****

**INSTITUTE OF INFORMATION TECHNOLOGY**

**JAHANGIRNAGAR UNIVERSITY**

|  |  |
| --- | --- |
| Number of Assignment | : 04 |
| Name of Assignment | **: Vulnerability Assessment & Port Scanning using ZenMap** |
| Course Tittle | **: Cyber Security** |
| Submission Date | **: 23/10/2024** |

**Submitted To Submitted By**

**Moinoddeen Quader Al Arabi**

Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber Security Consultant in Dhaka Division, Bangladesh.

**Md. Shakil Hossain**

ID: 2111258

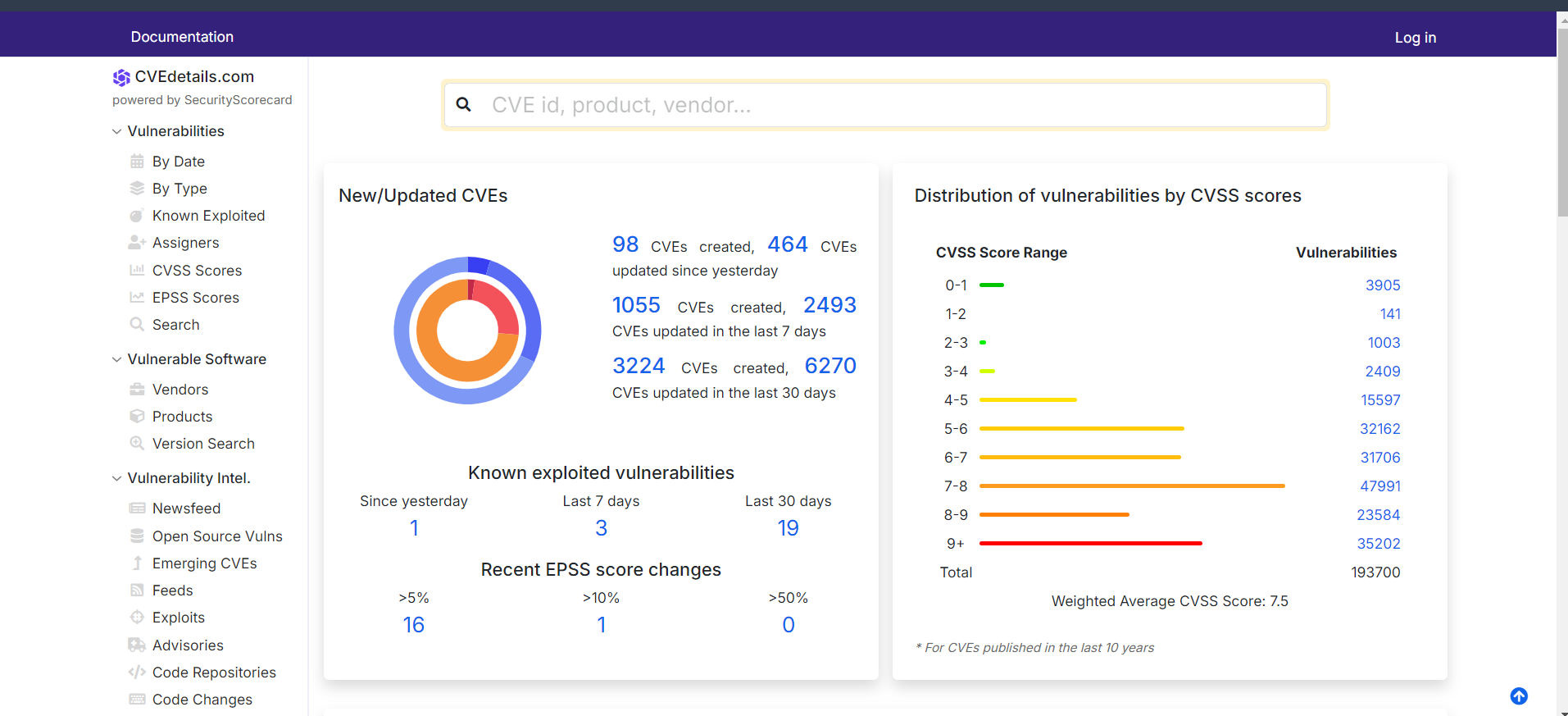
**Vulnerability Analysis and Research using Online Database:**

