VULNERABILITY -ANALYSIS

-ATHARVA KATKAR

Vulnerablity Analysis

Vulnerability Analysis (VA) is the process of identifying, classifying, and evaluating weaknesses in a system, network, application, or device that an attacker could exploit.

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication.

Why is Vulnerability Analysis Important?

- Prevents cyberattacks before they happen
- Helps organizations comply with standards (ISO 27001, PCI-DSS, HIPAA)
- Reduces risk by fixing weaknesses early
- Prioritizes high-risk issues using CVSS scoring

Types of Vulnerabilities Found in Analysis:

1. Network Vulnerabilities

- Open ports
- Weak firewall rules
- Unpatched OS services

2. System Vulnerabilities

- Outdated software
- Misconfigurations
- Weak passwords
- Privilege escalations

3. Application Vulnerabilities

- SQL injection
- XSS
- Broken authentication
- Insecure APIs

4. Cloud Vulnerabilities

- Public S3 buckets
- IAM misconfigurations
- No MFA for admin accounts

5. Human Vulnerabilities

- Social engineering
- Phishing susceptibility

Common Tools Used in Vulnerability Analysis:

1. **Network & System Scanners**

Tool	Use
Nmap	Port, service, OS discovery
Nmap NSE scripts	Identify specific vulnerabilities
Nessus	Full vulnerability scanning (most used)
OpenVAS	Open-source VA tool
QualysGuard	Enterprise cloud-based scanner
Nexpose/InsightVM	Risk-based scanning

2.Web Application Scanners

Tool	Use
Burp Suite	Web vulnerability scanning
OWASP ZAP	Free web scanner
Acunetix	Commercial web scanner

3.Cloud Scanners

- AWS Inspector
- GCP Security Command Center
- Azure Defender

Examples of Vulnerabilities Found in VA:

1. Open Port Vulnerability
   - Port 22 accessible from the internet

2. Missing Patches
   - Windows SMB vulnerability (EternalBlue CVE-2017-0144)

3. Default Passwords
   - admin : admin

4. Misconfigured Firewalls
   - Allowing all inbound traffic (0.0.0.0/0)

5. Web Vulnerabilities
   - Reflected XSS
   - SQL injection parameters

Vulnerability Analysis using Nikto

Nikto is a fast, automated web server vulnerability scanner that identifies outdated software, misconfigurations, dangerous files, and known vulnerabilities.

Nikto is an open-source web server vulnerability scanner used in cybersecurity to identify:

- Misconfigurations
- Outdated software
- Dangerous files
- Default credentials
- Insecure HTTP headers
- Known vulnerabilities (CVE-based)

Common Commands -:

- Man nikto – Details about nikto tool.
- Nikto -h for help.
- -host – specify a host name or domain name.

Key Features of Nikto:

- Scans over 6,700+ known vulnerabilities
- Detects default files and directories (e.g., /admin, /phpmyadmin, /test)
- Identifies outdated server versions
- Checks SSL/TLS issues
- Supports HTTP, HTTPS, and proxies
- Detects many CVE vulnerabilities
- Fast and automated

1)Command- **nikto -h**
(-h for help)

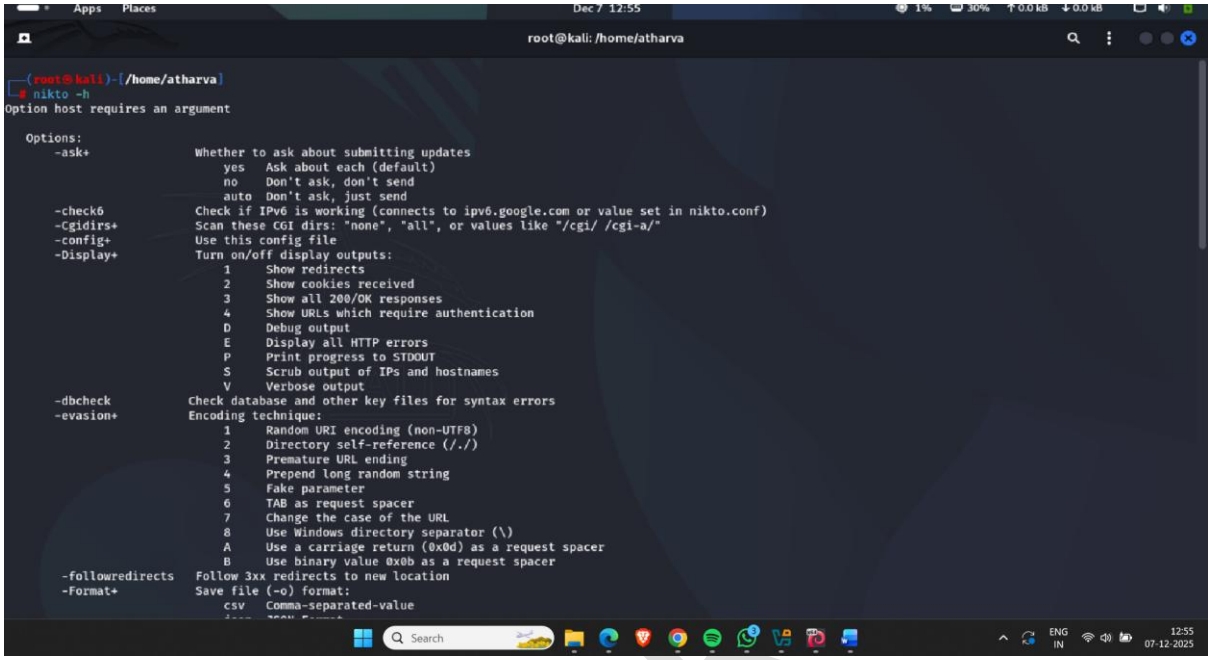


Figure 1

2)Command- **Display 3**

(**-**Display option is used to control what information is shown in the scan output and 3 used for only significant vulnerabilities or warnings.)

Figure 2

3)Command **-Display V** –

(-V :Verbose mode This command performs a full web server vulnerability scan and displays very detailed, verbose output.)

