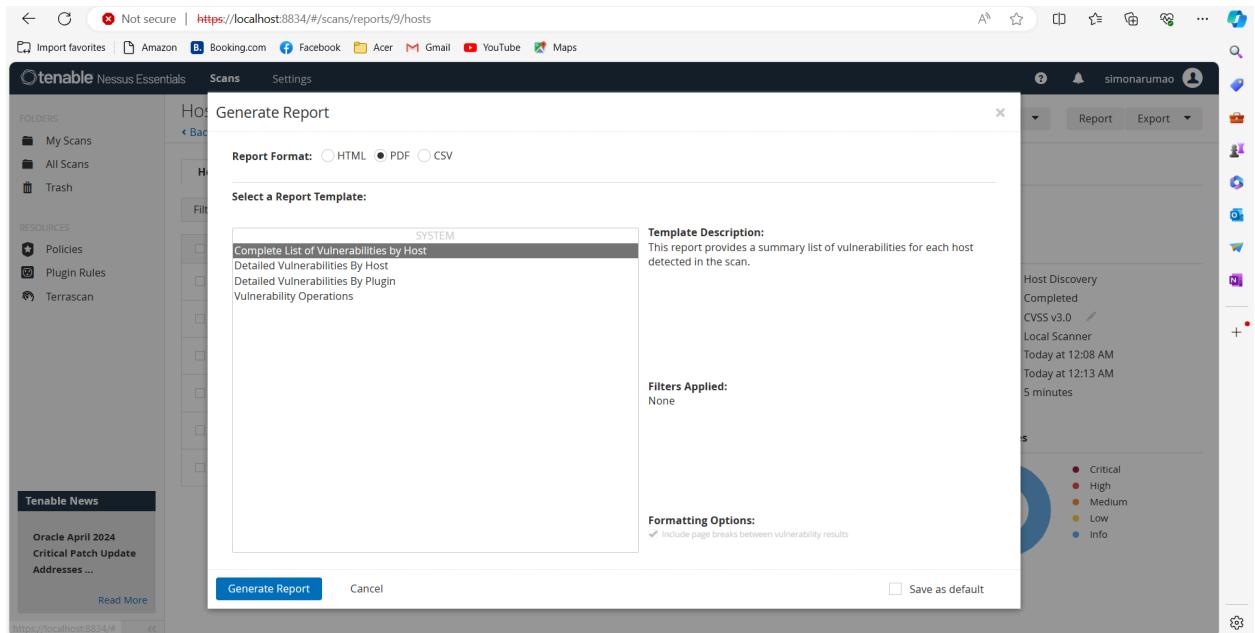
- Policy: Web Application Tests
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: April 19 at 11:44 PM
- End: Today at 12:14 AM
- Elapsed: 30 minutes

**Vulnerabilities:**



Sev	CVSS	VPR	Name	Family	Count	Actions
INFO	...	...	3 HTTP (Multiple Issues)	Web Servers	3	🔗 🔍
INFO	...	...	2 HTTP (Multiple Issues)	CGI abuses	2	🔗 🔍
INFO			External URLs	Web Servers	1	🔗 🔍
INFO			Nessus Scan Information	Settings	1	🔗 🔍
INFO			Nessus SYN scanner	Port scanners	1	🔗 🔍
INFO			Web Application Sitemap	Web Servers	1	🔗 🔍
INFO			Web Server Unconfigured - Default I...	Web Servers	1	🔗 🔍

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



The screenshot shows a PDF document generated from the Nessus scan. At the top, it displays the IP address **10.0.0.1**. Below this is a horizontal bar chart showing the distribution of vulnerabilities by severity: Critical (0), High (0), Medium (0), Low (0), and Info (2). The PDF then lists the vulnerabilities found:

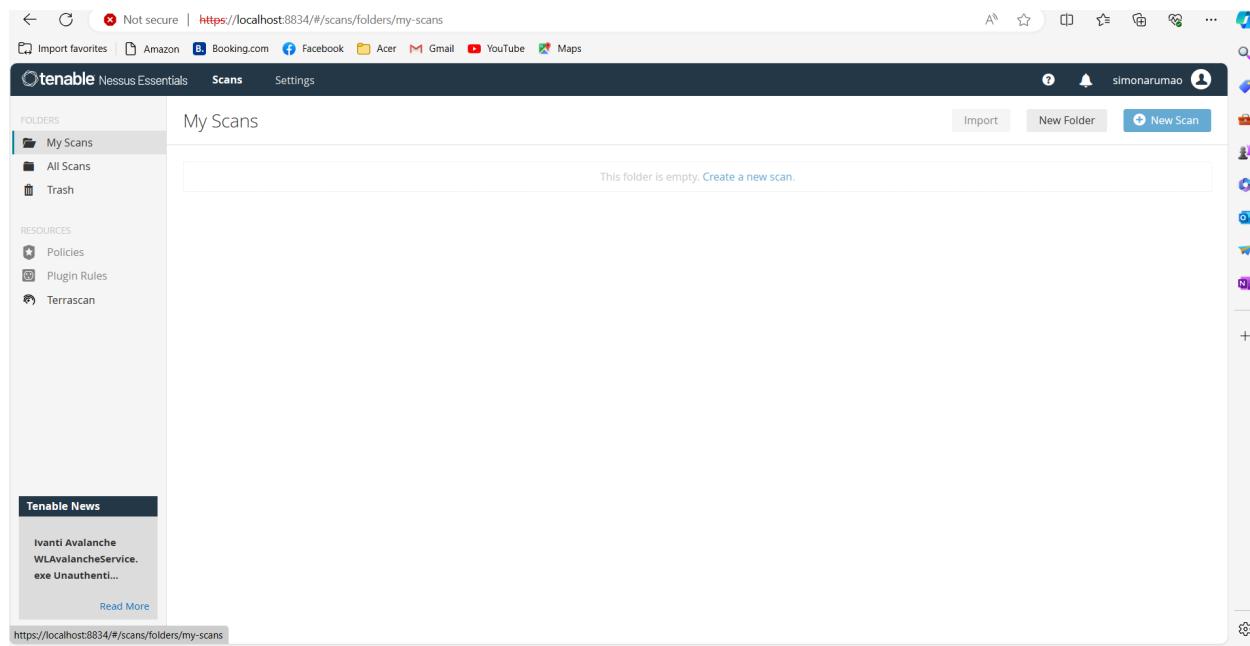
Severity	CVSS V3.0	VPR Score	Plugin	Name	Total
INFO	N/A	-	19506	Nessus Scan Information	2
INFO	N/A	-	10180	Ping the remote host	

A note at the bottom states: '\* indicates the v3.0 score was not available; the v2.0 score is shown.'

In the bottom right corner of the PDF, it says 'Powered by Adobe Acrobat'.

