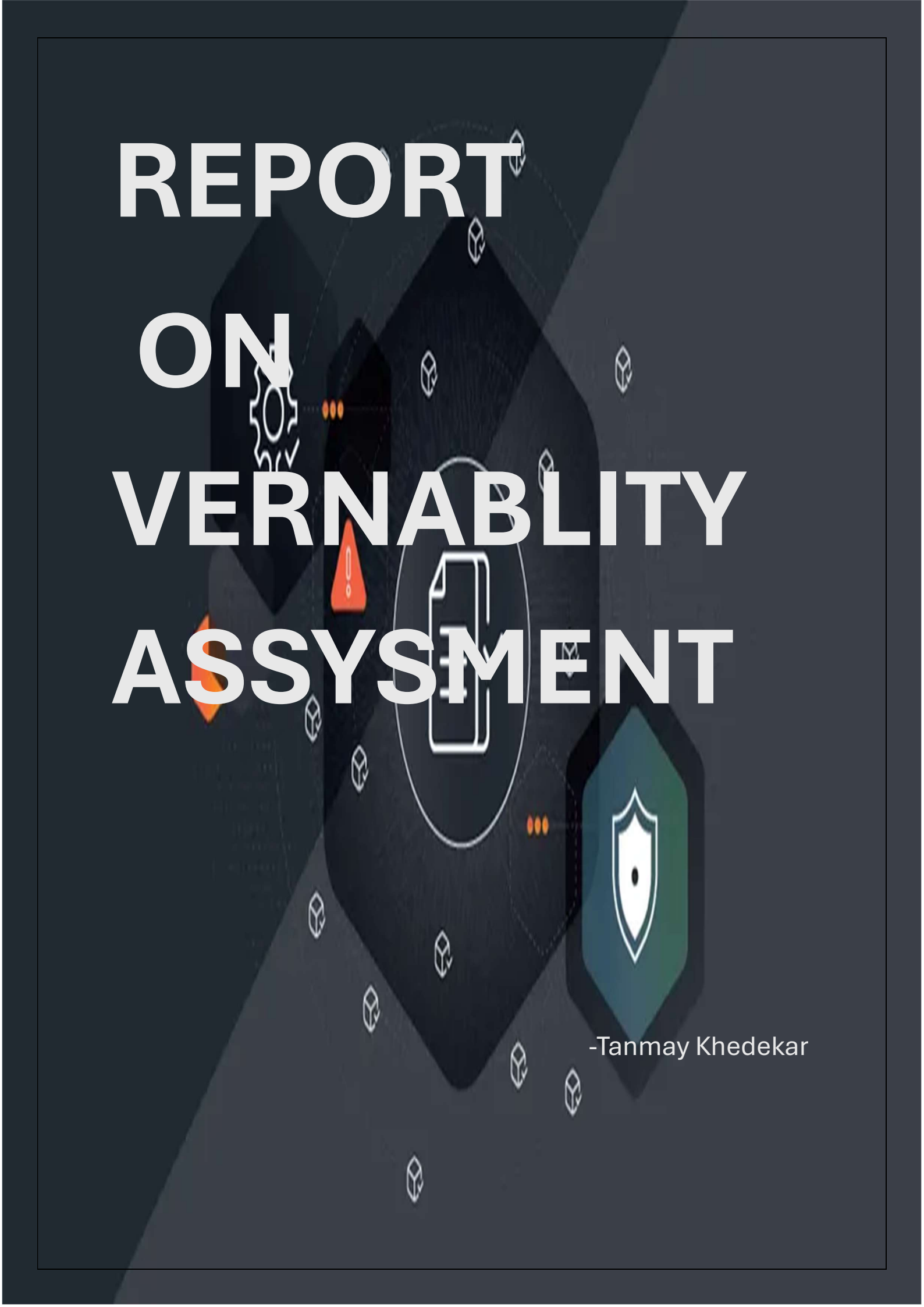
REPORT ON VERNABLITY ASSYSMENT



-Tanmay Khedekar

Table of Content-

Sr.no	Index	Page no.
1	Introduction	3
2	Objective	4
3	Perform Vulnerability Analysis Using NESSUS	5
4	Perform Vulnerability Assessment Using Smart Scanner	11
5	Perform Vulnerability Assessment Using Acunetix	15
6	Perform Vulnerability Assessment Using ZAP	20
7	Perform Vulnerability Assessment Using Microsoft Baseline Security Analyzer	30

Introduction

A Vulnerability Assessment is a systematic process used to identify, analyse, and prioritize weaknesses within a system, network, or application. Its main purpose is to find potential security gaps before attackers can exploit them. By performing a structured assessment, organizations can understand their current security posture and take effective steps to reduce risks.

During a vulnerability assessment, various tools and techniques are used to scan systems for known vulnerabilities such as outdated software, weak configurations, open ports, misconfigurations, missing patches, and insecure services. The assessment provides clear insights into which vulnerabilities are critical and require immediate action.

Vulnerability Assessment plays an essential role in strengthening cybersecurity defences. It helps improve awareness about potential threats, ensures compliance with security standards, and supports proactive risk management. The results of this assessment allow organizations to plan remediation activities and enhance the overall security of their digital environment.

Objective

The main objective of a Vulnerability Assessment is to identify and evaluate security weaknesses within an organization's systems, networks, applications, and devices. By conducting this assessment, organizations aim to discover vulnerabilities before they can be exploited by attackers. This proactive approach helps improve the overall security posture and reduces the possibility of data breaches, service interruptions, or unauthorized access.

Another key objective is to prioritize vulnerabilities based on their level of risk. Not all weaknesses carry the same impact, so the assessment helps classify them as low, medium, high, or critical. This prioritization enables organizations to focus their efforts and resources on addressing the most dangerous issues first, ensuring efficient and effective security management.

A vulnerability assessment also helps improve system visibility. Many organizations may not be aware of hidden risks, outdated software, weak configurations, or insecure services running in their environment. The assessment highlights these gaps, allowing IT teams to take corrective actions such as patching, reconfiguring systems, or implementing stronger security controls.

1. Perform Vulnerability Analysis Using NESSUS

Steps to setup Nessus and perform vulnerability assessment using nessus

1. **Install and Launch Nessus**

- Download Nessus from Tenable's official site.
- Install it on your system and start the Nessus service.
- Access the Nessus web interface (usually via `https://localhost:8834`).

2. **Create a New Scan**

- Navigate to **Scans** in the top menu.
- Click **New Scan** to start configuring a new vulnerability assessment.

3. **Choose a Scan Template**

- Select a template based on your needs (e.g., **Basic Network Scan**, **Advanced Scan**, or **Web Application Tests**).
- Templates define configurable settings and scanning behavior.

4. **Configure Scan Settings**

- Enter a **name** and **description** for the scan.
- Specify **target IP addresses, hostnames, or ranges**.
- Adjust advanced options like port scanning, credentials (for authenticated scans), and plugins.

5. **Launch the Scan**

- Save the configuration and click **Launch**.
- Nessus will begin scanning the defined targets, checking for vulnerabilities, misconfigurations, and outdated software.

6. **Monitor Scan Progress**

- View real-time progress in the **Scans dashboard**.
- Nessus categorizes findings by severity (Critical, High, Medium, Low, Informational).

7. **Analyze Results**

- Review the **scan report** once completed.
- Focus on **critical and high-severity vulnerabilities** first.
- Nessus provides detailed descriptions, CVE references, and remediation guidance.

8. **Remediate and Re-scan**

- Apply recommended patches, configuration changes, or updates.
- Run a **follow-up scan** to verify that vulnerabilities have been resolved.

