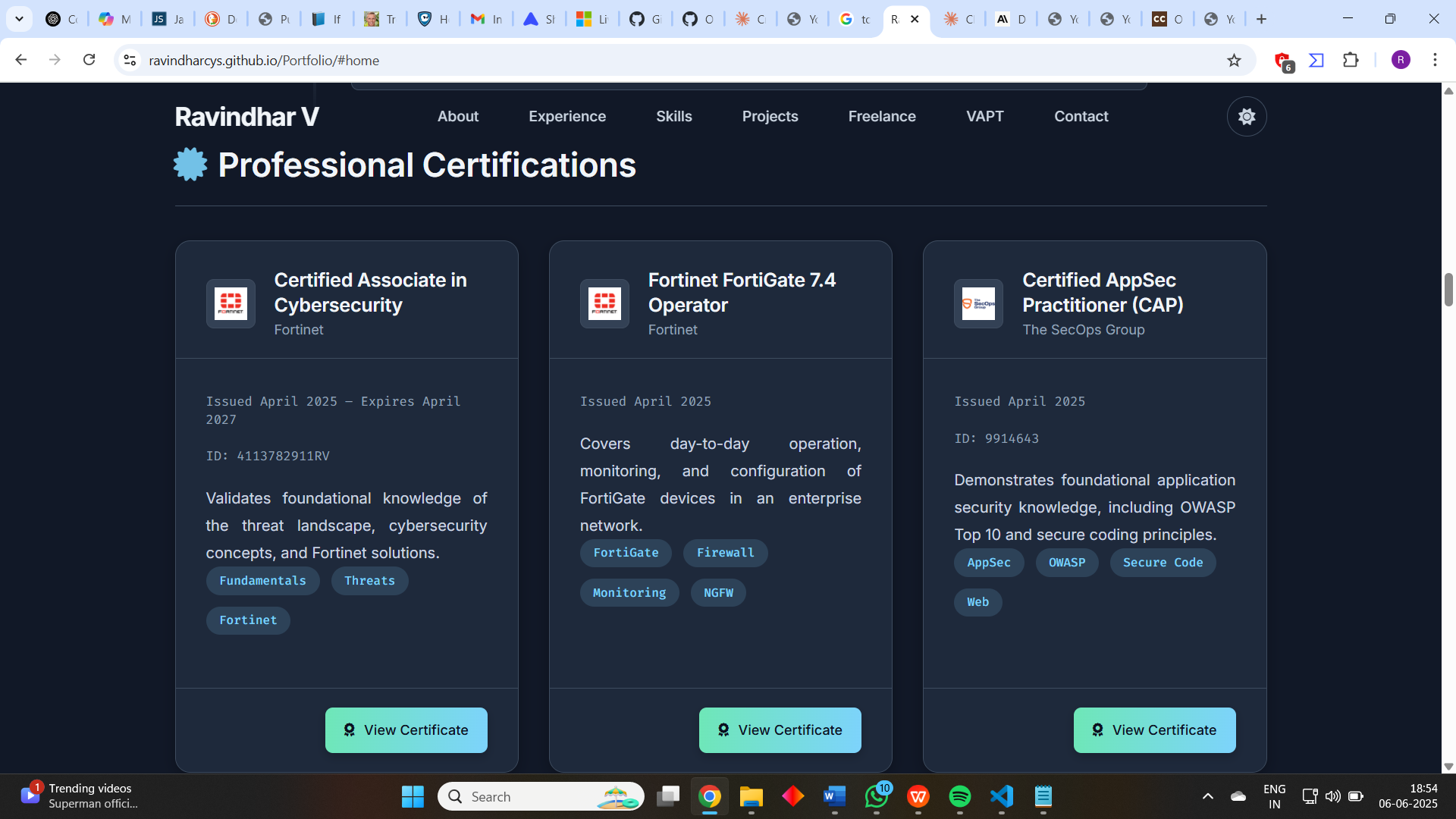
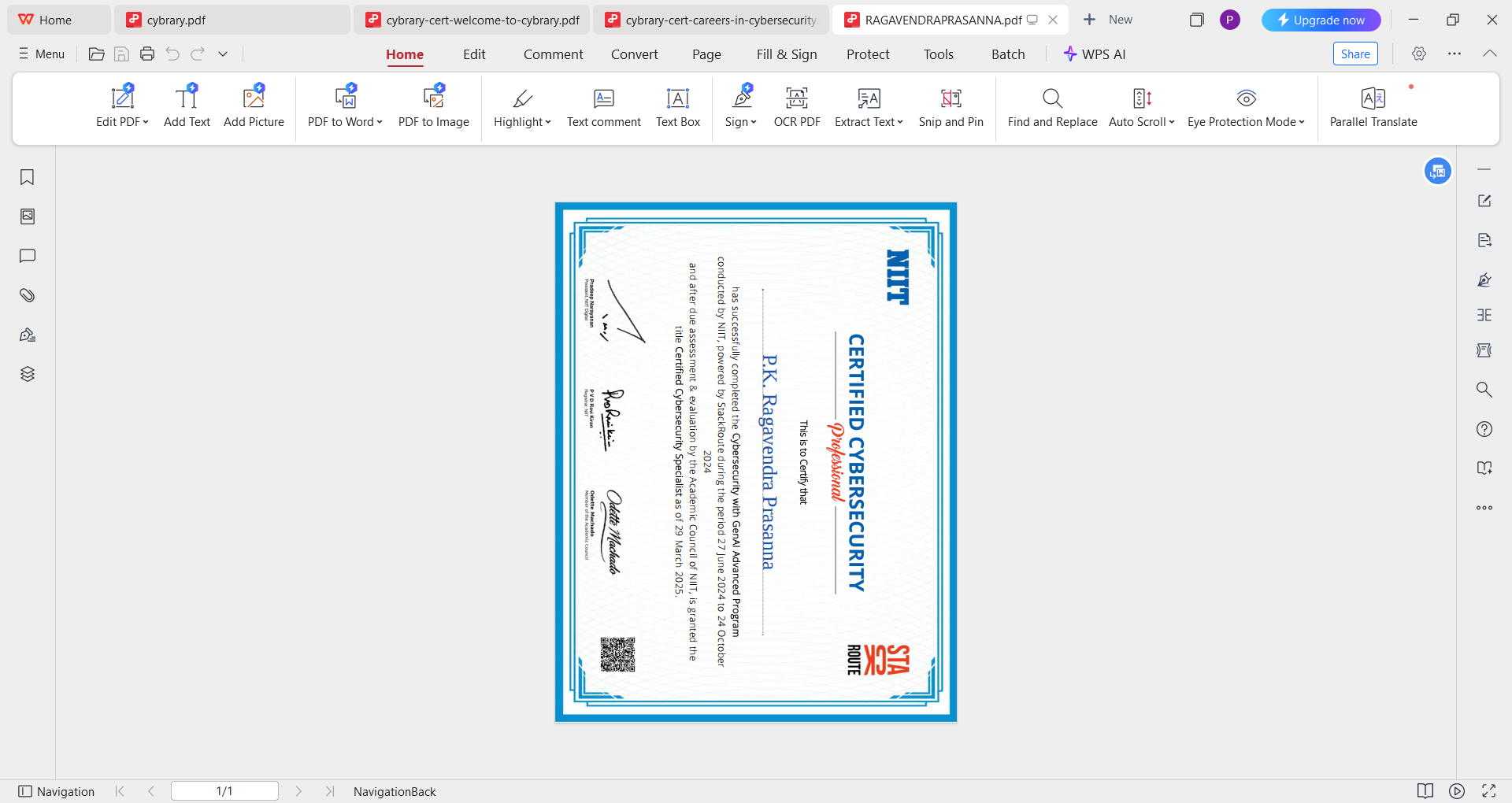