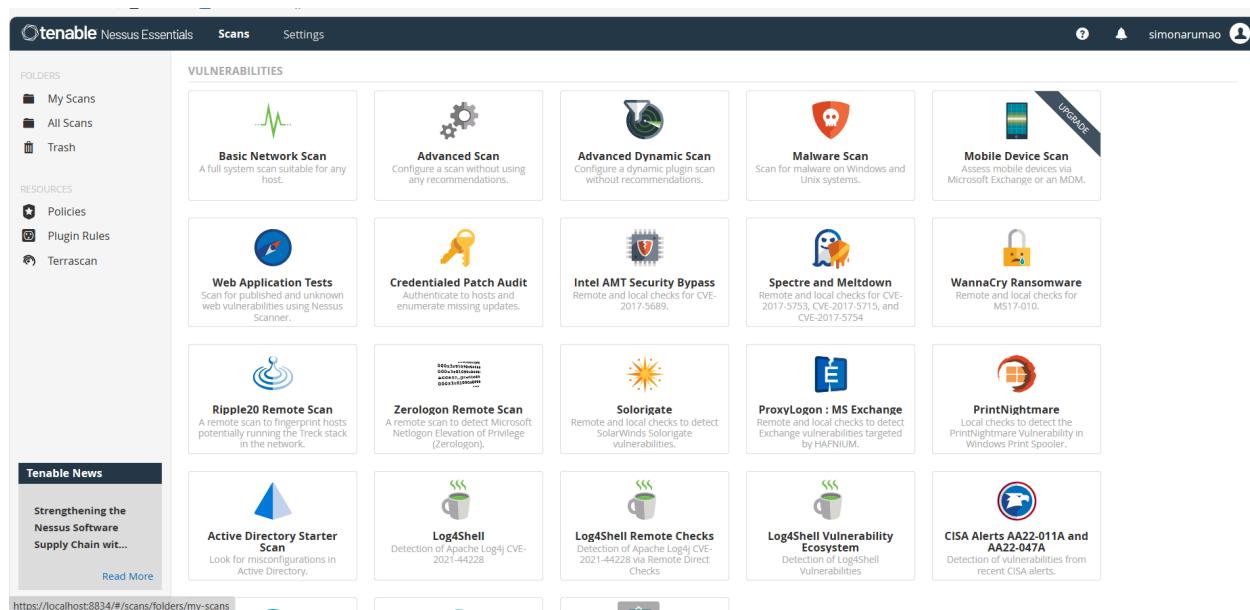
## Web application test on ShopperStop

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 .



The screenshot shows the Tenable Nessus Essentials interface. At the top, there's a navigation bar with links for Import favorites, Amazon, Booking.com, Facebook, Acer, Gmail, YouTube, and Maps. The main title is 'Tenable Nessus Essentials'. Below it, the 'Scans' tab is selected. On the left, there's a sidebar with 'FOLDERS' containing 'My Scans', 'All Scans', and 'Trash'. Under 'RESOURCES', there are links for Policies, Plugin Rules, and Terrascan. A 'Tenable News' section on the left has a link to 'Ivanti Avalanche' and a 'Read More' button. The main content area is titled 'My Scans' and displays a message: 'This folder is empty. Create a new scan.' A blue 'New Scan' button is located in the top right of this area. The URL in the address bar is https://localhost:8834/#/scans/folders/my-scans.

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



The screenshot shows the 'VULNERABILITIES' section of the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section on the left has a link to 'Strengthening the Nessus Software Supply Chain wit...' and a 'Read More' button. The main content area displays various scan templates in a grid. The 'Web Application Tests' template is highlighted with a yellow border. Other templates shown include: Basic Network Scan, Advanced Scan, Advanced Dynamic Scan, Malware Scan, Mobile Device Scan, Credentialled Patch Audit, Intel AMT Security Bypass, Spectre and Meltdown, WannaCry Ransomware, Ripple20 Remote Scan, ZeroLogon Remote Scan, Solarigate, ProxyLogon: MS Exchange, PrintNightmare, Active Directory Starter Scan, Log4Shell, Log4Shell Remote Checks, Log4Shell Vulnerability Ecosystem, and CISA Alerts AA22-011A and AA22-047A. The URL in the address bar is https://localhost:8834/#/scans/folders/my-scans.

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

The screenshot shows the Tenable Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section is also present. The main area is titled 'New Scan / Web Application Tests' and has a 'Back to Scan Templates' link. It features three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. Under 'Settings', there are sections for 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'Targets' section is expanded, showing fields for 'Name' (empty), 'Description' (empty), 'Folder' (set to 'My Scans'), and 'Targets' (containing 'shopperstop.com'). Below the targets field is a placeholder 'Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). There are 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

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

This screenshot shows the same configuration page as the previous one, but with changes made to the 'Targets' field. The 'Name' field now contains 'shopperstop'. The 'Targets' field now contains 'shopperstop.com'. The rest of the interface remains the same, with the 'Save' and 'Cancel' buttons at the bottom.

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

**Output**

Allow users to edit scan results  
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.

Designate hosts by their DNS name  
Uses the host name rather than IP address for report output.

Display hosts that respond to ping  
Reports hosts that successfully respond to a ping.

Display unreachable hosts  
When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.

Display Unicode characters  
When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.

Save Cancel

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

**Scan Type**: Port scan (common ports)

**General Settings:**  
Always test the local Nessus host  
Use fast network discovery

**Port Scanner Settings:**  
Scan common ports  
Use netstat if credentials are provided  
Use SYN scanner if necessary

**Ping hosts using:**  
TCP  
ARP  
ICMP (2 retries)

Save Cancel

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

New Scan / Web Application Tests

Scan Type

- Scan for all web vulnerabilities (quick)
- Scan for known web vulnerabilities
- Scan for all web vulnerabilities (quick) **(selected)**
- Scan for all web vulnerabilities (complex)
- Custom

Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 5 minutes (max)

Save Cancel

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

Scan Type

Default

General Settings:

- Avoid potential false alarms
- Disable CGI scanning

Web Applications:

- Disable web application scanning

Save Launch Cancel

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

Otenable Nessus Essentials Scans Settings simonarumao

shopperstop < Back to My Scans Configure

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News Tenable and Thales Collaborate to Provide Cyber De... Read More

Hosts 1 Vulnerabilities 3 History 1 Filter Search Hosts 1 Host

Host	Vulnerabilities	%
shoppersstop.com	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

28°C Haze ENG IN 00:52 20-04-2024

shopperstop < Back to My Scans Configure

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News Oracle April 2024 Critical Patch Update Addresses ... Read More

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

28°C Haze ENG IN 00:52 20-04-2024

https://localhost:8834/#/scans/reports/24/vulnerabilities

**Description**  
The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

**Solution**  
Configure the remote web server to use HSTS.

**See Also**  
<https://tools.ietf.org/html/rfc6797>

**Output**  

```
HTTP/1.1 301 Moved Permanently
Connection: close
Content-Length: 0
Retry-After: 0
Location: https://www.shopperstop.com/
Accept-Ranges: bytes
Date: Mon, 19 Apr 2024 19:06:46 GMT
Accept-CH: newport-width,downlink,dpr,device-memory,ect,rtt
Accept-CH-Lifetime: 300
X-Cache: HIT
X-NV-Ver: V4
```

**Plugin Details**

Severity:	Medium
ID:	142960
Version:	1.12
Type:	remote
Family:	Web Servers
Published:	November 17, 2020
Modified:	March 22, 2024

**Risk Information**

Risk Factor:	Medium
<b>CVSS v3.0 Base Score 6.5</b>	
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/U:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score:	5.8
CVSS v2.0 Vector:	CVSS2:AV:N/AC:M/Au:N/C:P/I:A:N

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

**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**  Save as default

The screenshot shows a security audit report for host **10.0.0.1**. The report includes a severity distribution bar and a table of vulnerabilities.

