🔍 **Nessus Essentials Vulnerability Scan Report**

🛠 **Tools Used:**

- **Scanner**: Nessus Essentials
- **Environment**: Kali Linux
- **Target**: Localhost (127.0.0.1)
- **Scan Policy**: Web Application Tests

✅ **Steps Performed:**

1. **Installed Nessus Essentials**
   - Downloaded and installed Nessus Essentials from Tenable's official site.
   - Registered with an activation code to unlock scanning capabilities.

2. **Configured Scan Target**
   - Target: localhost (127.0.0.1)
   - Policy: *Web Application Tests*

3. **Started Full Vulnerability Scan**
   - Scan initiated at **2:57 PM** and completed by **3:33 PM**.
   - Total Scan Time: **36 minutes**

4. **Scan Results Summary**
   - **Total Vulnerabilities Detected**: 32
     - **High Severity**: 4 (≈ 7.84%)
     - **Medium Severity**: 13
     - **Low Severity and Info**: 15+
   - **Screenshot Reference**:

5. **Identified Vulnerabilities**
   - Example from scan results:

Severity	Vulnerability Name	Plugin Family	Plugin ID
HIGH	phpMyAdmin Installation Detected	CGI Abuses	40352
HIGH	phpMyAdmin prior to 4.x vulnerabilities	CGI Abuses	-

Severity Vulnerability Name	Plugin Family Plugin ID
INFO phpMyAdmin Detection	CGI Abuses -

- **Screenshot Reference**:

6. **Fix/Mitigation Research**

   o *phpMyAdmin vulnerabilities* may be resolved by:

      - Updating phpMyAdmin to the latest version

      - Restricting access via .htaccess or firewall rules

      - Disabling unused features and enforcing strong authentication

7. **Critical Vulnerabilities to Address**

   o Prioritize fixing **HIGH** severity issues related to phpMyAdmin.

   o Consider removing or securing unused web applications.

8. **Documentation & Reporting**

   o This document serves as a summary report.

   o Screenshots are attached as evidence of vulnerability findings.

🔖 Kali Linux 🔖 Kali Training 🔖 Kali Tools 🌶 Kali Docs 🔖 Kali Forums 🔖 NetHunter ▮ Offensive Security 🔴 Exploit-DB 🔴 GHDB 🔖 MSFU

nessus
Essentials   **Scans**   Settings   🔔

FOLDERS

📁 My Scans
📁 All Scans
🗑 Trash

RESOURCES

🛡 Policies
🔘 Plugin Rules

TENABLE

📖 Community
🔍 Research

Tenable News

Rockwell Automation FactoryTalk Multiple

Mutillidae Test
‹ Back to My Scans

Configure   Audit Trail   Launch ▾   Report ▾   Exp

| Hosts 1 | Vulnerabilities 32 | History 3 |

Filter ▾   Search Hosts 🔍   1 Host

☐	Host	Vulnerabilities ▾
☐	localhost	[High: 4 (7.84%)] 13 33 ✕

Scan Details

Policy:	Web Application Tests
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 2:57 PM
End:	Today at 3:33 PM
Elapsed:	36 minutes

Vulnerabilities

---

nessus
Essentials   **Scans**   Settings   🔔

FOLDERS

📁 My Scans
📁 All Scans
🗑 Trash

RESOURCES

🛡 Policies
🔘 Plugin Rules

TENABLE

📖 Community
🔍 Research

Tenable News

Rockwell Automation FactoryTalk Multiple

Mutillidae Test / Phpmyadmin (Multiple Issues)
‹ Back to Vulnerabilities

Configure   Audit Trail   Launch ▾   Report ▾   Exp

| Hosts 1 | Vulnerabilities 32 | History 3 |

Search Vulnerabilities 🔍   3 Vulnerabilities

☐	Sev ▾	Name ▲	Fan [Plugin ID: 40352]	Count ▾	⚙
☐	HIGH	phpMyAdmin Installatio…	CGI abuses	1	⊘ ✎
☐	HIGH	phpMyAdmin prior to 4….	CGI abuses	1	⊘ ✎
☐	INFO	phpMyAdmin Detection	CGI abuses	1	⊘ ✎

Scan Details

Policy:	Web Application Tests
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 2:57 PM
End:	Today at 3:33 PM
Elapsed:	36 minutes

Vulnerabilities