



Date: 09/02/2025

Lab Practical 09:

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

Nessus:

Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services and other network resources.

As an open-source network vulnerability scanner, Nessus uses the Common Vulnerabilities and Exposures architecture to make it easy for compliant security solutions to cross-link. The Nessus Attack Scripting Language (NASL), a straightforward language used by Nessus, is used to specify specific threats and potential attacks.

It checks a computer and sends an alert if it detects any [security vulnerabilities](#) that hackers could use to get into any of your computers connected to a network. It does this by checking a machine more than 1200 times to see if malicious actors could use any such attacks to get into the system or do other harm.

Nessus identifies software flaws, [missing patches](#), malware, [denial-of-service](#) vulnerabilities, default passwords and misconfiguration errors, among other potential flaws. When Nessus discovers vulnerabilities, it issues an alert that IT teams can then investigate and determine what -- if any -- further action is required.

How does it work?

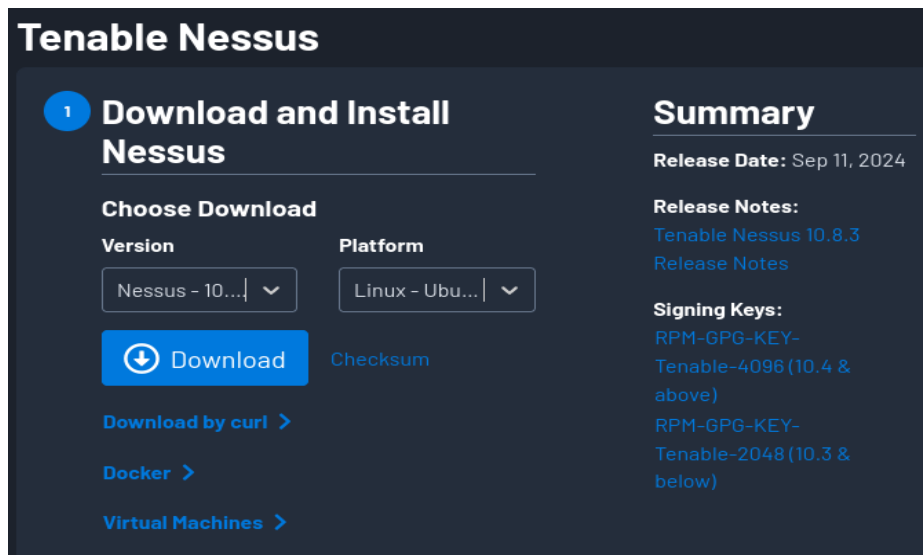
Nessus and related port-scanning security systems work by having an understanding of how different services (a web server, Simple Mail Transfer Protocol or SMTP server, File Transfer Protocol or FTP server, etc.) are reached by distant servers. Emails, web pages, and other high-level network traffic are typically transmitted to servers using TCP streams carrying an encrypted high-level protocol. The majority of high-level network traffic is transported by this protocol.

A computer would divide its physical connection to the network into numerous logical pathways, known as ports, in order to prevent multiple streams from becoming entangled with one another. Consequently, to communicate with a web server running on a specific machine.

Installation

→ Download Nessus

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



→ Install Nessus:

- Open a terminal and navigate to the directory where the Nessus package was downloaded.
- Run the following command : `sudo dpkg -I ./Nessus-10.8.3-ubuntu1604_amd64.db`

