

# MD.HASIB ISLAM

+8801773743025

[ihasib199@gmail.com](mailto:ihasib199@gmail.com)

<https://github.com/khuttess>

[hasib.live](http://hasib.live)



I'm Md. Hasib Islam, a Computer Science and Engineering graduate from Bangladesh with a strong focus on cybersecurity. I currently work with HelpYard, where I specialize in web and network penetration testing, bug bounty hunting, and the development of practical security tools.

Throughout my journey in cybersecurity, I have designed and developed more than ten security-focused projects, including a malware behavior analysis system, a graphical password authentication model, and several penetration testing utilities aimed at identifying real-world vulnerabilities. These projects reflect both my technical skills and my commitment to solving complex security challenges.

I strongly believe that cybersecurity is a field driven by continuous learning and adaptation. To stay aligned with evolving threats and technologies, I actively contribute to the cybersecurity community through open-source projects, technical write-ups, and knowledge sharing. My goal is to continually grow as a security professional while helping organizations strengthen their digital defenses.

## Education

---

- ✓ Varendra University Rajshahi, Bachelor of Science in Computer Science and Engineering, Pass 2024.( 2.36 CGPA) .
- ✓ Naogaon Govt. Collage, Higher Secondary Certificate In Science, Pass 2019.(3.50GPA) .
- ✓ Naogaon KD Govt. High School, Secondary School Certificate In Science, pass 2017.(5.00GPA) .

## Certifications

---

- ❖ IBM:  
[Cybersecurity Careers](#) .
- ❖ HP Foundation:  
[Professional Networking For Career Growth](#) ,  
[Cybersecurity Awareness](#) .
- ❖ Skillup by SimpliLearn:  
[CISSP](#) , [Cyber Security](#) , [Ethical Hacking](#) , [Kali Linux](#) .
- ❖ Greate Learning:  
[Network Security](#) , [Mobile Platforms and Network Architecture](#) , [Advanced Cyber Security-Threats and Governance](#) , [Ethical Hacking](#) .

## Skills

<b>Penetration Testing</b>	<b>Bug Bounty</b>
<ul style="list-style-type: none"> <li>➤ Web Application Testing</li> <li>➤ API Security</li> <li>➤ Network Penetration</li> <li>➤ Wireless Security</li> <li>➤ Social Engineering</li> <li>➤ OWASP Top10</li> </ul>	<ul style="list-style-type: none"> <li>➤ IDOR &amp; Access Control</li> <li>➤ XSS &amp; Injection</li> <li>➤ CSRF &amp; XXE</li> <li>➤ Authentication ByPass</li> <li>➤ OAuth Attacks</li> </ul>
<b>Security Tools</b>	<b>Programming</b>
<ul style="list-style-type: none"> <li>➤ Burp Suite</li> <li>➤ Metasploit</li> <li>➤ Nmap</li> <li>➤ Wireshark</li> <li>➤ Hashcat</li> <li>➤ Bettercap</li> </ul>	<ul style="list-style-type: none"> <li>➤ Python</li> <li>➤ JavaScript</li> <li>➤ Bash Scripting</li> <li>➤ PowerShell</li> <li>➤ HTML,CSS</li> <li>➤ C/C++</li> </ul>
<b>Marketing &amp; Branding</b>	<b>Business Strategy</b>
<ul style="list-style-type: none"> <li>➤ Brand Strategy</li> <li>➤ Growth Hacking</li> <li>➤ Content Marketing</li> <li>➤ Community Buiding</li> <li>➤ Social Media</li> </ul>	<ul style="list-style-type: none"> <li>➤ Go-to-Market Strategy</li> <li>➤ Stantup Planning</li> <li>➤ Revernue Modeling</li> <li>➤ Investor Relations</li> <li>➤ Product Launch</li> <li>➤ Market Research</li> </ul>
<b>Risk Management</b>	<b>Startup &amp; Product</b>
<ul style="list-style-type: none"> <li>➤ Digital Risk Assessment</li> <li>➤ Operational Risk</li> <li>➤ Brand Risk</li> <li>➤ Compliance planning</li> <li>➤ Incident Response</li> <li>➤ Crisis Management</li> </ul>	<ul style="list-style-type: none"> <li>➤ Product Development</li> <li>➤ Tean Leadership</li> <li>➤ Ambassador Programs</li> <li>➤ Platform Sealing</li> <li>➤ User Acquisition</li> <li>➤ Pitch Decks</li> </ul>

## Projects

---

- ❖ **CS-GPAS-Client-Side-Graphical-Password-Authentication-System** [GitHub](#)
  - Traditional passwords are weak and prone to attacks. This paper introduces a client-side Graphical Password Authentication System using HTML, CSS, and JavaScript. Users select a sequence of four images to log in. Data is stored in localStorage. The system boosts security with image randomization and no backend dependency.
- ❖ **Brute-Force-Attack-Simulator-for-passwords** [GitHub](#)
  - A mobile-friendly brute-force attack simulator in a single HTML file. Users enter a password, start the attack, and watch real-time attempts as the app tries all combinations to crack it. Features live progress, a clean modern UI (max 600×350px), async JS logic, and smooth demo performance.

- ❖ **Local-Voice-Controlled-Assistant** [GitHub](#)
  - The "Local Voice-Controlled Assistant" project is a prototype demonstrating a voice command pipeline. It currently functions as a proof-of-concept, with a broader vision for advanced features outlined but not yet implemented.
- ❖ **Home-Automation-System** [GitHub](#)
  - A smart home automation system seamlessly integrates devices, allowing control of lighting, security, climate, and appliances via apps or voice commands, enhancing convenience, energy efficiency, and security.
- ❖ **AI Phishing Detector** [GitHub](#)
  - This repository contains an experimental implementation of an AI-based phishing detection system. It combines header analysis, content intent, URL inspection, and attachment features to classify emails.
- ❖ **AI SOC Analyst Copilot** [GitHub](#)
  - A Local-First Security Operations Center (SOC) Assistant designed to ingest, normalize, and analyze security logs locally. Using Retrieval-Augmented Generation (RAG), it provides context-aware AI analysis without ever sending sensitive data to the cloud.

## Declaration

---

I hereby declare that all the details mentioned above are in accordance with the truth and fact as per my knowledge and I hold the responsibility for the correctness of the above-mentioned particulars.

**Place:**

Naogaon,Rajshahi,Bangladesh.  
Email: [ihasib199@gmail.com](mailto:ihasib199@gmail.com)  
Phone: +8801773743025  
GitHub: [github.com/khutttes](https://github.com/khutttes)  
Portfolio: [hasib.live](https://hasib.live)