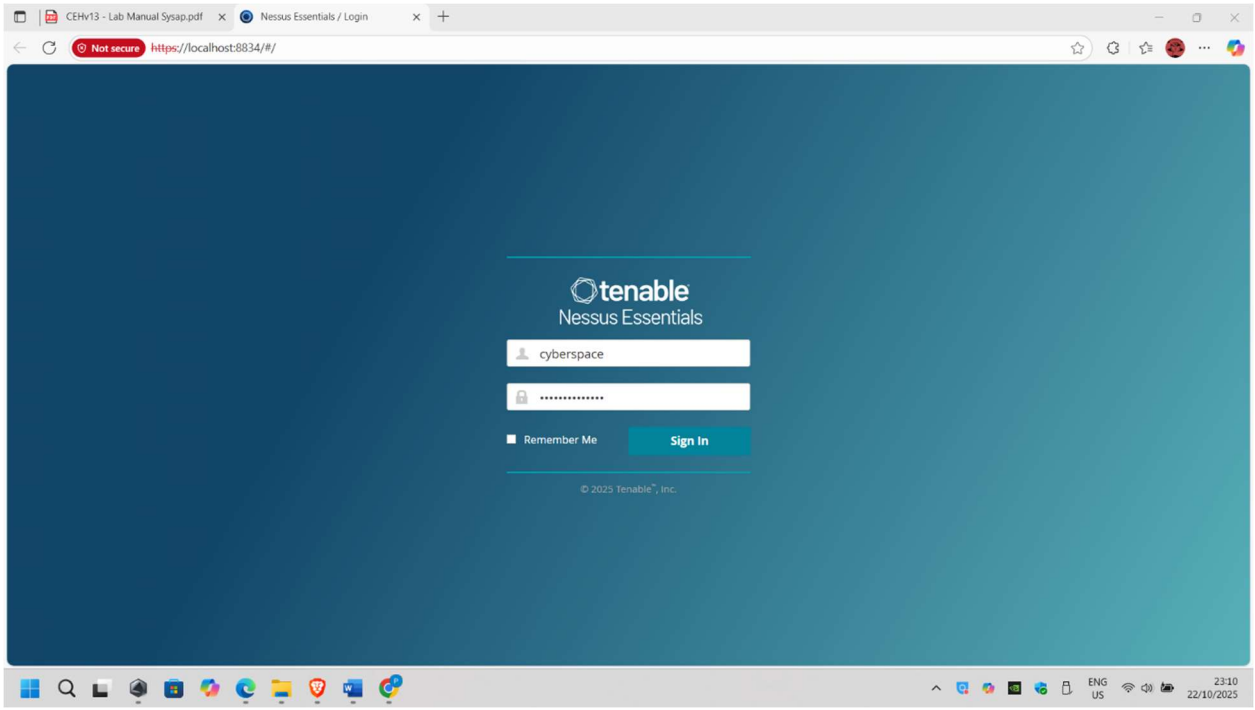


FIGURE 1 : NESSUS LOGIN PAGE

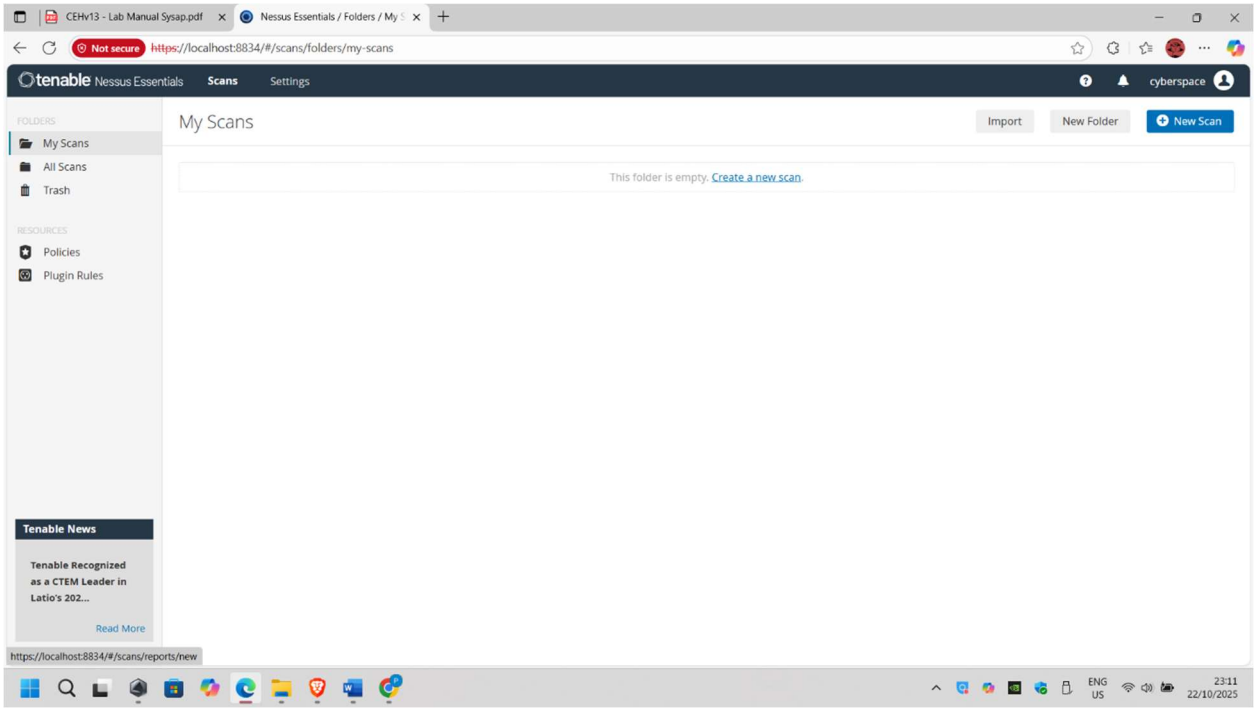


FIGURE 2 : NESSUS DASHBOARD

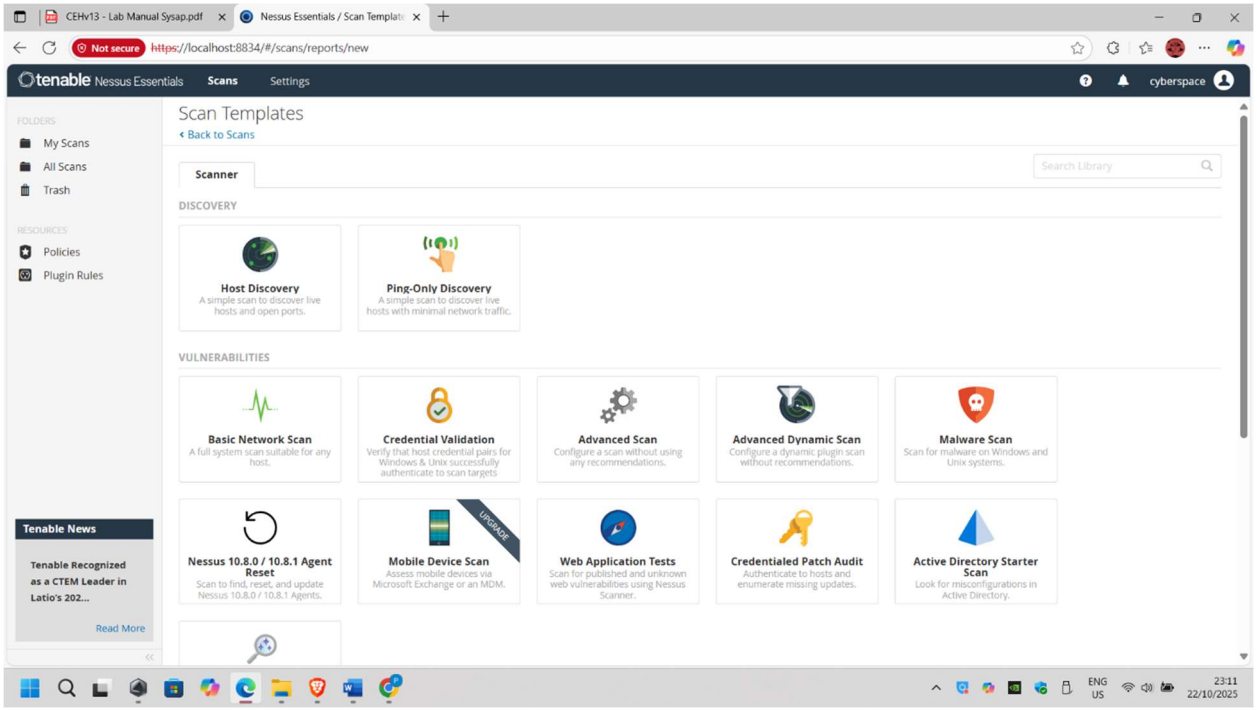


FIGURE 3 : LIST OF SCANS PROVIDED BY NESSUS

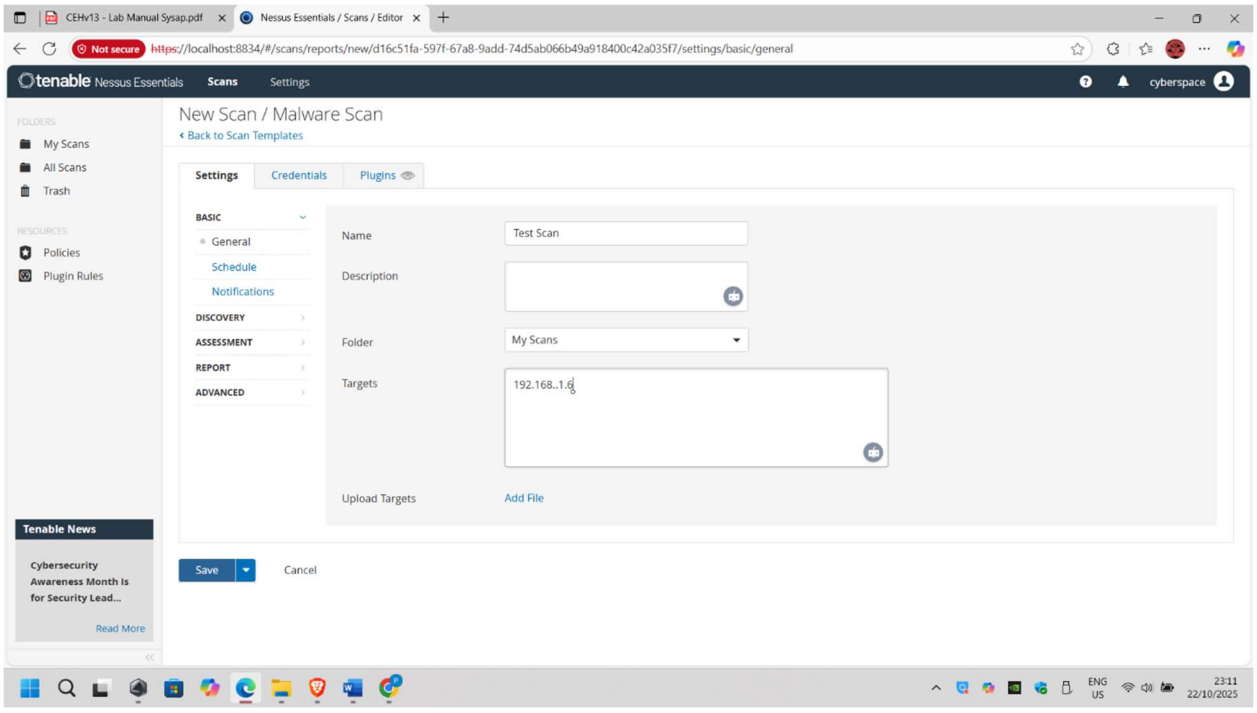


FIGURE 1 : SUBMITTING TARGET DETAILS FOR SCAN

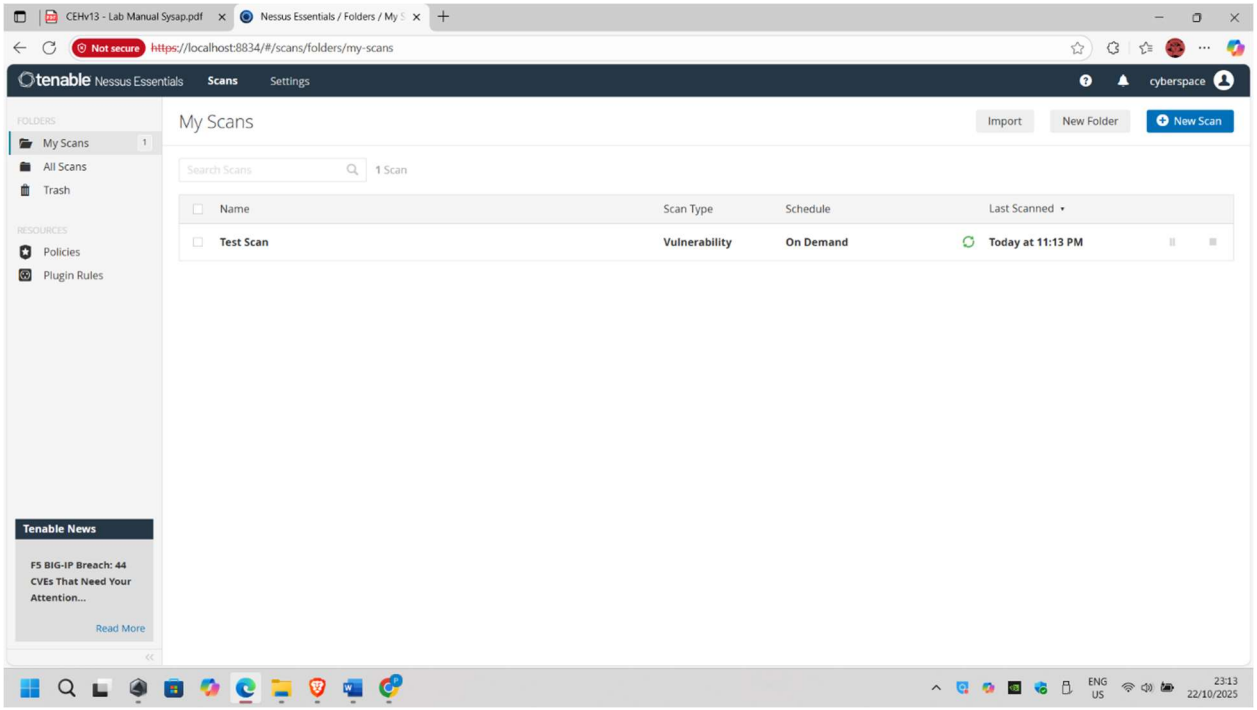


FIGURE 52 : SCAN INITIATED

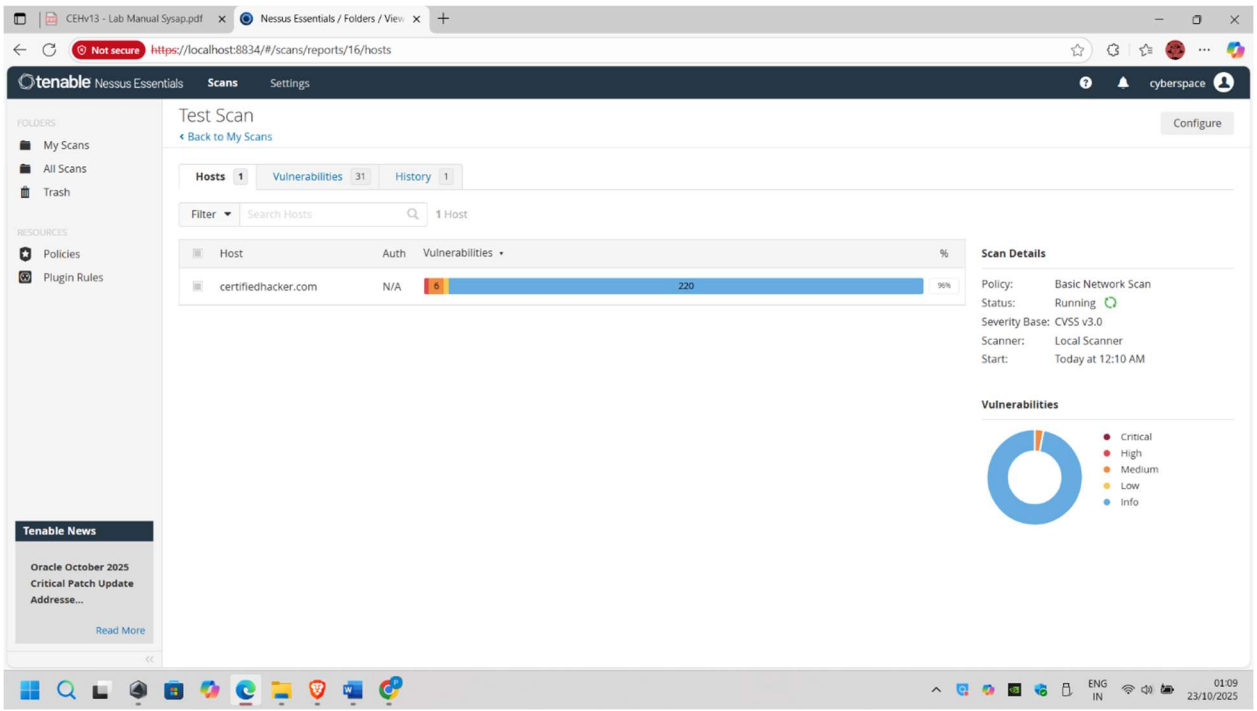


FIGURE 63 : RESULT OF SCAN

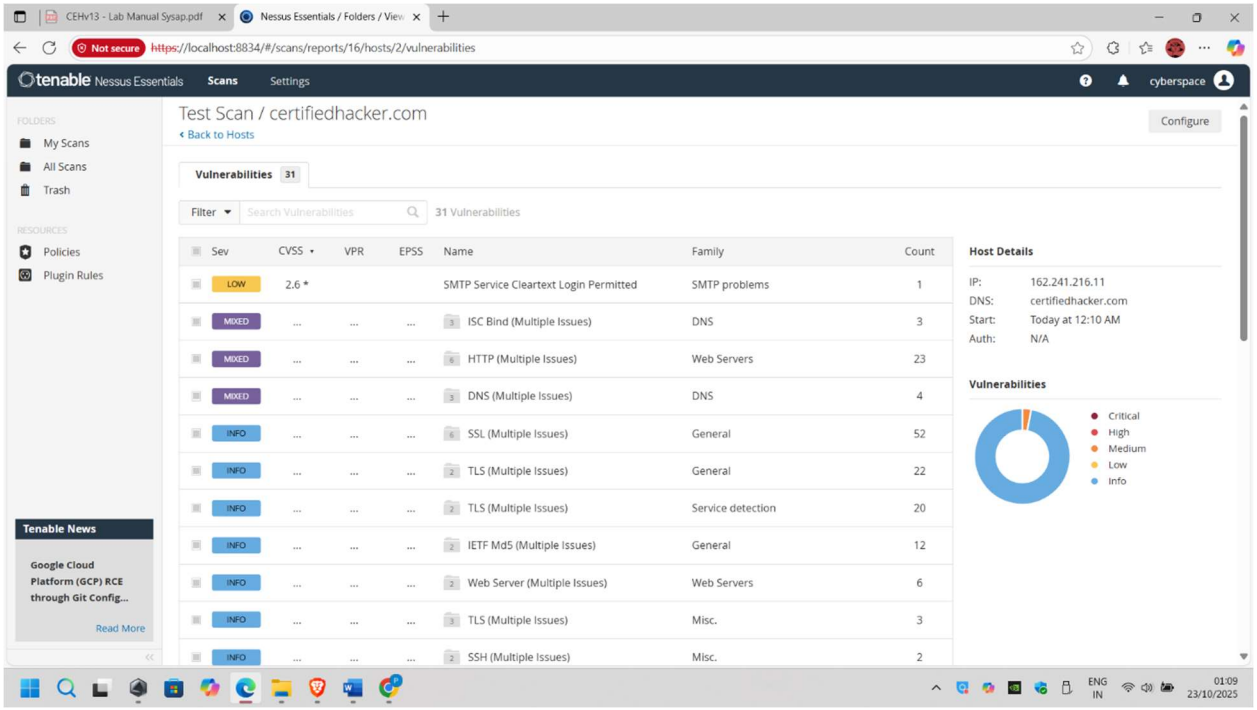


FIGURE 7 : LIST OF VULNERABILITIES ON TARGET

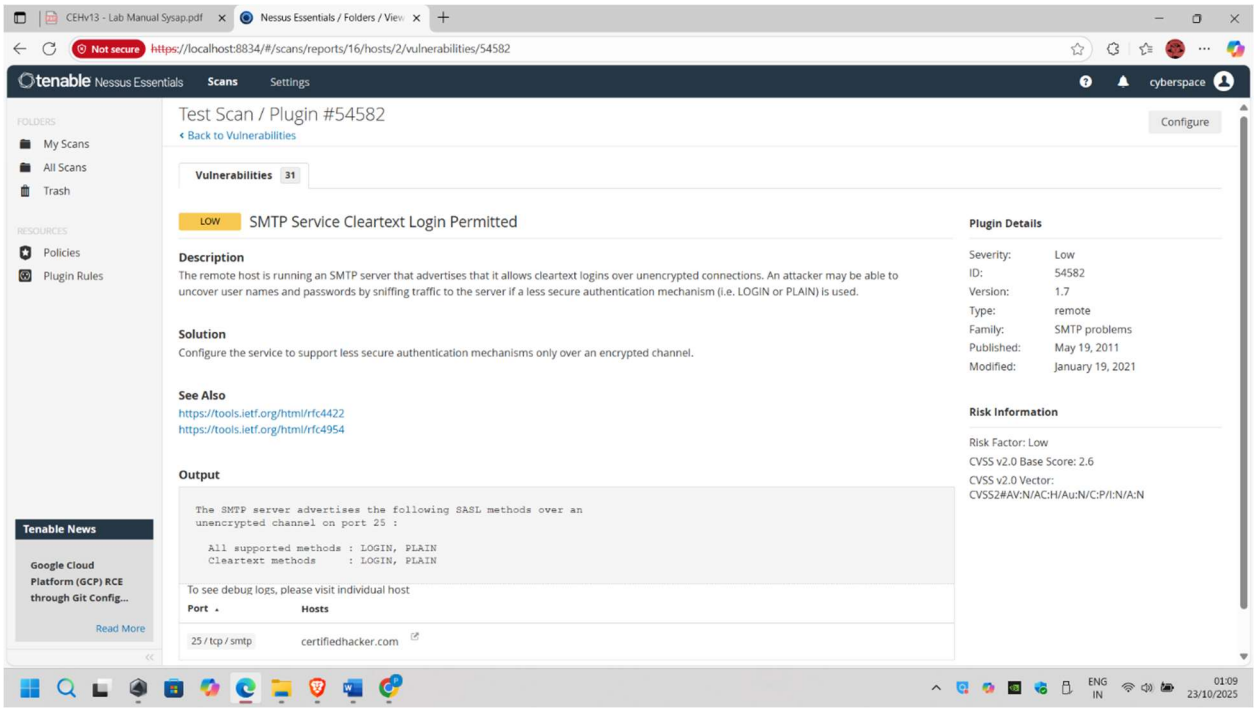


FIGURE 8 : VULNERABILITY INFORMATION IN DETAIL

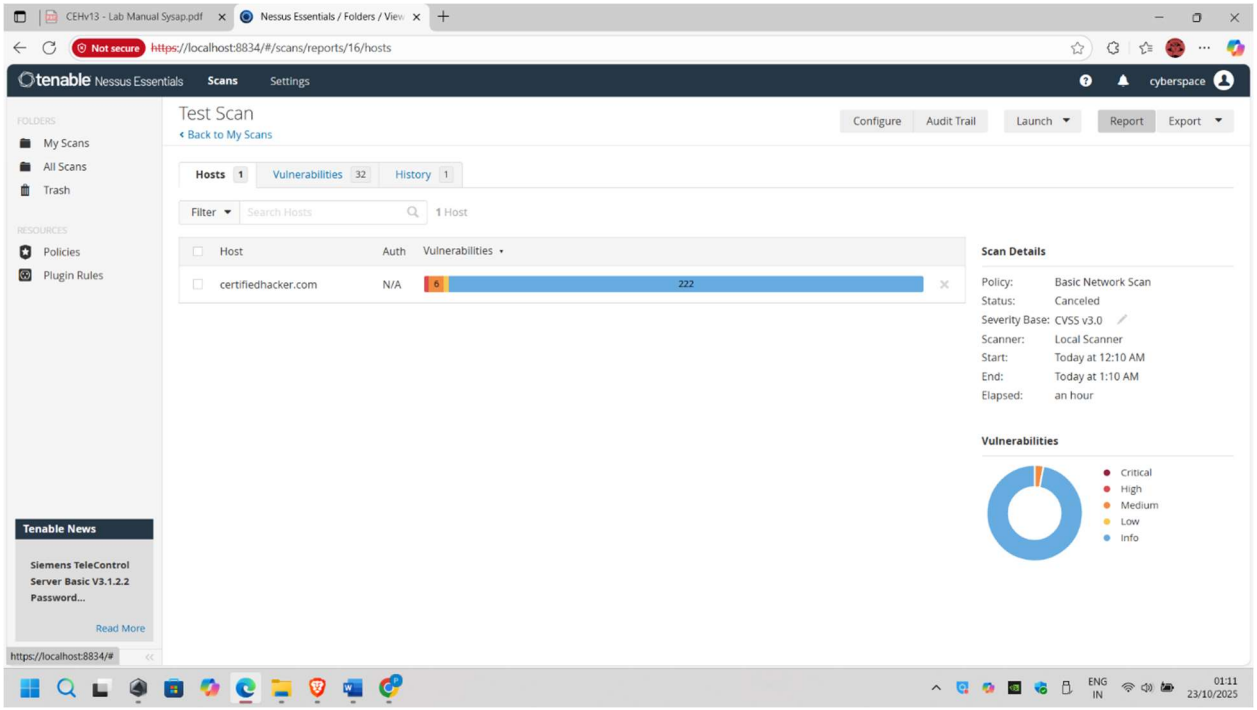


FIGURE 9: EXPORTING REPORT

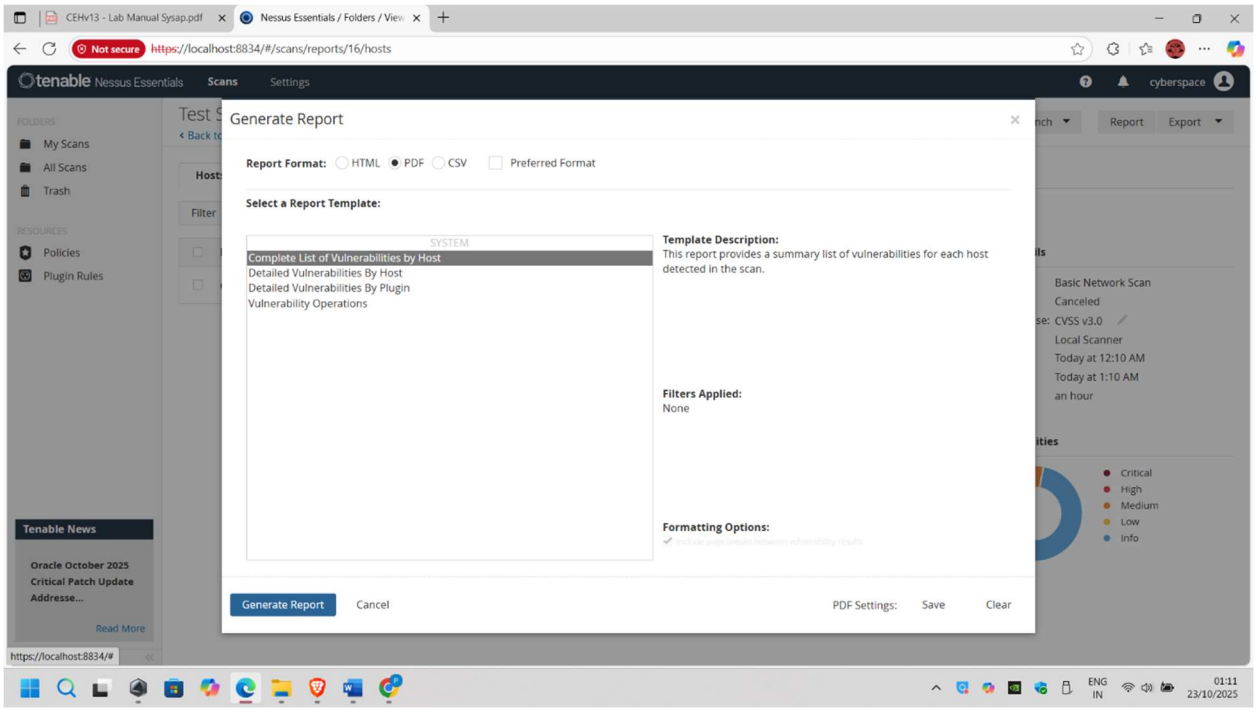


FIGURE 10: DOWNLOADING SCAN REPORT IN PDF

2.Perform Vulnerability Assessment Using Smart Scanner

Steps to perform Vulnerability Assessment Using Smart Scanner

1. **Download and Install SmartScanner**

- Get the app from SmartScanner's official site.
- Install it on your system or mobile device.
- Activate your license or free version as required.