**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

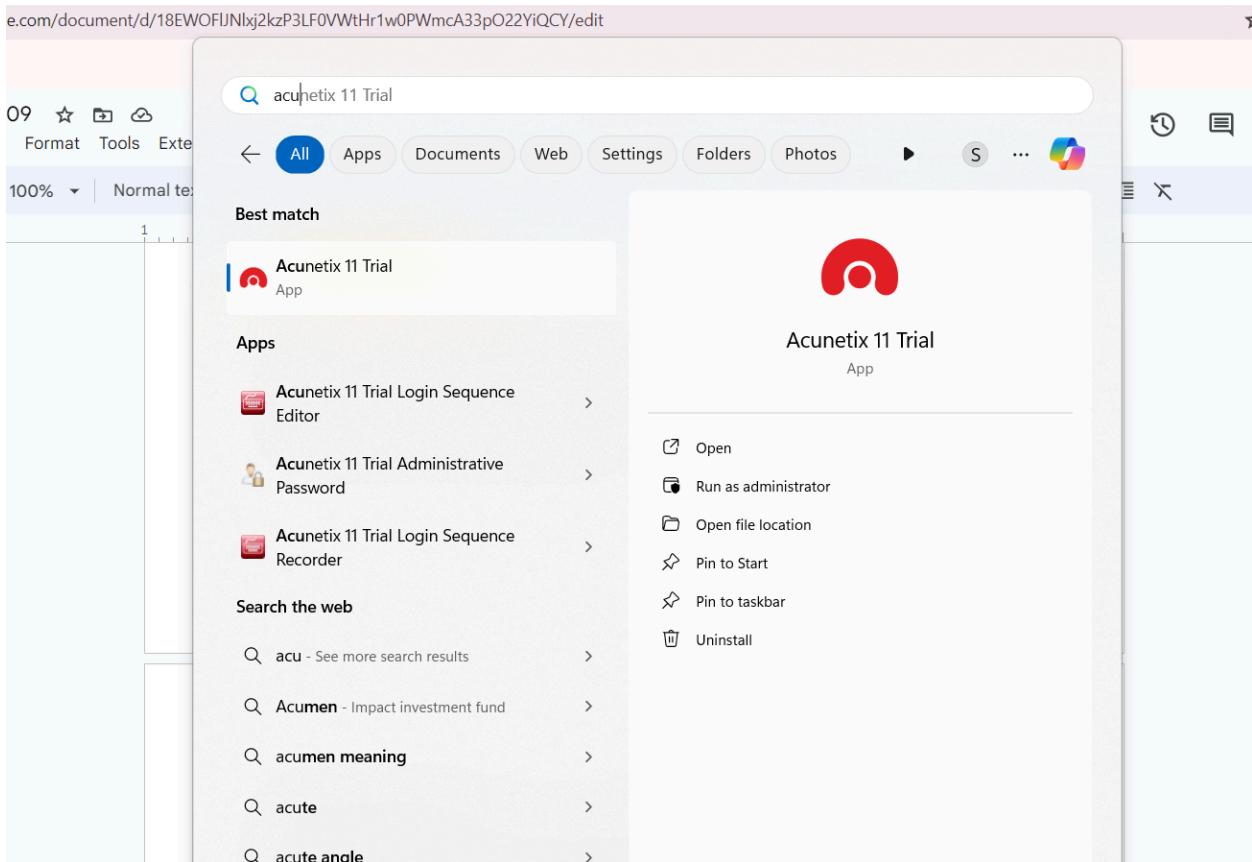
C. Scan the below-mentioned targets Using the Acunetix Vulnerability scanner:

- a) <https://www.ebay.com/>
- b) <https://shopping.rediff.com/>

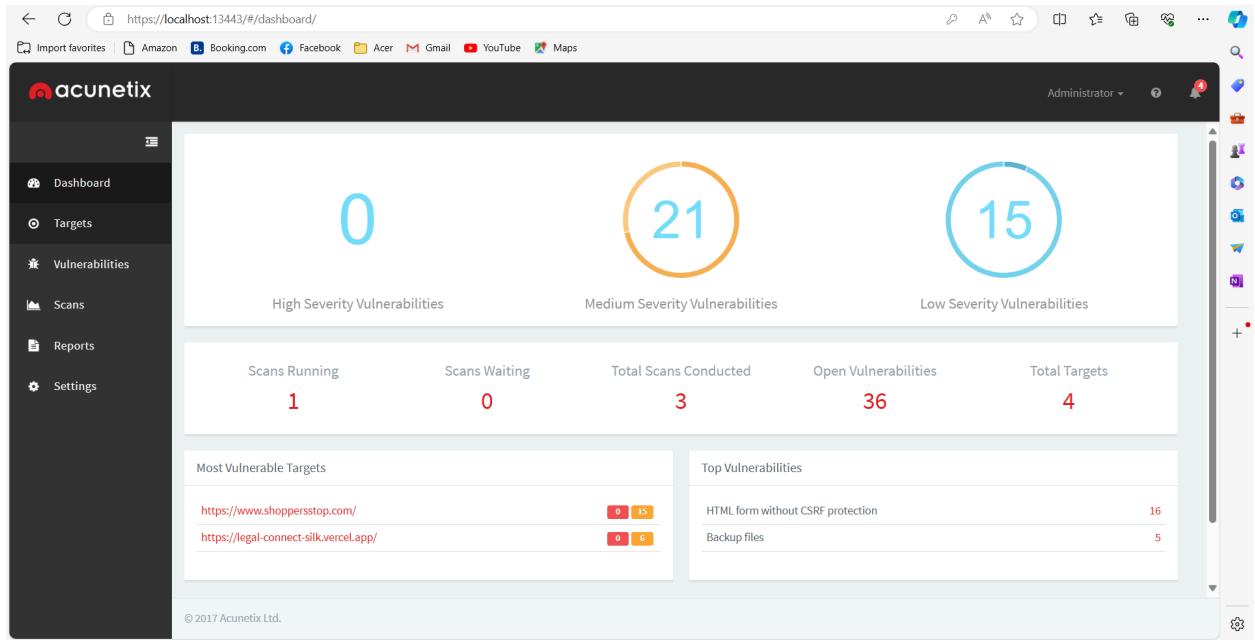
Website 1 : <https://shopping.rediff.com/>

