RATNADEEP BOSE

Full-Stack Developer • Cybersecurity Expert • Educator

West Bengal, India | +91 7001005520 | ratnadeepbusiness321@gmail.com

LinkedIn: linkedin.com/in/ratnadeepbose | GitHub: github.com/ratnadeepbose

SUMMARY

Passionate and results-driven full-stack developer, cybersecurity specialist, and educator with a proven record of creating robust, secure web applications and actively contributing to enterprise security through bug bounty hunting. Recognized for critical vulnerability discoveries benefiting 20+ companies, including Porsche, Remitly, M-Pesa, and REI. Adept at translating complex technical issues into actionable insights for diverse audiences. Dedicated teaching faculty with a talent for developing engaging, accessible curricula that drive measurable student success.

TECHNICAL SKILLS

- **Languages:** HTML5, CSS3, JavaScript, React, Node.js, Python, SQL
- **Cybersecurity:** Kali Linux, Bug Bounty (HackerOne, Bugcrowd), nmap, ffuf, httpx, nikto, Burp Suite, OWASP ZAP, penetration testing, CORS exploitation, subdomain takeover, API security, reconnaissance, vulnerability assessment, information disclosure, authentication bypass, WAF evasion
- **Development Tools:** Git, Docker, VMware, CI/CD, REST APIs, responsive design, database management
- **Education Tools:** Curriculum design, lesson planning, interactive teaching, student engagement, educational technology

KEY ACHIEVEMENTS

- Reported **50+ vulnerabilities** including **15+ critical findings** across fintech, automotive, and infrastructure domains; recognized by major organizations including Porsche, Remitly, M-Pesa, and REI (over **$2,000 in bounties and recognition**)
- Discovered **critical CORS misconfiguration** on Porsche identity platform allowing complete user data exfiltration
- Identified **critical subdomain takeover vulnerability** on Remitly financial infrastructure enabling potential phishing and malware hosting

- Successfully **bypassed WAF protections** on M-Pesa platform exposing internal configuration files and security keys
- Developed and launched **10+ secure, scalable web tools and applications** for productivity, education, and entertainment
- Improved student academic performance at Gurukul Jalpaiguri through tailored lesson plans and engaging educational materials

PROFESSIONAL EXPERIENCE

Web Developer Intern

➢ **Easy Solutions** | September 2025 – Present

- Developed and maintained business websites using modern web technology stacks; integrated REST APIs for seamless user experience
- Supported server management and deployment processes, increasing service uptime and overall performance
- Collaborated with cross-functional teams to deliver high-quality solutions for local businesses and organizations
- Gained hands-on experience in software deployment, debugging, and production environment management

Teaching Faculty

➢ **GURUKUL JALPAIGURI** | April 2025 – Present

- Design and deliver interactive courses in English, History, and Humanities for grades 6–12 with focus on student engagement
- Mentor students in writing skills, comprehension strategies, and exam preparation techniques for measurable academic improvement
- Create simplified study materials and innovative lesson plans that enhance understanding of complex concepts
- Cultivate a positive, supportive classroom environment encouraging communication, critical thinking, and independent problemsolving

Teaching Assistant (Internship)

➢ **GURUKUL JALPAIGURI | January 2025 – March 2025**

- Taught students using interactive lessons and simplified notes to enhance comprehension and engagement
- Mentored students in exam preparation and writing skills, contributing to improved academic performance

- Fostered a supportive learning environment that encourages critical thinking and creativity

Full-Stack Developer & Bug Bounty Hunter

➢ **HackerOne | Bugcrowd | Independent Projects** | October 2024 – Present

- Specialize in web application and API security; perform comprehensive reconnaissance, vulnerability assessment, and penetration testing for major platforms including financial services, automotive, and e-commerce
- Conduct end-to-end development of responsive, secure web applications for personal and open-source projects
- Maintain multi-VM development and testing environment using Kali Linux and Windows 11 with VMware for isolated workflows
- Utilize advanced security tools including nmap, ffuf, httpx, nikto, Burp Suite for vulnerability discovery and exploitation Contribute to enterprise security through responsible disclosure of critical vulnerabilities

Educator & Founder

➢ **Smart Learn Academy** | 2021 – Present

- Provide personalized coaching in English, History, Political Science, and Geography for students from grades 6–12
- Develop innovative teaching methodologies combining traditional arts and humanities education with modern technical knowledge
- Successfully mentor students in comprehensive academic development with focus on critical thinking and communication skills
- Create affordable, quality educational content accessible to diverse student populations