2. **Set Up Your Account**

- Log in with your credentials.
- Configure licensing and authentication settings if needed.

3. **Define the Target**

- Enter the **IP address, domain, or URL** of the system/web application you want to scan.
- SmartScanner automatically detects the underlying technologies (OS, CMS, frameworks).

4. **Configure Scan Options**

- Choose between **quick scan** or **full scan**.
- Enable authentication if you want deeper visibility (e.g., scanning behind login).
- Adjust configurations such as ports, protocols, or specific vulnerability checks.

5. **Run the Scan**

- Click **Start Scan**.
- The app will automatically test for:

  ✓ Web application vulnerabilities (SQL injection, XSS, CSRF).
  ✓ Server misconfigurations.
  ✓ Outdated software components.
  ✓ Weak encryption or insecure protocols.

6. **Monitor Progress**

- Use the **scan dashboard** to track progress in real time.
- SmartScanner uses AI-powered detection to speed up scanning and reduce false positives.

7. **Review the Report**

- Once complete, the app generates a **detailed vulnerability report**.
- Vulnerabilities are categorized by severity: **Critical, High, Medium, Low**.
- Each entry includes CVE references, descriptions, and recommended remediation steps.

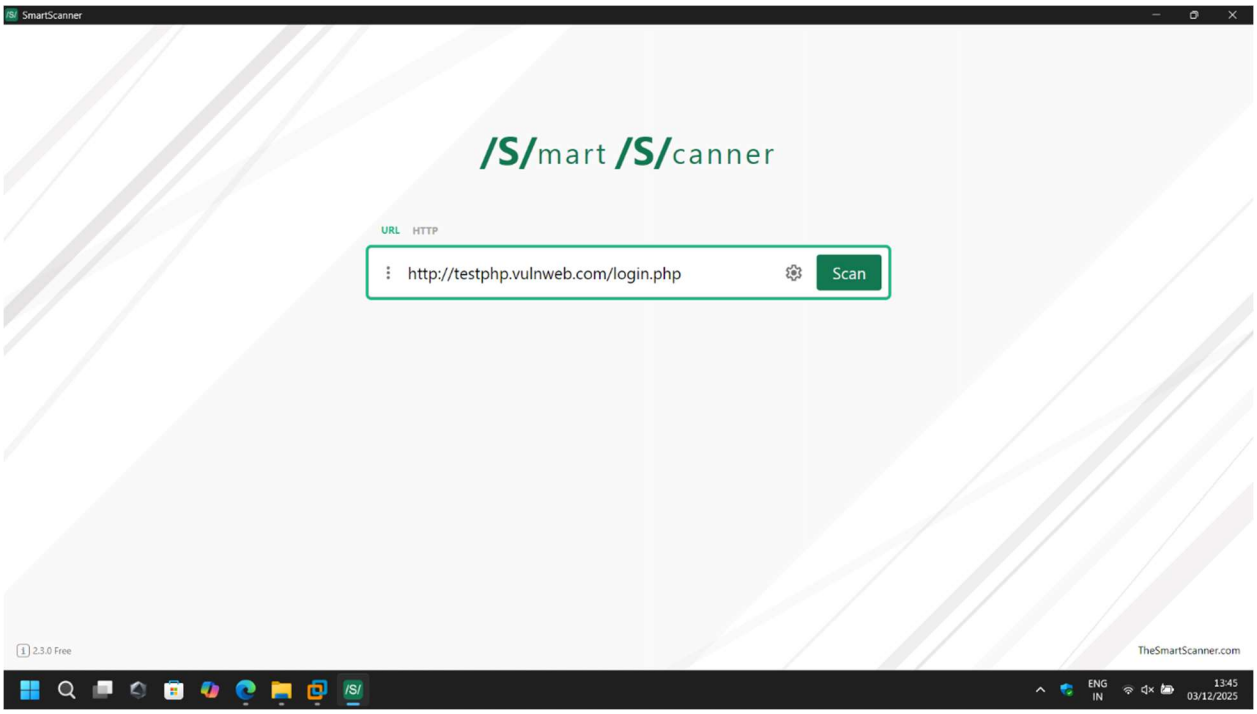


FIGURE 11: INSERT THE TARGET LINK TO SMART SCANNER FOR V.A.

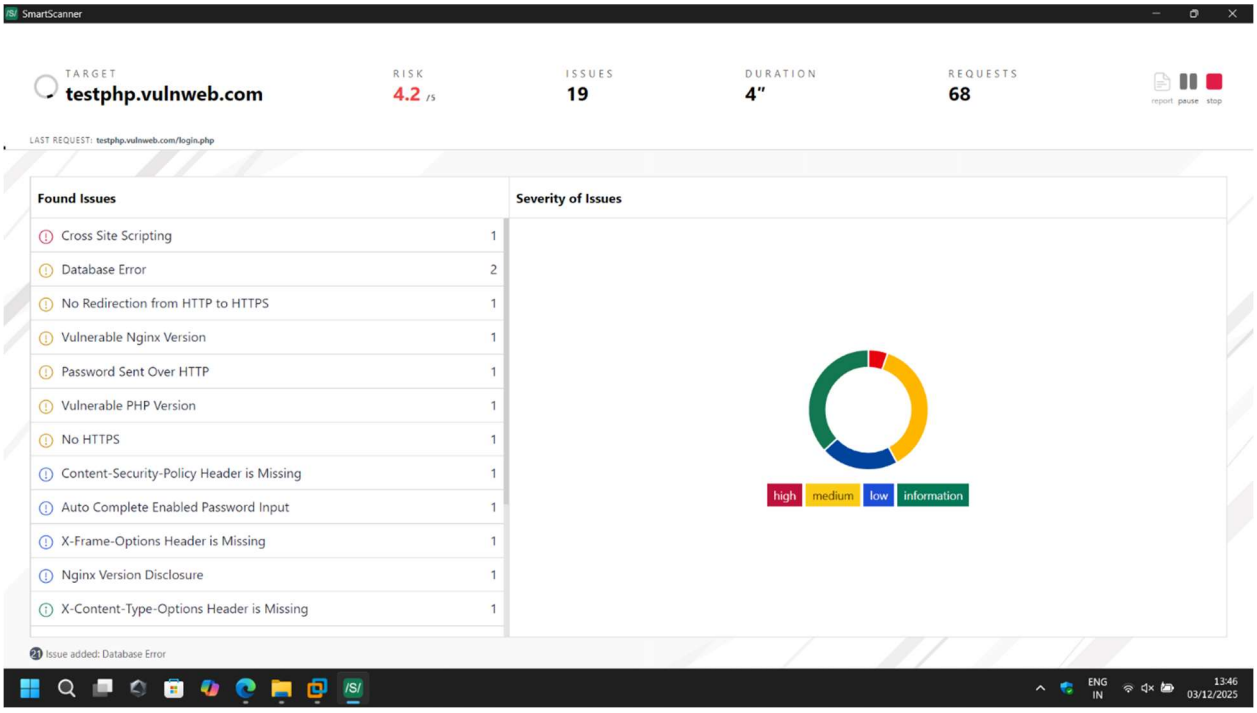


FIGURE 12 : RESULT OF THE VULNERABILITY ASSESSMENT

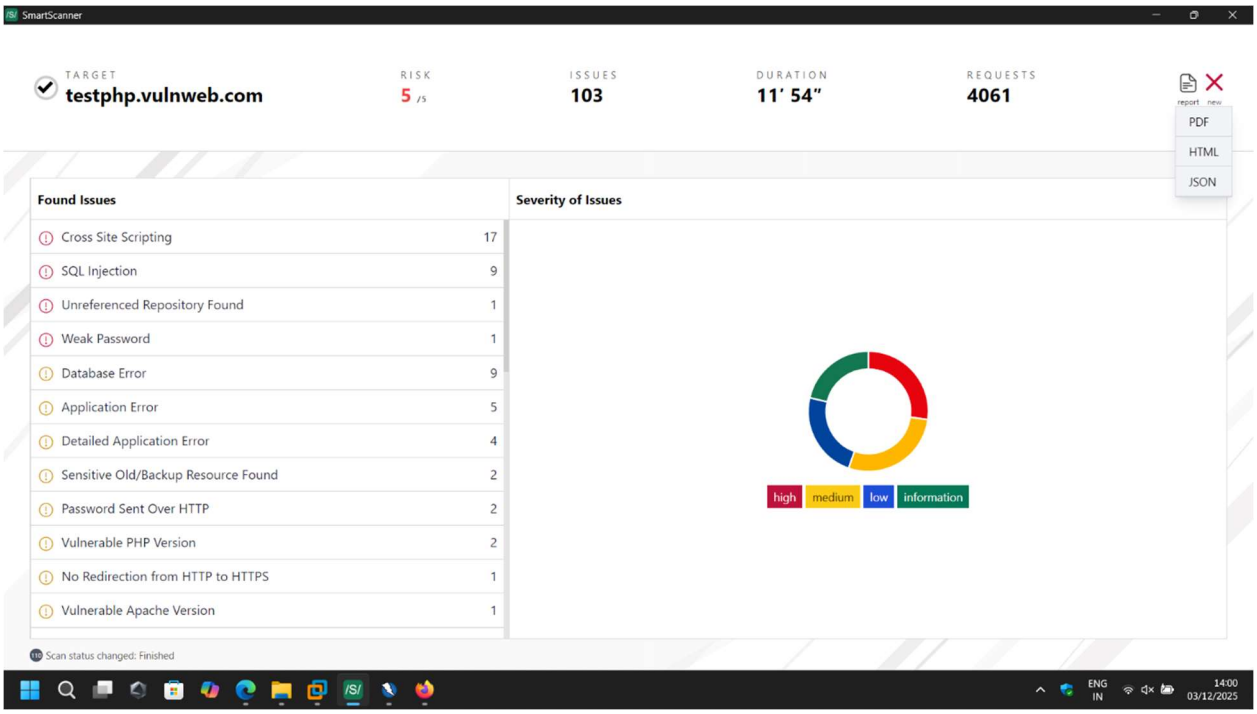


FIGURE 4 : STUDYING THE RESULT OF THE ASSESSMENT

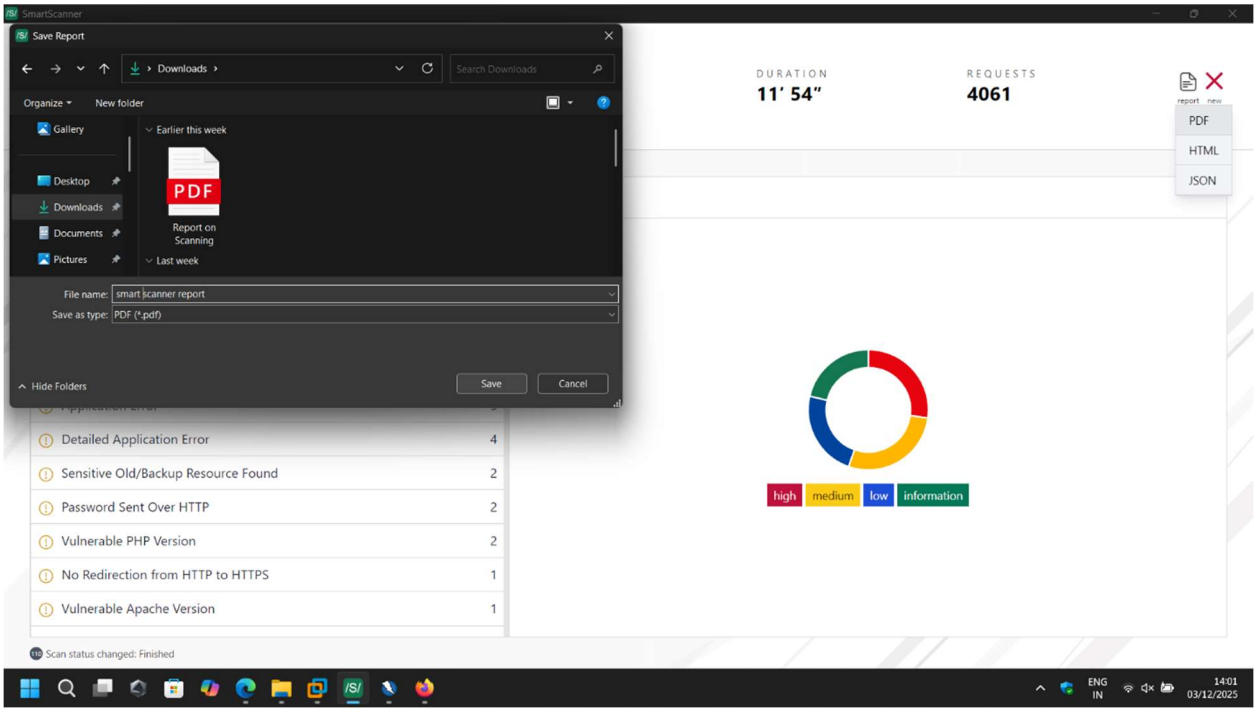


FIGURE 14 : DOWNLOADING THE ASSESSMENT REPORT IN PDF

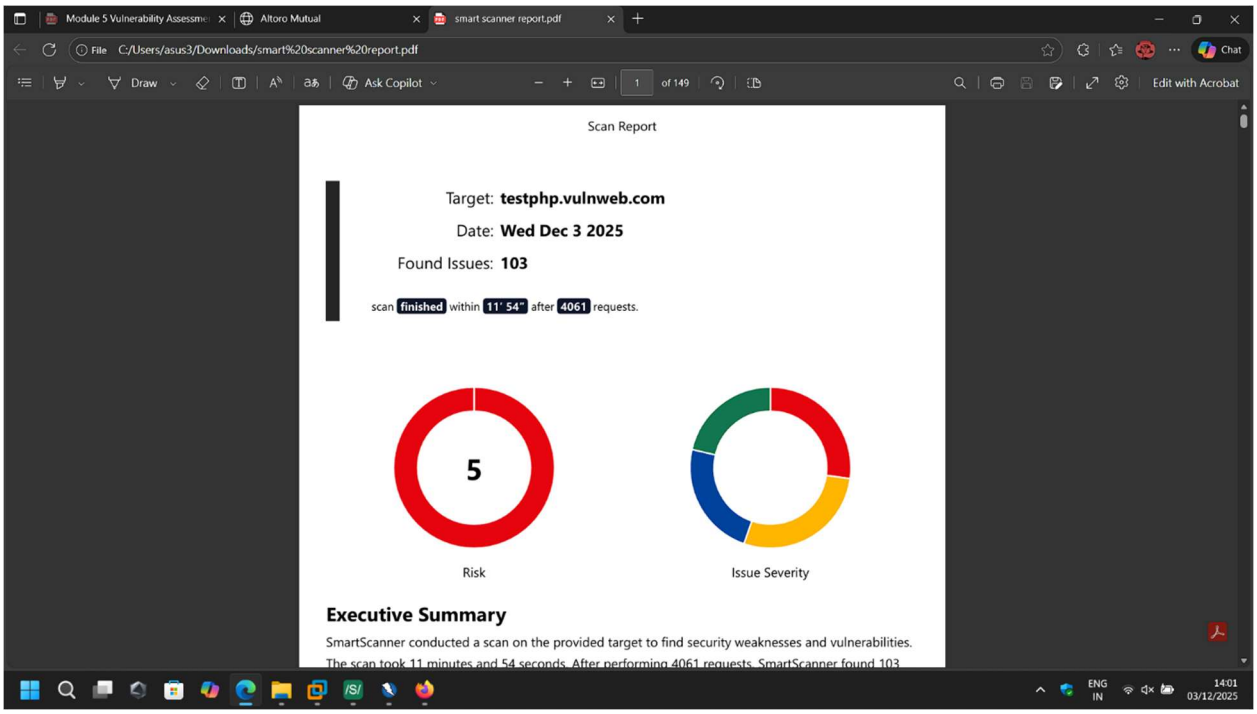


FIGURE 15 : DOWNLOADED REPORT OF ASSESSMENT USING SMART SCANNER

3. Perform Vulnerability Assessment Using Acunetix

Steps to Setup and Perform Vulnerability Assessment Using Acunetix

1. **Install and Set Up Acunetix**

- Download Acunetix from the official website.
- Install it on your system and activate your license.
- Log in to the Acunetix dashboard with your credentials.

2. **Add a Target**

- In the dashboard, go to **Targets**.
- Click **Add Target** and enter the **URL or IP address** of the web application you want to scan.
- Configure target details such as description, business criticality, and authentication if needed.

3. **Configure Scan Settings**

- Choose the **scan type** (Quick Scan, Full Scan, or Custom Scan).
- Define options like login credentials (for authenticated scans), excluded paths, and scanning depth.
- Acunetix automatically detects the technologies used (e.g., PHP, ASP.NET, CMS platforms).

