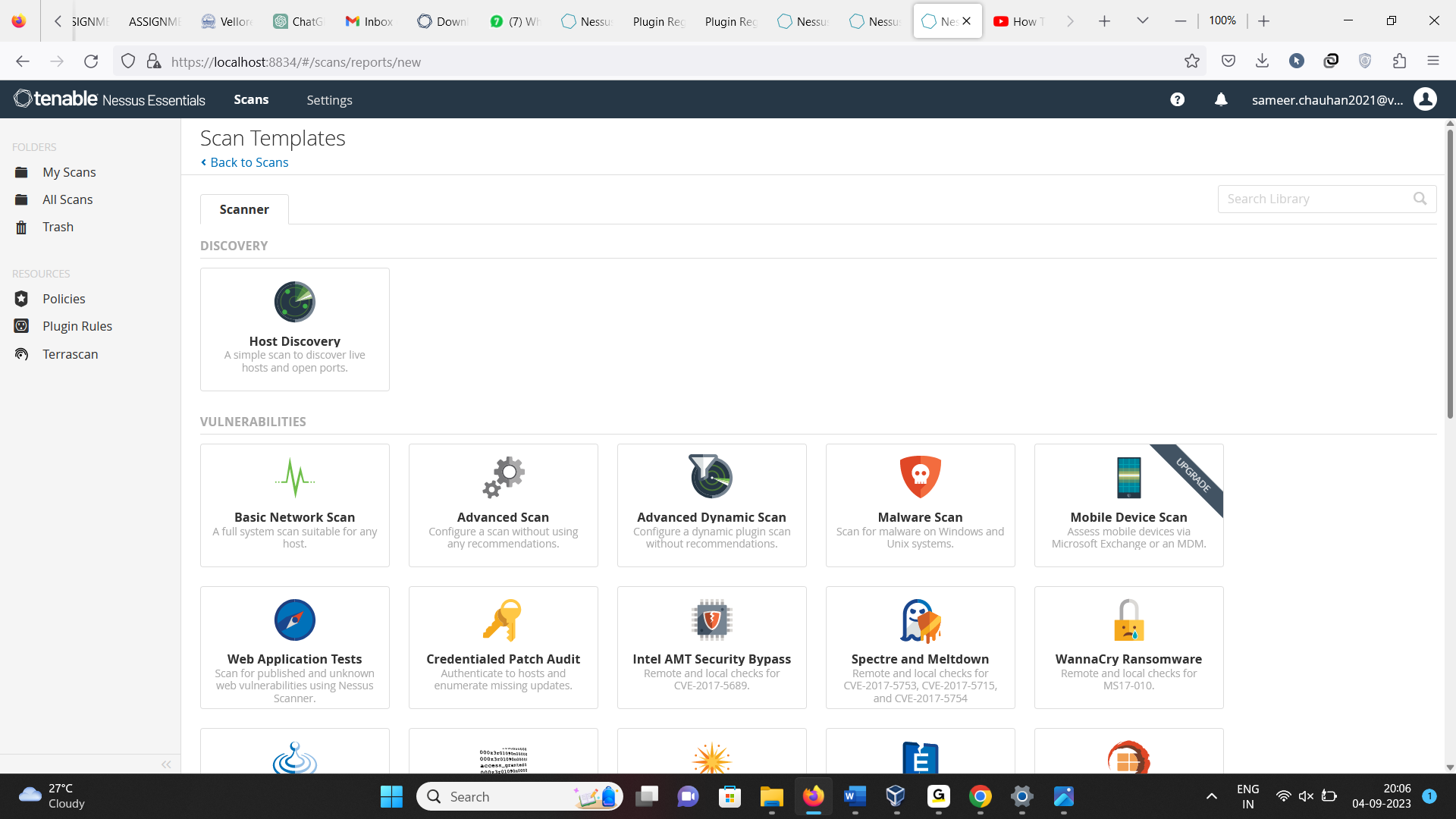
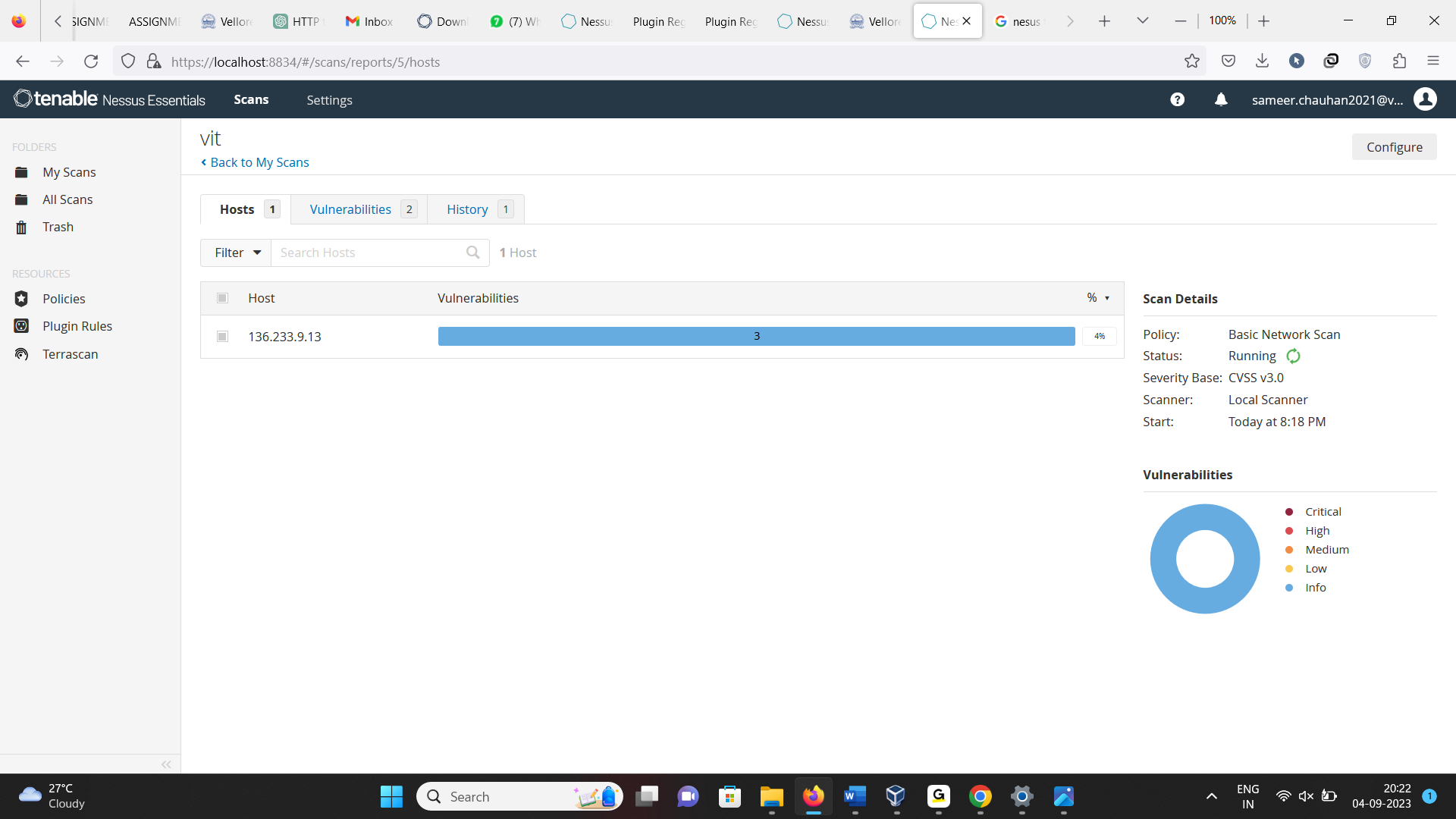
**TASK -8 04-09-23 Monday**