**Understanding the Vulnerability Landscape:**

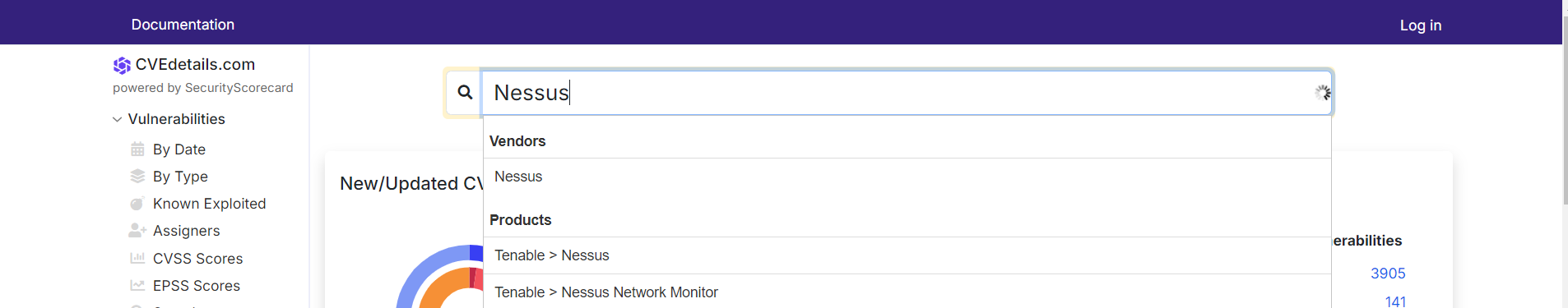
**Online Database:**

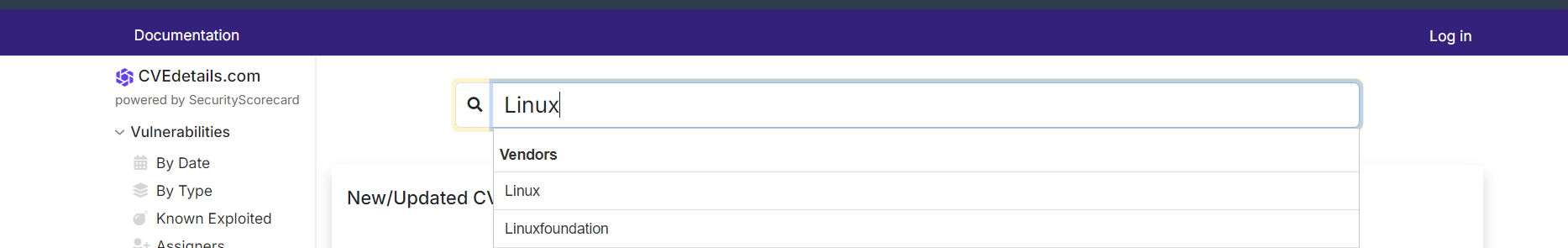
**CVEDetails:** CVEDetails is a platform that provides detailed information about publicly known cybersecurity vulnerabilities, known as Common Vulnerabilities and Exposures (CVEs). It aggregates data from sources like the National Vulnerability Database (NVD) and CVE.org, offering insights into vulnerabilities, associated exploits, risk scores, and related advisories. Users can search for CVEs by products, vendors, or vulnerability types, making it easier to assess and manage potential security risks. The site also presents metrics like CVSS scores and trends over time to help organizations prioritize vulnerability management.

Link: <https://www.cvedetails.com/>

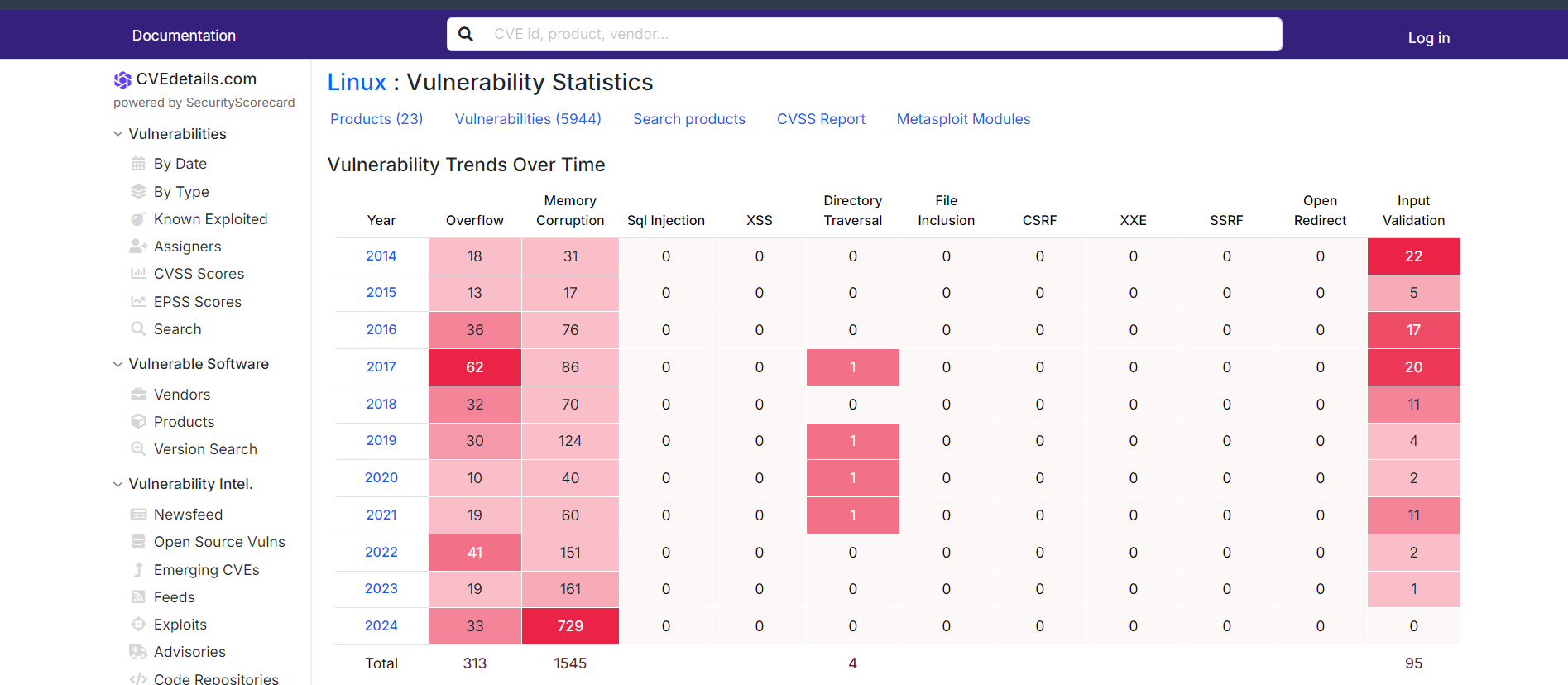


There has option for search any product, vendor etc.



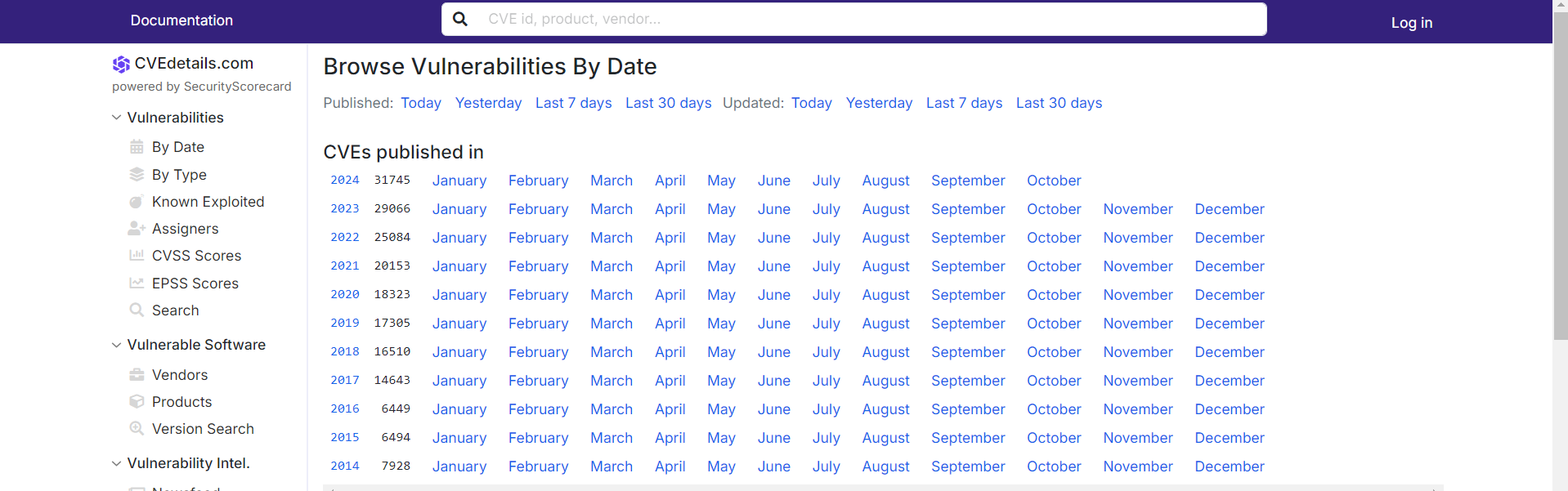


Here details of vulnerability is show until present month of the Year:



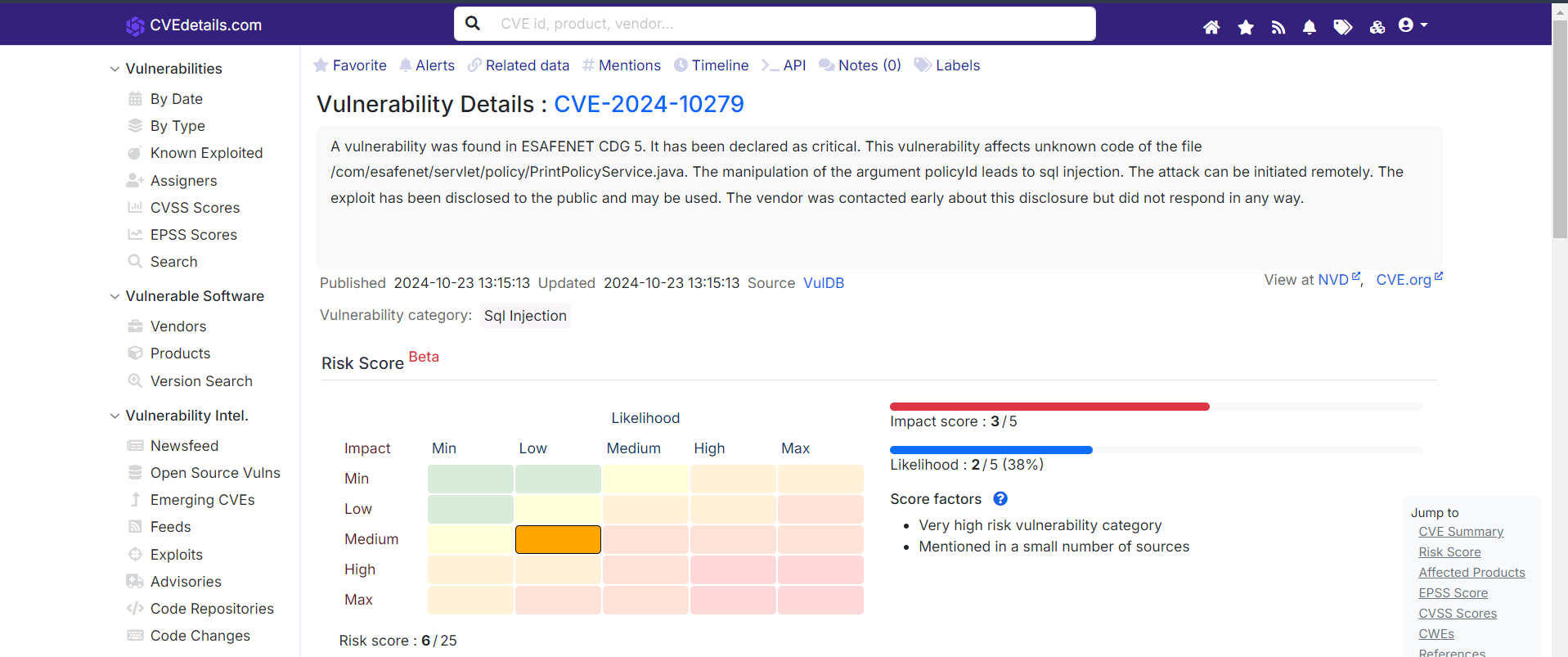
We can search by date, type.

Result of search by Date:



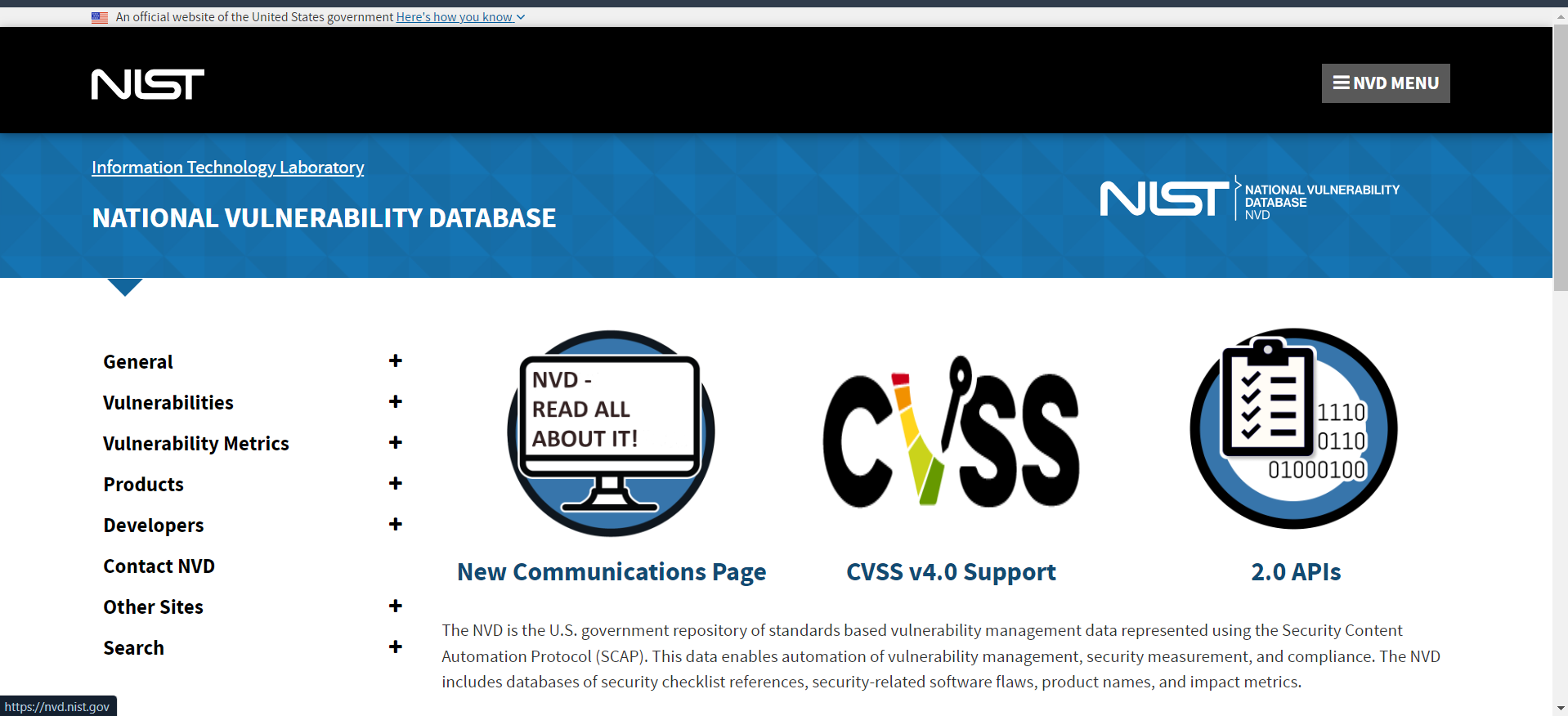
Today’s vulnerability (Green is good condition, orange is for risk medium and red for high risk of Base Severity):