Date: 09/02/2025

```
L$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
[sudo] password for mohit:
Selecting previously unselected package nessus.
(Reading database ... 394062 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-ubuntu1604_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

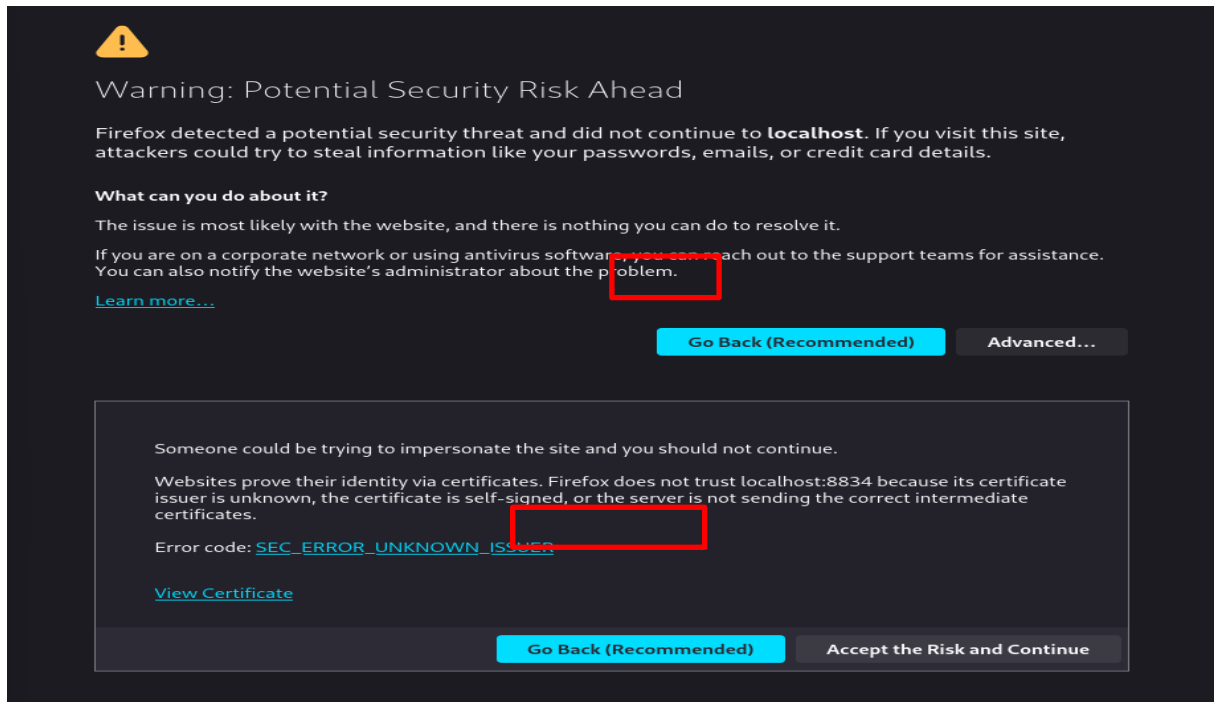
→ Start Nessus Service

- `sudo /bin/systemctl start nessusd.service`