**SAMEER CHAUHAN**

**Aim-We have to do vulnerability scanning and prepare a report of the scan according the format with the help of Nessus tool**



**Nessus tool-Nessus is a widely used vulnerability assessment and management tool that helps organizations identify and remediate security vulnerabilities within their computer systems, network infrastructure, and applications.**



**As we can see we are scanning our college site vit.ac.in and its peforming scan**

**Report-**

**Vulnerablity name-JQuery 1.2 < 3.5.0 Multiple XSS**

**CWE-The Common Weakness Enumeration (CWE) identifier for "JQuery 1.2 < 3.5.0 Multiple XSS" vulnerabilities typically falls under the category of "Cross-Site Scripting (XSS)" and is specifically identified as CWE-79.**

**OWASP-IT falls under third category that is injection acc to 2021 OWASP and cross site scripting seventh category acc to 2017 OWASP**

**Description- According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.**

**Buisness impact-**

**Data Exposure: If the college website stores sensitive information about students, faculty, or staff, such as personal details, academic records, or financial information, XSS vulnerabilities could lead to data exposure. This can result in privacy violations, identity theft, and legal liabilities for the institution.**

**Academic Integrity: If the website hosts online learning materials, assessments, or student records, XSS attacks could compromise academic integrity by allowing unauthorized access to exams, assignments, or grading systems.**

**Affected URL- 136.233.9.13**

**POC-**

****

**Remidiation-Upgrade to JQuery version 3.5.0 or later.**