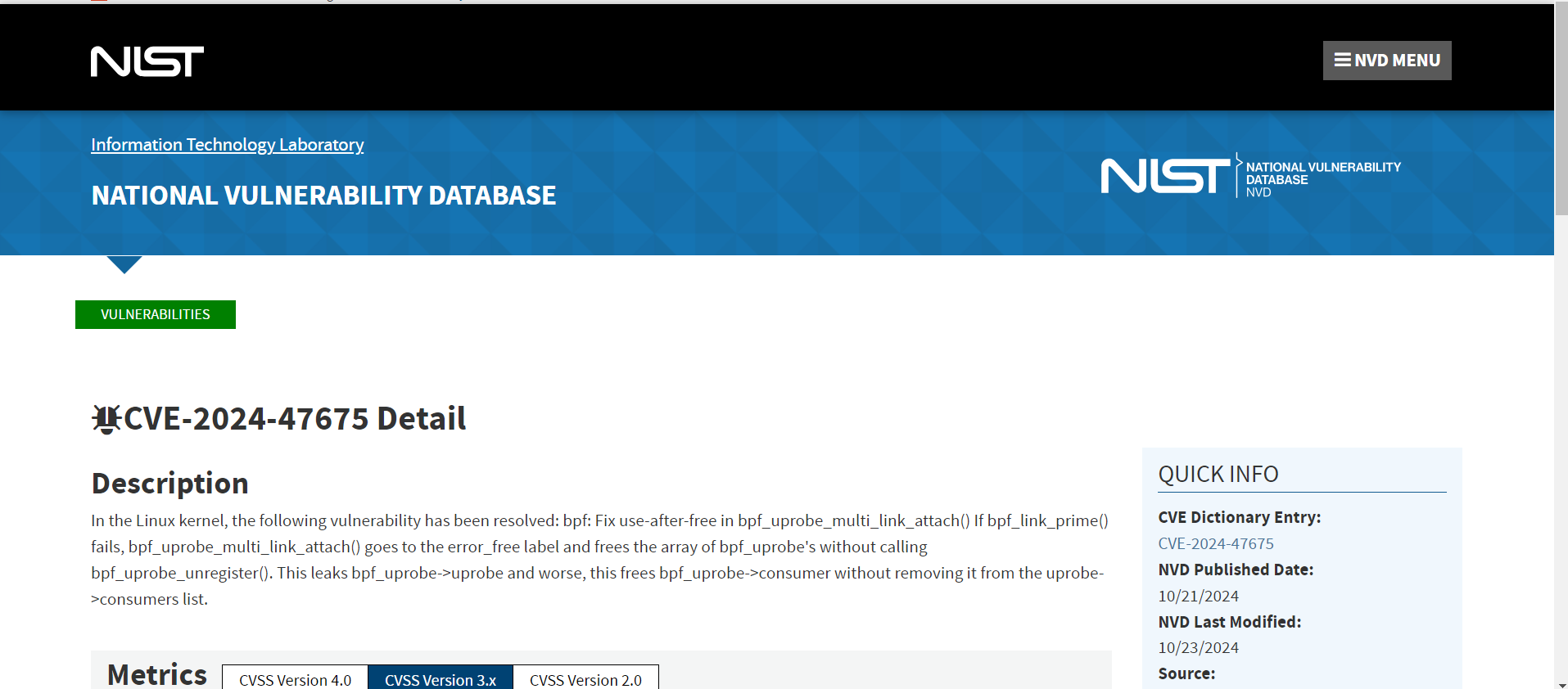


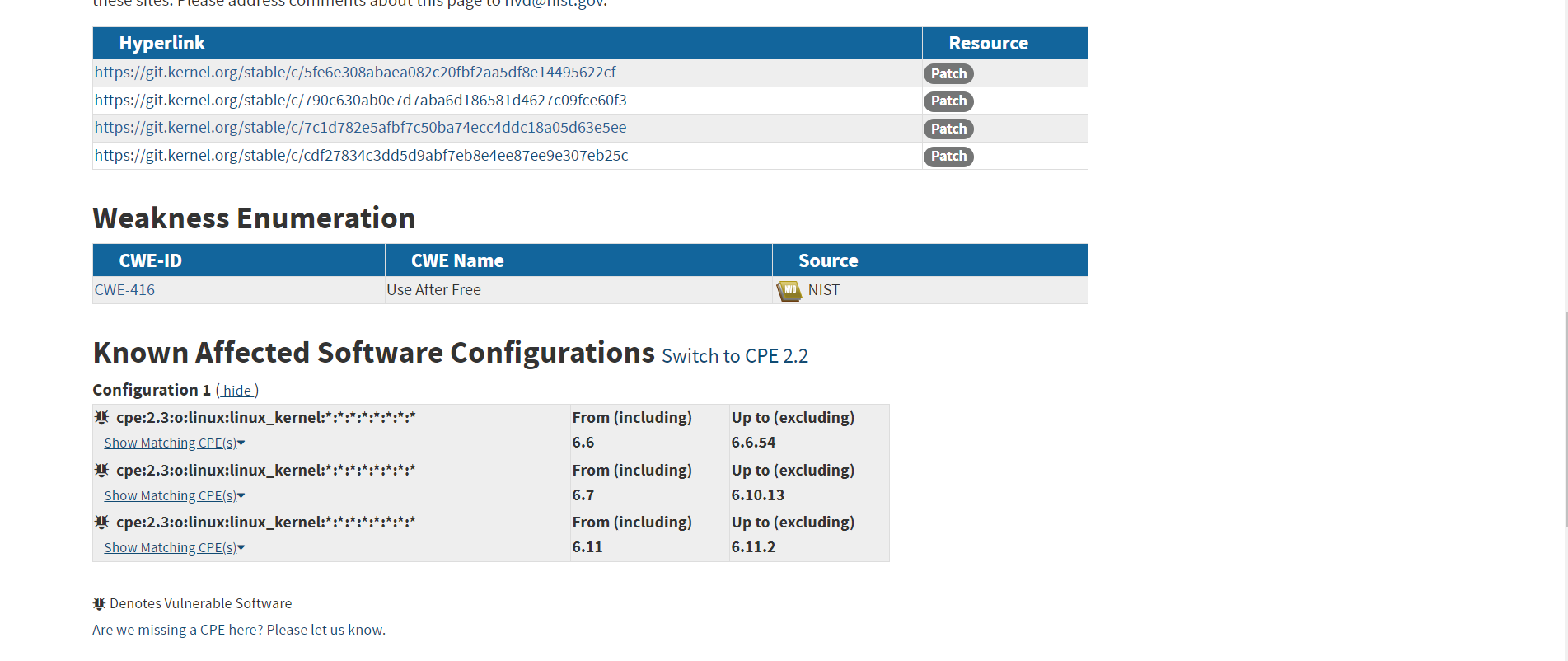


**NVD:** The National Vulnerability Database (NVD) is a U.S. government repository of standards-based vulnerability management data. Managed by the National Institute of Standards and Technology (NIST), NVD enhances CVE vulnerability data by adding details like severity scores, impact ratings, and fix information. It helps organizations prioritize vulnerabilities and guides them in applying appropriate security patches or mitigations. NVD also includes tools for searching and analyzing vulnerabilities, making it a crucial resource for cybersecurity professionals to manage threats effectively.

Link: <https://nvd.nist.gov/>

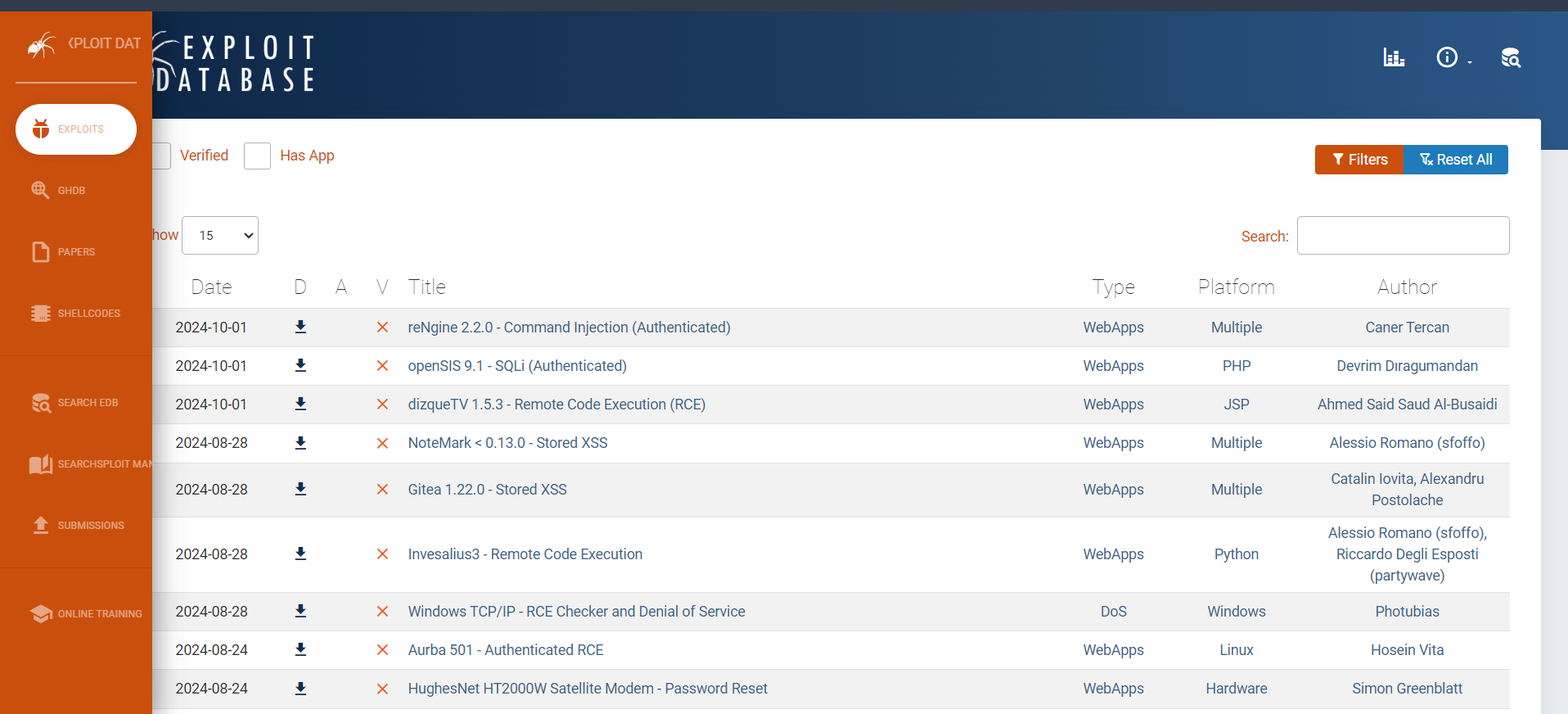






**Exploit-DB:** Exploit-DB (Exploit Database) is an archive of public exploits and software vulnerabilities, maintained by Offensive Security. It serves as a platform for security researchers and ethical hackers to share proof-of-concept exploit code. Exploit-DB offers a searchable database of exploits for various platforms, applications, and vulnerabilities, providing detailed information such as the vulnerability description, exploitation method, and sometimes links to patches. It is a valuable resource for penetration testers and cybersecurity professionals to study real-world vulnerabilities and their potential risks.