4. **Start the Scan**

- Click **Scan Target** to begin.
- Acunetix performs three main tasks:

- **Target Identification** – Confirms the site is active and identifies server type.
- **Site Crawling** – Maps the site structure, parsing links, forms, scripts, and images.
- **Vulnerability Testing** – Executes automated tests for SQL injection, XSS, CSRF, misconfigurations, and more.

5. **Monitor Progress**

- Track the scan in real time via the dashboard.
- Acunetix categorizes findings by severity: **Critical, High, Medium, Low, Informational**.

6. **Review the Report**

- Once complete, Acunetix generates a **detailed vulnerability report**.
- Each finding includes:

- Description of the vulnerability.
- CVE references.
- Proof of exploit (where applicable).

- Recommended remediation steps.

7. **Remediate Issues**

- Apply patches, update software, or fix misconfigurations based on the report.
- Prioritize **critical and high-severity vulnerabilities** first.

8. **Re-scan for Validation**

- Run another scan after remediation to confirm vulnerabilities have been resolved.
- Schedule regular scans to maintain ongoing security posture.

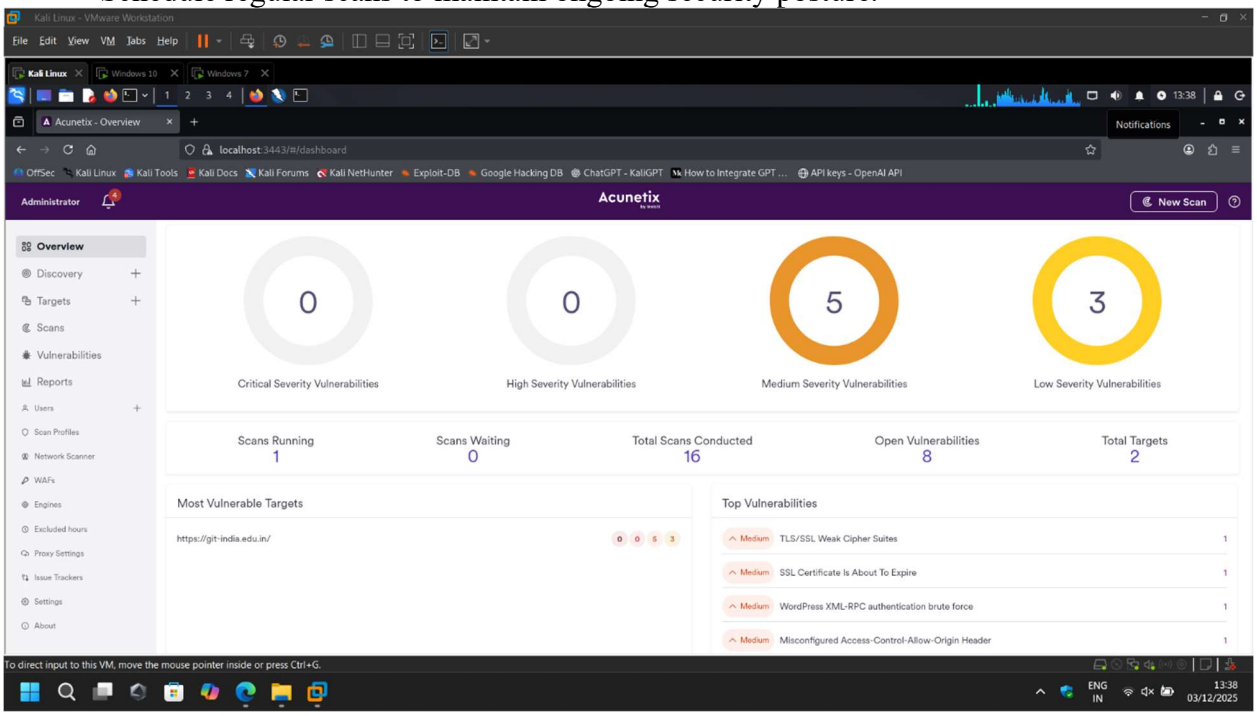


FIGURE 16: ACUNETIX DASHBOARD

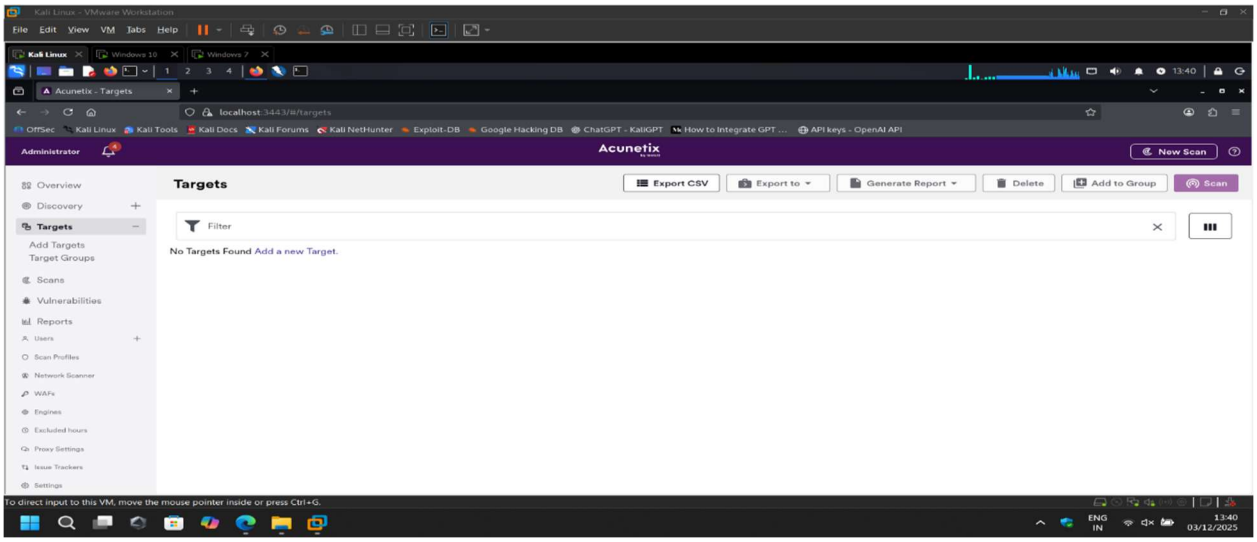


FIGURE 17 : ADDING TARGET FOR THE VULNERABILITY ASSESSMENT

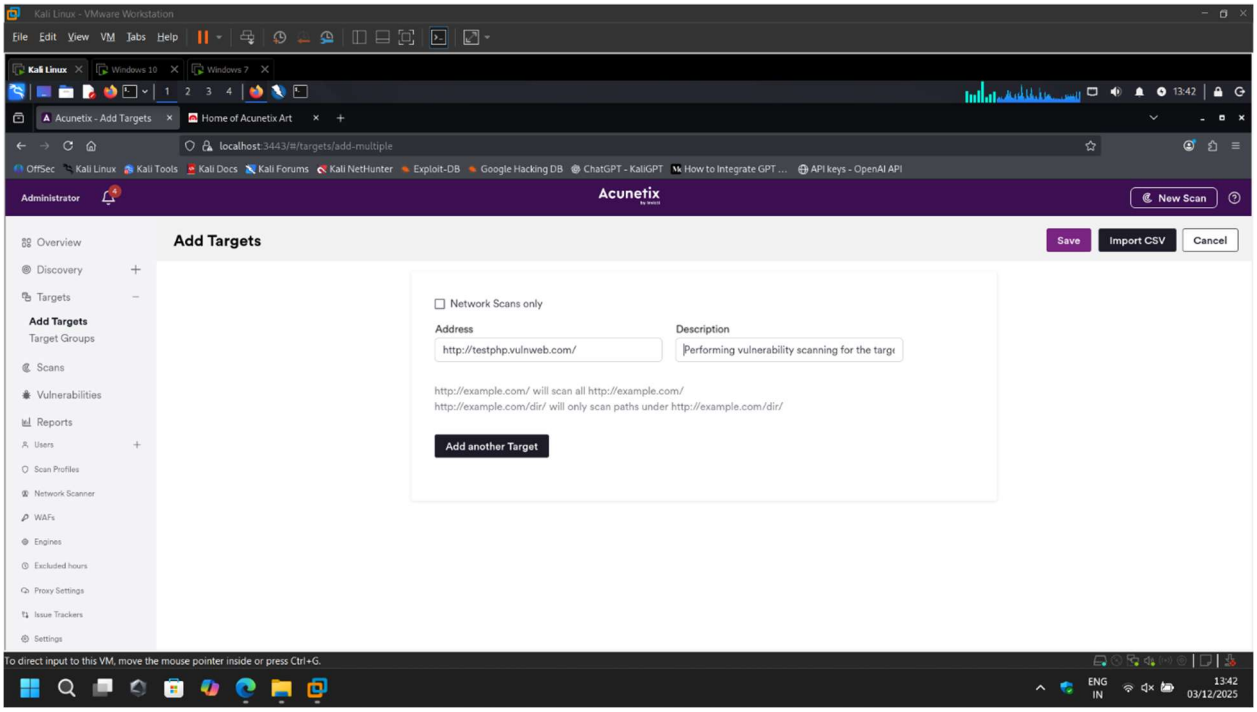


FIGURE 18: SUBMITTING TARGET DETAILS

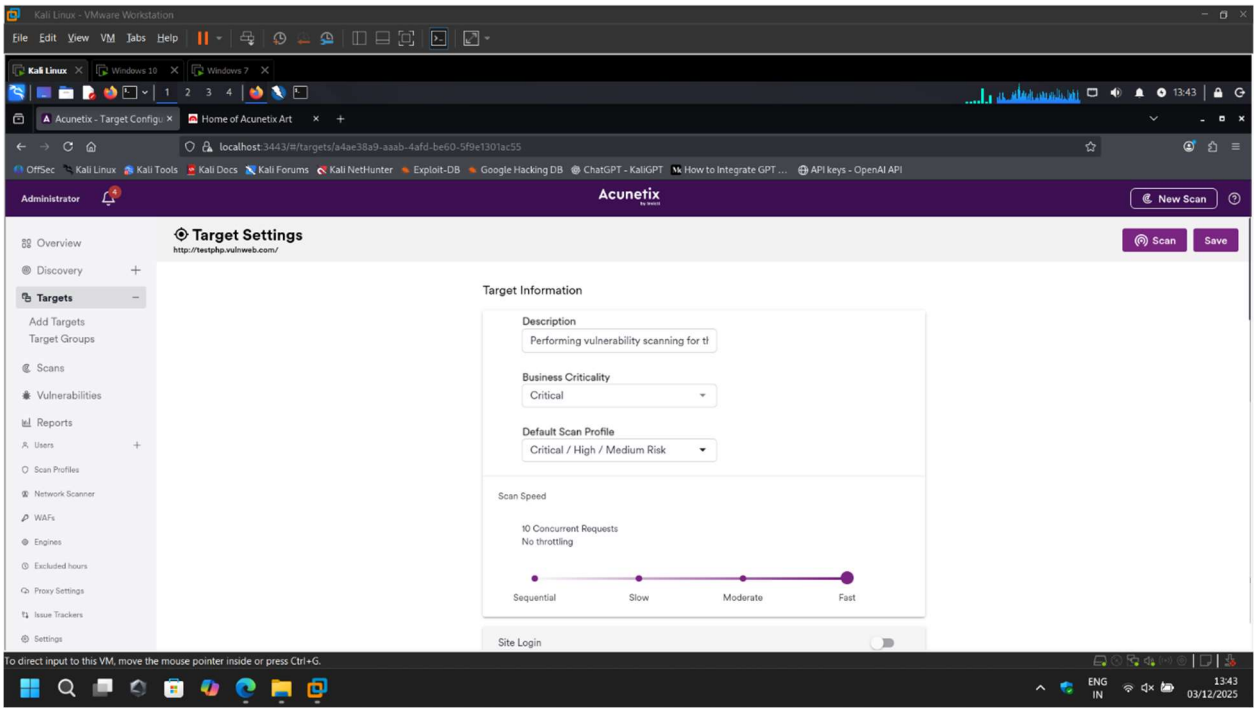


FIGURE 19 : SETTING SCAN SPECIFICATIONS 1

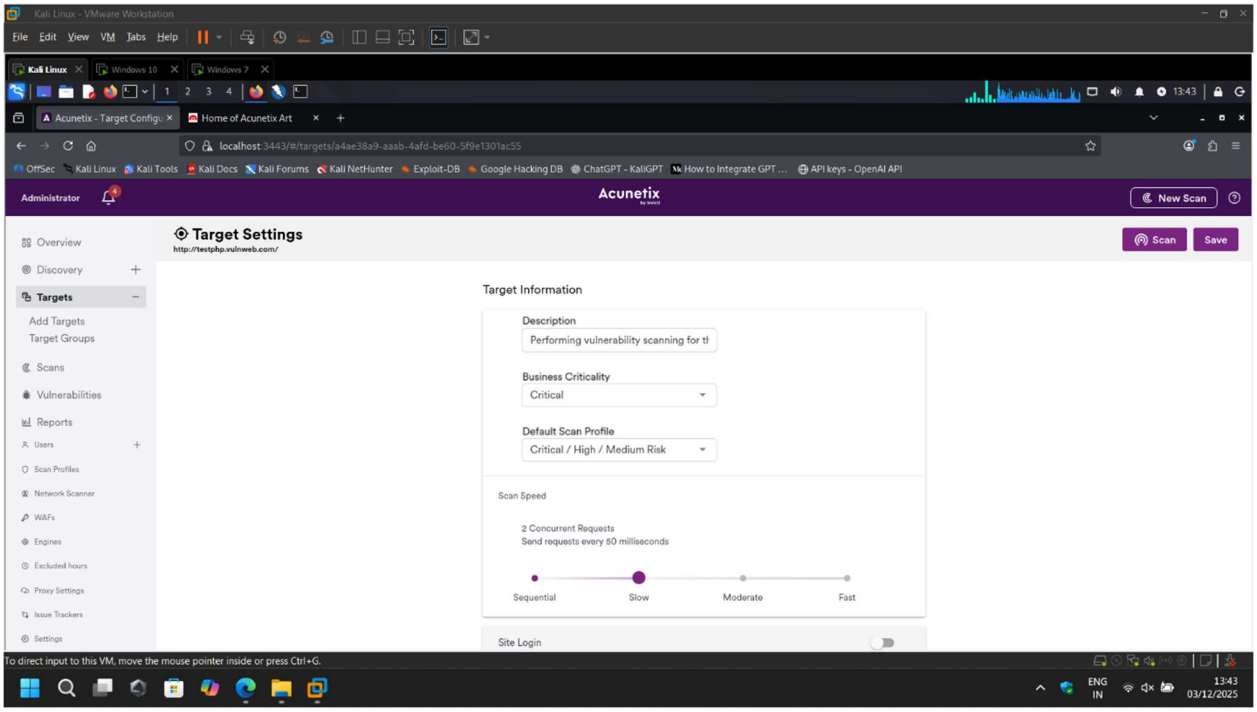


FIGURE 20 : SETTING SCAN SPECIFICATIONS 2

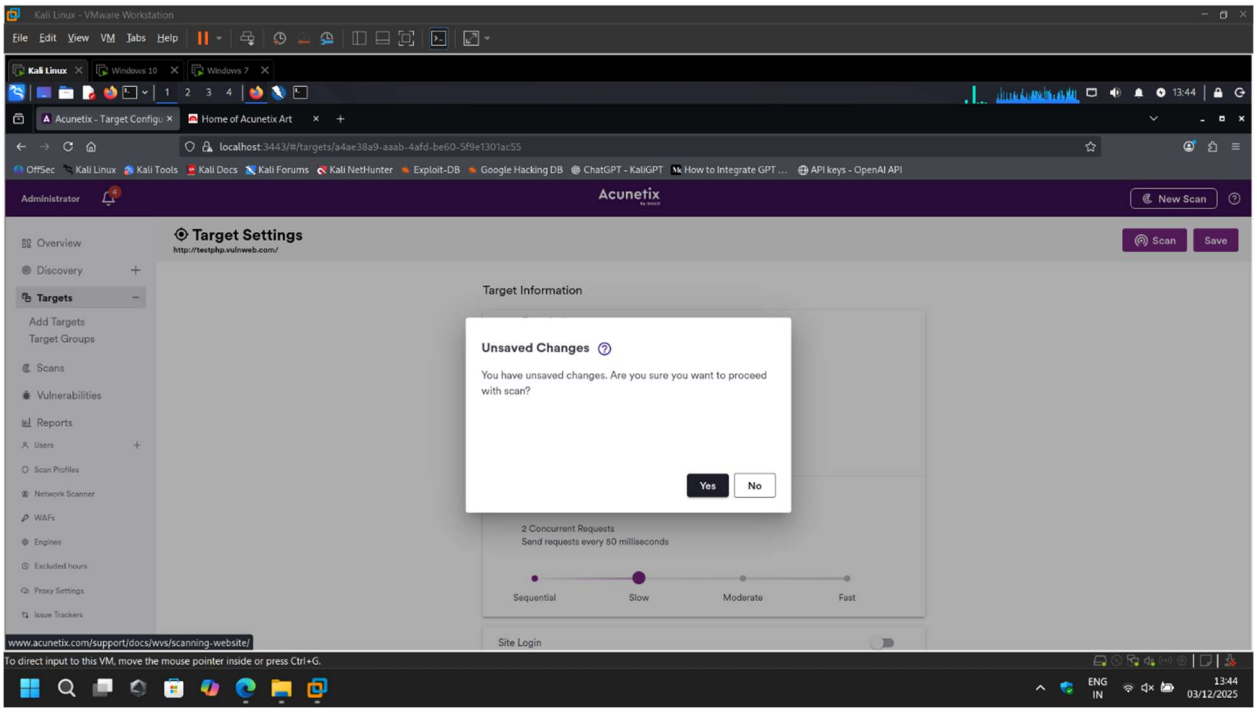


FIGURE 21 : SAVING THE TARGET AND SCAN DETAILS FOR VULNERABILITY ASSESSMENT

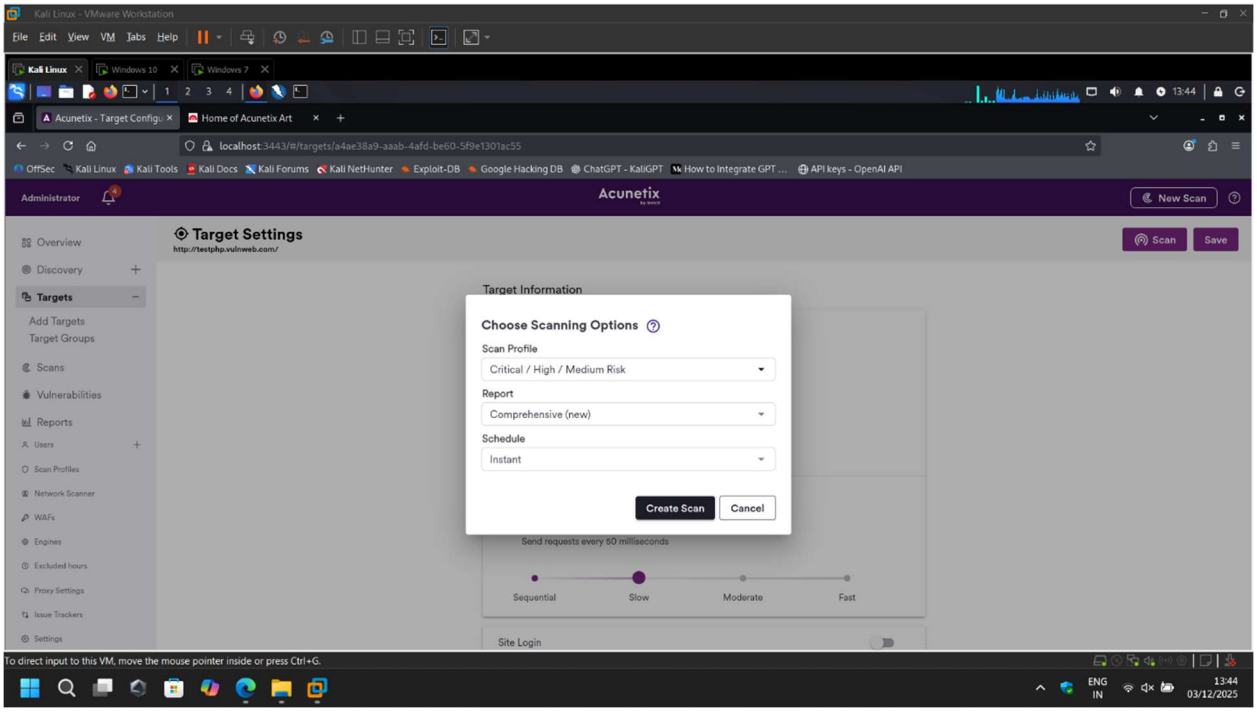


FIGURE 225 : CREATING SCAN

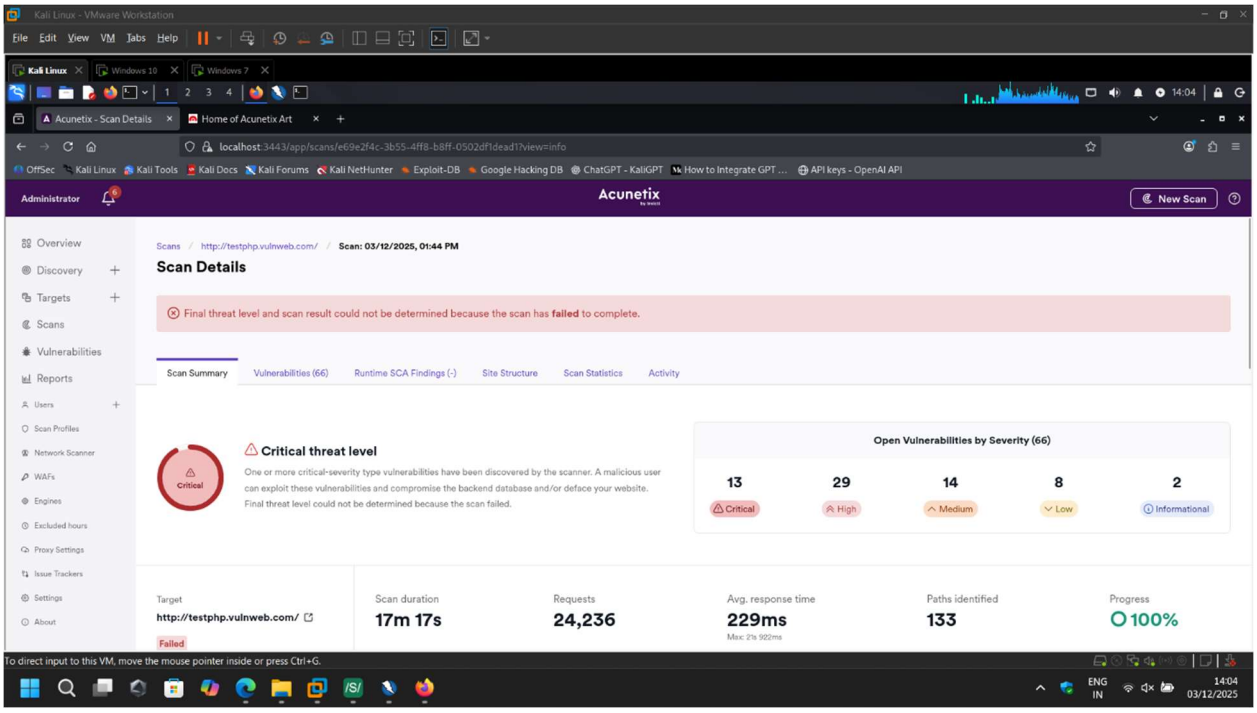


FIGURE 236: RESULT OF THE SCAN WHICH DISPLAYED THE DETAILS OF VULNERABILITIES OF TARGET

4. Perform Vulnerability Assessment Using ZAP

OWASP ZAP (Zed Attack Proxy) is a free, open-source vulnerability assessment tool widely used for web application security testing. It acts as a proxy to intercept traffic, supports both passive and active scanning, and helps identify issues like SQL injection, XSS, and misconfigurations, making it suitable for both beginners and professionals.

Steps to perform vulnerability assessment using ZAP

1. **Install and Launch ZAP**

- Download OWASP ZAP from the official site.
- Install it on your system and start the application.
- ZAP runs as a proxy, intercepting traffic between your browser and the target application.

2. **Configure Browser Proxy**

- Set your browser to use ZAP as its proxy (default: `localhost:8080`).
- This allows ZAP to capture and analyze all HTTP/HTTPS requests and responses.

3. **Add Target Application**

- Enter the target URL in ZAP's **Quick Start tab**.
- Alternatively, browse the application through your browser with ZAP running to let it capture traffic.

4. **Spider the Application (Crawling)**

- Use the **Spider tool** to crawl the application and discover pages, forms, and parameters.
- This builds a map of the application for deeper scanning.

5. **Passive Scanning**

- As traffic flows through ZAP, it automatically performs **passive scanning**.
- This identifies issues like missing security headers, cookie flags, or weak SSL configurations without altering requests.

6. **Active Scanning**

- Select the target and run an **Active Scan**.
- ZAP sends crafted requests to test for vulnerabilities such as:

  ✓ SQL Injection
  ✓ Cross-Site Scripting (XSS)

- ✓ CSRF
- ✓ Directory traversal
- ✓ Authentication flaws

7. **Review Alerts**

- ZAP categorizes findings by severity (High, Medium, Low, Informational).
- Each alert includes a description, evidence, and recommended remediation steps.

8. **Generate Reports**

- Export results in formats like HTML, XML, or JSON.
- Reports include detailed vulnerability descriptions, CVE references, and remediation guidance.

9. **Remediate and Re-scan**

- Apply patches, fix misconfigurations, or update components.
- Run another scan to confirm vulnerabilities have been resolved.