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

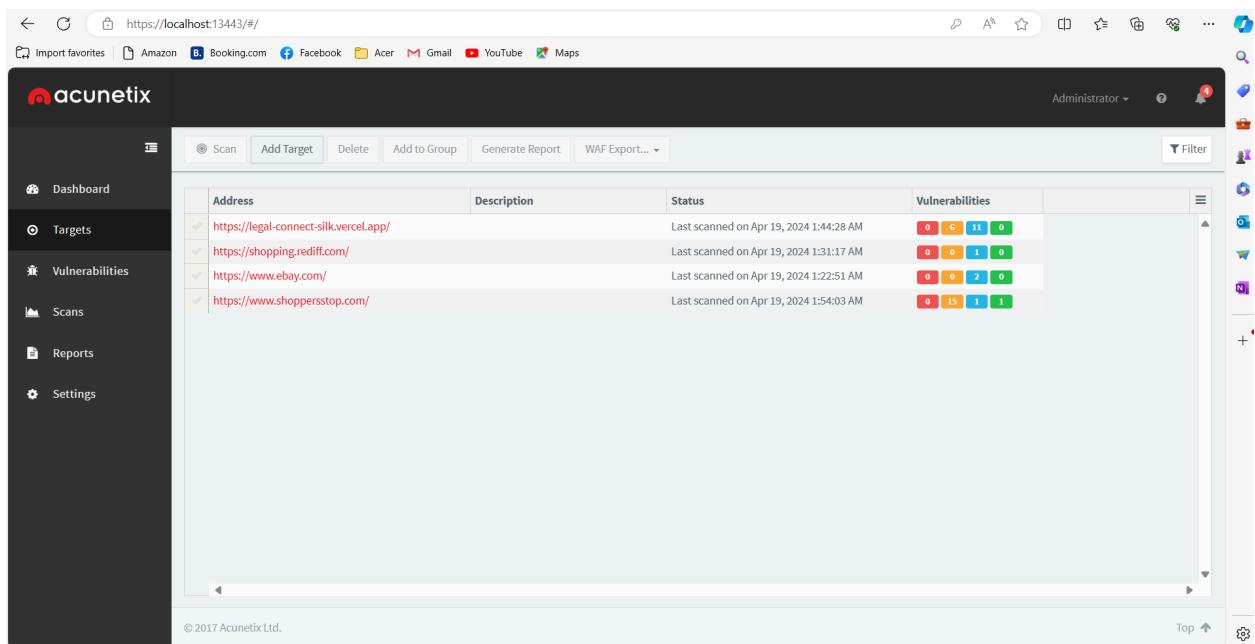
Step 2: If you have the exe just download click on the file and open it and follow the default installation process and simply just click finish



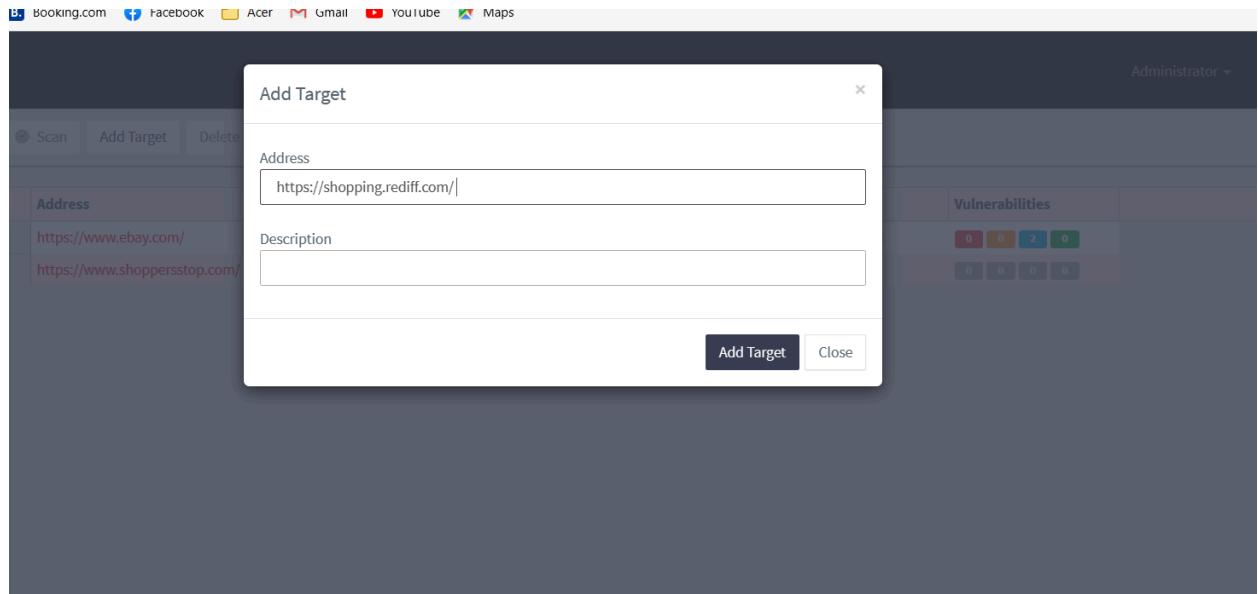
Step 3 : Once you open the tool , we can see some interface like which has multiple options like dashboard,targets,scans etc



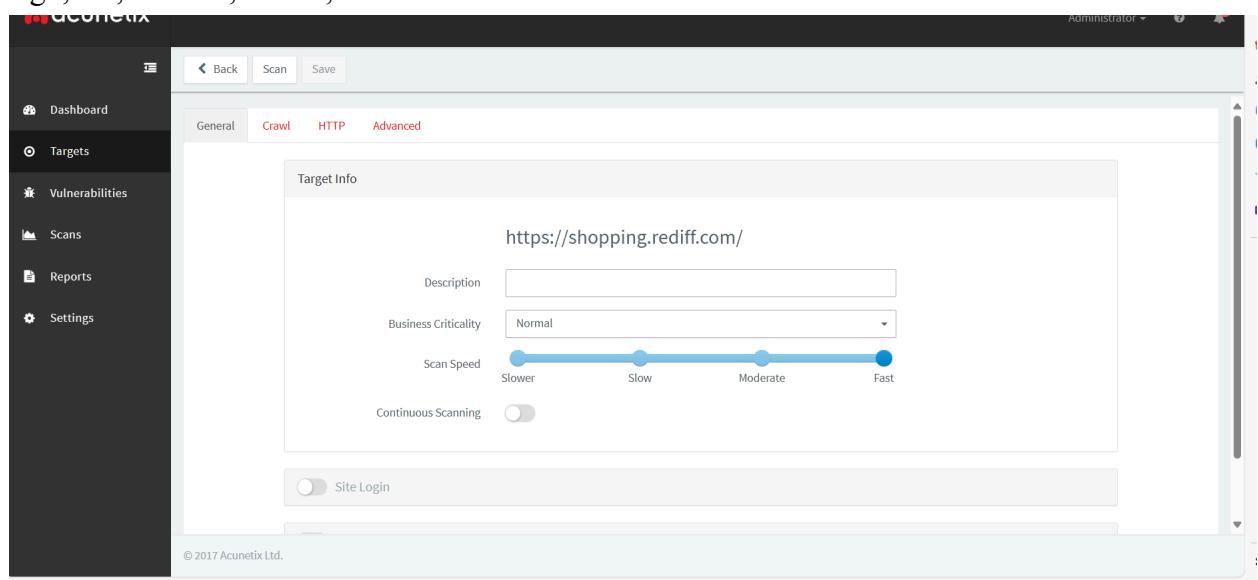
Step 4 : Go to the targets open and click on add target , In top there is a add target button



