Day 51

Exploitation Analyst

AI powered solutions for OT Security Tasks:

What value AI can add to vulnerability scanning?

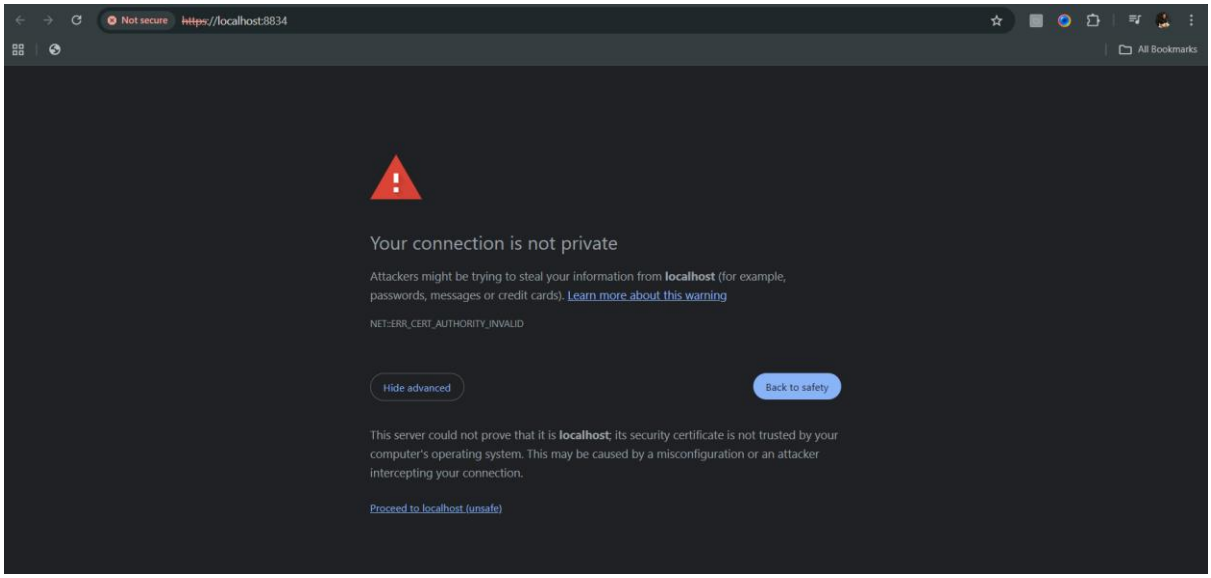
AI can add value to Vulnerability Assessment (VA) by making it faster, smarter, and more adaptive. In brief:

- **Automated Prioritization** – AI predicts which vulnerabilities are most likely to be exploited, reducing noise from long scan reports.
- **Threat Contextualization** – Correlates vulnerabilities with threat intelligence and asset criticality.
- **Pattern Recognition** – Detects hidden risks by analyzing system configurations, code, and historical attack data.
- **Real-Time Adaptation** – Learns from new exploits/zero-days to update risk scoring.
- **Reduced False Positives** – Improves accuracy of VA by filtering out non-exploitable issues.

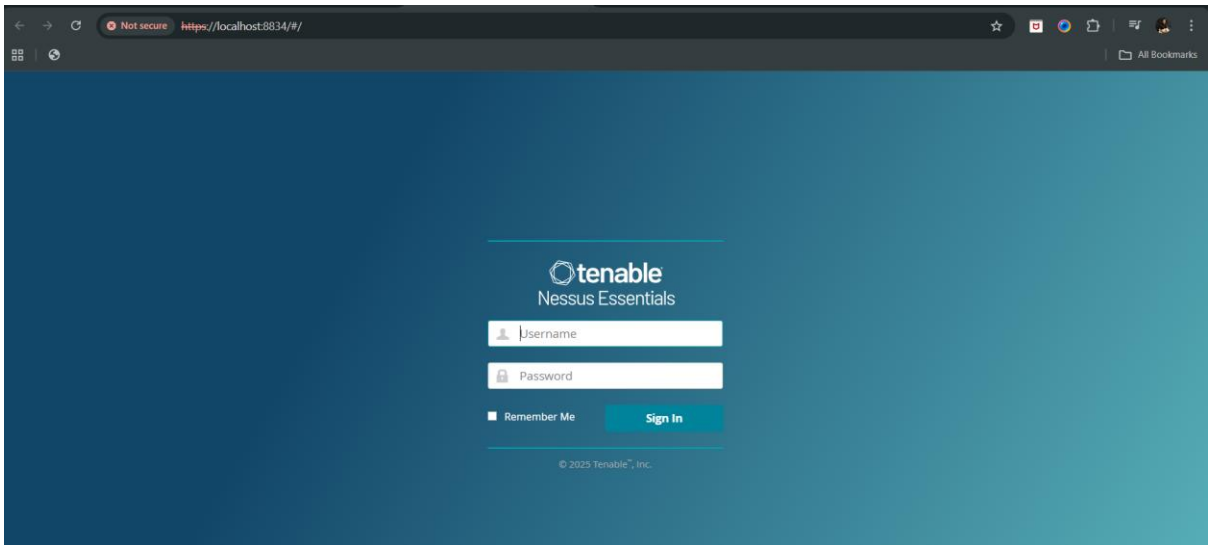
Vulnerability scanning and AI:

Steps:

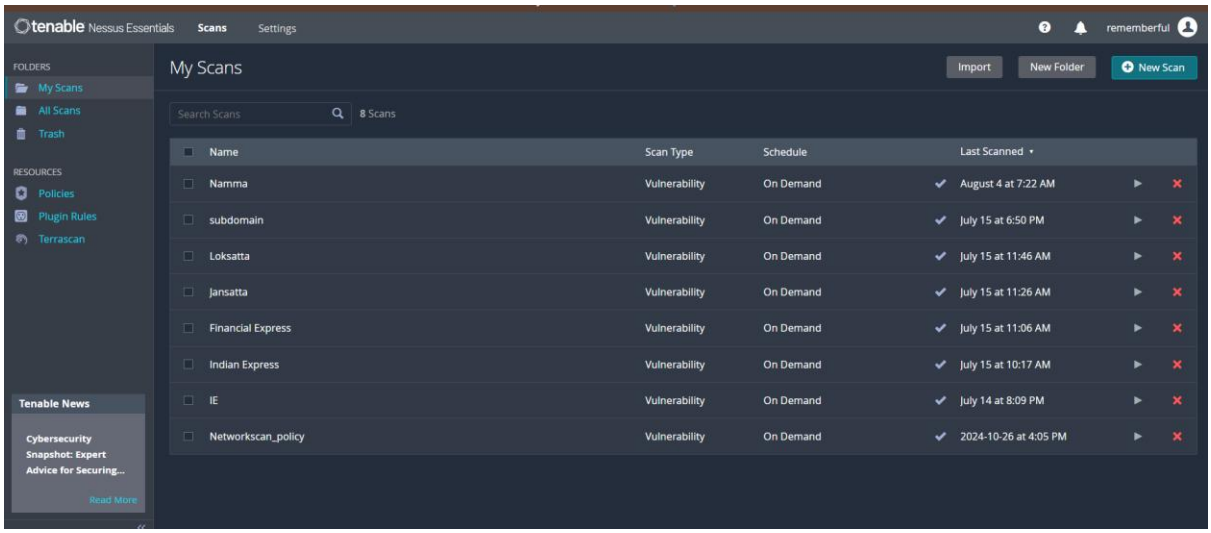
Open Nessus:



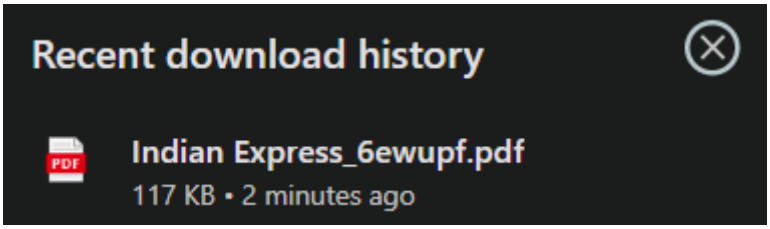
Following window will appear:



Login, following screen will appear:



Download any of the previous scan reports:



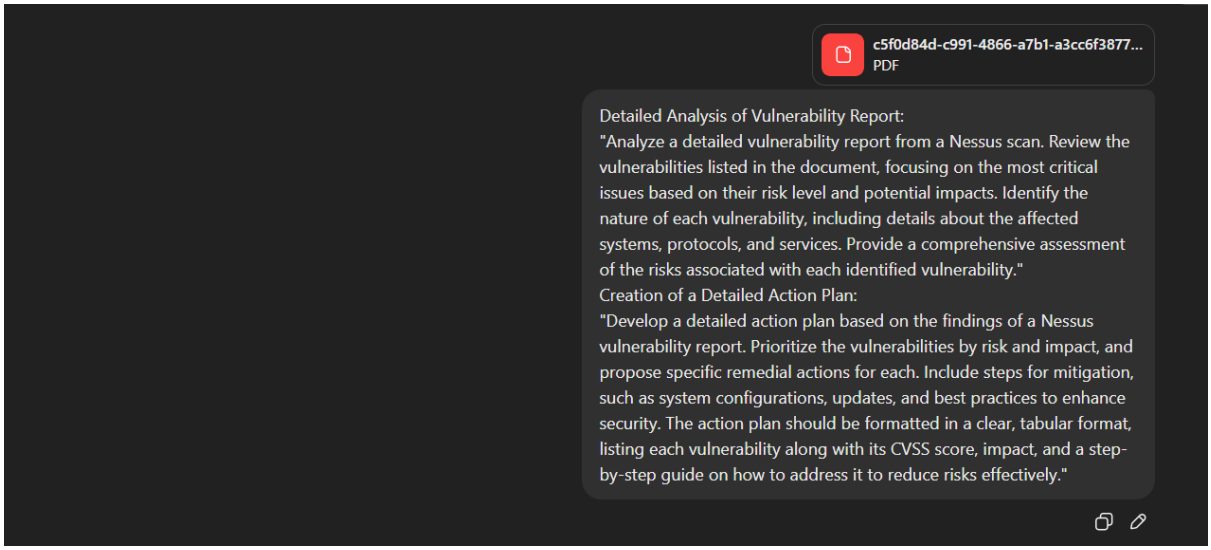
Now, upload in the ChatGPT, and use the following prompt to analyse:

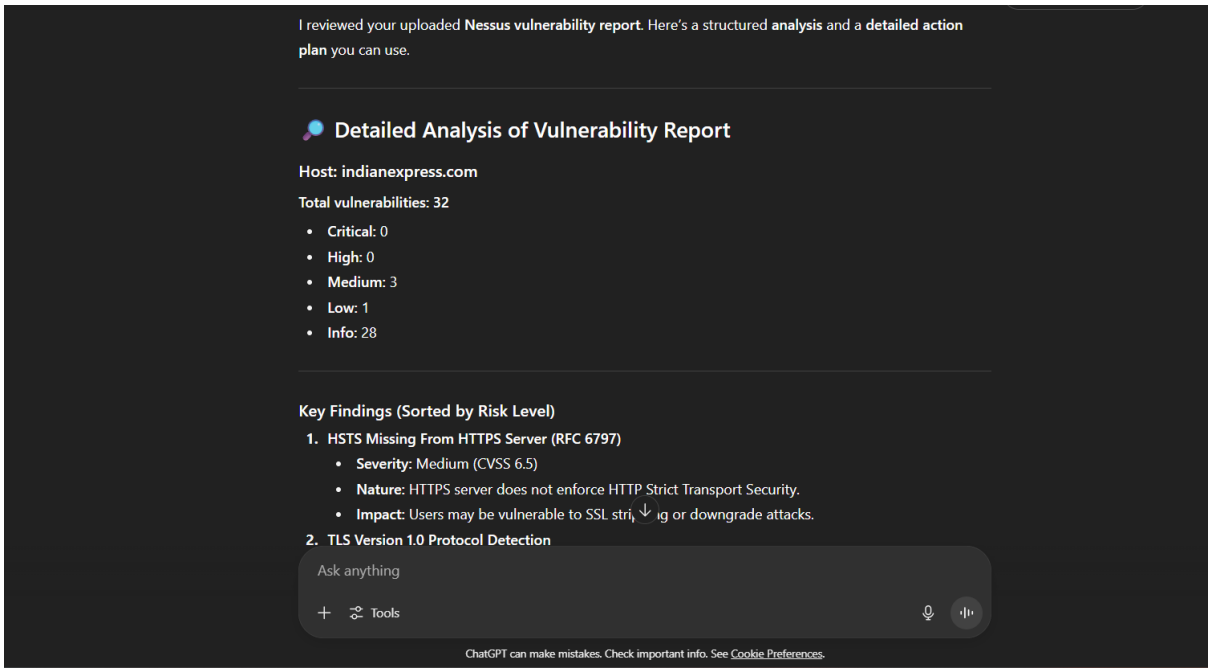
Detailed Analysis of Vulnerability Report:

"Analyze a detailed vulnerability report from a Nessus scan. Review the vulnerabilities listed in the document, focusing on the most critical issues based on their risk level and potential impacts. Identify the nature of each vulnerability, including details about the affected systems, protocols, and services. Provide a comprehensive assessment of the risks associated with each identified vulnerability."

Creation of a Detailed Action Plan:

"Develop a detailed action plan based on the findings of a Nessus vulnerability report. Prioritize the vulnerabilities by risk and impact, and propose specific remedial actions for each. Include steps for mitigation, such as system configurations, updates, and best practices to enhance security. The action plan should be formatted in a clear, tabular format, listing each vulnerability along with its CVSS score, impact, and a step-by-step guide on how to address it to reduce risks effectively."





--The End—