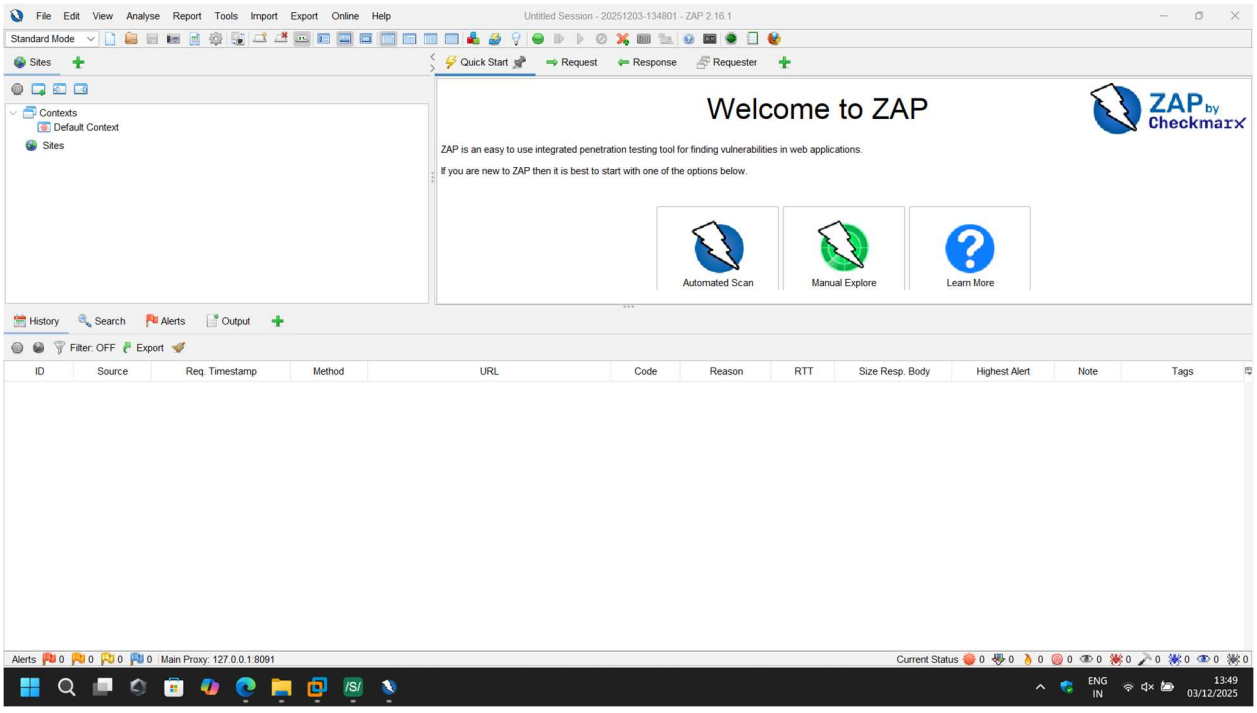


FIGURE 247 : DASHBOARD OF ZAP

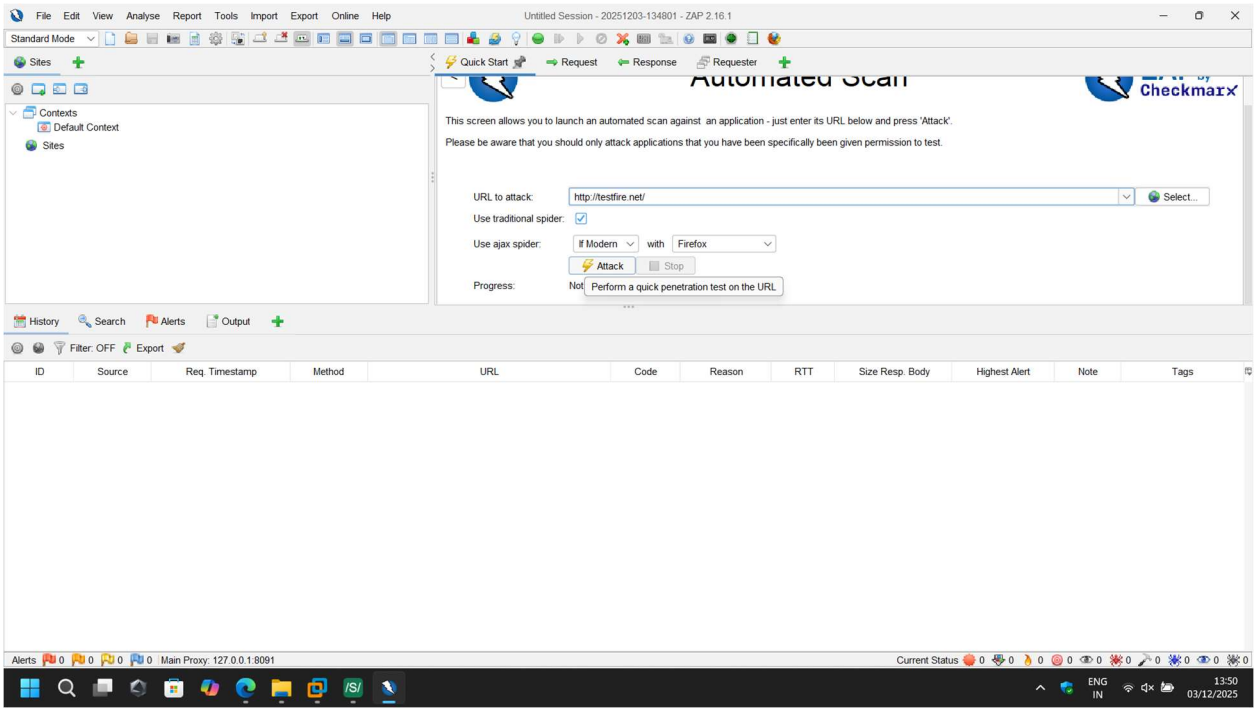


FIGURE 25 : SUBMITTING TARGET DETAILS

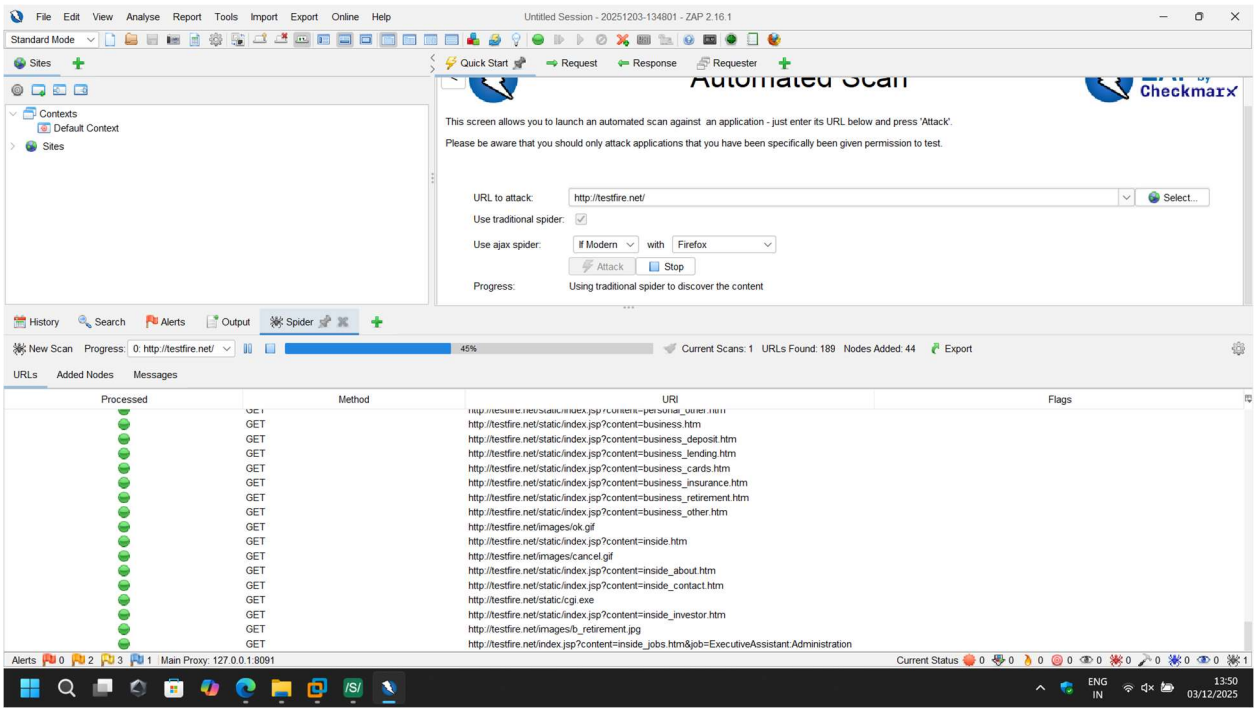


FIGURE 26 : SCAN IS STARTED

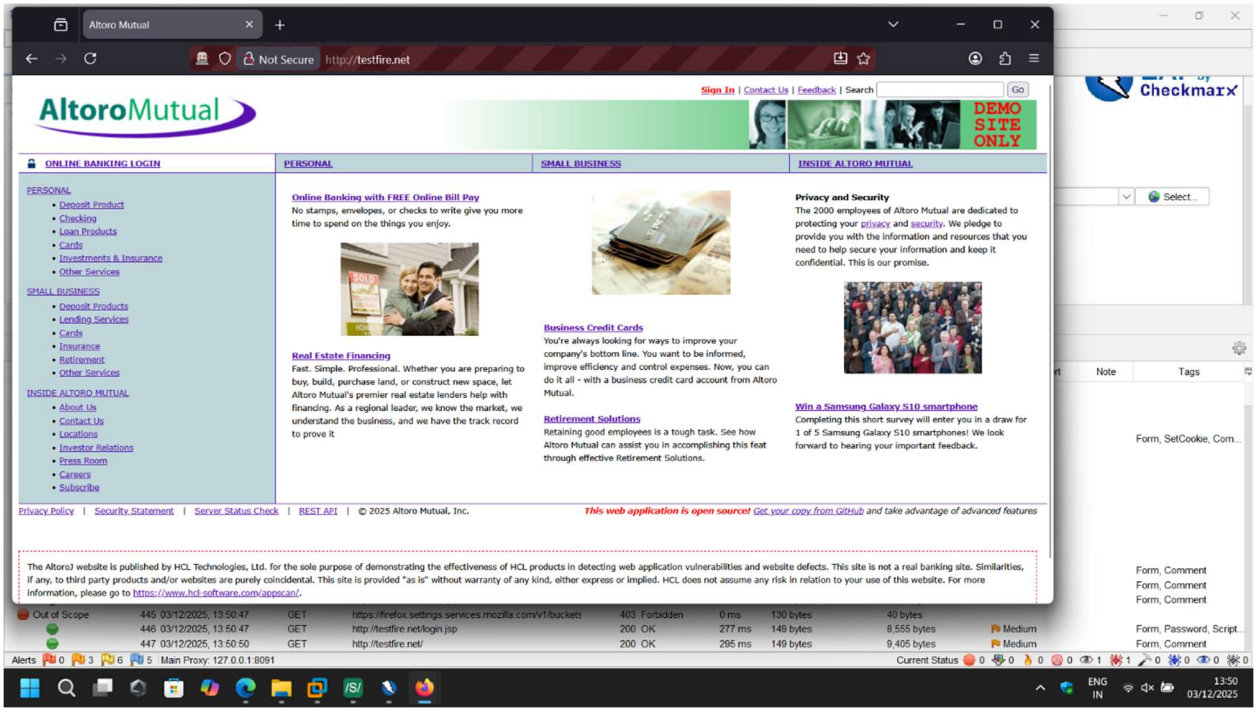


FIGURE 28 : OPENING EACH PAGE TO CHECK VULNERABILITY 1

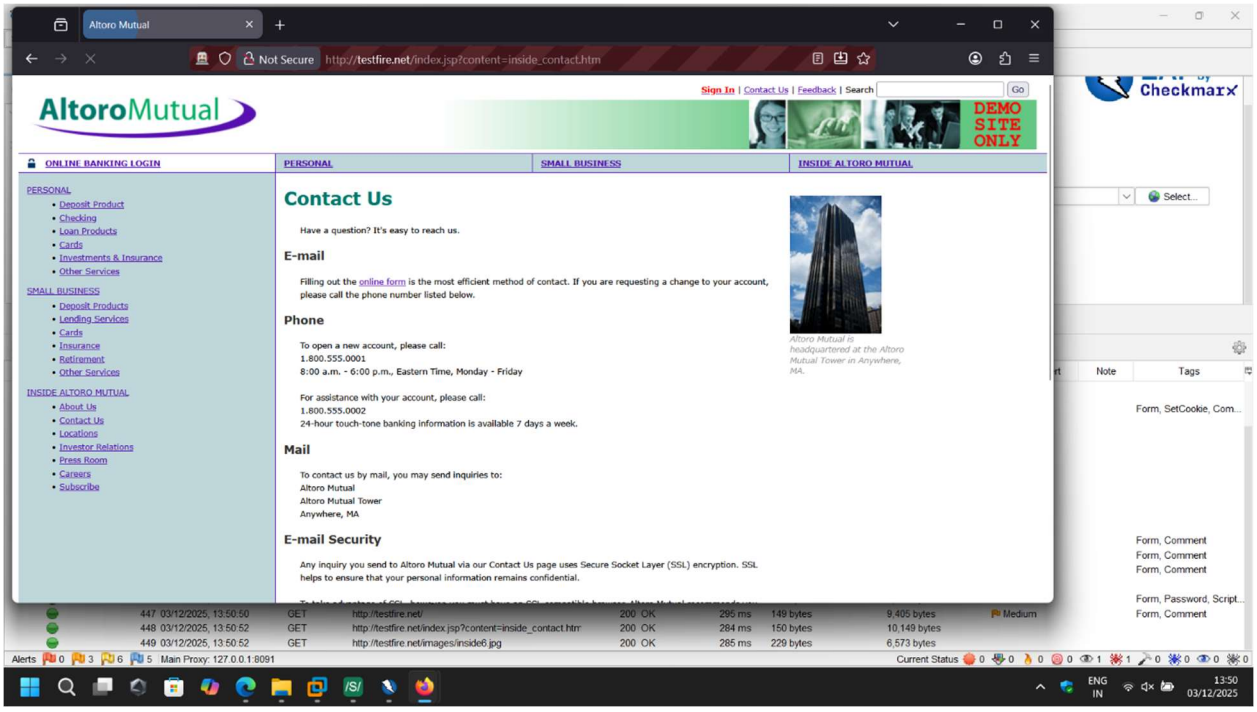


FIGURE 28 : OPENING EACH PAGE TO CHECK VULNERABILITY 2

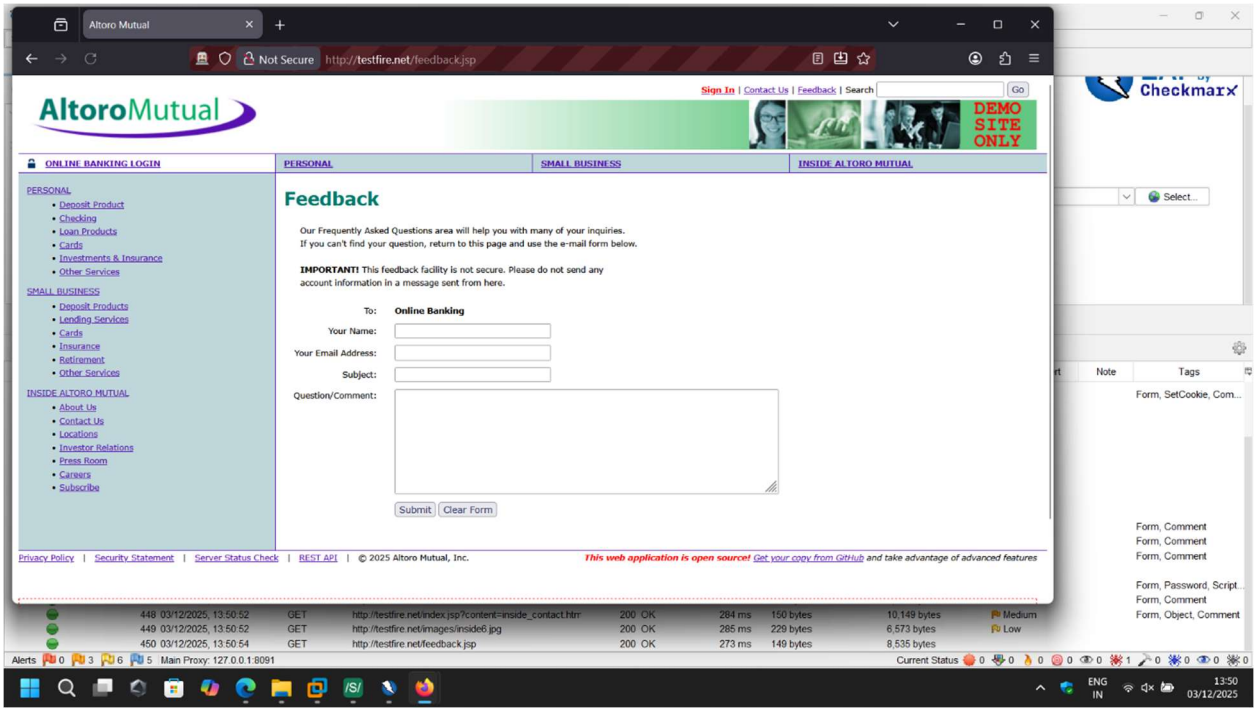


FIGURE 29: OPENING EACH PAGE TO CHECK VULNERABILITY 3

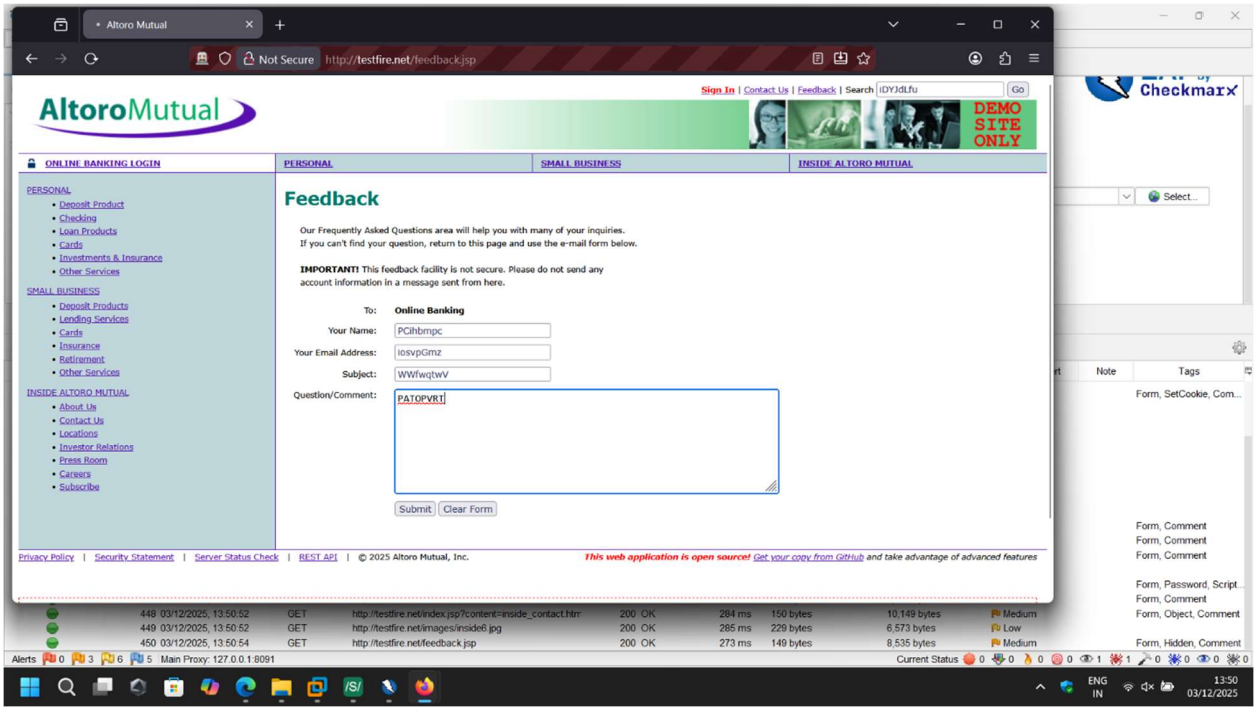


FIGURE 308 : OPENING EACH PAGE TO CHECK VULNERABILITY 4

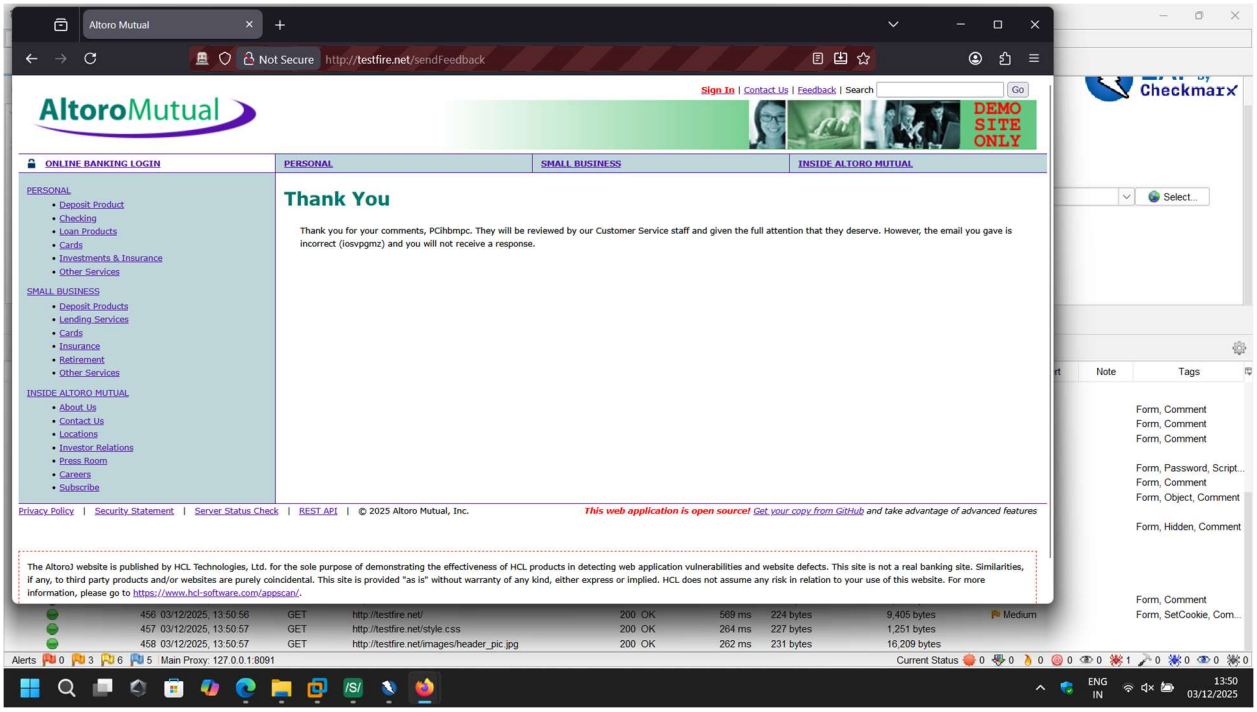


FIGURE 9: OPENING EACH PAGE TO CHECK VULNERABILITY 5