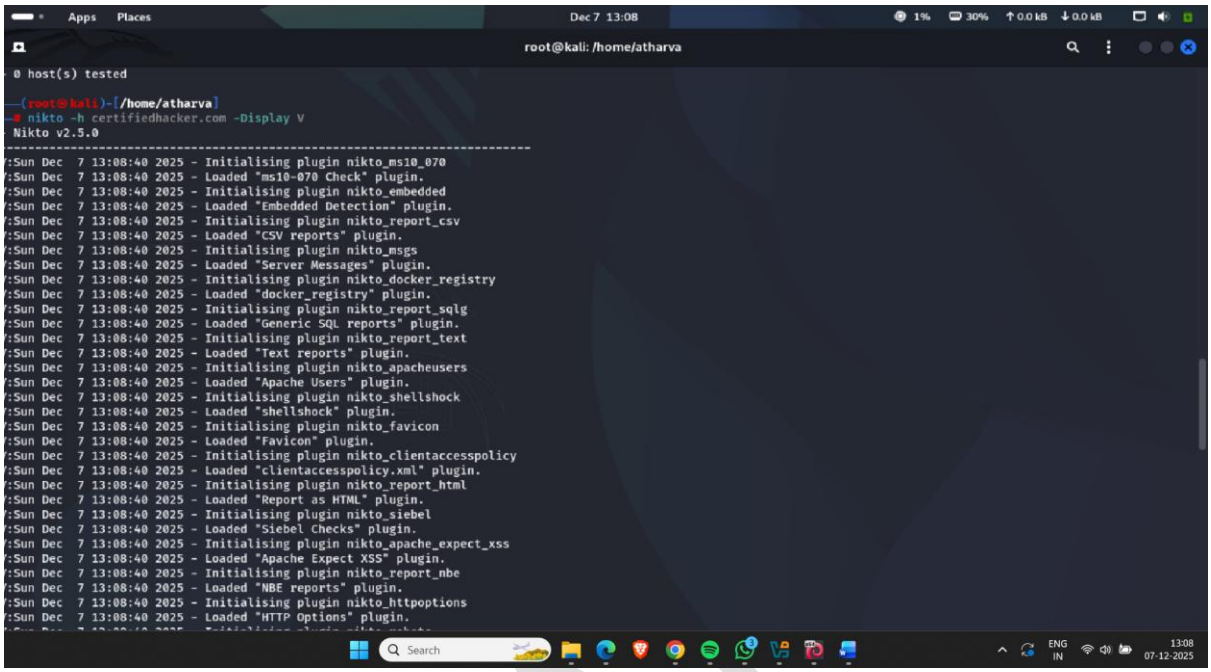


Figure 3

4)Command: **-Tuning x**

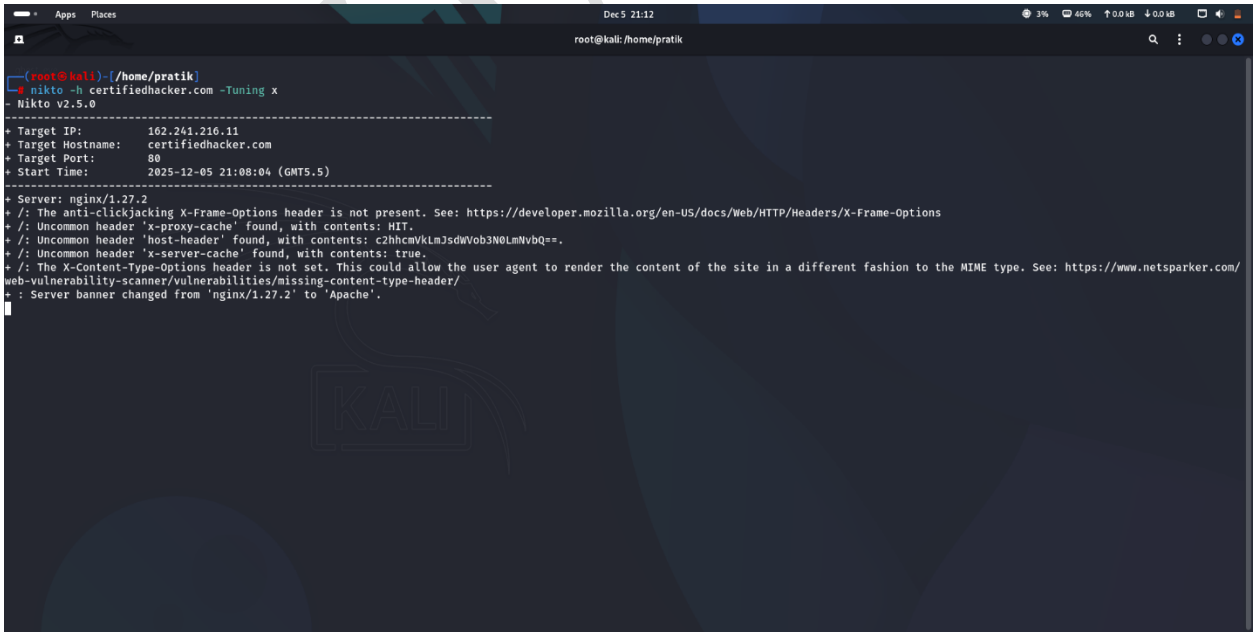


Figure 4

Vulnerability Analysis using Acunetix

Acunetix is a web vulnerability scanner designed to identify and help fix security issues in websites, web applications, and APIs. It automates the process of checking for vulnerabilities.

It identifies:

- SQL Injection
- Cross-Site Scripting (XSS)
- Authentication vulnerabilities
- Server misconfigurations
- Weak SSL/TLS
- Exposed files and directories
- OWASP Top 10 issues

It is one of the most accurate and industry-standard scanners used by:

- Penetration testers
- Bug bounty hunters
- Web security teams
- Enterprises

Advantages:

- Very low false positives
- Modern JS application scanning
- User-friendly interface
- Accurate payload engine
- DevSecOps integration

Key Features of Acunetix:

- Detects 7000+ web vulnerabilities
- Powerful crawler to analyze entire websites
- DeepScan engine (scans JavaScript-heavy apps, SPA, AJAX)
- Advanced Login sequence recorder (handles authentication)
- Detects OWASP Top 10 vulnerabilities
- Built-in Network Scanner for ports, services, CVEs
- Detailed risk scoring and remediation guidelines
- Supports CI/CD pipelines (DevSecOps)

How to use it:

Step1: open Kali Linux terminal
Step2: run cmd **service acunetix status**
Step3: shows status (active)

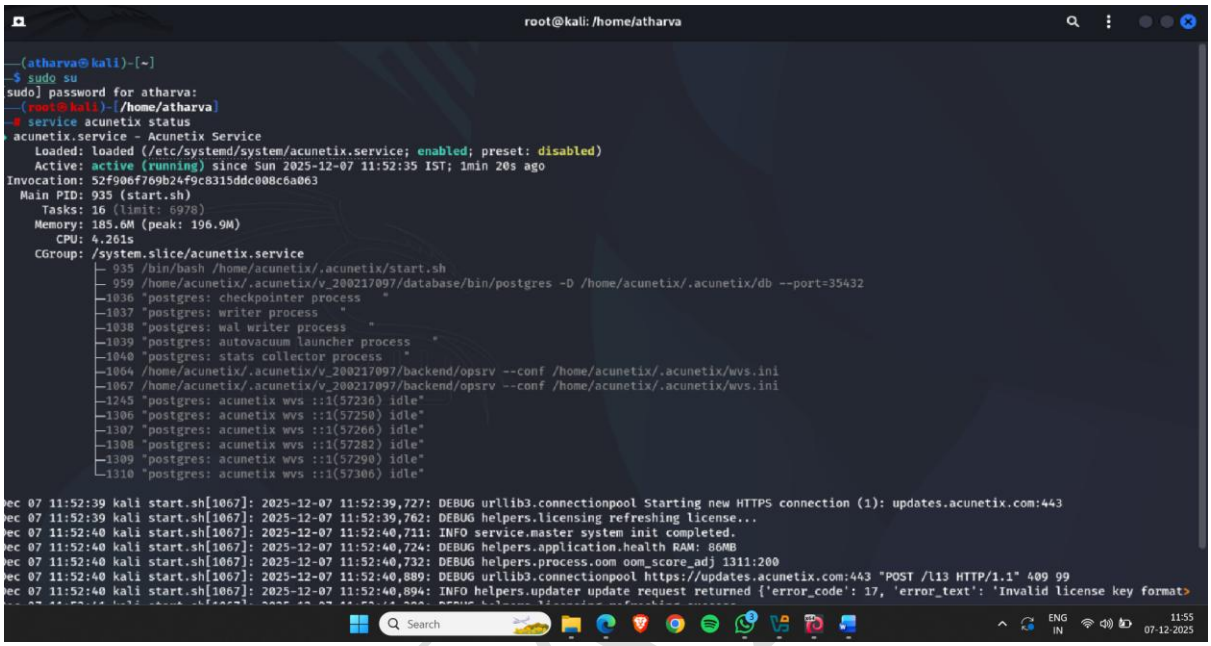


Figure 5

Step4: go on browser and search for (https://127.0.0.1:3443)