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



The screenshot shows the Acunetix web application interface. On the left, there's a sidebar with icons for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main area has tabs for General, Crawl, HTTP, and Advanced. Under General, there's a 'Target Info' section with a URL input field containing 'https://shopping.rediff.com/'. Below it are dropdown menus for Business Criticality (set to High), Scan Speed (set to High), and Continuous Scanning. There's also a Site Login toggle button. At the bottom of the main area, there are Back, Scan, and Save buttons. The top right corner shows an Administrator status and a notification icon with a red dot.

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

The screenshot shows a 'Choose Scanning Options' modal dialog. Inside the dialog, there are three dropdown menus: 'Scan Type' (set to 'Full Scan'), 'Report' (set to 'None'), and 'Schedule' (set to 'Instant'). Below these, a message states '1 scan will be created'. At the bottom right of the dialog are 'Create Scan' and 'Close' buttons. In the background, the 'General' tab of the target configuration is visible, showing the URL 'https://shopping.rediff.com/' and other settings like Business Criticality set to 'High'. The top navigation bar and sidebar are also visible.

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

The screenshot shows the Acunetix web interface. On the left, there's a sidebar with icons for Dashboard, Targets, Vulnerabilities (which is selected), Scans, Reports, and Settings. The main area has tabs for Scan Stats & Info, Vulnerabilities (which is active), Site Structure, and Events. A large circular icon indicates 'Acunetix Threat Level 1' with a 'LOW' rating. Below it, a message says 'One or more low-severity type vulnerabilities have been discovered by the scanner.' To the right, there's a section titled 'Activity' showing 'Overall progress' at 97% with a blue bar. A log entry says 'Scanning of shopping.rediff.com started' on April 19, 2024, at 1:31:17 AM. Below this, there are sections for 'Scan Duration' (1m 30s), 'Requests' (1,547), 'Avg. Response Time' (152ms), and 'Locations' (0). There's also a 'Target Information' table with columns for Address (shopping.rediff.com) and Server (Apache). A 'Latest Alerts' section shows one alert: 'Clickjacking: X-Frame-Options header missing' from April 19, 2024, at 1:31:19 AM. The bottom of the screen shows a Windows taskbar with various icons.

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

This screenshot shows the same Acunetix interface as above, but the 'Vulnerabilities' tab is now active. The main content area displays a table of detected vulnerabilities. The first row shows a single entry: 'Clickjacking: X-Frame-Options header missing' with the URL 'https://shopping.rediff.com/' and a status of 'Open'. The table has columns for 'Se...', 'Vulnerability', 'URL', 'Parameter', and 'Status'. The bottom of the screen shows a browser address bar with 'https://localhost:13443' and a status bar indicating 'Top ↑'.

The screenshot shows the Acunetix web application interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area has a title "Clickjacking: X-Frame-Options header missing" with a "Low" severity level and an "Open" status. Below the title is a "Vulnerability description" section. It states: "Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages." It also notes that the server didn't return an X-Frame-Options header. There are sections for "Attack details", "HTTP request", "The impact of this vulnerability", and "How to fix this vulnerability". At the bottom of the page is a copyright notice: "© 2017 Acunetix Ltd."

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

The screenshot shows the Acunetix web application interface with the "Site Structure" tab selected. The sidebar remains the same. The main content area displays the site structure for "https://shopping.rediff.com/". A table lists vulnerabilities found at this URL. The table has columns for Severity, Vulnerability, URL, and Parameter. One row is shown: "Se... Vulnerability URL Parameter" with a severity of 1 and the URL "https://shopping.rediff.com/". The vulnerability description is "Clickjacking: X-Frame-Options header missing".

Severity	Vulnerability	URL	Parameter
1	Clickjacking: X-Frame-Options header missing	https://shopping.rediff.com/	

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

Administrator   

Back Stop Scan Generate Report WAF Export... ▾

Dashboard Targets Vulnerabilities Scans Reports Settings

Scan Stats & Info Vulnerabilities Site Structure Events

Acunetix Threat Level 1

LOW 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

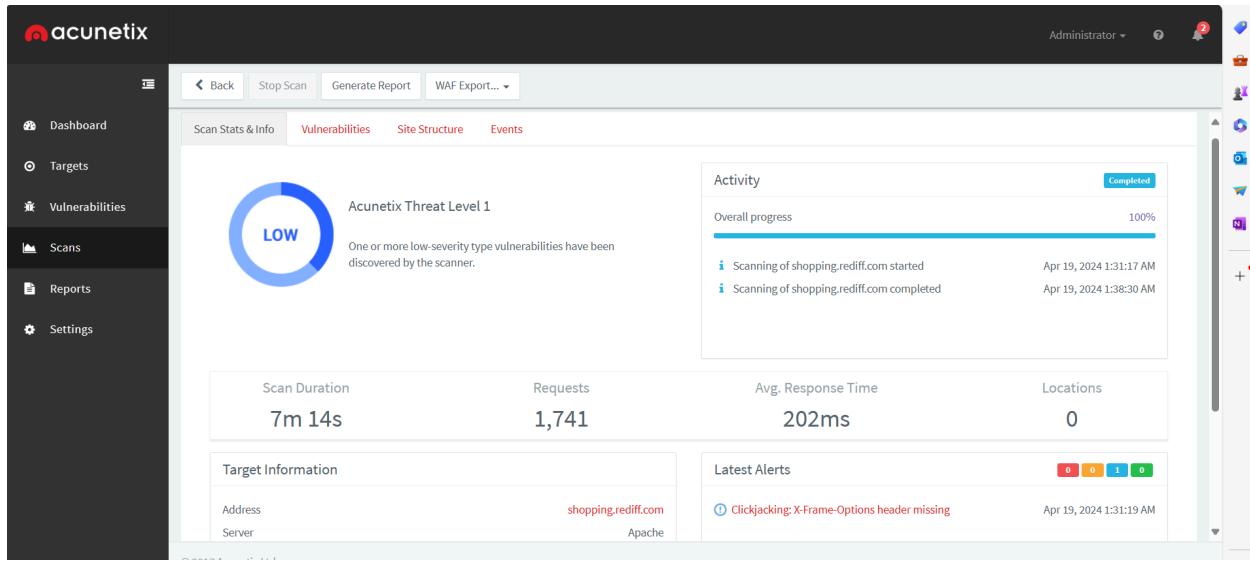
Scan Duration Requests Avg. Response Time Locations