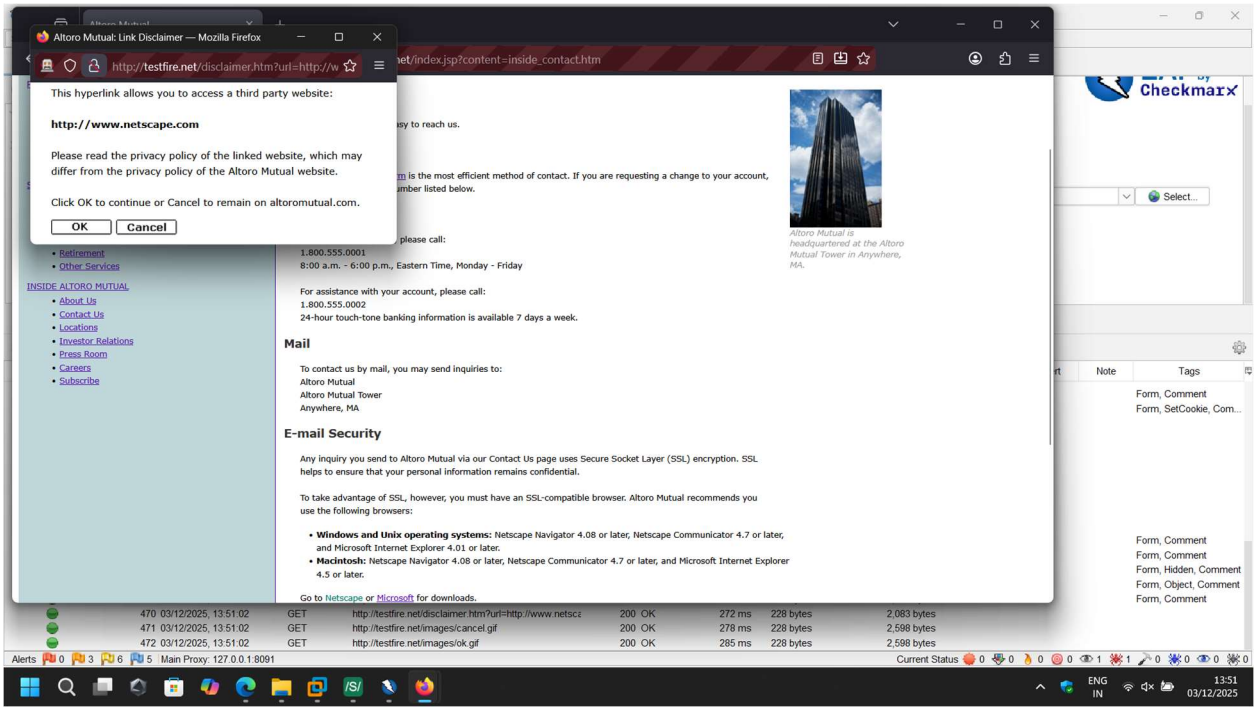


FIGURE 32: OPENING EACH PAGE TO CHECK VULNERABILITY 6

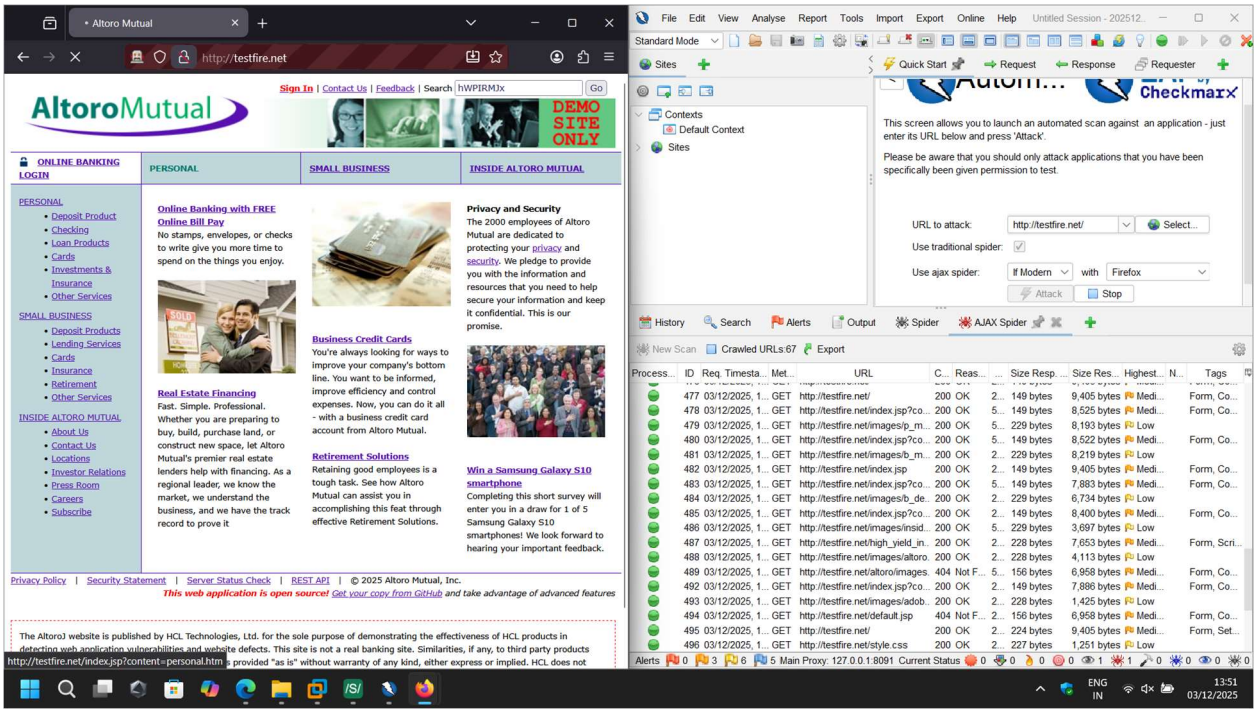


FIGURE 33:OPENING EACH PAGE TO CHECK VULNERABILITY 7

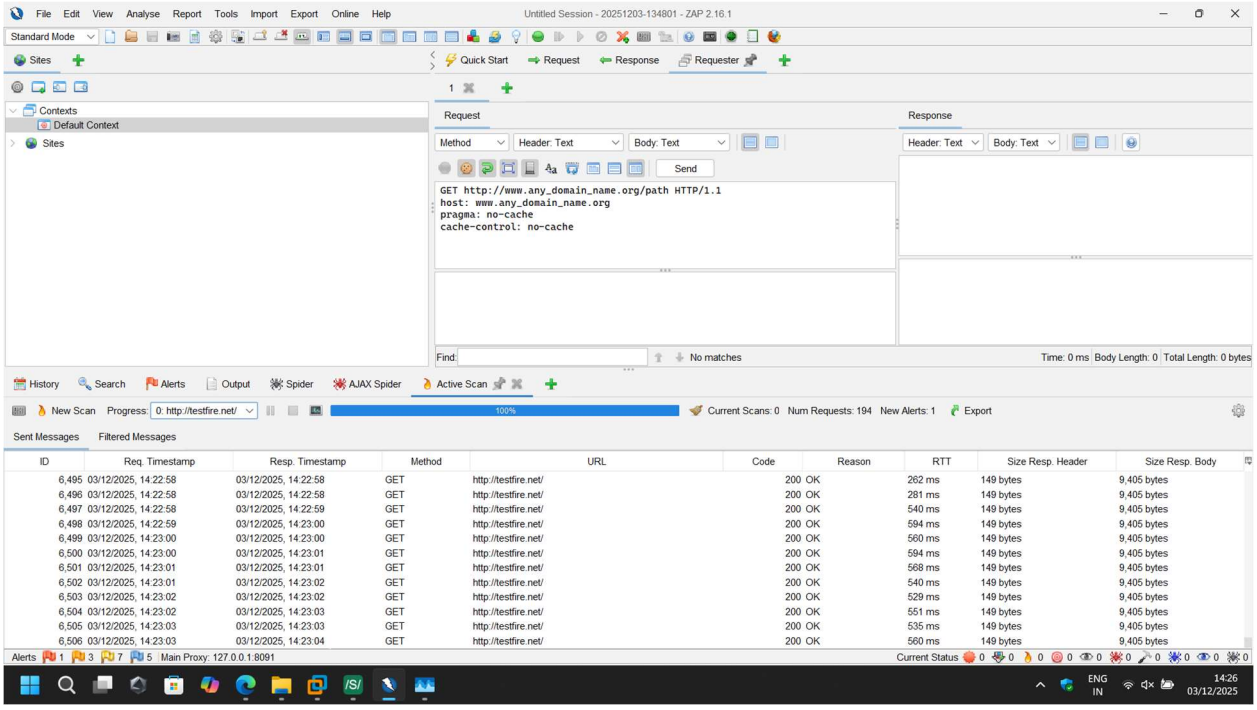


FIGURE 34: SCAN IS COMPLETED AND SHOWING VULNERABILITIES IN THE "ALERT" SECTION

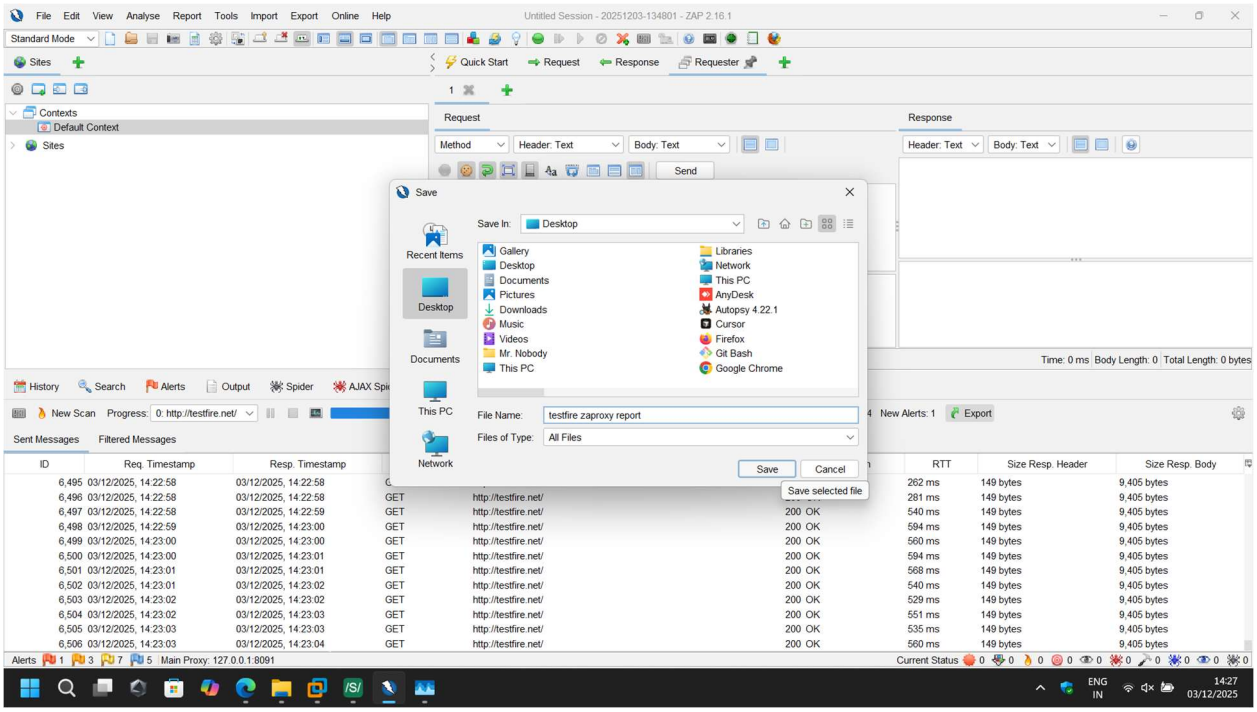


FIGURE 35: DOWNLOADING THE ASSESSMENT REPORT IN PDF

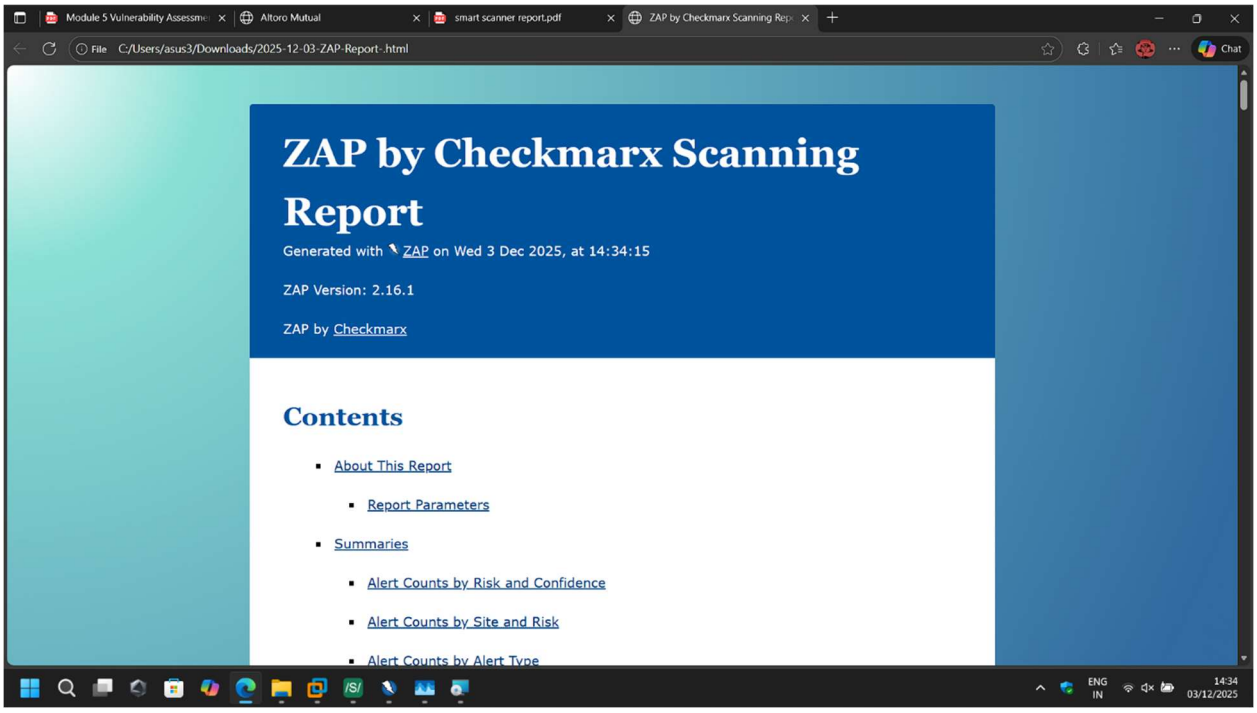


FIGURE 36: VULNERABILITY ASSESSMENT REPORT GENERATED BY ZAP 1

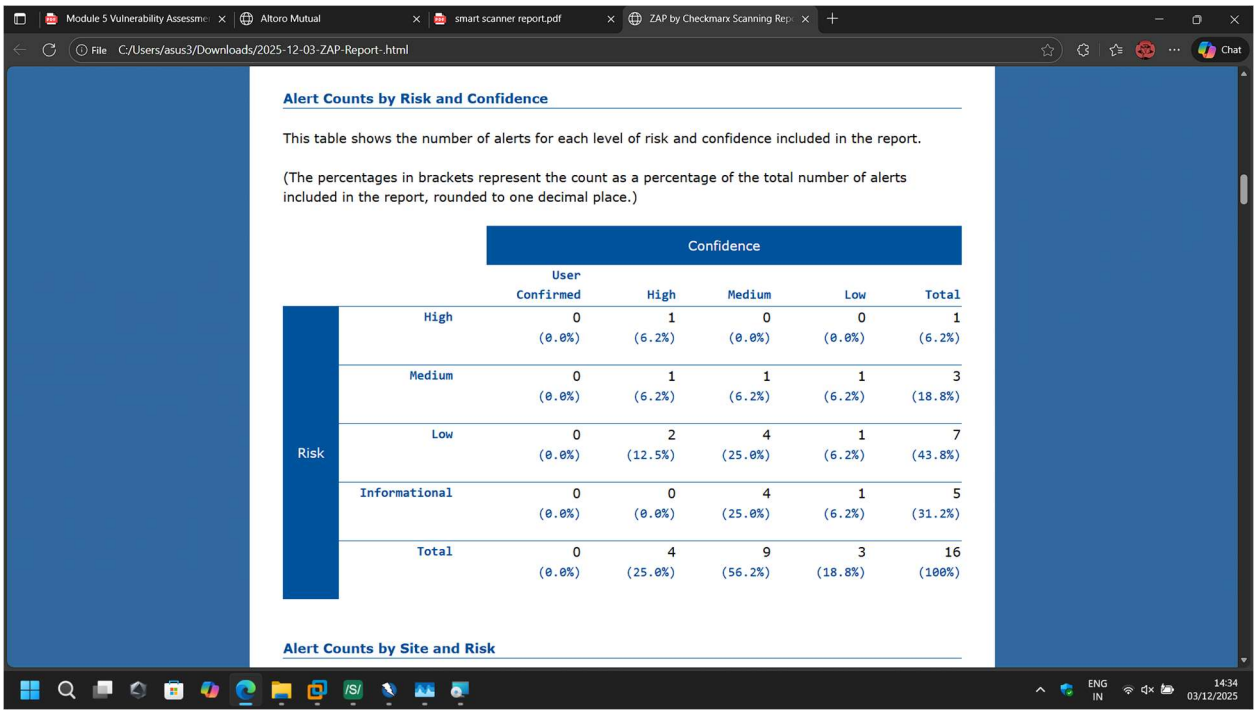


FIGURE 37: VULNERABILITY ASSESSMENT REPORT GENERATED BY ZAP 2

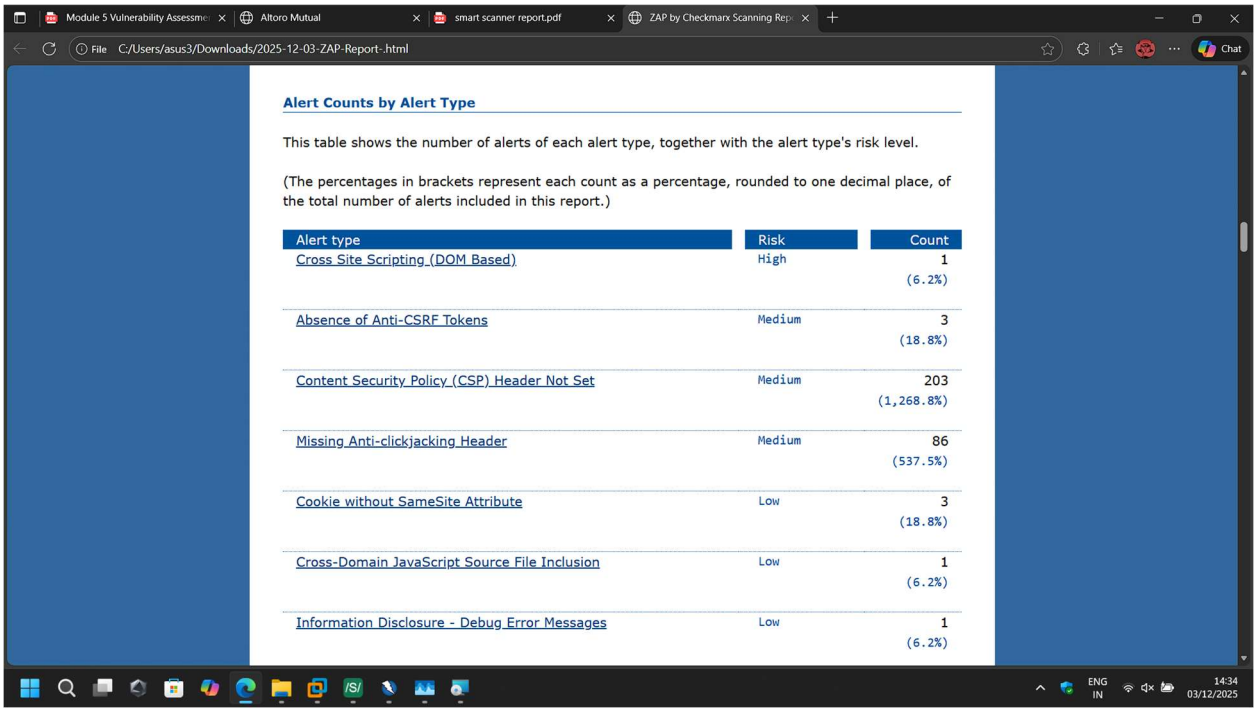