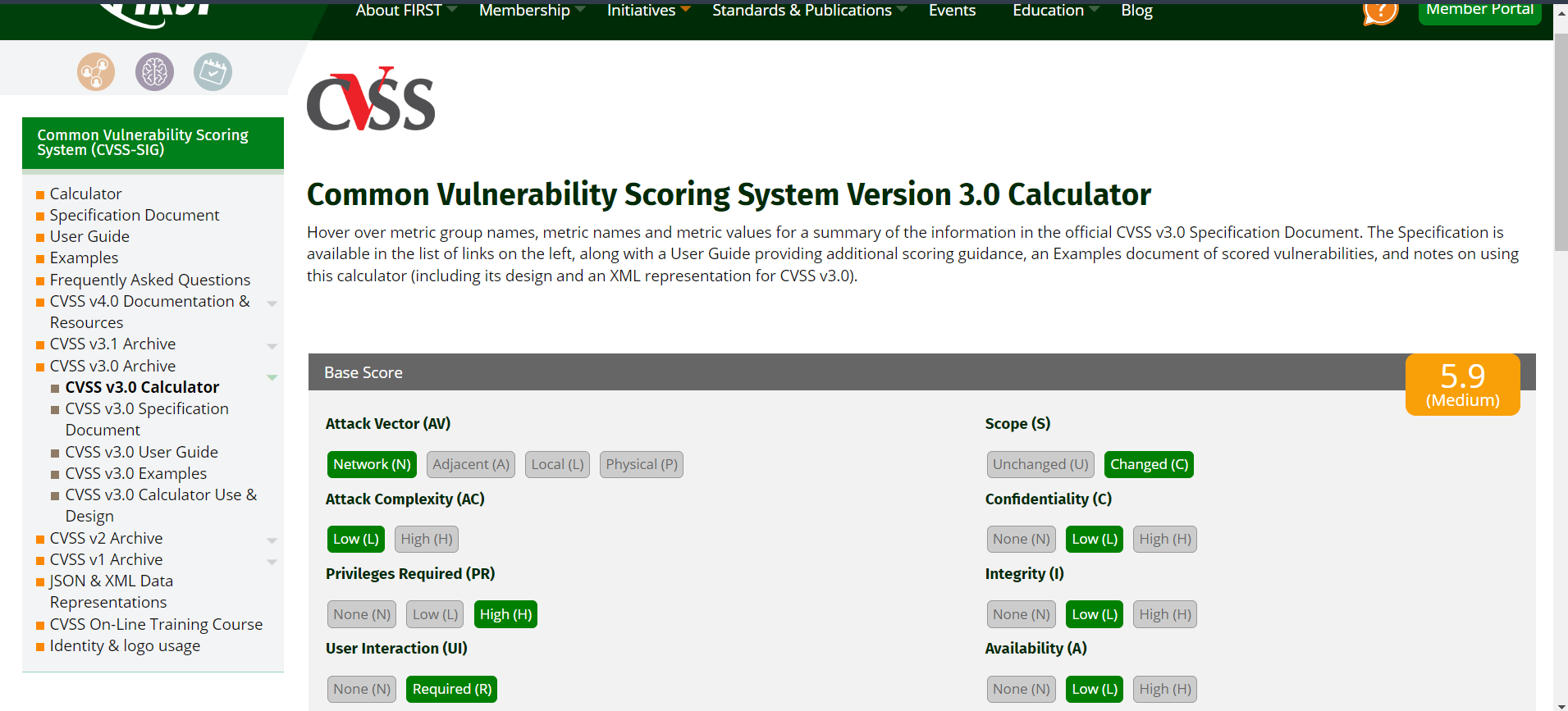
Link: <https://www.exploit-db.com/>



**Research Methodology:**

**CVSS scores**: CVSS (Common Vulnerability Scoring System) scores are a standardized way of assessing the severity of security vulnerabilities. They range from 0 to 10, with higher scores indicating more critical vulnerabilities. The CVSS score is based on several factors, including the ease of exploitation, the impact on system integrity, confidentiality, and availability. The score helps organizations prioritize patching and mitigating vulnerabilities by assigning a numerical value to the risk. CVSS is widely used in tools like NVD and CVEDetails to guide security efforts.