```
(mohit@kali)~[~/Downloads]
$ sudo /bin/systemctl start nessusd.service
```

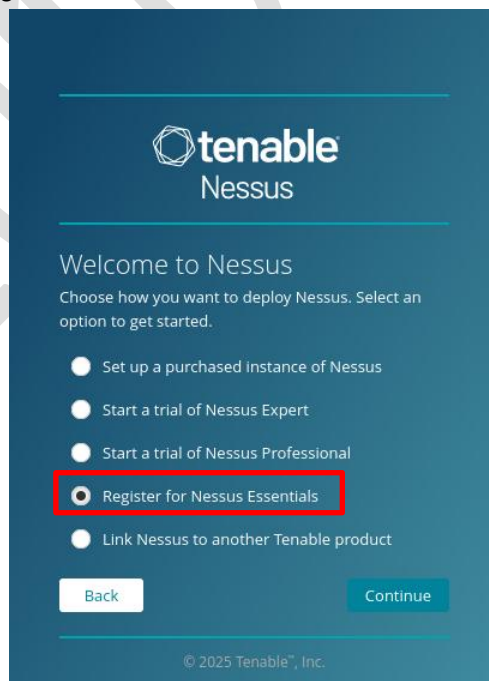
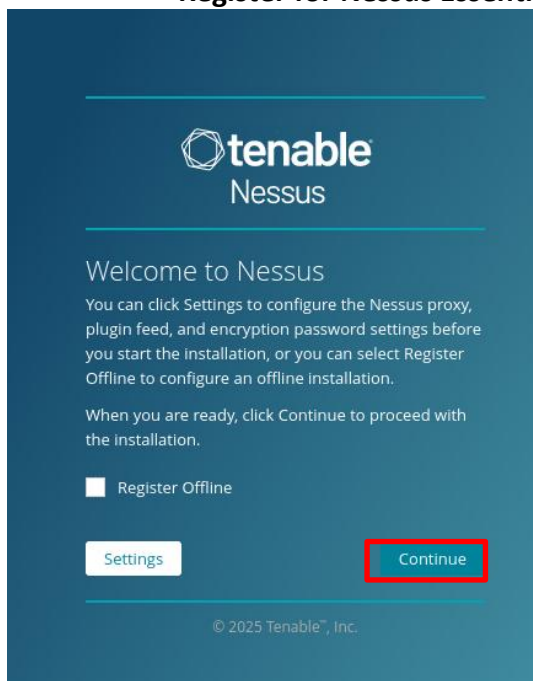
→ Open browser

- <https://localhost:8834>
- Click Advanced then Accept the Risk and Continue



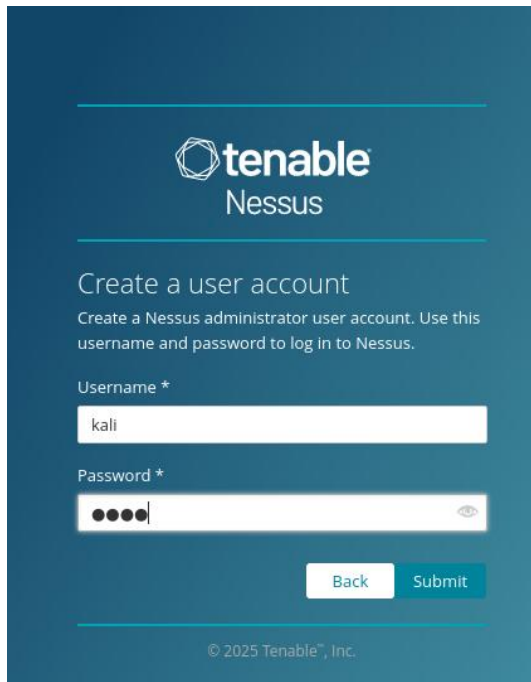
→ Register

▪ Register for Nessus Essentials

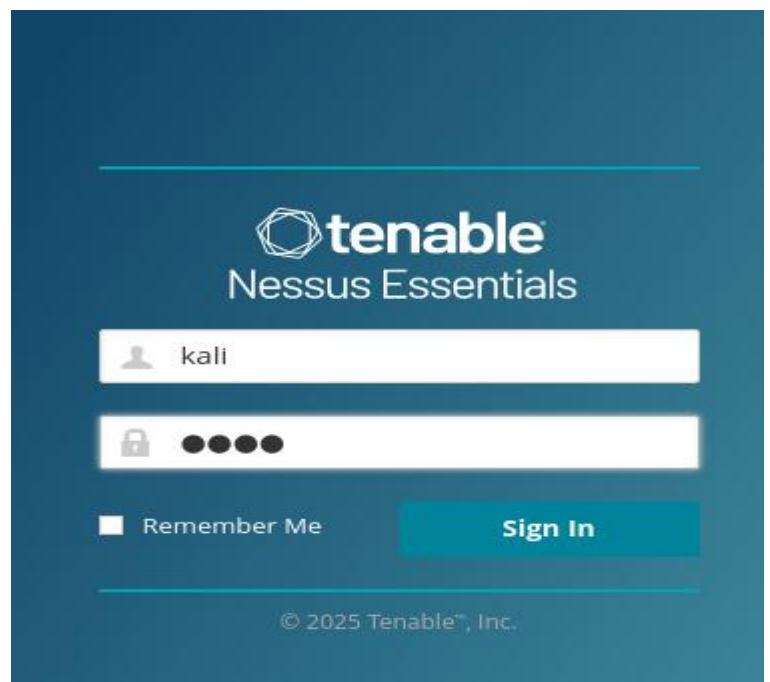


- **Create User Account**
 - Enter Username and Password
 - Click Submit
 - Enter username and password which entered at time of creation

Date: 09/02/2025



The screenshot shows the 'Create a user account' page in Tenable Nessus. It includes the Tenable Nessus logo, a heading 'Create a user account', and a sub-heading 'Create a Nessus administrator user account. Use this username and password to log in to Nessus.' Below this, there are input fields for 'Username *' (containing 'kali') and 'Password *' (containing four dots). At the bottom right, there are 'Back' and 'Submit' buttons. The footer shows '© 2025 Tenable™, Inc.'

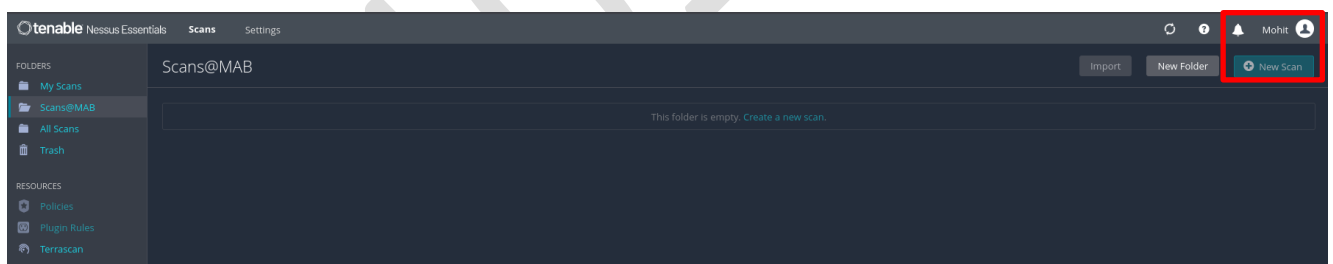


The screenshot shows the Tenable Nessus Essentials login screen. It features the Tenable Nessus Essentials logo, a username input field (containing 'kali'), and a password input field (containing four dots). Below the password field, there is a 'Remember Me' checkbox and a 'Sign In' button. The footer shows '© 2025 Tenable™, Inc.'