FIGURE 38: VULNERABILITY ASSESSMENT REPORT GENERATED BY ZAP 3

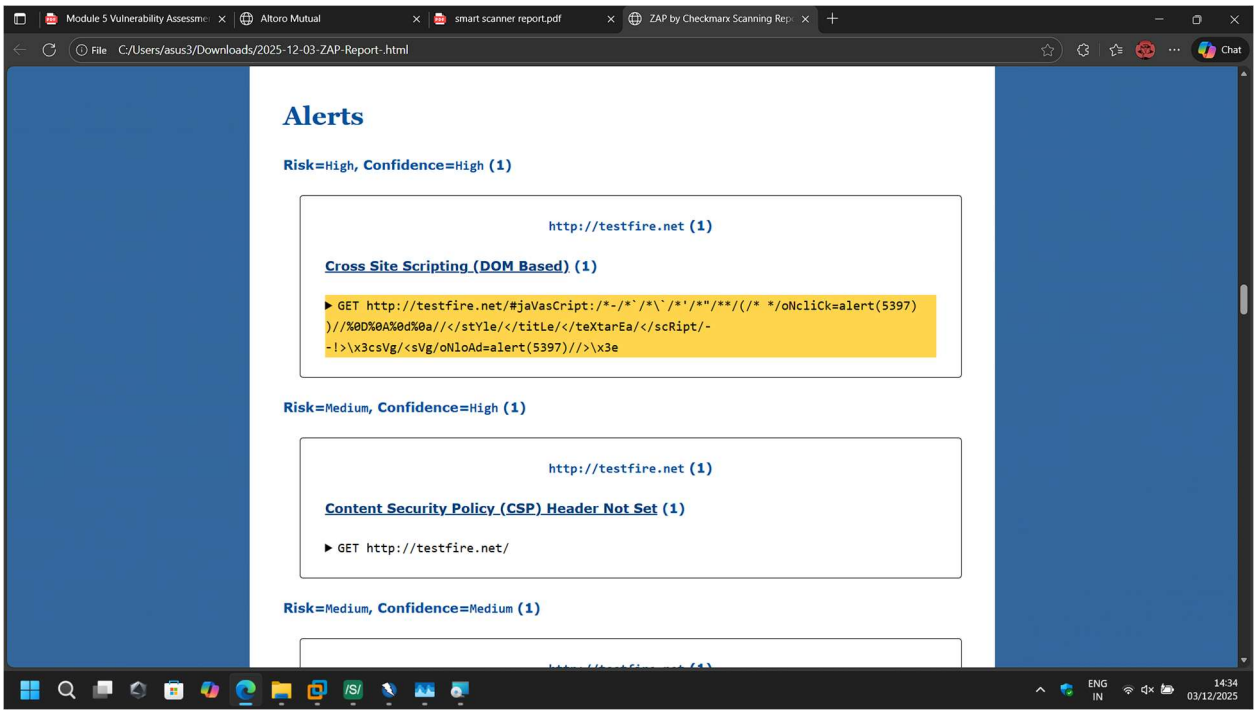


FIGURE 39: VULNERABILITY ASSESSMENT REPORT GENERATED BY ZAP 4

5.Perform Vulnerability Assessment Using Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) is a free tool from Microsoft that helps identify common security misconfigurations and missing patches in Windows systems. Below are the structured steps to perform a vulnerability assessment using MBSA:

Steps to Perform Vulnerability Assessment with MBSA

1. **Download and Install MBSA**

- Obtain MBSA from Microsoft's official site (though note it is now deprecated, but still usable for legacy systems).
- Install it on your Windows machine.