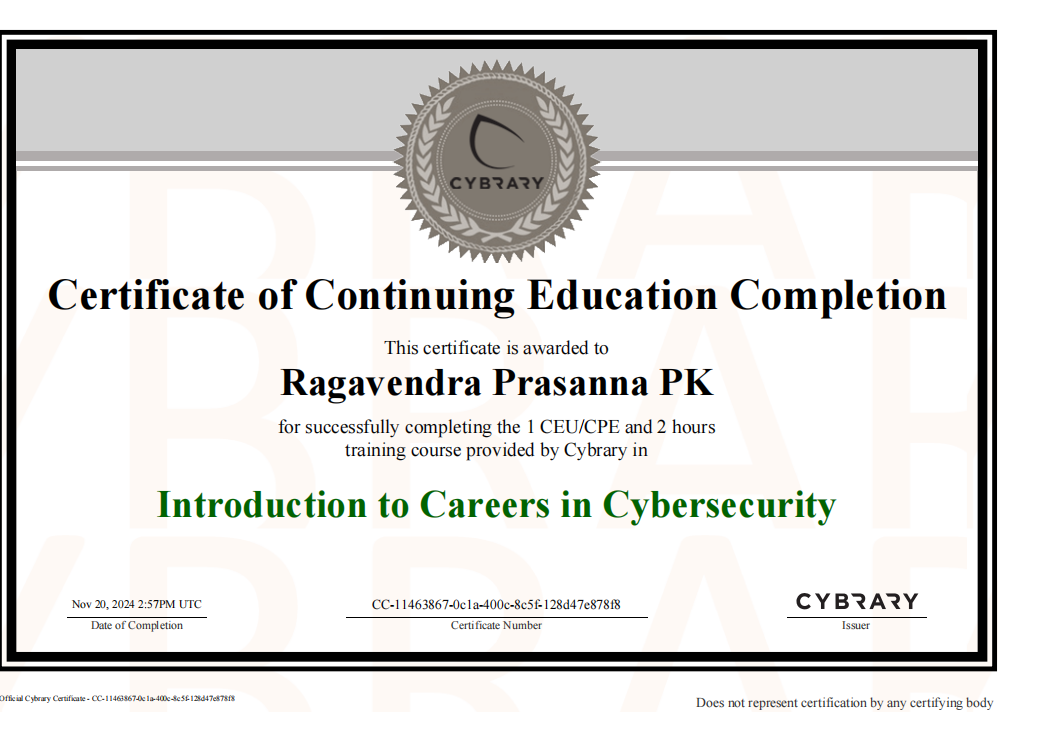