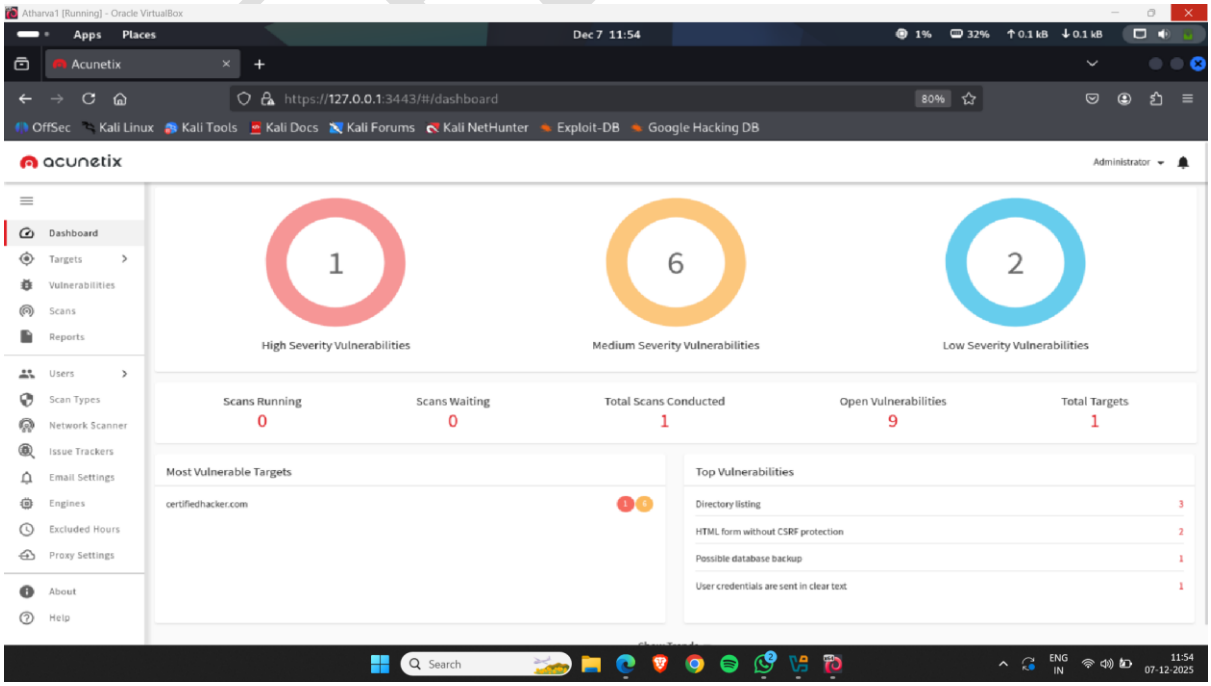


Figure 6

Step5: go on Scans and click on new scan

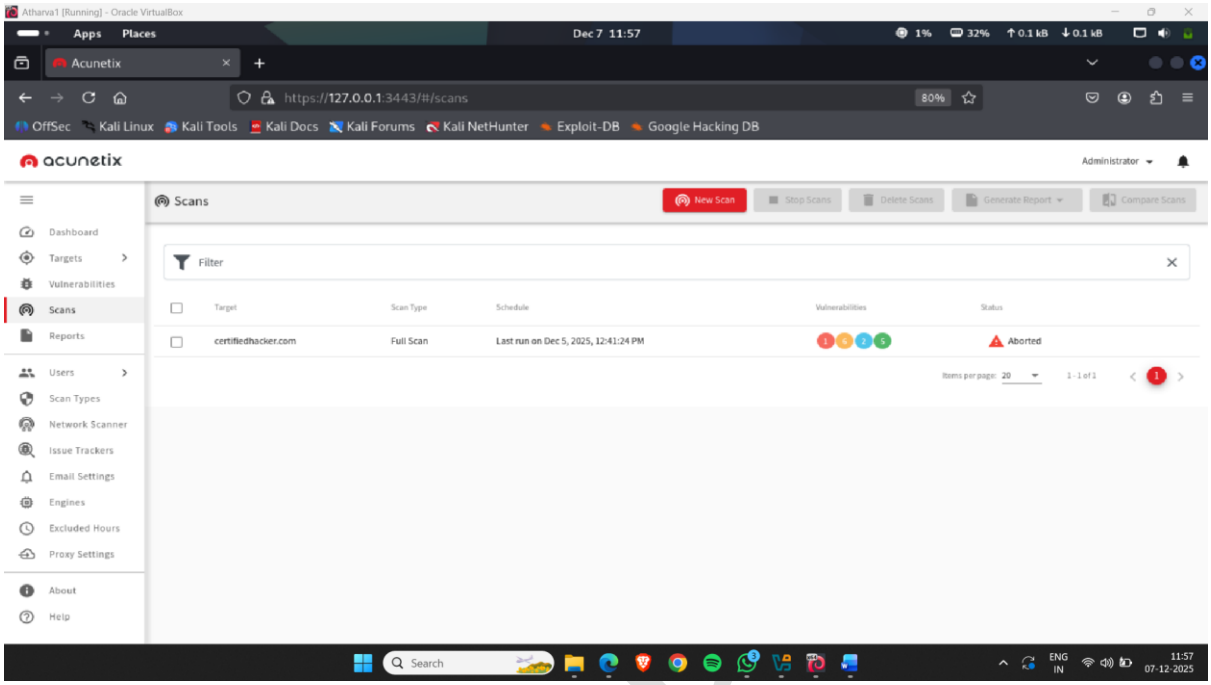


Figure 7

Step6: add the target name or ip address & click on save.

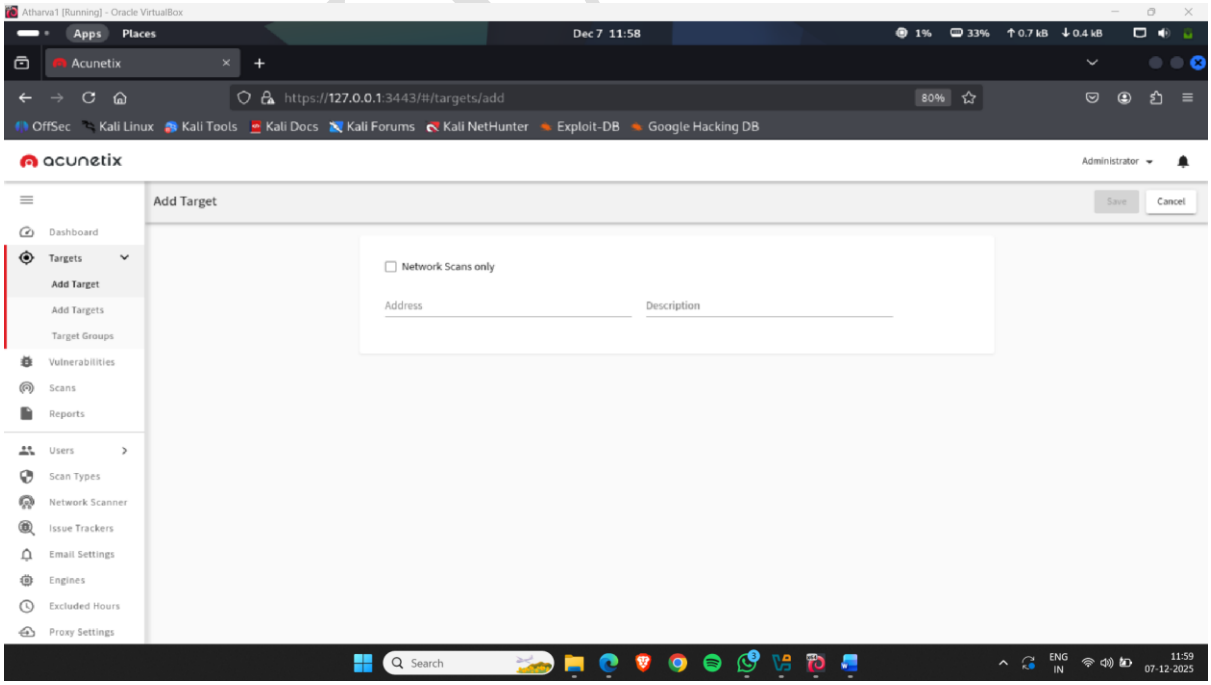


Figure 8

Step7:choose scan options which type of scan you want to do & click on create scan.