Link: <https://www.first.org/cvss/calculator/3.0>

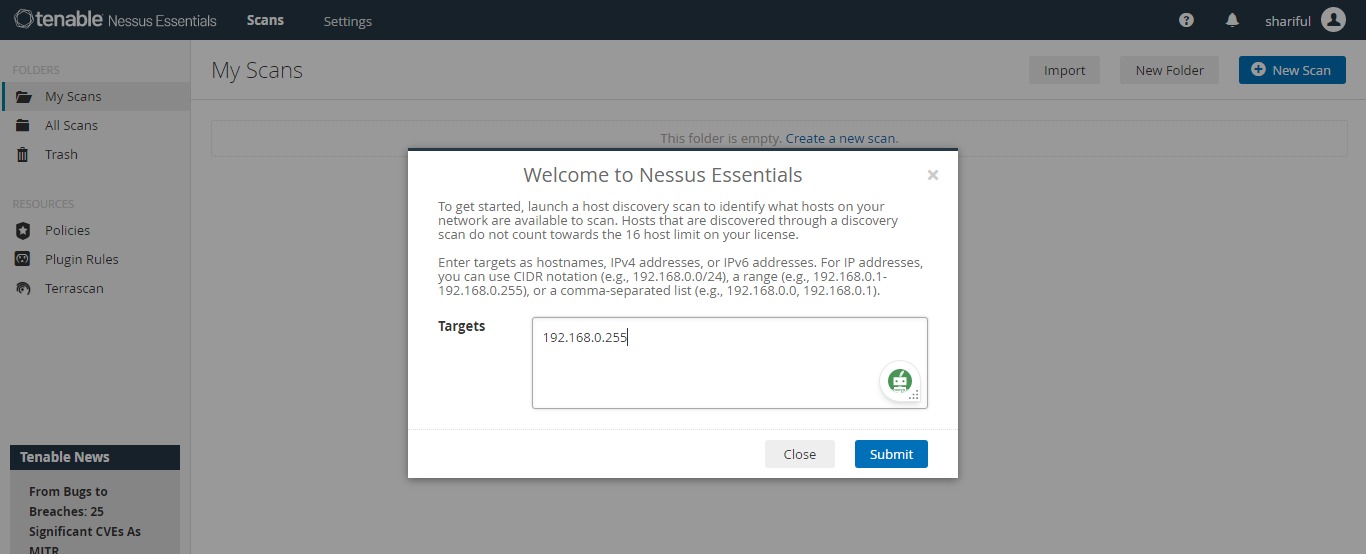


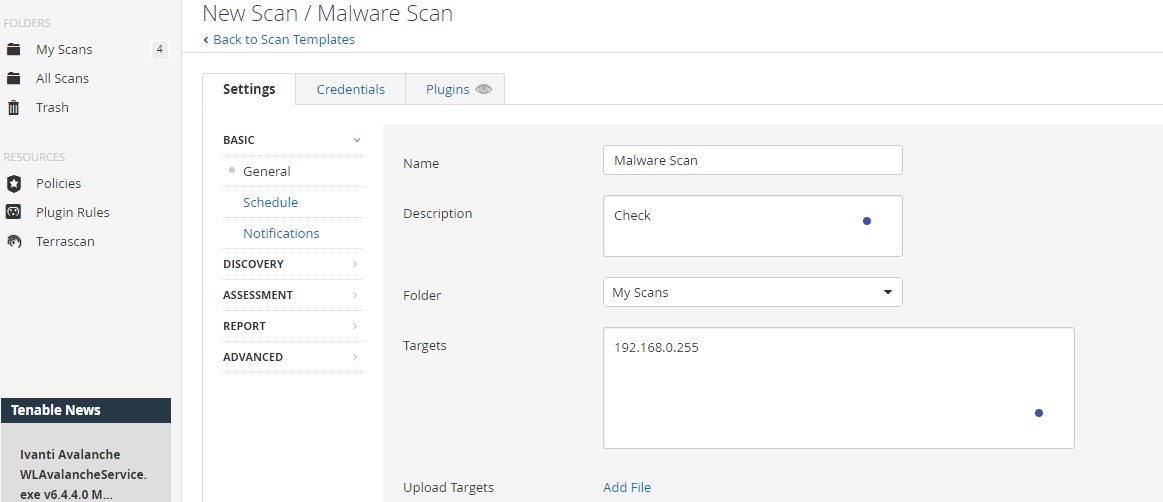
**Vulnerability Scanning using Manual Tools**