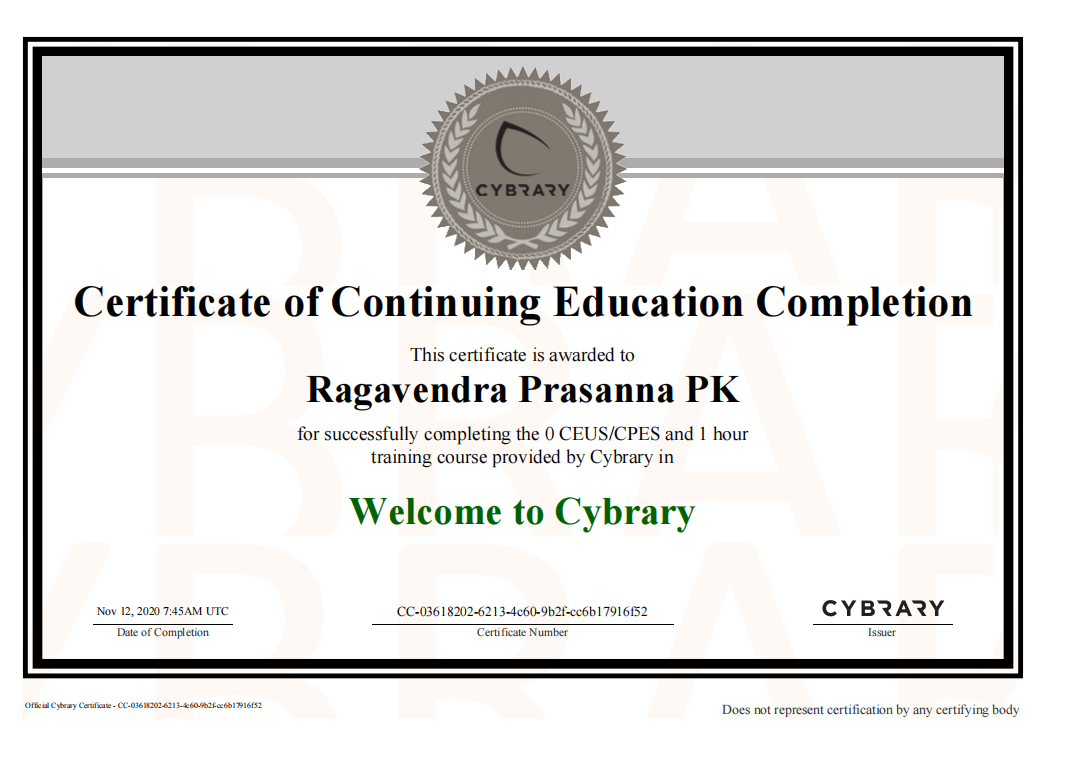
In certificaten see the below sample pic