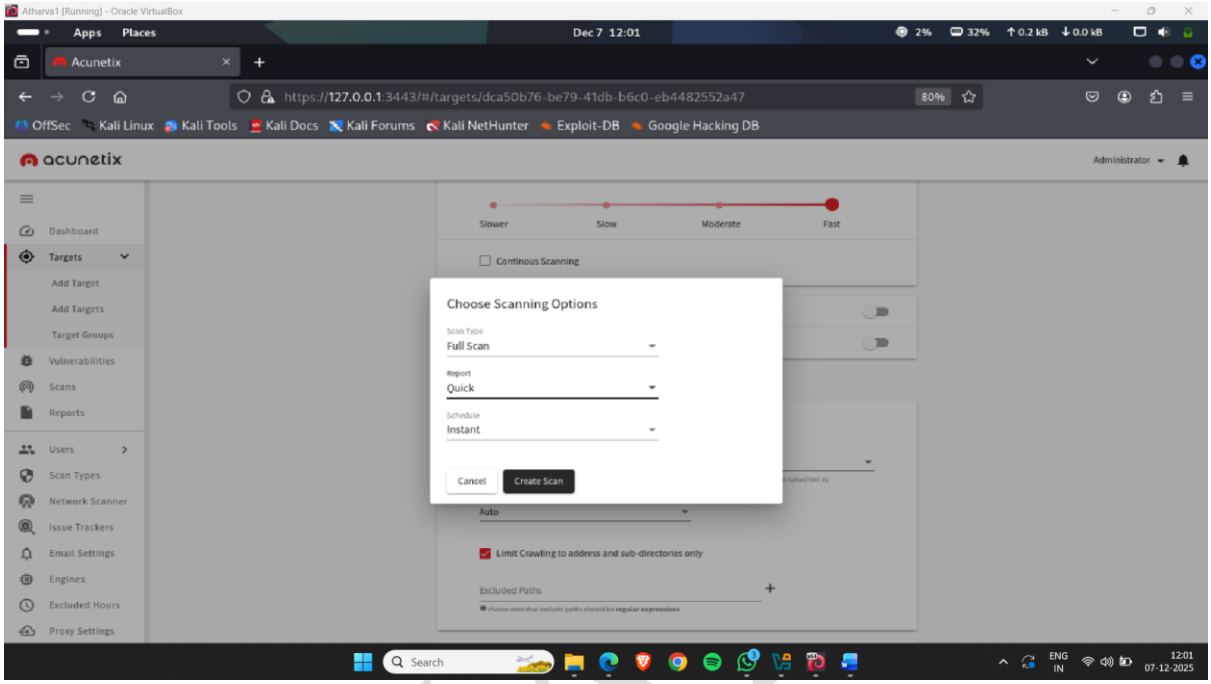


Figure 9

Step8: scanning process will start

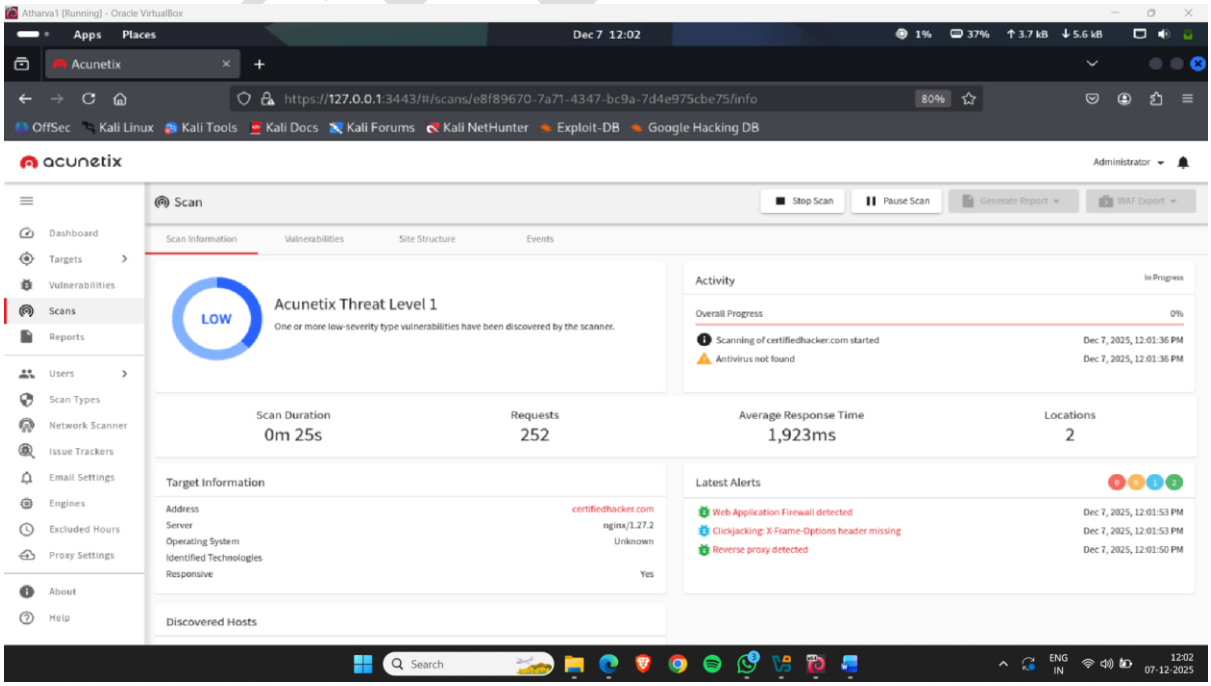


Figure 10

Report:

acunetix

Quick Report

Acunetix Security Audit

Scan of certifiedhacker.com

Scan details

Scan information	
Start time	05/12/2025, 07:03:42
Start url	certifiedhacker.com
Host	certifiedhacker.com
Scan time	70 minutes, 53 seconds
Profile	Full Scan
Server information	nginx/1.27.2
Responsive	True
Server OS	Unknown
Scan status	aborted

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	24
High	1
Medium	13
Low	3
Informational	7

Alerts

Possible database backup	
Affected item	Web Server
Affected parameter	
Request	

```
GET /certifiedhacker.zip HTTP/1.1
Range: bytes=0-99999
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Online%20Booking/js/
Affected parameter	
Request	

```
GET /Online%20Booking/js/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Online%20Booking/js/hotels/
Affected parameter	
Request	

```
GET /Online%20Booking/js/hotels/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/Online%20Booking/js/hotels/
Affected parameter	

Request

```
GET /Online%20Booking/js/hotels/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/js/
Affected parameter	

Request

```
GET /js/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Directory listing (verified)	
Affected item	/js/source/
Affected parameter	

Request

```
GET /js/source/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

HTML form without CSRF protection	
Affected item	Web Server
Affected parameter	

Request

```
GET / HTTP/1.1
Referer: http://certifiedhacker.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Subresource Integrity (SRI) not implemented	
Affected item	Web Server
Affected parameter	
Request	