7m 14s 1,741 202ms 0

Target Information Latest Alerts

Address shopping.rediff.com 0 0 1 0  
Server Apache 0 0 0 0

Clickjacking: X-Frame-Options header missing Apr 19, 2024 1:31:19 AM



Administrator   

Import favorites  Amazon  Booking.com  Facebook  Acer  Gmail  YouTube  Maps 

Generate Report WAF Export... ▾

Dashboard Targets Vulnerabilities Scans Reports Settings

Vulnerabilities

Se... Vulnerability

Clickjacking: X-Frame-Opti...  
Clickjacking: X-Frame-Opti...  
Cookie(s) without HttpO...

Generate Report

Template Developer

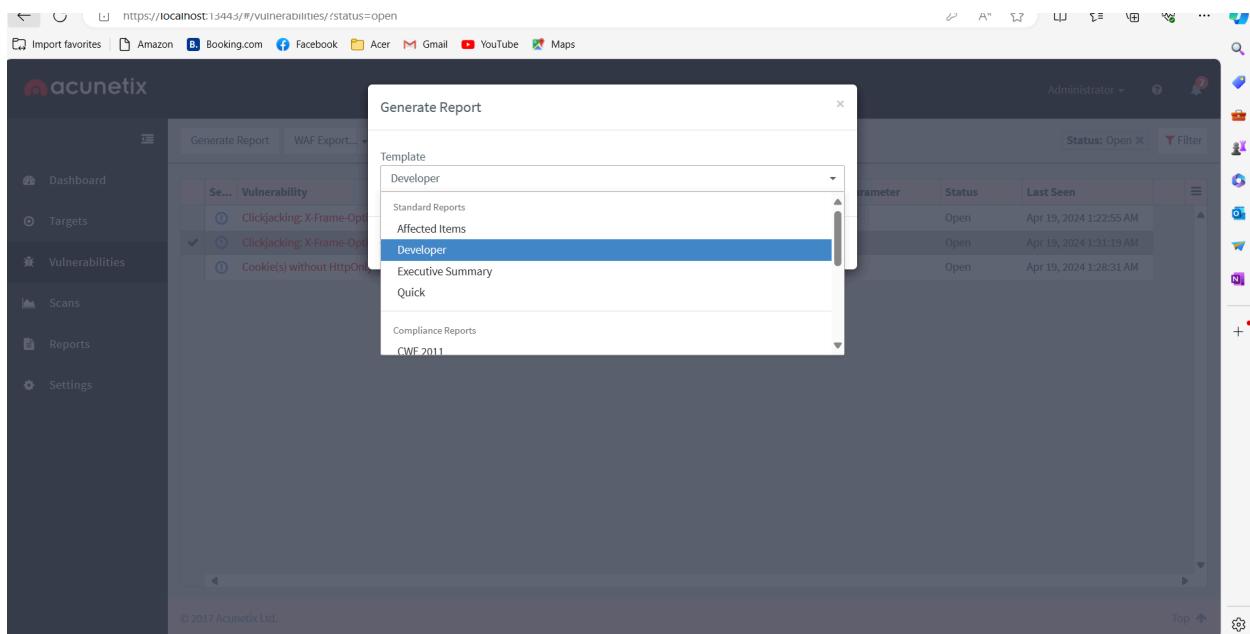
Developer  
Standard Reports  
Affected Items  
Developer  
Executive Summary  
Quick  
Compliance Reports  
CWE 2011

Parameter Status Last Seen

Open Apr 19, 2024 1:22:55 AM  
Open Apr 19, 2024 1:31:19 AM  
Open Apr 19, 2024 1:28:31 AM

Filter

Top  



**Selected vulnerabilities**

---

**Scan details**

Scan information	
Start url	<a href="https://shopping.rediff.com/">https://shopping.rediff.com/</a>
Host	<a href="https://shopping.rediff.com/">https://shopping.rediff.com/</a>