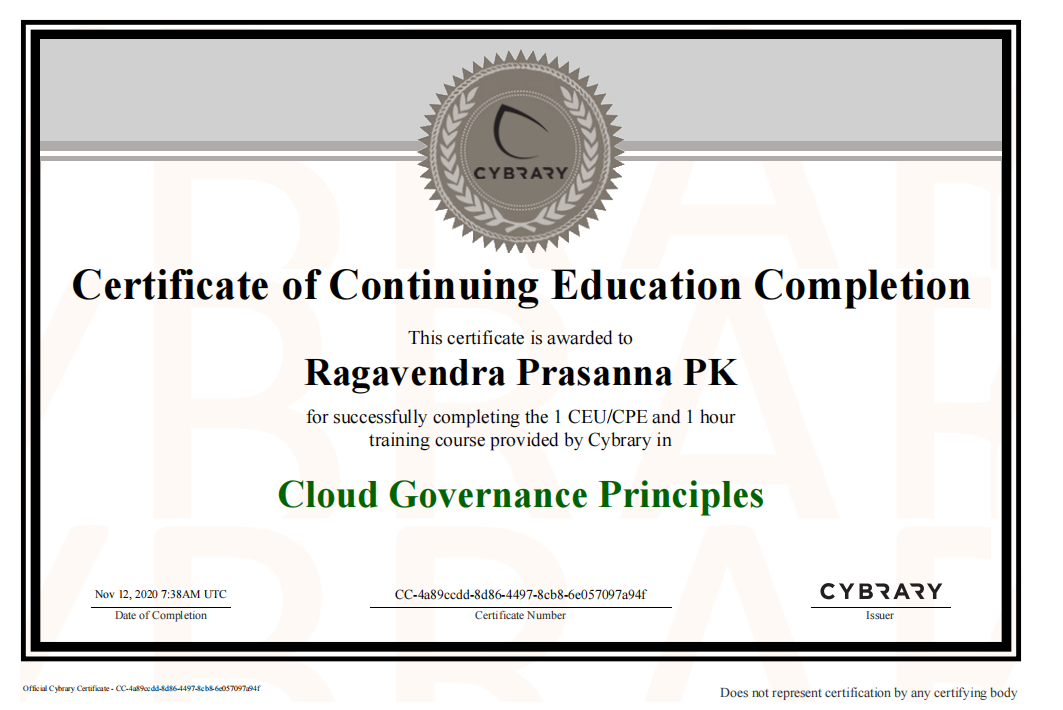


1



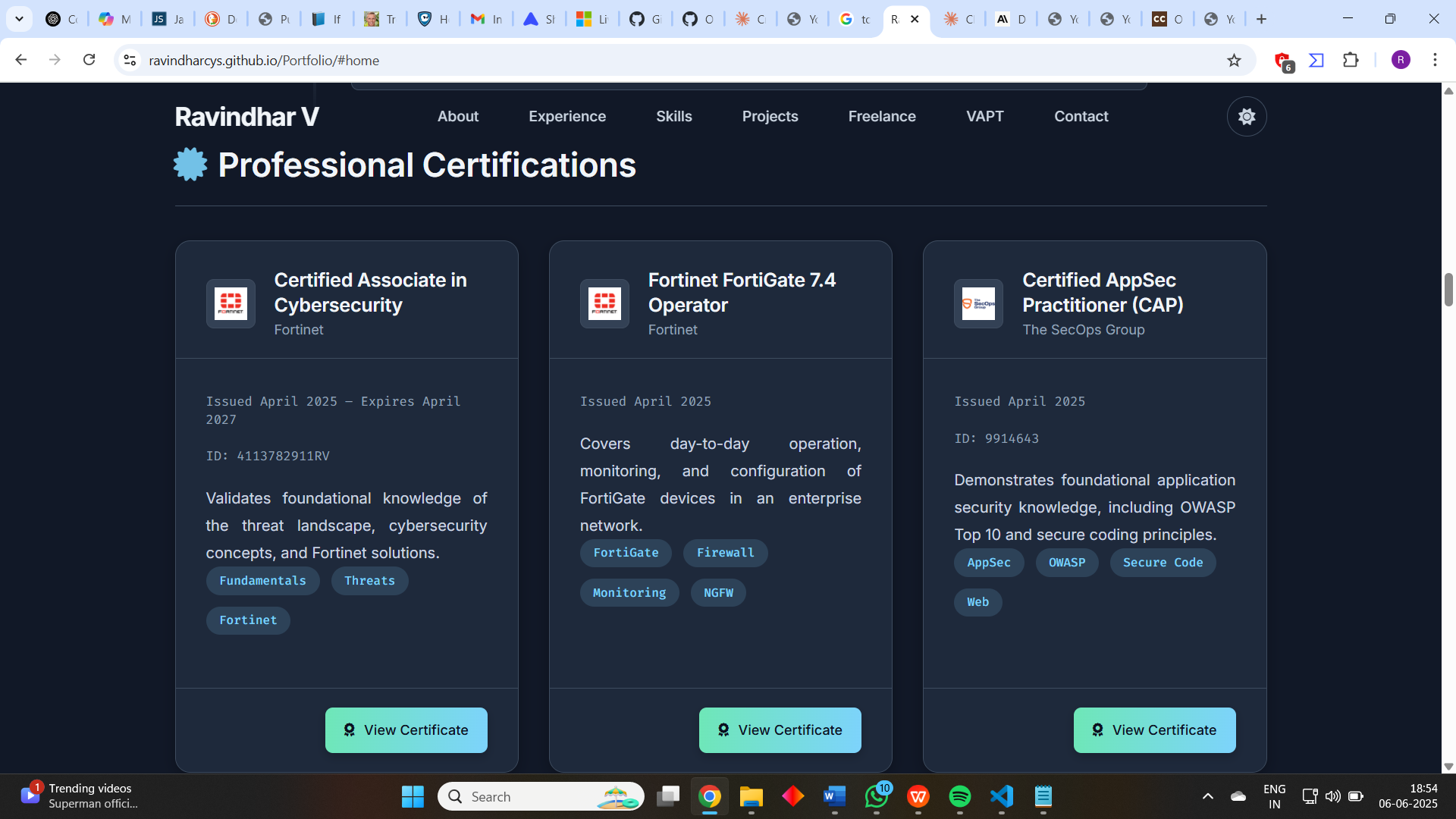
2

 3

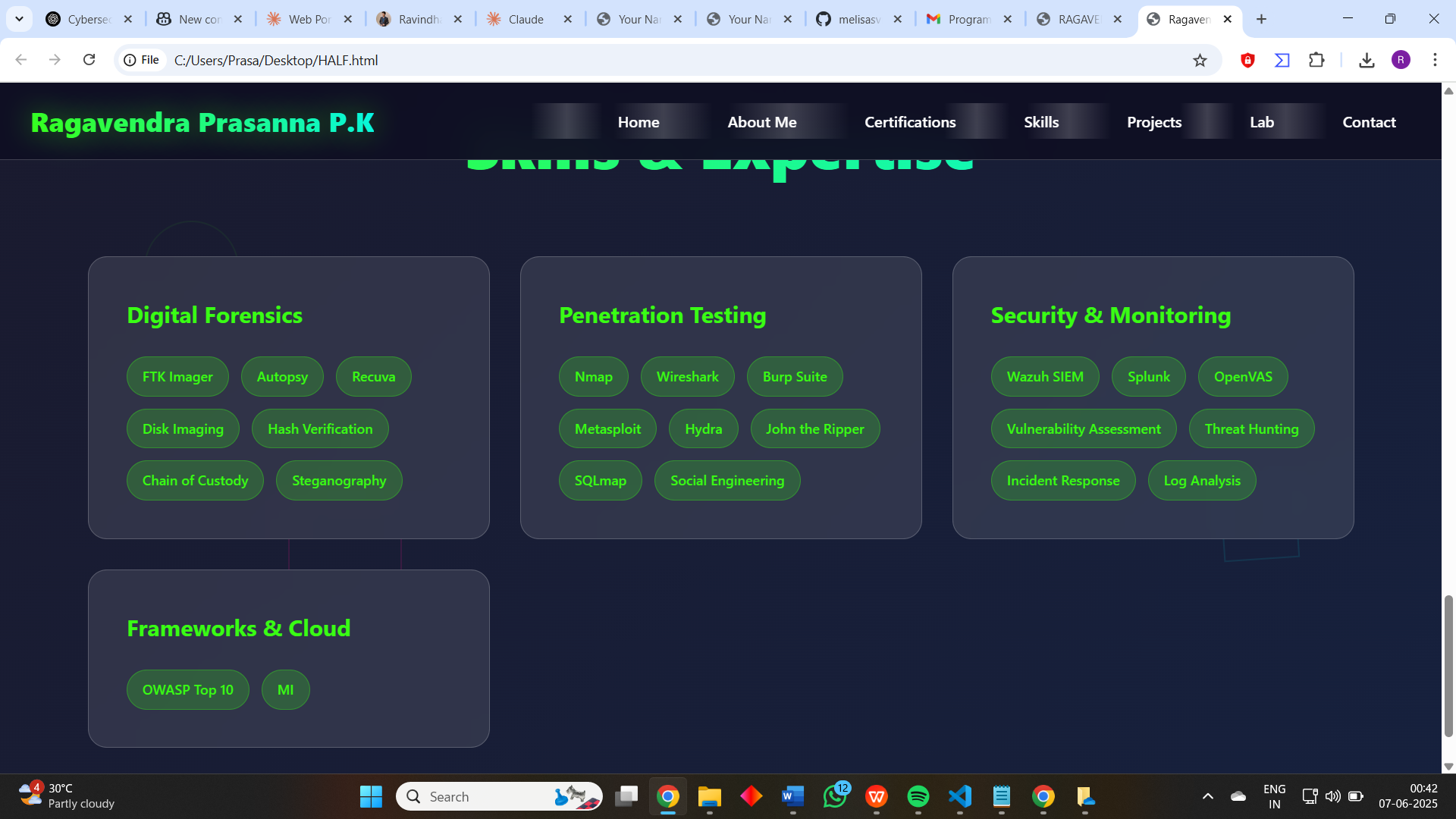


4

Pic to first showing opion like

like this then if we click it has to show the respective picture

old code left alone on mttre attck due to freeee pass expired



Make these small green like clickable when click it the below has to show the below info for its respectively to its name asiisgn it

**Digital Forensics**

* **FTK Imager:** FTK Imager is a standalone disk imaging tool (part of AccessData’s Forensic Toolkit) that creates bit-for-bit copies of storage media for forensic analysis. It calculates MD5 and SHA1 hash values to verify that the forensic image matches the original data[en.wikipedia.org](https://en.wikipedia.org/wiki/Forensic_Toolkit#:~:text=FTK%20is%20also%20associated%20with,4). I have used FTK Imager to capture disk images and verify their hash integrity in digital forensics labs.
* **Autopsy:** Autopsy is an open-source digital forensics platform that provides a graphical interface to The Sleuth Kit and other tools, automating tasks like hash matching, keyword searching, and artifact extraction[sumble.com](https://sumble.com/tech/autopsy#:~:text=Autopsy%20is%20a%20digital%20forensics,disk%20images%20and%20recover%20evidence). I used Autopsy in coursework to analyze disk images and recover evidence from digital media.