```
GET / HTTP/1.1
Referer: http://certifiedhacker.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Subresource Integrity (SRI) not implemented	
Affected item	/Online%20Booking/index.htm
Affected parameter	
Request	

```
GET /Online%20Booking/index.htm HTTP/1.1
Referer: http://certifiedhacker.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: certifiedhacker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

The report shows an overall Threat Level 3, which means high-severity vulnerabilities were detected that could allow attackers to compromise the database or deface the website.In total, 24 security alerts were found, including several high-risk, medium-risk, and low-risk issues. High-risk issues indicate serious vulnerabilities such as misconfigurations or exposed files that attackers can exploit. Medium and low issues point to configuration weaknesses or missing security headers.

Overall, the report indicates that the website needs urgent security fixes, especially for the high-severity vulnerabilities, to prevent hacking and data exposure.

Vulnerability Analysis Using ZAP

ZAP (Zed Attack Proxy) is a free and open-source web application security scanner used to perform vulnerability analysis. During a scan, ZAP intercepts web traffic, crawls the entire website, and automatically detects issues like SQL Injection, XSS, insecure cookies, missing security headers, and exposed files. It provides both active scanning (attacking the app with payloads) and passive scanning (analyzing traffic without sending attacks).

How ZAP works (high level):

- **Proxy mode**: ZAP sits between your browser and the app and records requests/responses. Passive scanning analyzes traffic without changing requests.
- **Spidering / Crawling**: ZAP discovers links, forms, and endpoints.
- **Active Scanning**: ZAP sends attack payloads to test for exploitable vulnerabilities (this is intrusive).
- **Scripts & Add-ons**: Extend functionality (authentication, scanners, advanced checks).
- **Reporting / Alerts**: Finds are classified (High/Medium/Low/Info) with reproduction steps and remediation suggestions.

Key ZAP features & add-ons (must-know):

- **Passive scanner** (non-intrusive checks).
- **Active scanner** (exploit-like checks).
- **AJAX Spider** and **Classic Spider**.
- **Authentication** add-ons (form auth, script-based).
- **Fuzzer** (custom payloads).
- **Forced browse** (discover hidden endpoints).
- **Plug-n-Hack** integration & browser addons.
- **Scripting support** (JavaScript, Python/Jython, Zest, Ruby) to add custom scanners or auth flows.
- **Report generation** (HTML, JSON, XML) and export alerts.

How to use:

Step1:open kali linux terminal

Step2: Open Terminal And type **sudo apt install zaproxy**

Step3: run cmd **zaproxy**

Figure 11

Step4: following window will appear.

- Click on automated scan

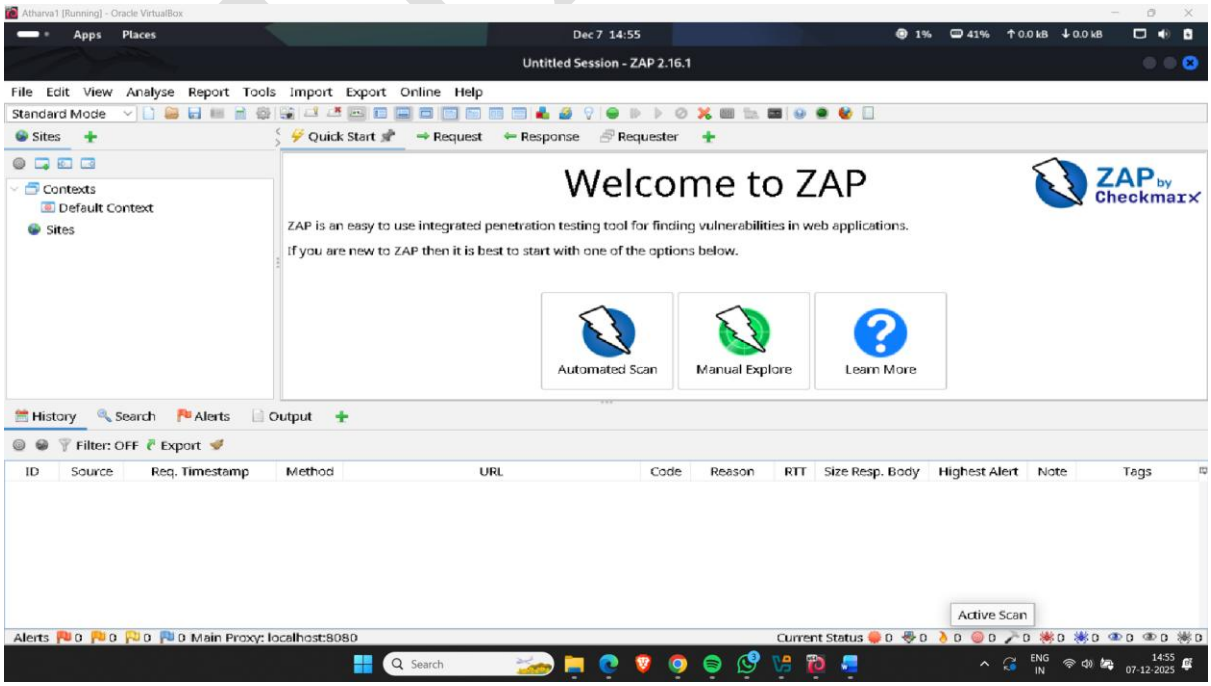


Figure 12

Step5:Enter the target in url section & click on attack

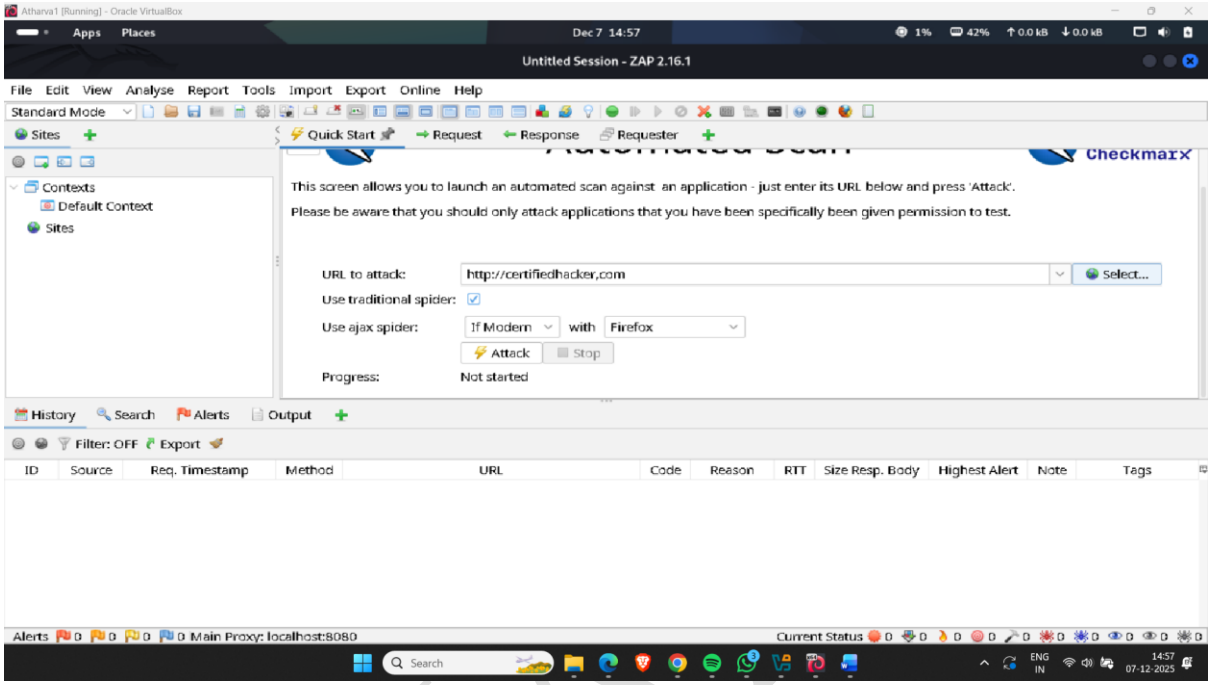


Figure 13

Step6: attack will start on given target

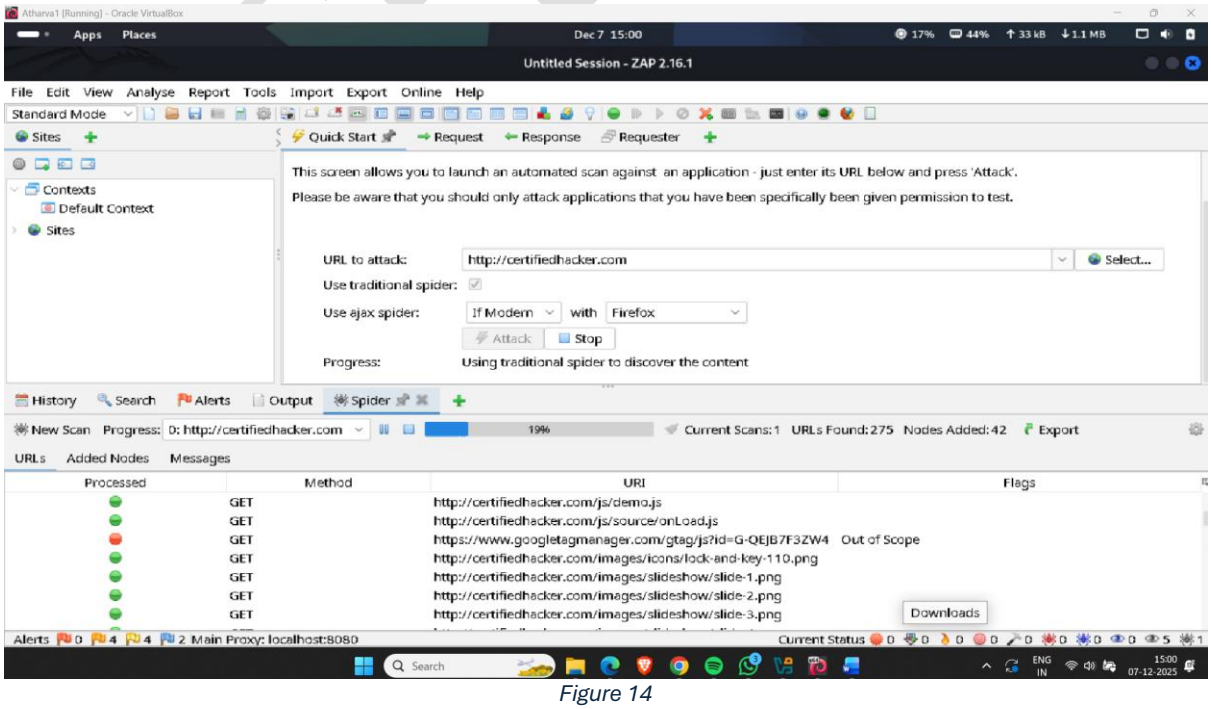


Figure 14

Report:

ZAP by Checkmarx Scanning Report

Generated with ZAP on Fri 5 Dec 2025, at 13:34:31

ZAP Version: 2.16.1

ZAP by Checkmarx

Contents

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- http://testfire.net

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	2 (15.4%)	0 (0.0%)	2 (15.4%)
	Medium	0 (0.0%)	1 (7.7%)	1 (7.7%)	1 (7.7%)	3 (23.1%)
	Low	0 (0.0%)	1 (7.7%)	3 (23.1%)	0 (0.0%)	4 (30.8%)
	Informational	0 (0.0%)	0 (0.0%)	4 (30.8%)	0 (0.0%)	4 (30.8%)
	Total	0 (0.0%)	2 (15.4%)	10 (76.9%)	1 (7.7%)	13 (100%)

Alerts

Risk=High, Confidence=Medium (2)

http://testfire.net (2)

Cross Site Scripting (Reflected) (1)

► POST http://testfire.net/sendFeedback

SQL Injection (1)

► POST http://testfire.net/doLogin

Risk=Medium, Confidence=High (1)

http://testfire.net (1)

Content Security Policy (CSP) Header Not Set (1)

► GET http://testfire.net

Risk=Medium, Confidence=Medium (1)

http://testfire.net (1)

Missing Anti-clickjacking Header (1)

► GET http://testfire.net

Risk=Medium, Confidence=Low (1)

http://testfire.net (1)

Absence of Anti-CSRF Tokens (1)

► GET http://testfire.net/login.jsp

Risk=Low, Confidence=High (1)

http://testfire.net (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

► GET http://testfire.net

Alert type	Risk	Count
Cross Site Scripting (Reflected)	High	2 (15.4%)
SQL Injection	High	1 (7.7%)
Absence of Anti-CSRF Tokens	Medium	3 (23.1%)
Content Security Policy (CSP) Header Not Set	Medium	164 (1,261.5%)
Missing Anti-clickjacking Header	Medium	62 (476.9%)
Cookie without SameSite Attribute	Low	3 (23.1%)
Cross-Domain JavaScript Source File Inclusion	Low	1 (7.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	206 (1,584.6%)
X-Content-Type-Options Header Missing	Low	101 (776.9%)
Information Disclosure - Suspicious Comments	Informational	10 (76.9%)

The ZAP report shows that the website http://testfire.net was scanned and a total of 13 vulnerabilities were found. These include 2 high-risk issues (Cross-Site Scripting and SQL Injection), 3 medium-risk issues (missing security headers and Anti-CSRF tokens), 4 low-risk issues (information leakage, insecure cookies), and 4 informational issues (comments, headers, etc.).

The tables summarize the vulnerabilities based on risk level, confidence, and alert type, showing that the website has several security weaknesses. High-risk issues are dangerous because they allow attackers to inject code or access sensitive data, while medium and low issues weaken user protection. Overall, the report indicates that the site needs urgent fixing of high-risk vulnerabilities and improvement of its security headers and configurations.

Vulnerablity Analysis using Smart Scanner

A Smart Scanner is an advanced automated cybersecurity tool designed to scan websites, networks, servers, or applications to identify security vulnerabilities. It uses modern technologies like machine learning, signature analysis, pattern matching, and intelligent heuristics to detect threats more accurately than traditional scanners.

Smart Scanners are commonly integrated into:

- Vulnerability Assessment
- Penetration Testing
- Bug Bounty Recon
- DevSecOps pipelines
- Continuous monitoring

Advantages of Smart Scanner:

1) High Speed
2) Intelligent Detection
3) Easy to Use
4) Generates automated Reports
5) Continuous Security

Key Features of a Smart Scanner:

✓ **AI-based Analysis**
Machine learning detects new or unknown attack patterns.
✓ **Fast Automated Scanning**
Able to test hundreds of pages or IPs quickly.
✓ **Real-time Monitoring**
Tracks changes in security posture over time.

Download link: https://www.thesmartscanner.com/download

Step1: Open smart scanner
Step2: Enter the Target & click scan

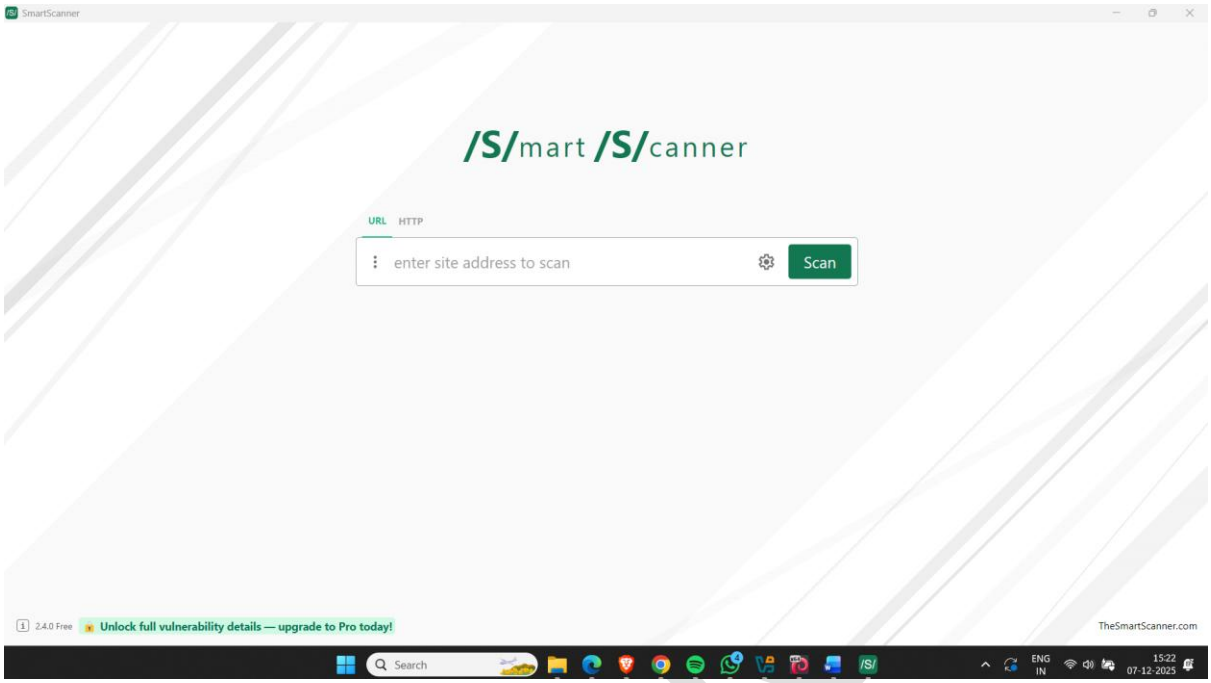


Figure 15

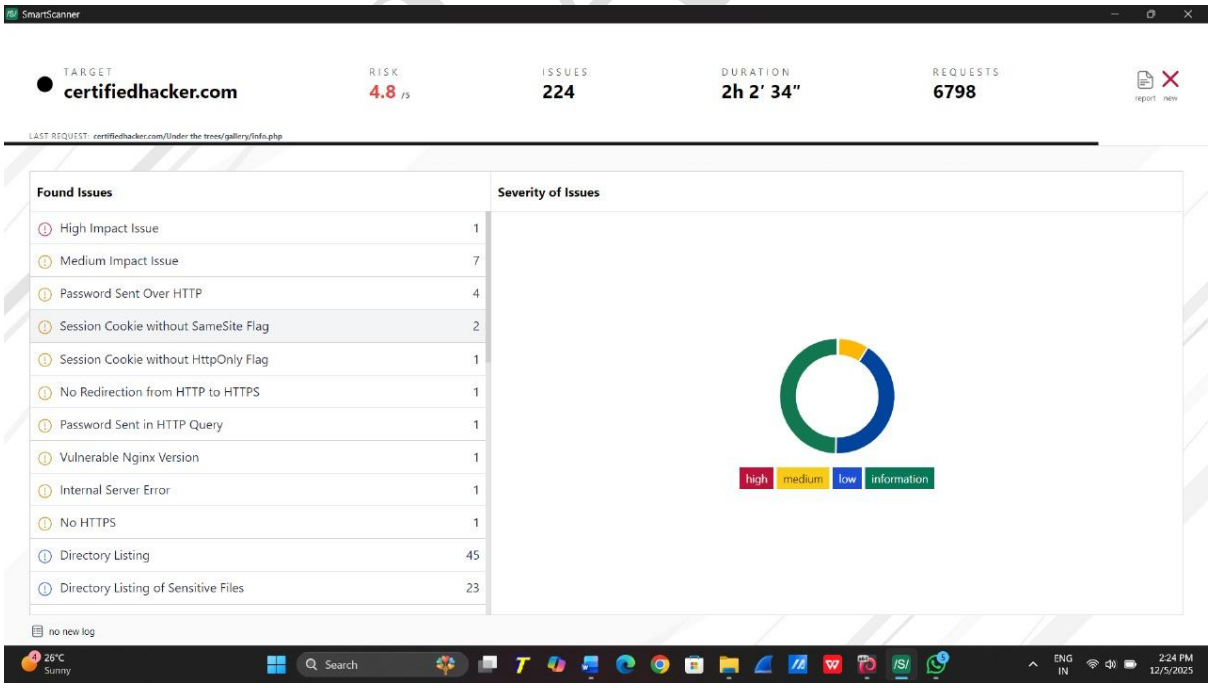


Figure 16

Report:

Scan Report

Target: **certifiedhacker.com**

Date: **Fri Dec 5 2025**

Found Issues: **224**

scan **stopped** within **2h 2' 34"** after **6798** requests.

Risk

Issue Severity

Executive Summary

SmartScanner conducted a scan on the provided target to find security weaknesses and vulnerabilities. The scan took 2 hours and 2 minutes and 34 seconds. After performing 6798 requests, SmartScanner found 224 issues in which 1 of them is highly severe. The overall security risk rating for the target is 4.8 out of 5. It is recommended to fix the found issues as soon as possible to mitigate the security risk. Technical details, as well as remediation of results, can be found in the following. *

* DISCLAIMER: This report reflects only the findings discovered by SmartScanner during this scan and may not represent a comprehensive security assessment.

List of Issues

1– High Impact Issue
- 1.1– http://certifiedhacker.com

2– Medium Impact Issue
- 2.1– http://certifiedhacker.com
- 2.2– http://certifiedhacker.com
- 2.3– http://certifiedhacker.com
- 2.4– http://certifiedhacker.com
- 2.5– http://certifiedhacker.com
- 2.6– http://certifiedhacker.com
- 2.7– http://certifiedhacker.com

3– Password Sent Over HTTP
- 3.1– http://certifiedhacker.com
- 3.2– http://certifiedhacker.com/Online Booking/checkout.htm
- 3.3– http://certifiedhacker.com/Online Booking/index.htm
- 3.4– http://certifiedhacker.com/Social Media/sample-login.html

4– Session Cookie without SameSite Flag
- 4.1– https://certifiedhacker.com:2096
- 4.2– https://certifiedhacker.com:2096?locale=es

5– Session Cookie without HttpOnly Flag
- 5.1– https://certifiedhacker.com:2096?locale=es

6– No Redirection from HTTP to HTTPS
- 6.1– http://certifiedhacker.com

7– Password Sent in HTTP Query
- 7.1– http://certifiedhacker.com/Online Booking/index.htm

8– Vulnerable Nginx Version
- 8.1– http://certifiedhacker.com

9– Internal Server Error
- 9.1– https://certifiedhacker.com:2096

10– No HTTPS
- 10.1– http://certifiedhacker.com

Full Report:

smart scanner.pdf

Vulnerablity Analysis using NESSUS

Nessus is one of the most widely used vulnerability assessment tools that scans systems, networks, servers, and applications for security weaknesses. It is developed by Tenable and trusted by cybersecurity professionals worldwide.

Nessus is mainly used to identify:

- Missing security patches
- Misconfigurations
- Weak passwords
- Outdated software
- Known vulnerabilities (CVEs)
- Malware, backdoors, and policy violations

Types of Scans in Nessus:

1)Basic Network Scan

General scan of IP ranges and networks.

2)Web Application Scan

Checks for:

- SQL injection
- XSS
- Web misconfigurations

3)Credentialed Scan

Uses valid login credentials to check:

- System patches
- Permissions
- Registry issues
- Local vulnerabilities

4)Malware Scan

Detects known malware signatures and backdoors.

5)Policy Compliance Scan

Checks compliance with:

- CIS Benchmarks
- PCI DSS
- ISO 27001
- NIST

Download link: https://www.tenable.com/products/nessus/nessus-essentials

How to use it:
Step1: Open NESSUS
Step2: put login credentials
Step3: Click on create a new scan

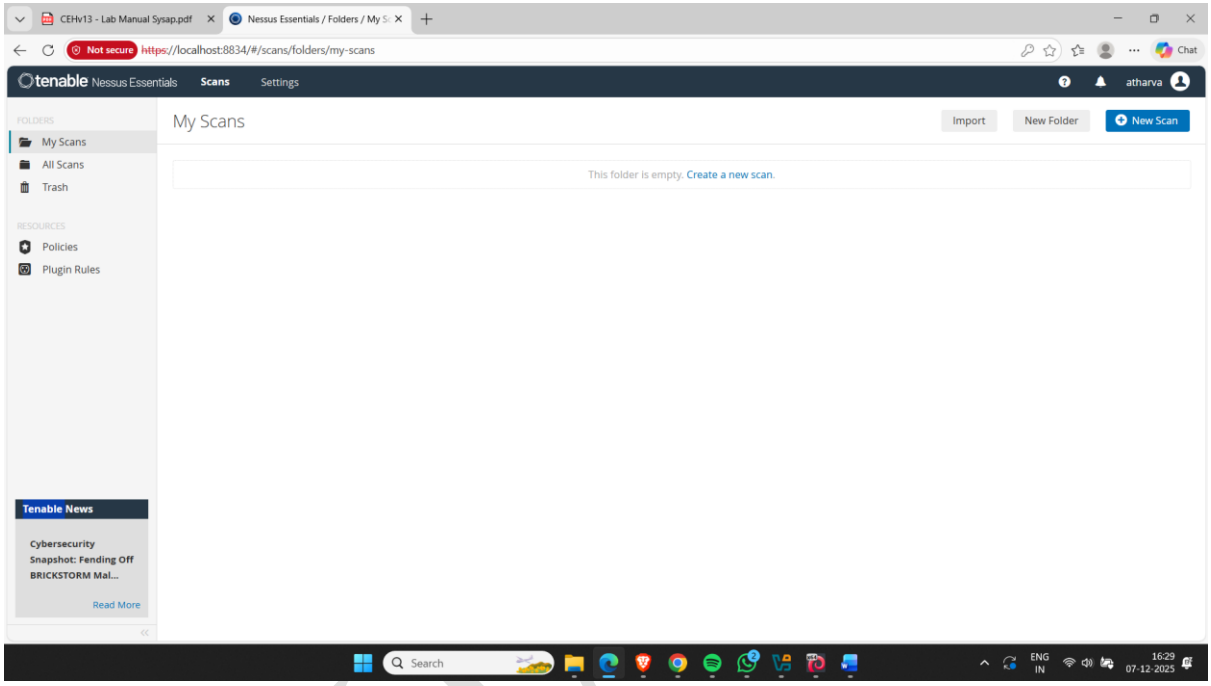


Figure 17

Step5:Select the Host Discovery scan

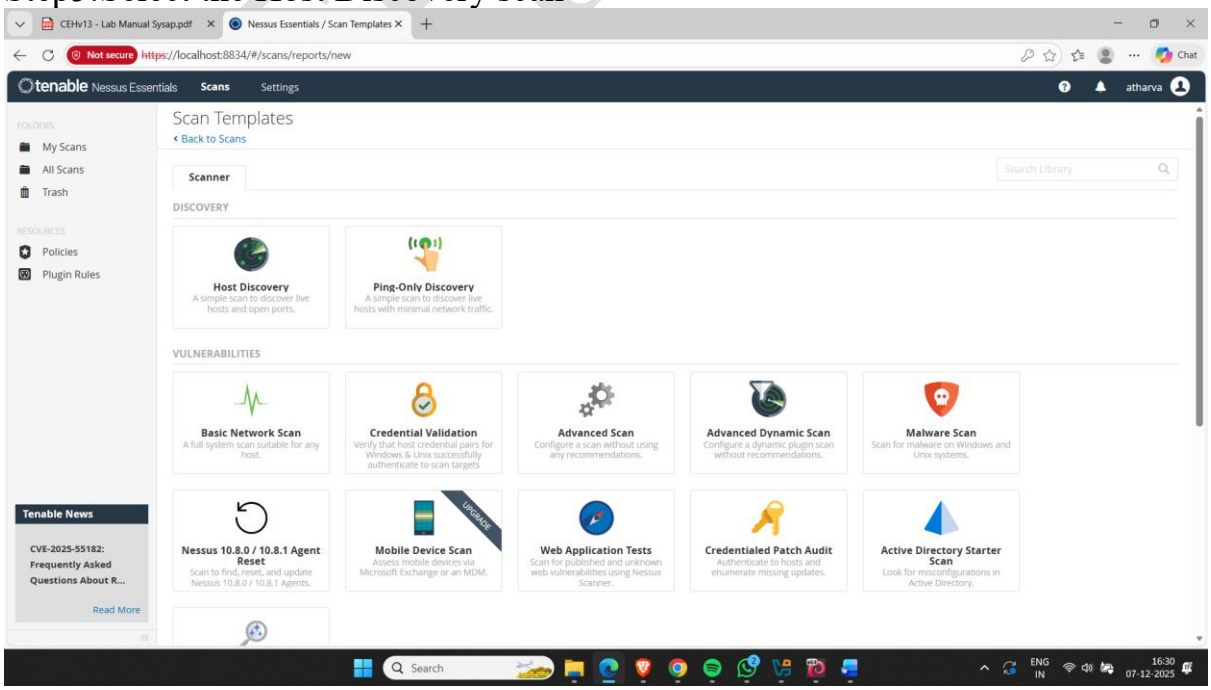


Figure 18

Step6: -Give scan details and target name
-Tap on scan & click on launch scan

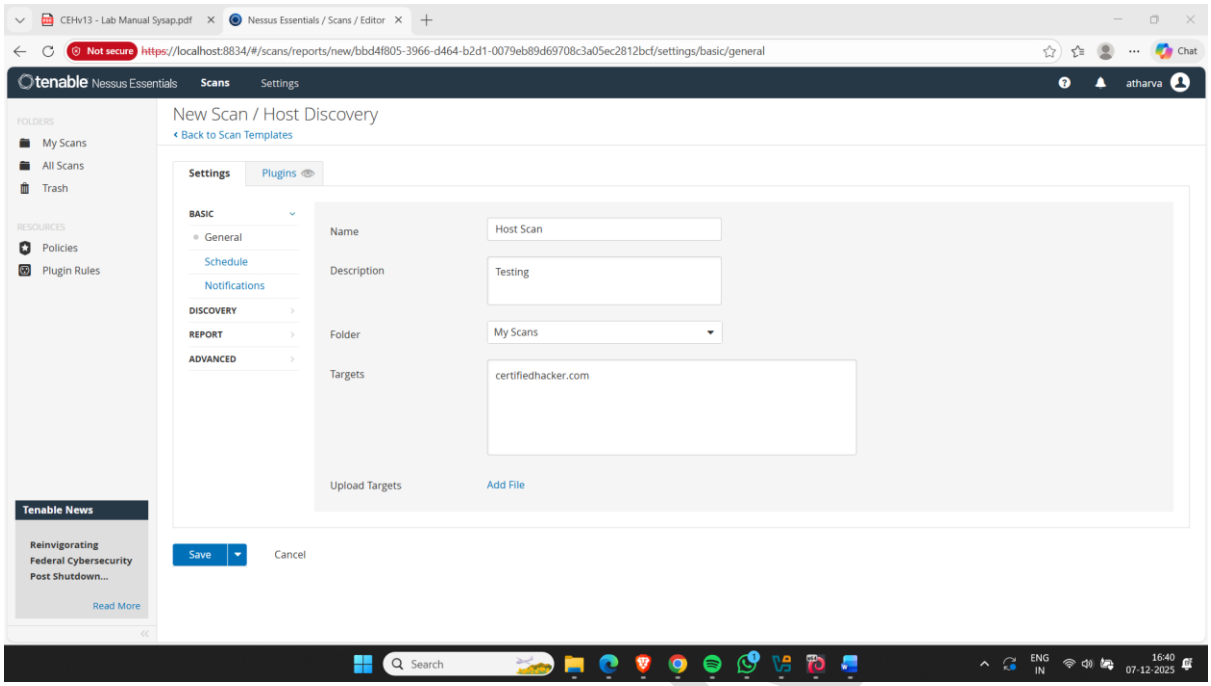


Figure 19

Step7:Scanning in process

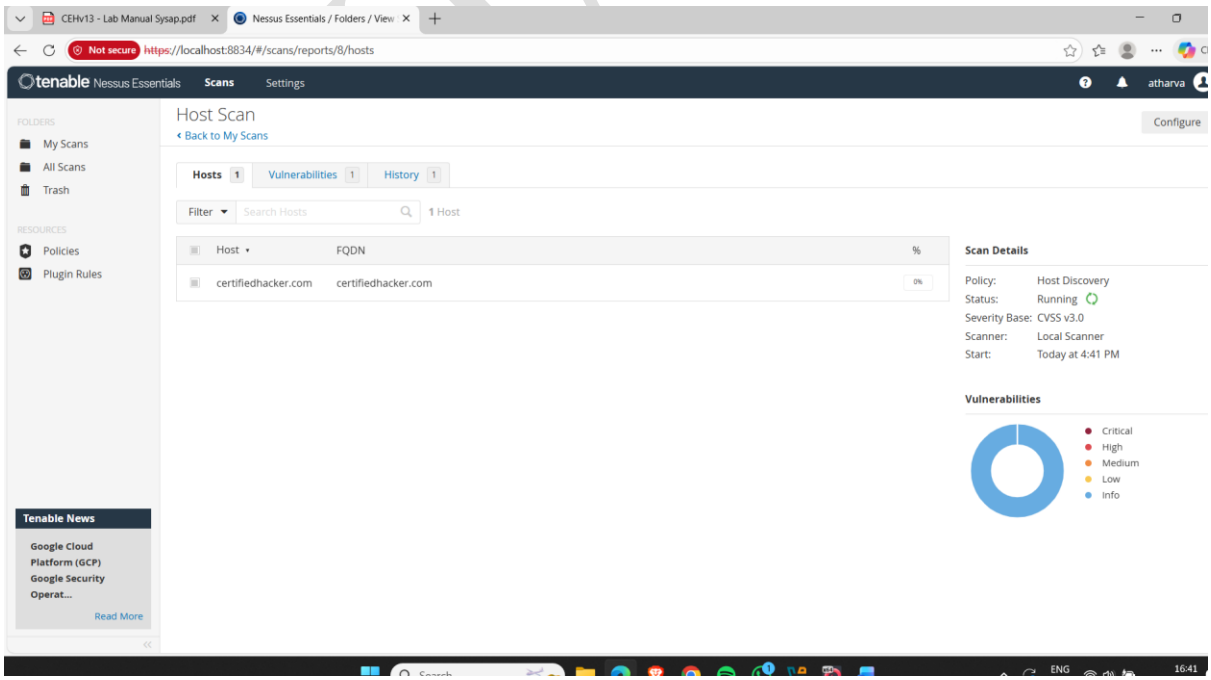


Figure 20

Report:

certifiedhacker.com

Report generated by Tenable Nessus™ Sun, 07 Dec 2025 11:09:05 India Standard Time

Vulnerabilities by Host

162.241.216.11

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	2

Scan Information

Start time:	Sun Dec 7 11:01:37 2025
End time:	Sun Dec 7 11:09:05 2025

Host Information

DNS Name:	box5331.bluehost.com
IP:	162.241.216.11

Vulnerabilities

35450 - DNS Server Spoofed Request Amplification DDoS

Synopsis

The remote DNS server could be used in a distributed denial of service attack.

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

EPSS Score

0.4121

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2006-0987

Plugin Information

Published: 2009/01/22, Modified: 2023/10/27

Plugin Output

udp/53/dns