Welcome screen will be displayed

Perform Web Application Test

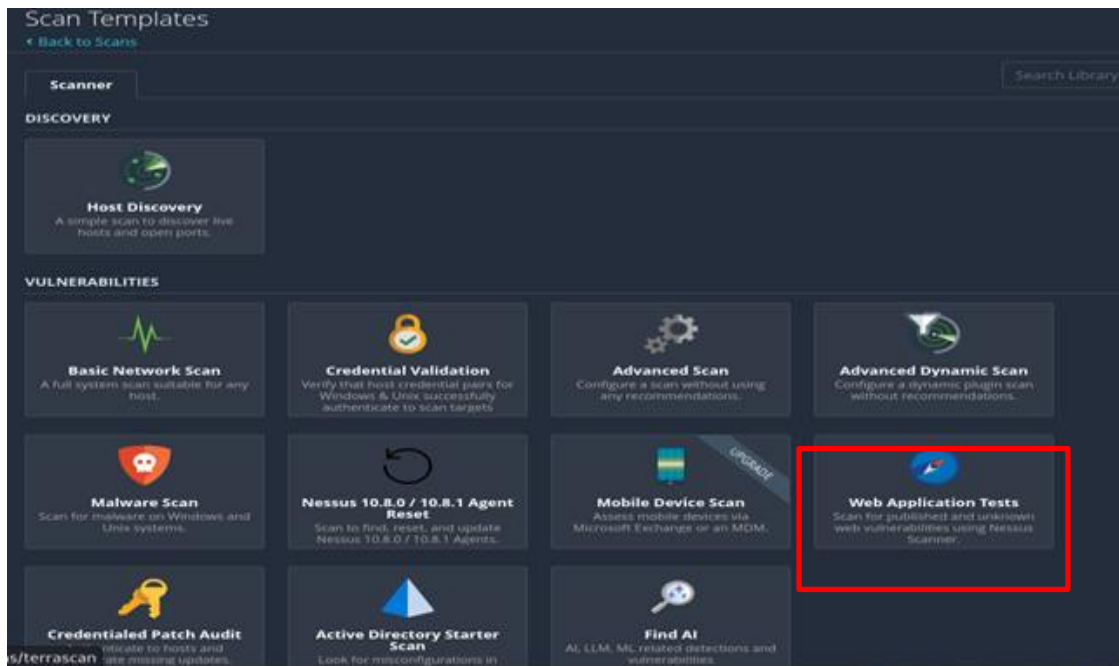
Click on New Scan button displayed on right hand side



New Screen will be displayed

Choose Web Application Tests

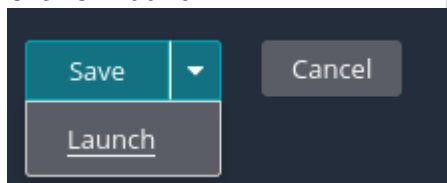
Date: 09/02/2025



Fill details as per requirements

Click down on arrow displayed along with save button

Click on Launch



Nessus will start performing the test

Name	Scan Type	Schedule	Last Scanned
DVWA	Vulnerability	On Demand	Today at 1:06 PM

It will take time to complete scanning

So wait for it.

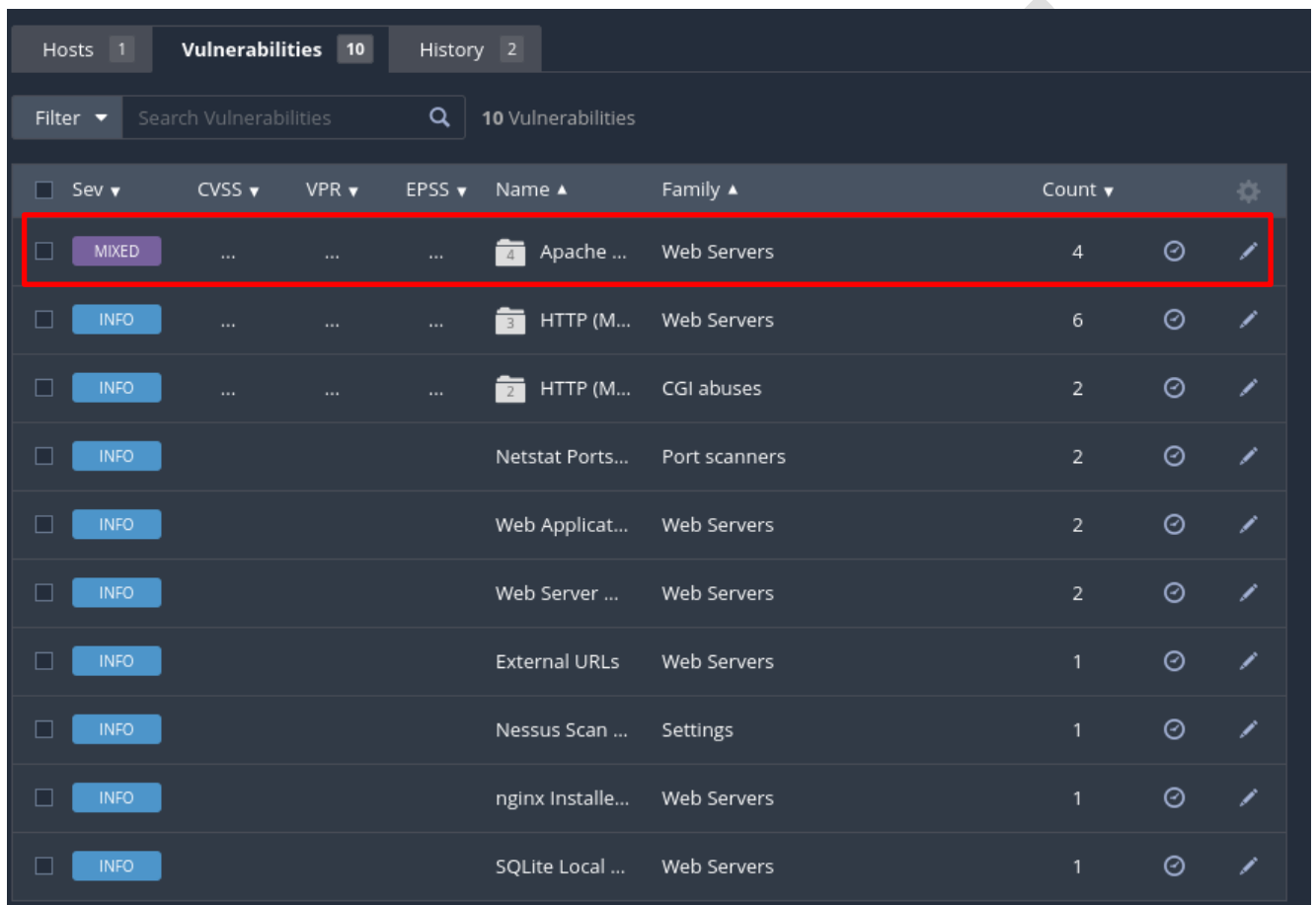
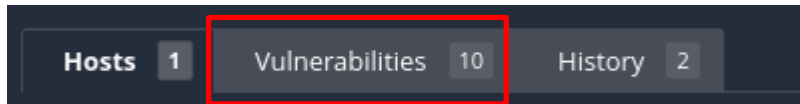
After completing scanning below will be displayed

DVWA	Vulnerability	On Demand	✓ Today at 1:33 PM
------	---------------	-----------	--------------------

Date: 09/02/2025

Now double click on Name

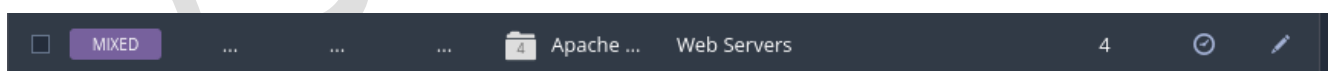
Go to Vulnerabilities tab and check vulnerabilities



The screenshot shows the 'Vulnerabilities' tab with a search bar and a list of 10 vulnerabilities. The first row is highlighted with a red rectangular box.

Sev	CVSS	VPR	EPSS	Name	Family	Count	