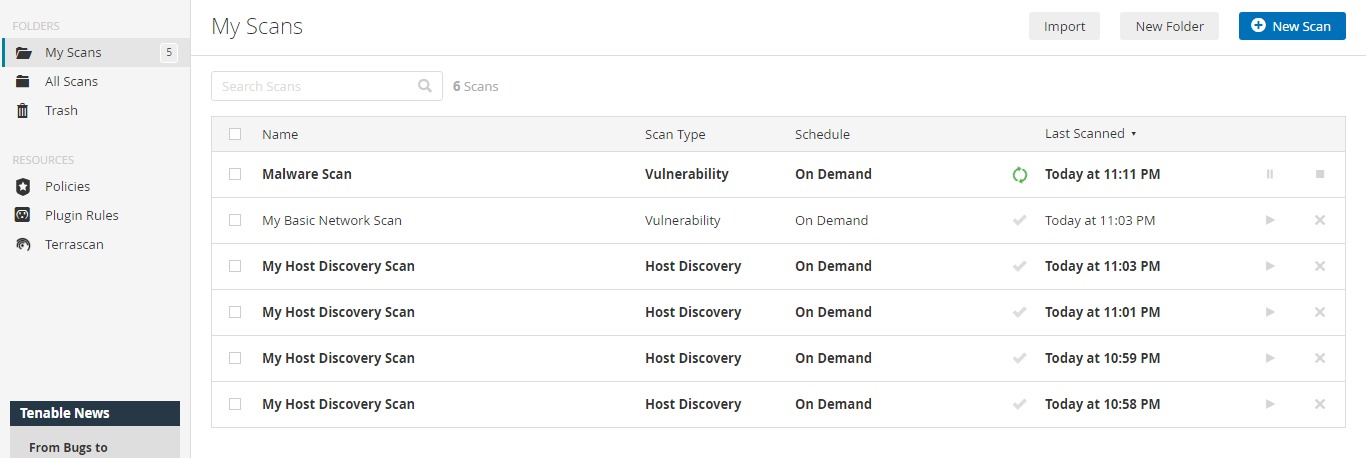
**Hands-on Assessment:**

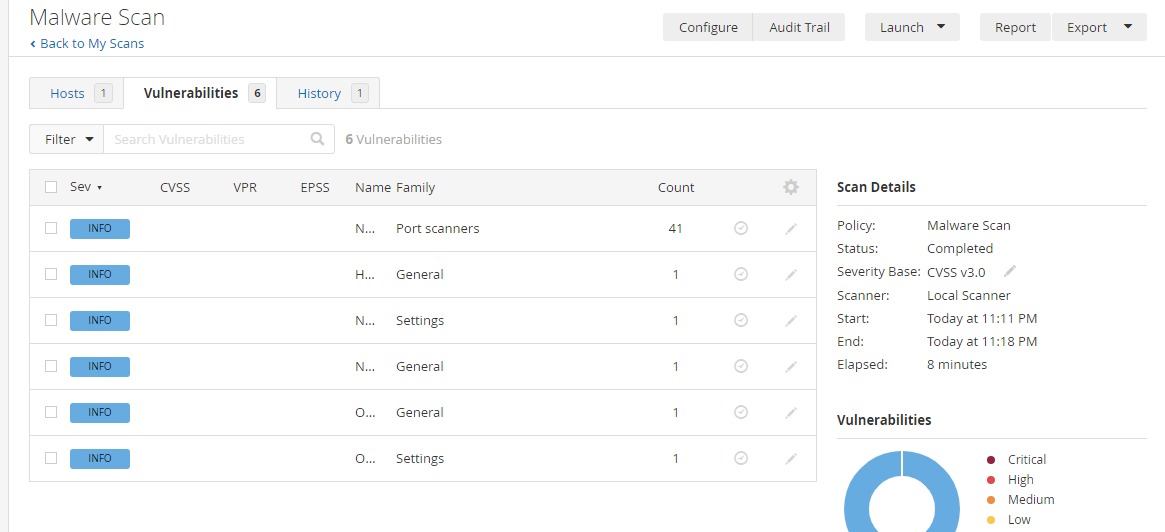
**Automated Tools:**

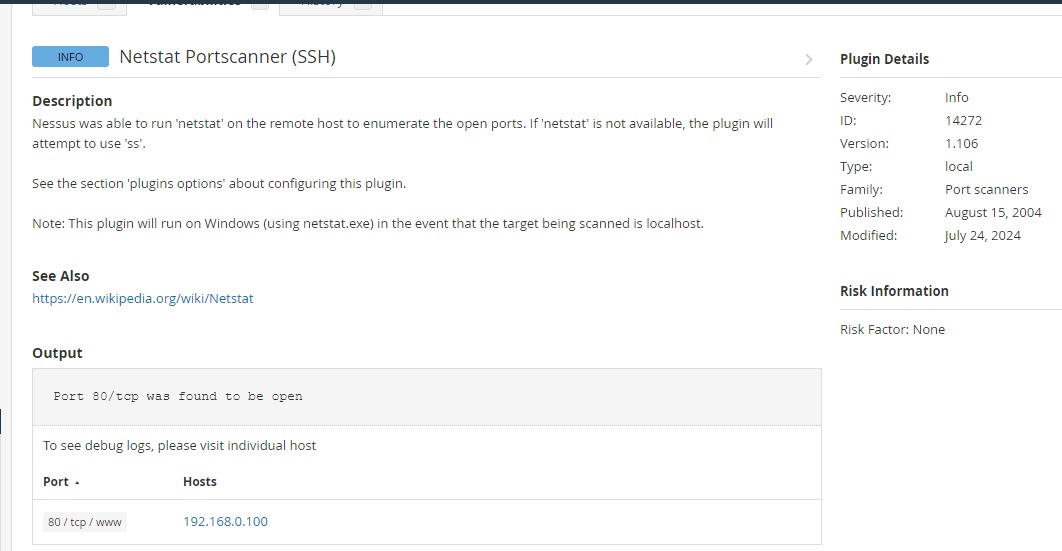
**Nessus:** Nessus is a popular vulnerability scanner developed by Tenable, used to detect security flaws in systems and networks. It performs thorough scans to identify vulnerabilities such as misconfigurations, weak passwords, missing patches, and more. Nessus provides detailed reports on identified issues, including severity ratings, and often suggests remediation steps. It is widely used by IT security professionals for network auditing and vulnerability assessment due to its robust scanning capabilities and ease of use.





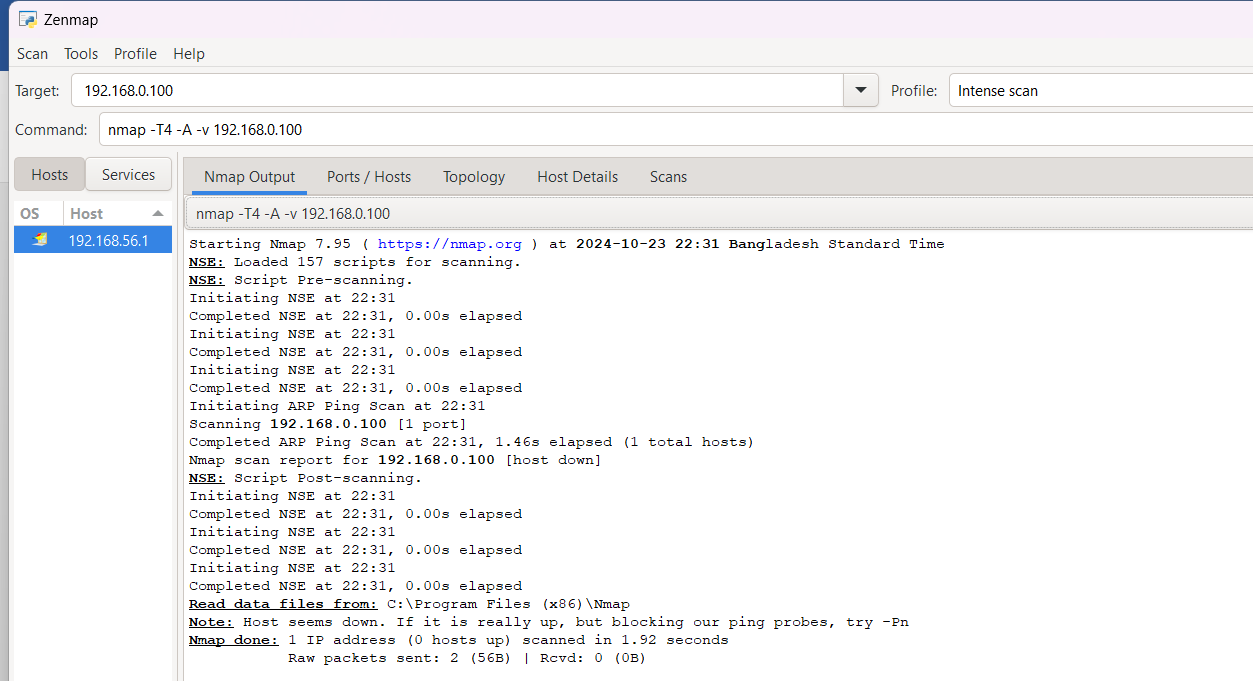


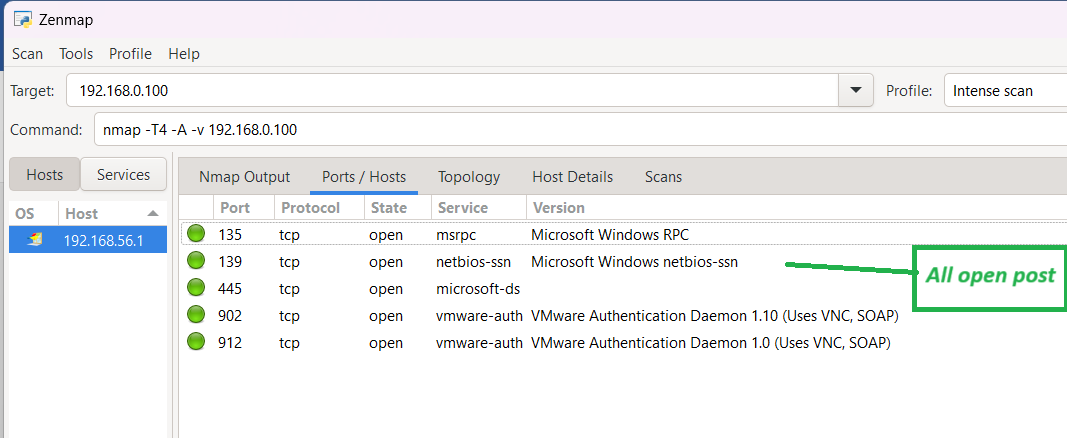




**Manual Tools:**

**Nmap:** Nmap (Network Mapper) is a widely used open-source tool for network discovery and security auditing. It is primarily used to scan and map networks, identify open ports, services running on hosts, and detect potential vulnerabilities. Nmap can also help with tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It supports various types of scanning techniques, such as TCP, SYN, and UDP scans, and is highly regarded by both network administrators and security professionals for its versatility and power.





**Manual Analysis:**

**Burp Suite:** Burp Suite is a powerful cybersecurity tool used for web application security testing. Developed by PortSwigger, it provides a comprehensive platform for identifying vulnerabilities like SQL injection, XSS (cross-site scripting), and others in web applications. Burp Suite includes features such as a proxy server for intercepting HTTP/S traffic, a scanner for automated vulnerability discovery, an intruder tool for automated custom attacks, and repeater for manual testing. It's widely used by penetration testers, security researchers, and ethical hackers to audit web applications effectively.