```
The DNS query was 17 bytes long, the answer is 64 bytes long.
```

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

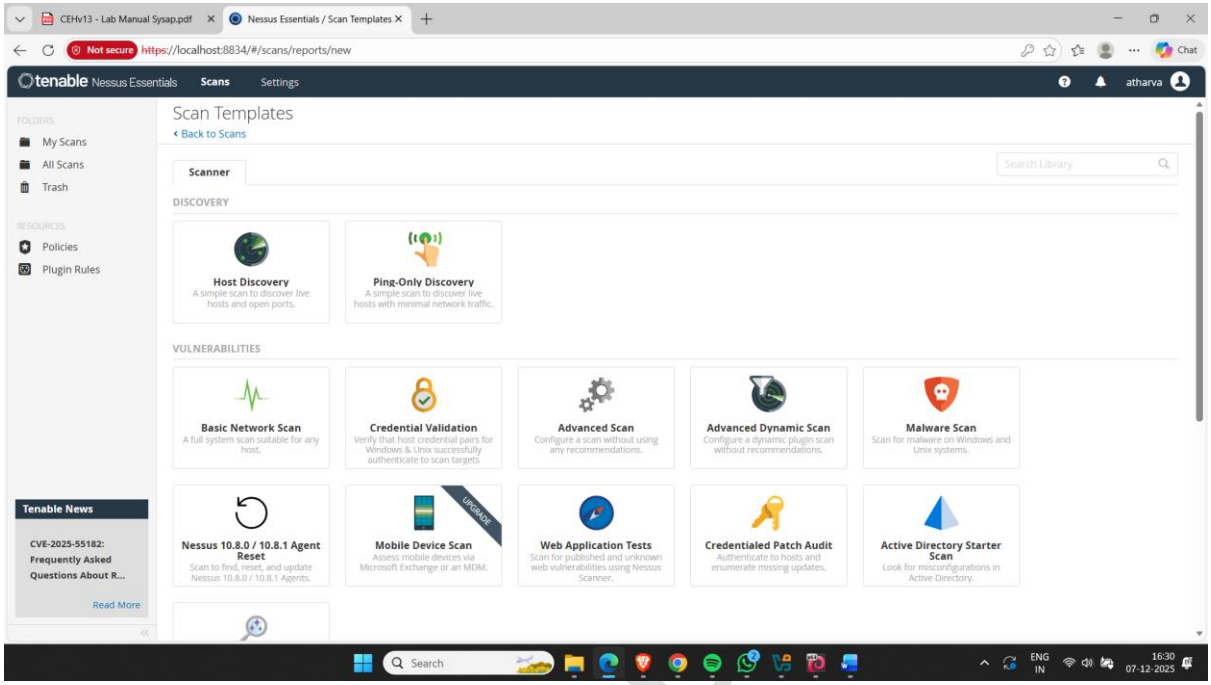
udp/53/dns