MIXED	Apache ...	Web Servers	4	🔍 ✎
INFO	HTTP (M...	Web Servers	6	🔍 ✎
INFO	HTTP (M...	CGI abuses	2	🔍 ✎
INFO				Netstat Ports...	Port scanners	2	🔍 ✎
INFO				Web Applicat...	Web Servers	2	🔍 ✎
INFO				Web Server ...	Web Servers	2	🔍 ✎
INFO				External URLs	Web Servers	1	🔍 ✎
INFO				Nessus Scan ...	Settings	1	🔍 ✎
INFO				nginx Installe...	Web Servers	1	🔍 ✎
INFO				SQLite Local ...	Web Servers	1	🔍 ✎

Double Click on vulnerability to display more detail



The screenshot shows the details of the first vulnerability, which is highlighted with a red rectangular box.

Sev	CVSS	VPR	EPSS	Name	Family	Count	
MIXED	Apache ...	Web Servers	4	🔍 ✎

Date: 09/02/2025

<input type="checkbox"/>	Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲	Family ▲	Count ▼		
<input type="checkbox"/>	MEDIUM	5.3			Apache mod...	Web Servers	1	🕒	✎
<input type="checkbox"/>	INFO				Apache HTTP...	Web Servers	1	🕒	✎
<input type="checkbox"/>	INFO				Apache HTTP...	Web Servers	1	🕒	✎
<input type="checkbox"/>	INFO				Apache HTTP...	Web Servers	1	🕒	✎

MEDIUM

Apache mod_status /server-status Information Disclosure

>

Description

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Solution

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

See Also

https://www.owasp.org/index.php/SCG_WS_Apache

Output

