

**Lab Practical 09:**

**Perform web application security scan using W3AF or any Web Application Scanning Tool(Nessus)**

**Nessus :**

- **Introduction:**

Nessus is a widely used vulnerability scanning tool in the field of cyber security and security testing. Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. It is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer, that you have connected with any network. It does this by running over 1200 checks on a given computer, to see if any of these attacks could be used to break into the computer or otherwise harm it.

- **Installation:**

1. **Download Nessus:**

- Navigate to the <https://www.tenable.com/downloads/nessus> page
- Choose the appropriate version for your operating system and Download

2. **Install Nessus:**

- Open a terminal and navigate to the directory where the Nessus package was downloaded.
- Run the following command:

```
(kali㉿kali)-[~]  
$ cd Downloads  
  
(kali㉿kali)-[~/Downloads]  
$ sudo dpkg -i ./Nessus-10.8.3-ubuntu1604_amd64.deb
```

3. **Start Nessus Service:**

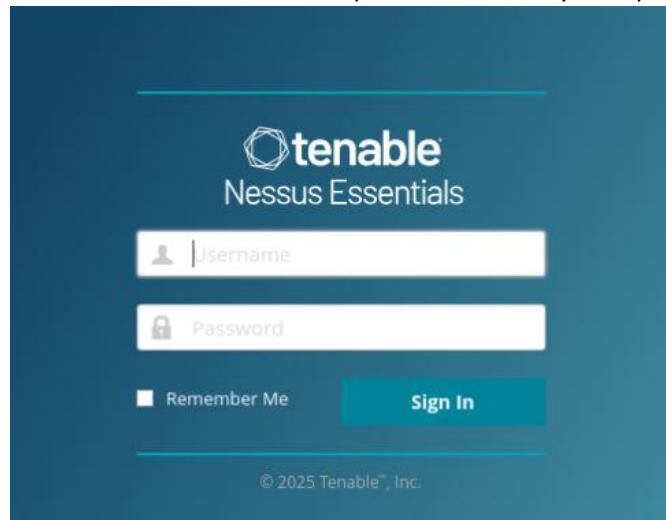
- start the Nessus service by following command:

```
(kali㉿kali)-[~/Downloads]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
  
(kali㉿kali)-[~/Downloads]  
$
```

Date: 07/ 02 /2025

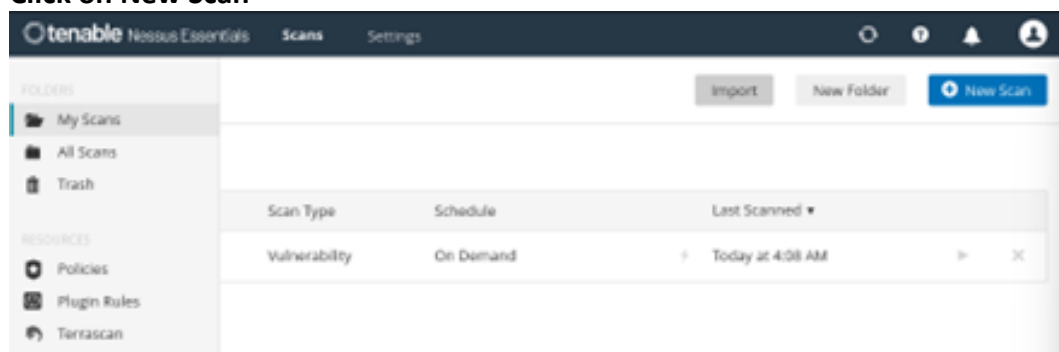
#### 4. Access Nessus Web Interface:

- Open a web browser and navigate to <https://localhost:8834>.
- Follow the setup instructions to create an administrator account and activate Nessus using the activation code obtained during the download process.
- The default username & password will be your operating system user's.