MAJOR PROJECTS

Aurevo – Fast-Fashion E-Commerce Platform

- Developed frontend features, product listing flows, and cart functionality for modern e-commerce experience
- Implemented performance optimizations ensuring smooth, responsive shopping experience across all devices
- Technologies: JavaScript, HTML5, CSS3, responsive design

Pacman Typing Test – Arcade Typing Game

- Created retro arcade-style typing game with engaging animations and sound effects
- Responsible for frontend development, game logic, and performance optimization
- Technologies: JavaScript, HTML5, CSS3, game development

Veronica – Ultimate Web Vulnerability Scanner

- Developed enterprise-grade web, API, and cloud vulnerability scanner with 50+ security checks
- Implemented multi-engine reconnaissance, API testing, continuous monitoring, and professional reporting features
- Designed for security teams and bug bounty hunters
- Technologies: Python, security automation, OWASP methodologies

Code OCR – Code Extraction Tool

- Built automated code extraction platform that scans folders and consolidates source code files
- Designed for code auditing, migration workflows, and quick code review processes
- Technologies: OCR, Python, automation, file processing

Indian Constitution Explorer

- Developed interactive web platform for browsing, searching, and studying the Constitution of India
- Implemented user-friendly interface presenting Articles, Schedules, and Amendments in accessible format
- Technologies: JavaScript, HTML5, CSS3, search algorithms, educational technology

Toolkit – 50+ Browser-Based Utilities

- Created comprehensive collection of client-side tools covering Text & Document, Links & Network, Security & Development, Study & Calculator, and Media & File categories
- All tools operate directly in browser without server requirements
- Technologies: JavaScript, HTML5, CSS3, client-side processing

Learn JavaScript – Interactive Learning Platform

- Developed comprehensive JavaScript handbook with 15 chapters covering core concepts
- Implemented practice sets, quiz functionality, and detailed explanations in simple language
- Features auto-generation of content and show answer functionality
- Technologies: JavaScript, HTML5, CSS3, educational technology

Dictionary – Fast Word Lookup Tool

- Built sleek, web-based dictionary with instant search functionality
- Implemented responsive, user-friendly interface with clear, precise definitions
- Technologies: JavaScript, API integration, responsive design

Notable Security Discoveries

Porsche Identity Platform – Critical CORS Misconfiguration

- Discovered critical cross-origin resource sharing misconfiguration allowing complete user data exfiltration
- Impact: Authentication bypass, complete user profile data theft
- Severity: Critical
- Recognition: HackerOne acknowledgment

Remitly – Critical Subdomain Takeover

- Identified unclaimed AWS S3 bucket enabling complete subdomain takeover of financial service infrastructure
- Impact: Potential phishing attacks, malware hosting, complete domain control
- Severity: Critical
- Recognition: Responsible disclosure acknowledgment

M-Pesa – WAF Bypass & Information Disclosure

- Successfully bypassed web application firewall protections using header manipulation techniques
- Exposed internal configuration files and security keys
- Impact: Internal infrastructure exposure, security control bypass
- Severity: High

REI API – Information Disclosure

- Uncovered unauthenticated access to internal API endpoints exposing reCAPTCHA keys and configuration data
- Impact: Security control bypass, internal infrastructure mapping
- Severity: High

Porsche Configurator – Business Intelligence Exposure

- Discovered permissive CORS policy exposing internal business data including vehicle configurations and pricing
- Impact: Competitive data leakage, business intelligence exposure
- Severity: Medium

EDUCATION

Bachelor of Arts in English (Minor: History, Political Science)
University of North Bengal | 2023 – 2027 (Expected)

- Interdisciplinary approach enhancing communication skills crucial for technical documentation and client interactions
- Actively integrating academic learning with practical development and security research
- Strong focus on analytical thinking, research methodologies, and effective communication

Additional Information

Availability: Open for remote work worldwide. Available for collaborations in web development, cybersecurity consulting, security assessments, and educational technology projects.

Languages: English (Fluent), Hindi (Fluent), Bengali (Native)

Specializations: Full-stack web development, ethical hacking, bug bounty hunting, web application security, penetration testing, API security, educational technology, curriculum design, and custom software solutions

References: Available upon request