* **Recuva:** Recuva is a Windows-based undelete and data recovery program that can recover deleted files from internal drives, USB sticks, memory cards, and other storage devices[en.wikipedia.org](https://en.wikipedia.org/wiki/Recuva#:~:text=Recuva%20,developed%20by%20%2062). I used Recuva in lab exercises to restore accidentally deleted files and understand file recovery techniques.
* **Disk Imaging:** Disk imaging is the process of creating an exact bit-for-bit copy of a storage device, preserving all files, metadata, and filesystem structure for analysis[en.wikipedia.org](https://en.wikipedia.org/wiki/Disk_image#:~:text=Forensic%20imaging%20is%20the%20process,how%20the%20crime%20was%20committed). In my labs, I created disk images (using tools like FTK Imager or dd) of drive contents to examine them without altering original evidence.
* **Hash Verification:** Hash verification involves computing cryptographic hashes (such as MD5 or SHA1) of data to confirm integrity. Forensic tools like FTK Imager calculate these hashes to ensure a disk image has not been altered[en.wikipedia.org](https://en.wikipedia.org/wiki/Forensic_Toolkit#:~:text=FTK%20is%20also%20associated%20with,4)[en.wikipedia.org](https://en.wikipedia.org/wiki/Disk_image#:~:text=Forensic%20imaging%20is%20the%20process,how%20the%20crime%20was%20committed). I routinely verify hash values of forensic images and files to prove that evidence has remained unchanged during analysis.
* **Chain of Custody:** Chain of custody is a documented process that tracks the handling of evidence from collection through analysis, noting each person who accessed it and when[csrc.nist.gov](https://csrc.nist.gov/glossary/term/chain_of_custody#:~:text=A%20process%20that%20tracks%20the,under%20Chain%20of%20Custody). I practiced chain-of-custody procedures in simulated investigations, carefully logging each step to maintain evidence validity.
* **Steganography:** Steganography is the practice of hiding secret data within ordinary files or messages to avoid detection[techtarget.com](https://www.techtarget.com/searchsecurity/definition/steganography#:~:text=Steganography%20is%20the%20technique%20of,to%20write). I experimented with steganography in a cybersecurity project, embedding and uncovering hidden messages in image files to understand covert communication techniques.