```
Version : 9.16.23-RH
```

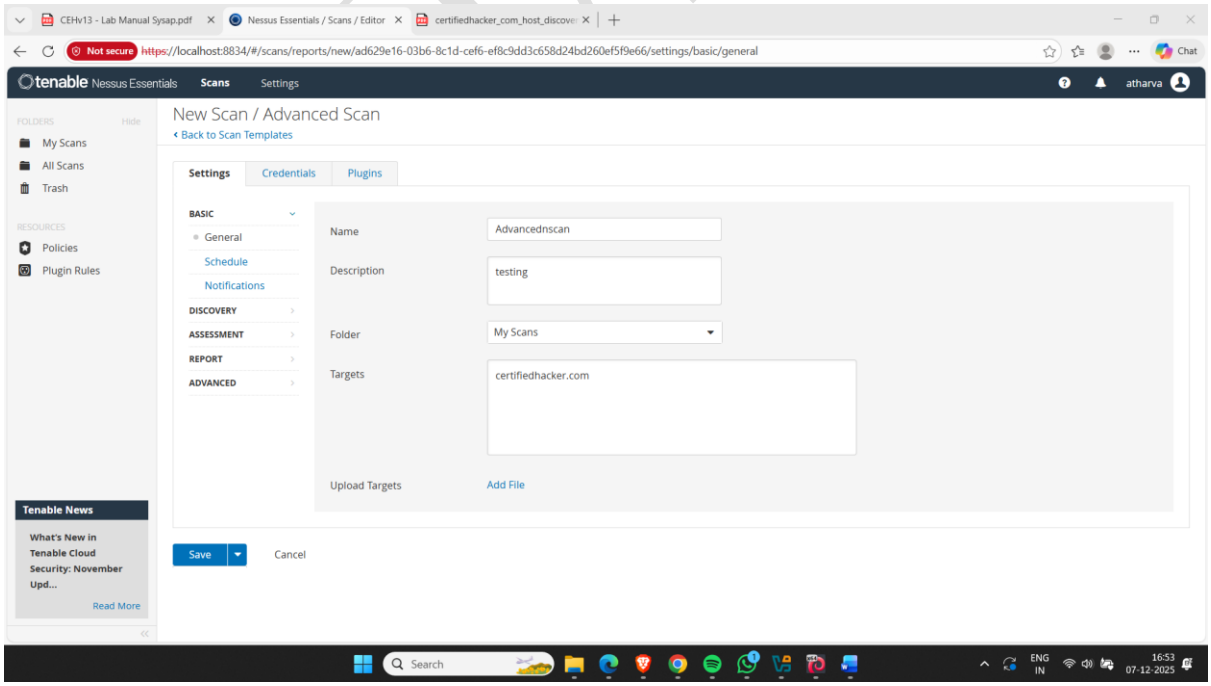
Full report:

certifiedhacker_com_host_discovery.pdf

Step8:Select Advanced scan



-Give scan details and target name
-Tap on scan & click on launch scan



Report:

certifiedhacker.com

Report generated by Tenable Nessus™ Sun, 07 Dec 2025 12:54:56 India Standard Time

35450 - DNS Server Spoofed Request Amplification DDoS

Synopsis

The remote DNS server could be used in a distributed denial of service attack.

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

EPSS Score

0.4121

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

References

CVE	CVE-2006-0987

Plugin Information

Published: 2009/01/22, Modified: 2023/10/27

Plugin Output

udp/53/dns