---

**Threat level**

**Acunetix Threat Level 1**

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

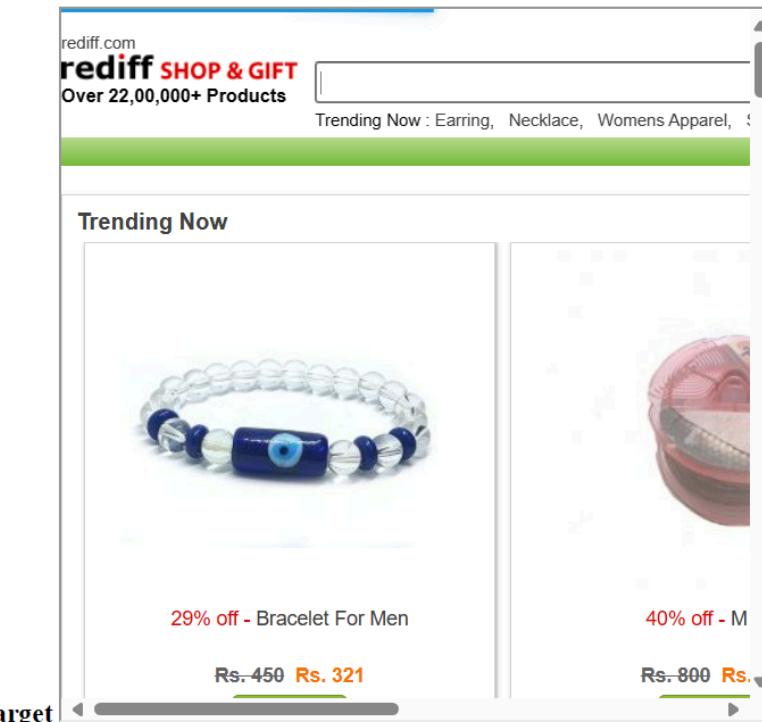
**Alerts distribution**

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

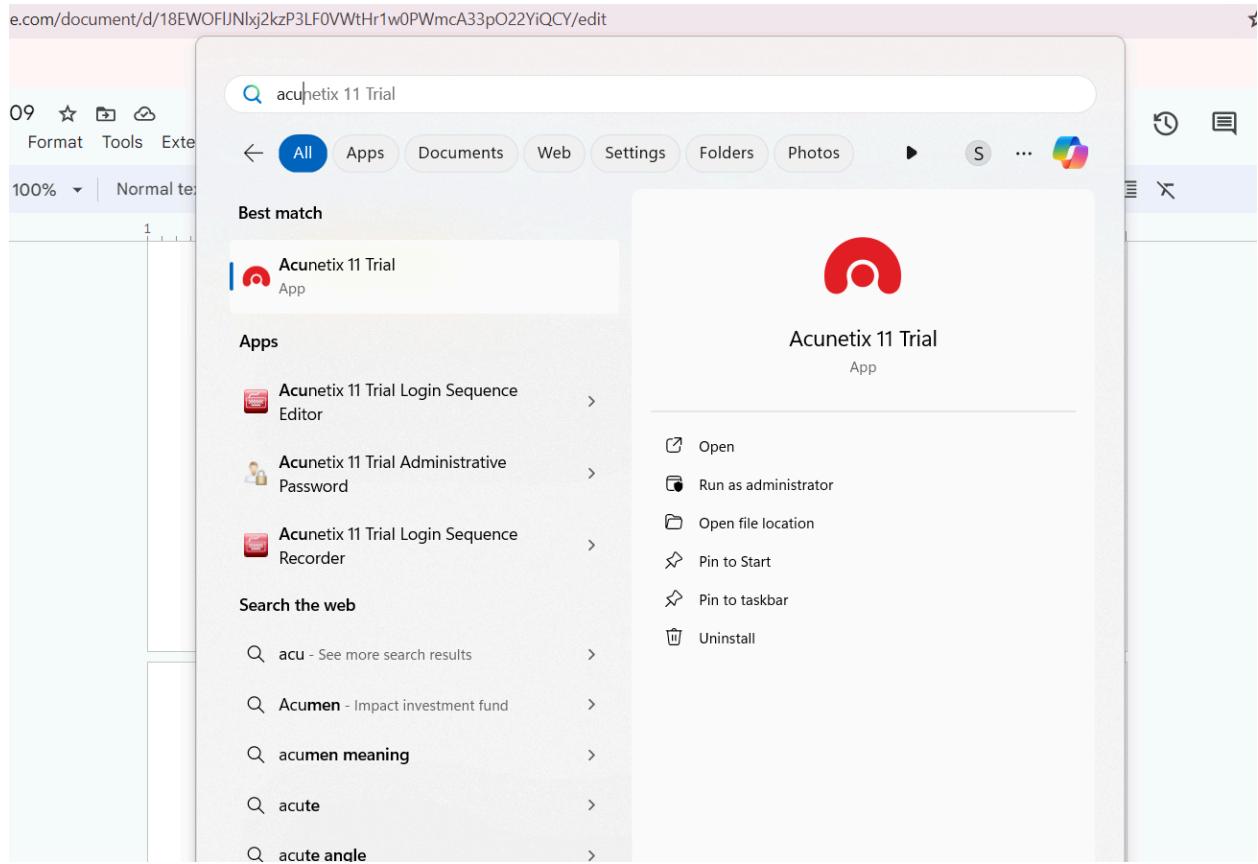
### iframe



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

Category	Value
High Severity Vulnerabilities	0
Medium Severity Vulnerabilities	21
Low Severity Vulnerabilities	15
Scans Running	1
Scans Waiting	0
Total Scans Conducted	3
Open Vulnerabilities	36
Total Targets	4

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

The screenshot shows the Acunetix web application interface. The top navigation bar includes links for Import favorites, Amazon, Booking.com, Facebook, Acer, Gmail, YouTube, and Maps. The main header has the Acunetix logo and an Administrator dropdown. Below the header is a toolbar with Scan, Add Target, Delete, Add to Group, Generate Report, and WAF Export... buttons. A Filter icon is also present. The left sidebar contains links for Dashboard, Targets, Vulnerabilities, Scans, Reports, and Settings. The main content area displays a table of targets:

Address	Description	Status	Vulnerabilities
<a href="https://legal-connect-silk.vercel.app/">https://legal-connect-silk.vercel.app/</a>	Last scanned on Apr 19, 2024 1:44:28 AM	<span style="color:red">0</span> <span style="color:orange">6</span> <span style="color:green">11</span> <span style="color:blue">0</span>	
<a href="https://shopping.rediff.com/">https://shopping.rediff.com/</a>	Last scanned on Apr 19, 2024 1:31:17 AM	<span style="color:red">0</span> <span style="color:orange">0</span> <span style="color:green">1</span> <span style="color:blue">0</span>	
<a href="https://www.ebay.com/">https://www.ebay.com/</a>	Last scanned on Apr 19, 2024 1:22:51 AM	<span style="color:red">0</span> <span style="color:orange">0</span> <span style="color:green">2</span> <span style="color:blue">0</span>	
<a href="https://www.shoppersstop.com/">https://www.shoppersstop.com/</a>	Last scanned on Apr 19, 2024 1:54:03 AM	<span style="color:red">0</span> <span style="color:orange">15</span> <span style="color:green">1</span> <span style="color:blue">1</span>	

At the bottom of the page, there is a copyright notice: © 2017 Acunetix Ltd.

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

The screenshot shows the Acunetix web application interface with the 'Add Target' dialog box open. The dialog box has two input fields: 'Address' containing 'https://www.ebay.com/' and 'Description' which is empty. At the bottom right of the dialog box are 'Add Target' and 'Close' buttons. The background shows the same dashboard as the previous screenshot, with the 'Targets' section highlighted in the sidebar.