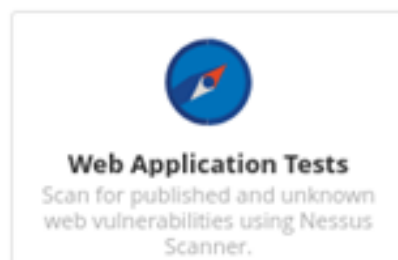


- Scan DVWA (<http://localhost/DVWA/index.php>)

#### 1. Click on New Scan



#### 2. Select Web Application test



Date: 07/ 02 /2025

### 3. Enter Name and Target and Click on launch (here the Target should be IP address or URL of Target)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Dwva\_scan

Description

Scan vulnerabilities of dwva

Folder

My Scans

Targets

http://localhost/DVWA/index.php

Upload Targets

Add File

Save

Cancel

### 4. Wait till it scan the Target (the running state will change to complete)

Hosts	Vulnerabilities	History
0	0	1

Search History

Start Time	Last Scanned	Status
Current Today at 11:58 AM	N/A	Running

### 5. After Some time, you will see the vulnerabilities in vulnerabilities section

Hosts

Vulnerabilities

History

Filter

Search Vulnerabilities

14 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
MEDIUM	5.3			Browsable Web Directories	CGI abuses	1	
MEDIUM	4.3 *			Web Application Potentially Vulnerable to Clickjacking	Web Servers	1	
INFO				HTTP (Multiple Issues)	Web Servers	3	
INFO				HTTP (Multiple Issues)	CGI abuses	2	
INFO				Web Server (Multiple Issues)	Web Servers	2	
INFO				Apache HTTP Server Version	Web Servers	1	
INFO				CGI Generic Tests Load Estimation (all tests)	CGI abuses	1	
INFO				External URLs	Web Servers	1	
INFO				Nessus SYN scanner	Port scanners	1	
INFO				Web Application Cookies Not Marked HttpOnly	Web Servers	1	
INFO				Web Application Cookies Not Marked Secure	Web Servers	1	
INFO				Web Application Potentially Sensitive CGI Parameter Detection	CGI abuses	1	
INFO				Web Application Sitemap	Web Servers	1	
INFO				Web mirroring	Web Servers	1	

Scan Details

Policy:

Web Application Tests

Status:

Canceled

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

February 2 at 6:37 AM

End:

February 2 at 8:14 AM

Elapsed:

2 hours

Vulnerabilities

Critical

High

Medium

Low

Info

**Date: 07/ 02 /2025**

• **Vulnerabilities & Solution:**

**1. Browsable Web Directories**

**Impact:** Allows attackers to list files and directories, which may reveal sensitive information or expose attack surfaces.

**Solution:** Disable directory listing (ex: Disable "Directory Browsing" in IIS Manager)

**2. Web Application Potentially Vulnerable to Common Attacks**

**Impact:** This suggests the web application may be vulnerable to attacks like SQL Injection, XSS, CSRF, etc.

**Solution:**

- Input Validation: Implement strong validation and sanitization for user inputs.
- Parameterized Queries: Use prepared statements for database interactions.
- Enable a Web Application Firewall (WAF): Use tools like ModSecurity.

**3. Apache HTTP Server Version Disclosure**

**Impact:** Attackers can determine the Apache version and exploit known vulnerabilities.

**Solution:** Hide the Apache version (ex: ServerSignature Off, ServerTokens Prod)

**4. External URLs Found**

**Impact:** This lists external URLs referenced by the web application, which may reveal third-party integrations.

**Solution:**

- Review external links to ensure they are necessary and secure.
- Use rel="noopener noreferrer" for external links.

**5. Web Application Cookies Not Marked HttpOnly and Secure (Info)**

**Impact:** Can lead to session hijacking or Man-in-the-Middle (MITM) attacks.

**Solution:** Set HttpOnly and Secure attributes for cookies (ex: Set-Cookie: session\_id=abc123; HttpOnly; Secure; SameSite=Strict)

**6. Web Mirroring Allowed**

**Impact:** Attackers can easily copy the entire website for phishing or reconnaissance.

**Solution:**

- Restrict web scrapers with a robots.txt file.
- Implement rate-limiting in the web server.