2. **Launch MBSA**

- Open the MBSA application.
- You'll be presented with options to scan a single computer, multiple computers, or a domain.

3. **Select Scan Options**

- Choose **Scan a computer** (enter the computer name or IP).
- Alternatively, select **Scan multiple computers** using IP ranges or domain membership.
- Configure scan options:

  ✓ Check for Windows updates.
  ✓ Look for weak passwords.
  ✓ Verify security updates and service packs.
  ✓ Inspect IIS, SQL Server, and other Microsoft products.

4. **Run the Scan**

- Click **Start Scan**.
- MBSA will analyze the system for missing patches, insecure configurations, and weak security settings.

5. **Review Results**

- Once complete, MBSA generates a **report** with findings categorized as:
  - **Red X** → Security issue found.
  - **Yellow exclamation** → Potential issue or warning.
  - **Green check** → No issues detected.
- Each finding includes a description and recommended remediation steps.

6. **Remediate Issues**

- Apply patches via Windows Update or WSUS.
- Fix misconfigurations (e.g., enabling firewalls, disabling guest accounts, enforcing strong passwords).
- Harden services like IIS or SQL Server based on MBSA's recommendations.

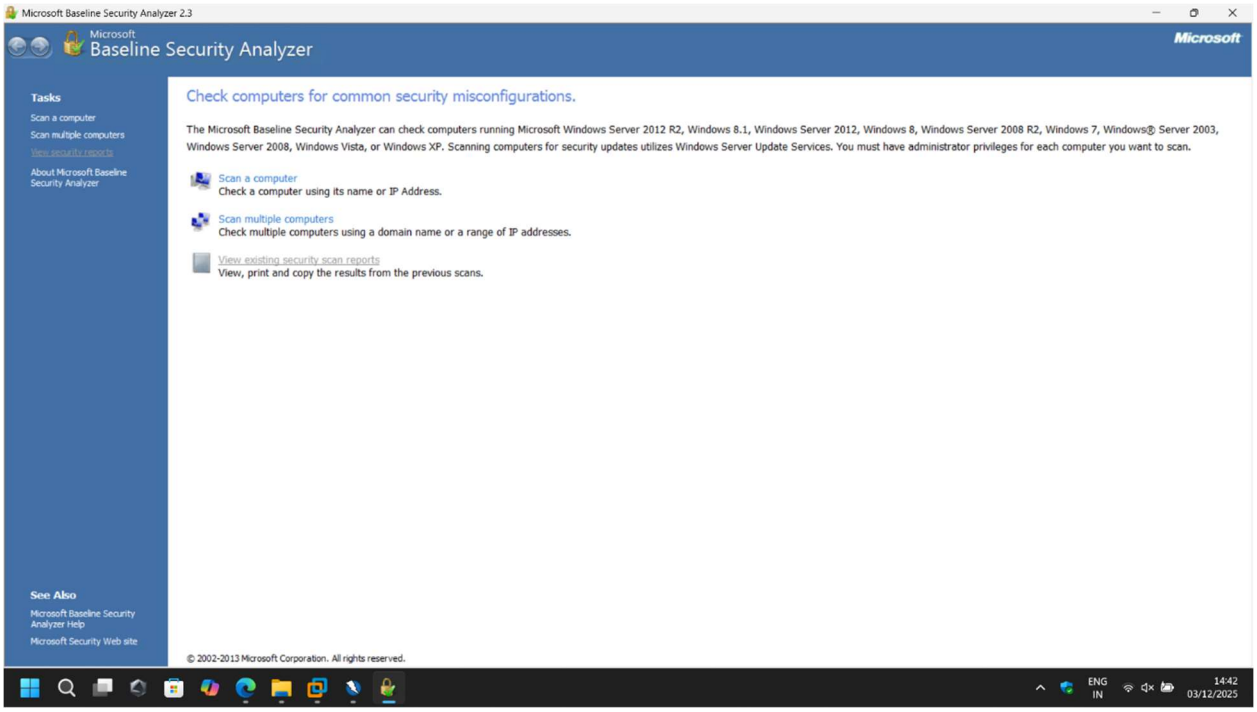


FIGURE 4010: DASHBOARD OF MICROSOFT BASELINE SECURITY ANALYZER

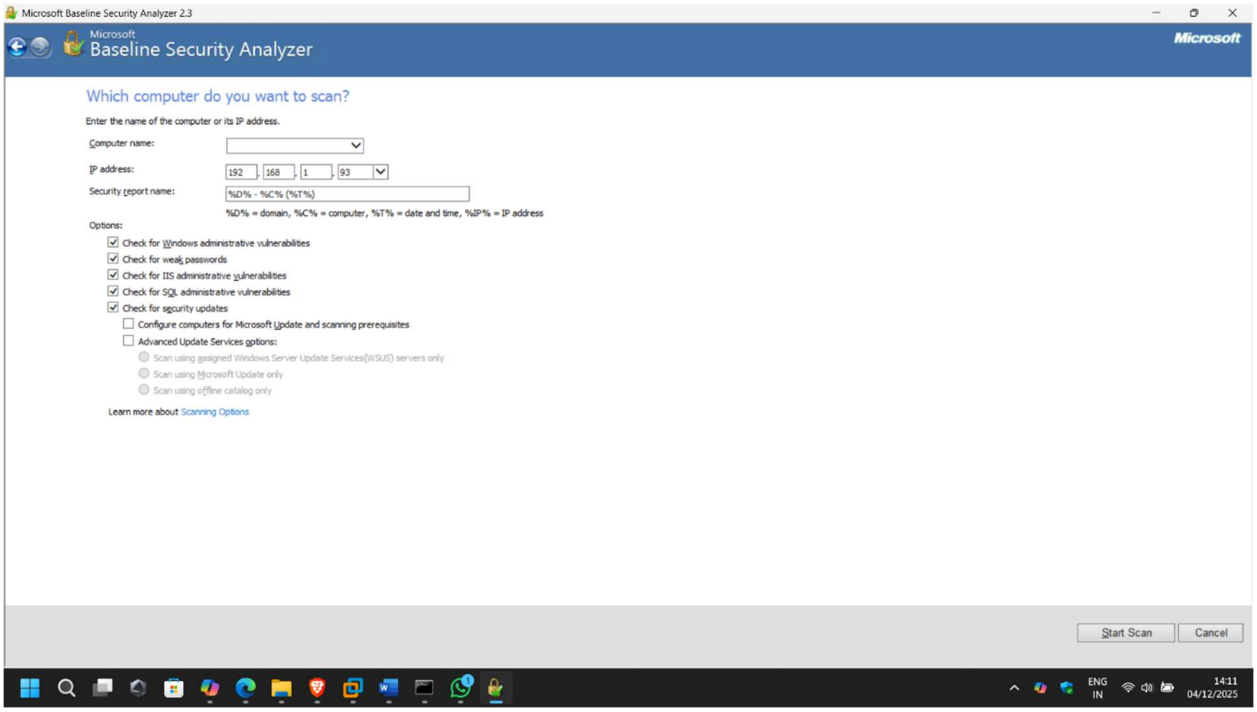


FIGURE41: SETTING TARGET DETAILS LIKE IP ADDRESS

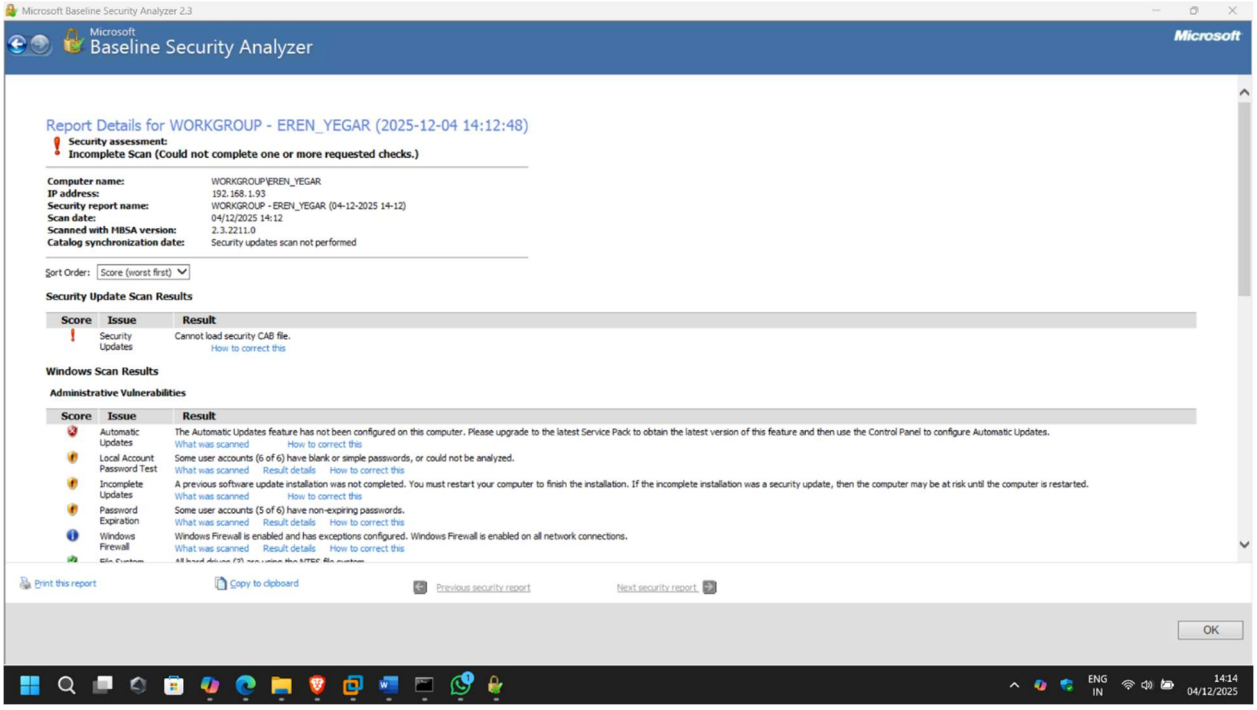


FIGURE 42 : RESULT OF THE SCAN

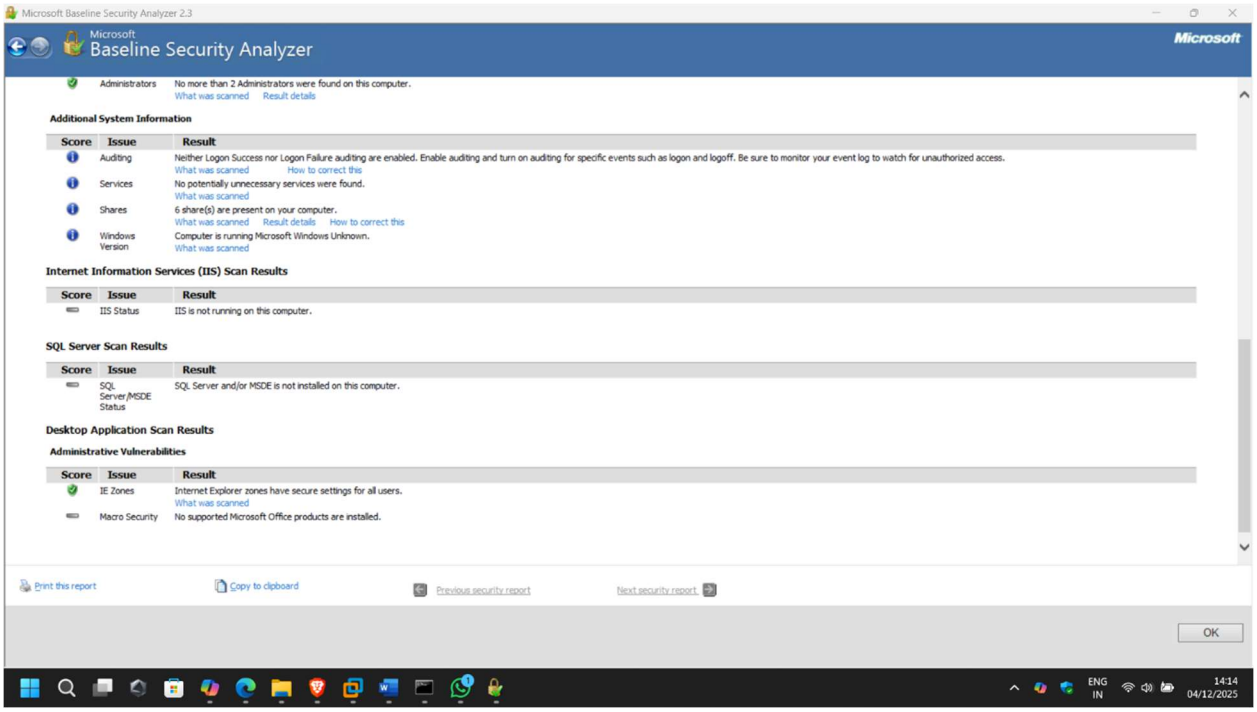


FIGURE 43: SCAN DISPLAYED THE WEAKNESS IN THE SYSTEM

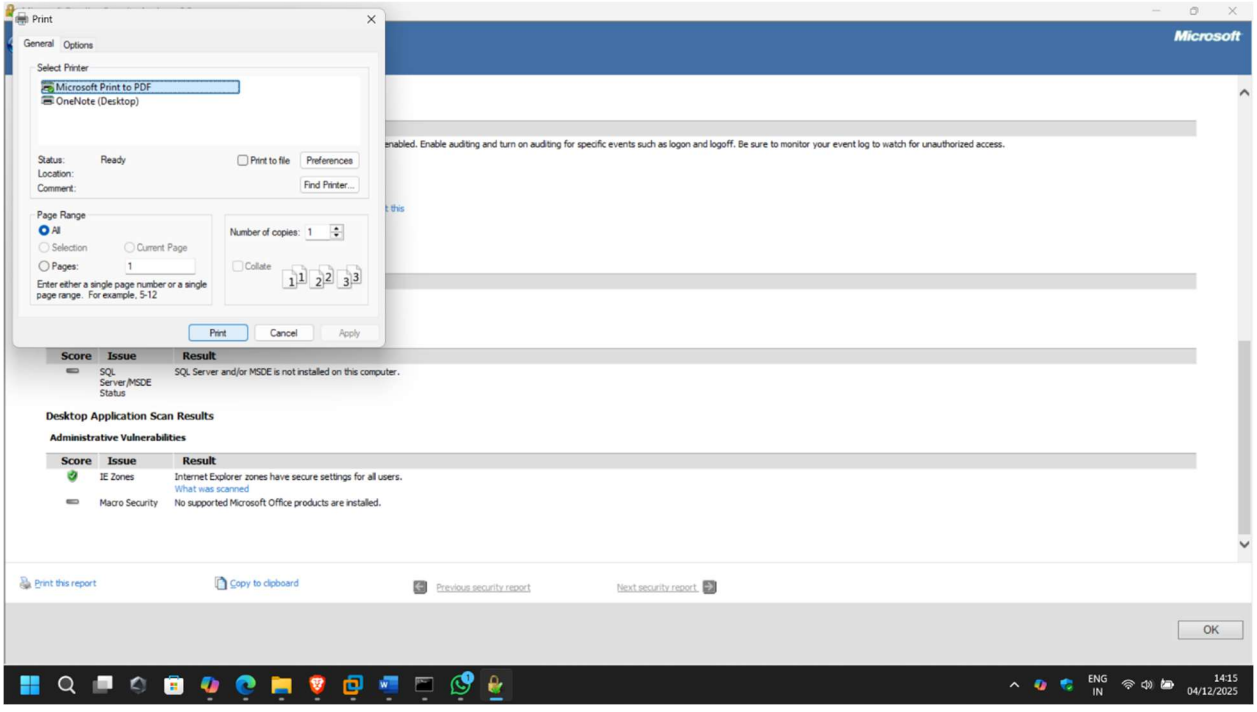


FIGURE 44: PRINTING THE ASSESSMENT REPORT GENERATED BY MICROSOFT BASELINE SECURITY ANALYZER