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

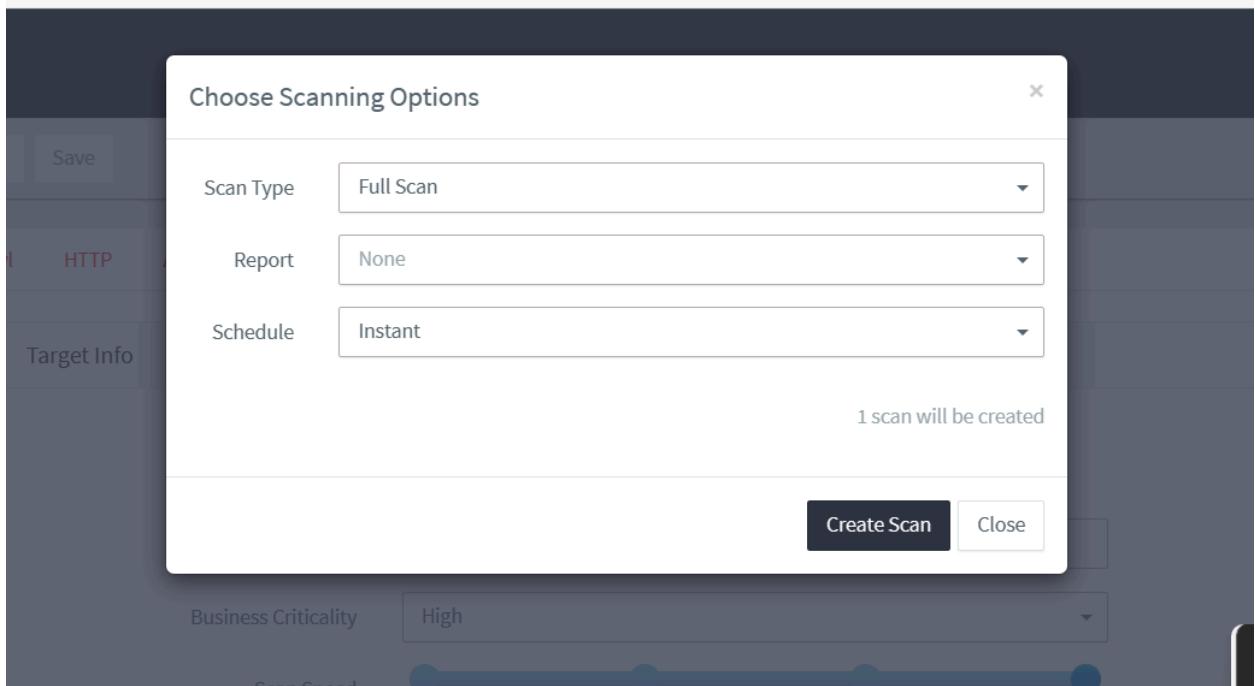
The image consists of two vertically stacked screenshots of the Acunetix web application interface. Both screenshots show the 'Targets' section with a target URL of <https://www.ebay.com/>.

**Screenshot 1:** The 'Business Criticality' dropdown menu is open, showing options: High, Critical, High (which is selected), Normal, and Low. The 'Scan Speed' slider is set to 'Slow'.

**Screenshot 2:** The 'Business Criticality' dropdown menu is closed, showing the selected value 'High'. The 'Scan Speed' slider is set to 'Slow'.

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

A screenshot of the Acunetix web application interface. The 'Scan' button is highlighted with a red box, indicating it is the next step to start the scan.



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

The screenshot shows the Acunetix web application interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities (selected), Scans, Reports, and Settings. The main content area has tabs at the top: Scan Stats & Info, Vulnerabilities (selected), Site Structure, and Events. Below these tabs is a table with columns: Seq., Vulnerability, URL, Parameter, and Status. One row is visible: "Clickjacking: X-Frame-Options header missing" with URL "https://www.ebay.com/" and status "Open". At the bottom of the main content area, there's a note: "© 2017 Acunetix Ltd." and a "Top ↑" button.

This screenshot shows the detailed view of the Clickjacking vulnerability. The title is "Clickjacking: X-Frame-Options header missing". It includes a "Low" severity indicator and an "Open" status. A section titled "Vulnerability description" explains that Clickjacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. Below this, it states that the server didn't return an X-Frame-Options header. The "Attack details" section notes that it's not available in the free trial. Other sections include "HTTP request", "The impact of this vulnerability", and "How to fix this vulnerability". The footer includes the copyright notice "© 2017 Acunetix Ltd." and a timestamp "01:27".

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

Administrator

Scan Stats & Info Vulnerabilities Site Structure Events

https://www.ebay.com/ https://www.ebay.com/ 0 0 1 0

Se...	Vulnerability	URL	Parameter
0	Clickjacking: X-Frame-Options header missing	https://www.ebay.com/	

© 2017 Acunetix Ltd.

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

Administrator

Scan Stats & Info Vulnerabilities Site Structure Events

Acunetix Threat Level 1

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

Activity

Overall progress 100%

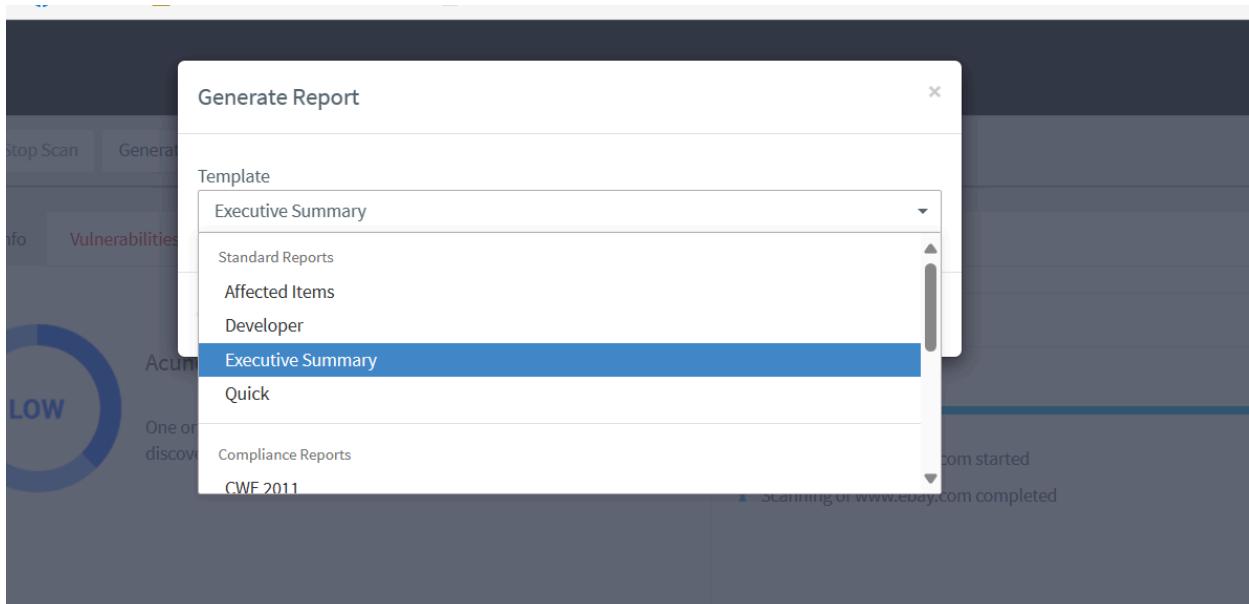
Scanning of www.ebay.com started Apr 19, 2024 2:09:16 AM

Scanning of www.ebay.com completed Apr 19, 2024 2:15:19 AM

Scan Duration	Requests	Avg. Response Time	Locations
6m 5s	1,628	170ms	0

Target Information	Latest Alerts
Address: www.ebay.com	Clickjacking: X-Frame-Options header missing (Apr 19, 2024 2:09:19 AM)

© 2017 Acunetix Ltd.



## Scan of [https://www.ebay.com/](https://www.ebay.com)

### Scan details

Scan information	
Start time	19/04/2024, 02:09:15
Start url	<a href="https://www.ebay.com/">https://www.ebay.com/</a>
Host	<a href="https://www.ebay.com/">https://www.ebay.com/</a>
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