**Penetration Testing**

* **Nmap:** Nmap ("Network Mapper") is a free, open-source utility for network discovery and security auditing[nmap.org](https://nmap.org/#:~:text=Nmap%20%28,runs%20on%20all%20major%20computer). It scans networks to identify live hosts, open ports, services, and operating systems. I have used Nmap to perform network reconnaissance and port scanning in penetration testing labs.
* **Wireshark:** Wireshark is a free, open-source network protocol analyzer that captures and inspects network packets[en.wikipedia.org](https://en.wikipedia.org/wiki/Wireshark#:~:text=Wireshark%20is%20a%20free%20and,5). It is widely used for network troubleshooting, protocol analysis, and security monitoring. In coursework, I used Wireshark to capture traffic and analyze packets for protocol details and potential issues.
* **Burp Suite:** Burp Suite is a proprietary web application security testing suite (developed by PortSwigger) used for finding and exploiting vulnerabilities in web apps[en.wikipedia.org](https://en.wikipedia.org/wiki/Burp_Suite#:~:text=Burp%20Suite%20is%20a%20proprietary,of%20automatable%20web%20tools%20like). It includes tools like an intercepting proxy, scanner, and repeater to facilitate web penetration testing. I used Burp Suite to intercept HTTP requests and test web forms and APIs for security flaws during class exercises.
* **Metasploit:** Metasploit Framework is an open-source penetration testing platform that provides tools for developing and executing exploit code against target machines[imperva.com](https://www.imperva.com/learn/application-security/metasploit/#:~:text=The%20Metasploit%20Project%20is%20a,code%20on%20remote%20target%20systems). It contains a large collection of exploits, payloads, and auxiliary modules. I practiced using Metasploit to exploit known vulnerabilities (e.g., on vulnerable virtual machines) and gain shell access in labs.
* **Hydra:** Hydra (THC Hydra) is a fast, parallelized password-cracking tool that performs brute-force and dictionary attacks against network login services[en.wikipedia.org](https://en.wikipedia.org/wiki/Hydra_(software)#:~:text=Hydra%20,defined%20patterns). It supports many protocols (FTP, SSH, HTTP, etc.) for attempting to guess usernames and passwords. I used Hydra during penetration testing exercises to crack weak credentials on target systems.
* **John the Ripper:** John the Ripper is an open-source password auditing and recovery tool available for multiple platforms[openwall.com](https://www.openwall.com/john/#:~:text=John%20the%20Ripper%20password%20cracker). It is typically used to perform brute-force or dictionary attacks on password hashes. In projects, I employed John the Ripper to crack password hashes extracted from compromised systems, helping reinforce lessons on password security.
* **SQLmap:** sqlmap is an open-source penetration testing tool that automates the detection and exploitation of SQL injection vulnerabilities in web applications[sqlmap.org](https://sqlmap.org/#:~:text=sqlmap%20is%20an%20open%20source,band%20connections). It can enumerate databases, extract data, and even execute commands on the database server. I used SQLmap in web-security labs to identify SQL injection points and dump sample databases.
* **Social Engineering:** Social engineering is a technique that uses psychological manipulation to trick people into revealing confidential information or performing actions[en.wikipedia.org](https://en.wikipedia.org/wiki/Social_engineering_(security)#:~:text=In%20the%20context%20of%20information,to%20take%20an%20action%20that). Common examples include phishing, baiting, and pretexting. I studied social engineering by analyzing phishing simulations and learning how to recognize and prevent these attacks.

