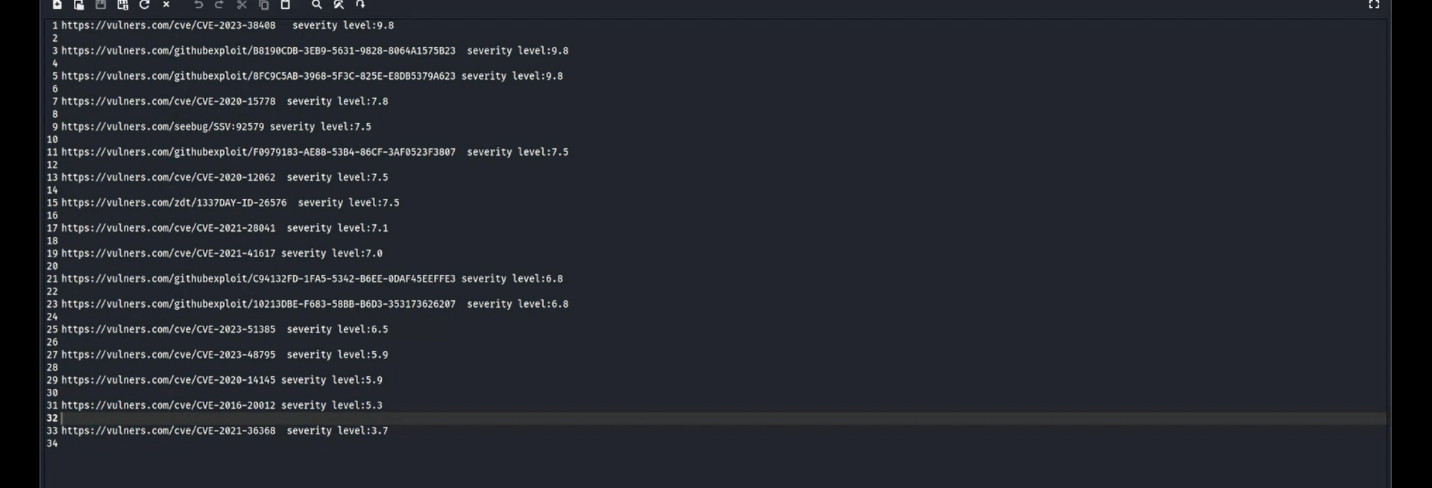
**UneeQ Interns – Cyber Security Internship**

**Vulnerability Assessment Report**

Here are all the vulnerable CVEs I’ve Found



Here Are The Mitigation Strategies :-

1-Technical Controls: This covers both hardware and software that is used to protect systems, networks and organizations. These include firewalls, intrusion detection systems (IDS), identification and authentication mechanisms, password management, and encryption. Endpoint security defenses are an important part of this.

2-Physical Access Controls: For example, security guards, perimeter security, video cameras, locks, limited access.

3-Compliance Controls: These include the various policies and procedures that an organization is obligated to have in place in order to be compliant with necessary laws and regulations. For example, internal auditing, monitoring, and awareness training.

4-Procedural Controls: Procedural controls usually take the form of standard operating procedures (SOPs) and “user manuals” such as an Incident Response plan.

**Examples From The Findings:-**