```
The DNS query was 17 bytes long, the answer is 64 bytes long.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

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.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/443/www

```
HTTP/1.1 302 Found
Date: Sun, 07 Dec 2025 06:27:32 GMT
Server: Apache
X-Robots-Tag: noindex, nofollow
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Location: /404.html
host-header: c2hhcnVkLmJsdWVob3N0LmNvbQ==
Cache-Control: no-cache, no-store, must-revalidate
```

162.241.216.11 8

```
Pragma: no-cache
Expires: 0
Content-Length: 0
Keep-Alive: timeout=5, max=75
Content-Type: text/html; charset=UTF-8

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

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.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/03/22

Plugin Output

tcp/2078/www

```
HTTP/1.1 401 Unauthorized
Date: Sun, 07 Dec 2025 06:27:36 GMT
Server: cPanel
Persistent-Auth: false
Host: 162.241.216.11:2078
Cache-Control: no-cache, no-store, must-revalidate, private
Connection: close
Vary: Accept-Encoding
WWW-Authenticate: Basic realm="Restricted Area"
```



```
Content-Length: 35
Content-Type: text/html; charset="utf-8"
Expires: Fri, 01 Jan 1990 00:00:00 GMT
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - box5331.bluehost.com
```

Full Report:

certifiedhacker_com_adv_scan.pdf