```

Nessus was able to exploit the issue to retrieve the contents of
'server-status' using the following request :

http://192.168.252.136/server-status

Attached is a copy of the response

```

Port ▲	Hosts			
80 / tcp / www	192.168.252.136	📄	server-status	1.5KB
	192.168.252.136			

As per above you can see details of each.

Explanation and Solution:

The above image describes a security vulnerability in Apache's mod_status module, where an unauthenticated attacker can access /server-status to retrieve sensitive information, such as active requests, CPU usage, and connected hosts.

- Solution:

To fix this issue:

1. Disable mod_status if not needed:
 - Open the Apache configuration file (httpd.conf or apache2.conf).
 - Comment out or remove the mod_status module:



Date: 09/02/2025

#LoadModule status_module modules/mod_status.so

2. Restrict Access: If mod_status is necessary, restrict access to trusted IP addresses only. In the configuration file:

<Location /server-status>

SetHandler server-status

Require ip 192.168.1.100 # Allow only specific IPs

</Location>

3. Enable Authentication: Use .htaccess or Apache authentication to require login credentials.
4. Firewall Rules: Block external access to /server-status using a firewall rule.

Other Vulnerabilities

- **Apache HTTP Server (Multiple Issues):** This might include outdated versions, misconfigurations, or known exploits.
- **HTTP (Multiple Issues):** Could indicate unsecured HTTP configurations.
- **Netstat Portscanner (SSH):** Suggests scanning for open SSH ports, which could be a security concern.
- **Web Server Directory Enumeration:** May indicate that directories are publicly accessible.
- **External URLs:** Could indicate external links that might be used for malicious purposes.

Solutions

1. **Patch and Update:**
 - Update Apache HTTP Server and any other web services (nginx, SQLite).
 - Ensure all web frameworks, databases, and dependencies are up to date.
2. **Secure Configurations:**
 - Restrict access to sensitive directories.
 - Configure SSH properly (disable root login, use key-based authentication).
3. **Monitor and Restrict Network Access:**
 - Limit exposure of unnecessary services.
 - Use a firewall to restrict access to specific IPs.
4. **Conduct Regular Scans:**
 - Schedule periodic vulnerability scans.
 - Address new issues as they appear.
5. **Log Monitoring and Incident Response:**
 - Keep track of unusual network activity.
 - Set up alerts for unauthorized access attempts.