**Security & Monitoring**

* **Wazuh SIEM:** Wazuh is a free, open-source security platform that unifies SIEM (Security Information and Event Management) and XDR capabilities for threat detection and compliance[documentation.wazuh.com](https://documentation.wazuh.com/current/getting-started/index.html#:~:text=Wazuh%20is%20a%20free%20and,based%20environments). It collects and analyzes log data from endpoints and cloud workloads to detect intrusions and policy violations. I set up Wazuh agents and dashboards to gather logs and trigger alerts in a home lab environment.
* **Splunk:** Splunk is a data platform that captures, indexes, and correlates machine-generated data (logs) to facilitate searching, analysis, and visualization[en.wikipedia.org](https://en.wikipedia.org/wiki/Splunk#:~:text=Splunk%20Inc,5). It is widely used for security monitoring, incident investigation, and operational intelligence. I have used Splunk in coursework to ingest log data, search for indicators of compromise, and build real-time security dashboards.
* **OpenVAS:** OpenVAS (Open Vulnerability Assessment Scanner) is a comprehensive open-source vulnerability scanning tool within Greenbone Vulnerability Management[en.wikipedia.org](https://en.wikipedia.org/wiki/OpenVAS#:~:text=OpenVAS%20,2). It performs authenticated and unauthenticated scans to identify security issues and misconfigurations. In labs, I ran OpenVAS scans on target networks to find known vulnerabilities and learned to interpret the reports.
* **Vulnerability Assessment:** Vulnerability assessment is a systematic process of identifying and evaluating security weaknesses in a system or network[imperva.com](https://www.imperva.com/learn/application-security/vulnerability-assessment/#:~:text=What%20is%20vulnerability%20assessment). It involves scanning for known vulnerabilities and ranking them by severity. I performed vulnerability assessments using tools like Nmap and OpenVAS, reviewing the findings to recommend remediation steps in coursework.
* **Threat Hunting:** Threat hunting is a proactive security practice where analysts actively search through networks or datasets to find malicious activities that existing tools might miss[ibm.com](https://www.ibm.com/think/topics/threat-hunting#:~:text=Threat%20hunting%2C%20also%20known%20as,cyberthreats%20in%20an%20organization%27s%20network). It goes beyond automated alerts by using hypotheses and analytics to uncover hidden threats. I practiced threat hunting by analyzing system logs and alerts to detect unusual patterns indicating a potential breach.
* **Incident Response:** Incident response is an organized and strategic approach to detecting, containing, and resolving cybersecurity incidents in order to minimize damage, recovery time, and costs[techtarget.com](https://www.techtarget.com/searchsecurity/definition/incident-response#:~:text=Incident%20response%20is%20an%20organized%2C,recovery%20time%20and%20total%20costs). It involves predefined steps and teams to handle incidents efficiently. I participated in simulated incident response exercises, following playbooks to investigate and mitigate mock security breaches.
* **Log Analysis:** Log analysis is the process of reviewing computer-generated event logs to detect and diagnose problems, identify anomalies, or uncover security incidents[crowdstrike.com](https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/log-analysis/#:~:text=Log%20analysis%20is%20the%20process,regulations%20or%20review%20user%20behavior). Logs can include system events, application messages, and network traffic details. In security labs, I regularly analyzed logs (using tools like Splunk) to troubleshoot issues and spot suspicious behavior or attacks.

**Frameworks & Cloud**

* **OWASP Top 10:** The OWASP Top 10 is a widely recognized list of the top ten most critical web application security risks, published by the Open Web Application Security Project[owasp.org](https://owasp.org/www-project-top-ten/#:~:text=The%20OWASP%20Top%2010%20is,security%20risks%20to%20web%20applications). It highlights common vulnerabilities like injection, broken access control, and cross-site scripting. I learned the OWASP Top 10 and applied it by testing web applications against these common risks.
* **MITRE ATT&CK:** MITRE ATT&CK is a comprehensive, publicly accessible knowledge base of adversary tactics and techniques based on real-world cyber attacks[attack.mitre.org](https://attack.mitre.org/#:~:text=MITRE%20ATT%26CK%C2%AE%20is%20a%20globally,cybersecurity%20product%20and%20service%20community). Security professionals use it to model threat behaviors and map detected activities. I have mapped penetration testing tools and techniques from projects to MITRE ATT&CK to understand the tactics behind each action.
* **NIST:** The NIST Cybersecurity Framework (CSF) provides guidelines and best practices for managing cybersecurity risk[nist.gov](https://www.nist.gov/cyberframework#:~:text=Cybersecurity%20Framework). It organizes security controls into five core functions (Identify, Protect, Detect, Respond, Recover). I applied the NIST CSF categories in a group project to evaluate the controls implemented in a sample organization’s security policy.
* **ISO 27001:** ISO 27001 is an international standard for information security management systems (ISMS) that specifies requirements to protect confidentiality, integrity, and availability of data[itgovernanceusa.com](https://www.itgovernanceusa.com/iso27001#:~:text=ISO%2FIEC%2027001%3A2022%20,information%20managed%20by%20third%20parties). It provides a structured framework for risk management and controls. In my studies, I used ISO 27001 controls to perform a gap analysis of a mock company’s security management system.
* **AWS EC2:** Amazon EC2 (Elastic Compute Cloud) is a cloud service providing scalable, on-demand virtual server instances[docs.aws.amazon.com](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html#:~:text=Amazon%20Elastic%20Compute%20Cloud%20,scale%20down%29%20again). Users can launch virtual machines with configurable CPU, memory, storage, and networking. I launched EC2 instances to host web and application servers in AWS, and practiced configuring security groups and SSH access for them.

I see a mild bug in menu option

In email [prasannasharma79@gmail.com](mailto:prasannasharma79@gmail.com)

Remove phone number box