AFTAB AHOMOD RIYAD (IZUMI)

Red Team & API Security Specialist | Security Automation Engineer | Offensive Security Researcher
Self-taught Cybersecurity & Automation Engineer

📍 Dhaka, Bangladesh • GMT+6 (Asia/Dhaka) • Remote Ready • Available for International Projects
📧 aftabahomodriyad@gmail.com
🔗 LinkedIn: linkedin.com/in/zeroizumi
🔗 Portfolio: https://portfolio-izumi.vercel.app
🔗 GitHub: (in development - to be published)
🔗 Upwork Profile: https://www.upwork.com/freelancers/~012d71f9fb100a123f
🔗 Fiverr: https://www.fiverr.com/s/xXRPgBx

PROFESSIONAL SUMMARY

Offensive Security Engineer and API Security Specialist with 6+ years of hands-on experience in red teaming, web application pentesting, and advanced security automation. Specialized in discovering critical authentication bypasses, API logic flaws, business logic vulnerabilities, and building automated reconnaissance systems that reduce manual assessment time by 70%.

Highly skilled in creating custom offensive tooling using Puppeteer, Node.js, Python, and Bash for offensive workflows, endpoint enumeration, session manipulation, JWT/OAuth exploitation, and exploit development. Proven expertise in fintech security, payment gateway analysis, reverse-engineering complex API flows, and GraphQL security testing.

Actively engaged in offensive security research, bug bounty programs (HackerOne, Bugcrowd), and red team simulation exercises — consistently delivering security outcomes aligned with real-world threat models and MITRE ATT&CK framework.

Key Differentiators:

- Developed proprietary API security framework (UltraAPI) adopted by security teams
- 98% client satisfaction with zero post-remediation security incidents
- Top 5% global ranking on TryHackMe offensive security platform
- Verified security researcher on major bug bounty platforms with disclosed vulnerabilities

---

CORE COMPETENCIES

Offensive Security & Penetration Testing

- Web & API Penetration Testing (OWASP Top 10, API Security Top 10)
- Authentication & Authorization bypass techniques
- API logic flaw discovery and exploitation
- Red Team simulation tactics (MITRE ATT&CK)
- Session & token analysis (JWT, OAuth 2.0, SAML)
- Business logic exploitation and abuse case discovery
- GraphQL security testing and introspection attacks
- Payment gateway security assessment

Security Automation & Engineering

- Automated reconnaissance frameworks (OSINT, subdomain enumeration)
- Browser automation for offensive workflows (Puppeteer, Selenium)
- Custom fuzzing toolkit development
- API endpoint discovery and enumeration automation
- Security tool integration and CI/CD pipeline security
- Custom scripting: JavaScript/Node.js, Python, Bash
- Webhook exploitation and callback abuse automation

Application & Infrastructure Security

- REST/GraphQL API security testing
- Microservices security architecture analysis
- Server misconfiguration exploitation (SSRF, XXE, SSTI)
- Network enumeration & lateral movement techniques
- Container security (Docker escape techniques)
- Cloud security assessment (AWS, GCP misconfigurations)
- Vulnerability triage, risk assessment & remediation guidance
- DevSecOps integration and secure SDLC implementation

KEY ACHIEVEMENTS & METRICS

🏆 Offensive Security Impact

- Conducted 50+ comprehensive penetration tests across fintech, healthcare, SaaS, and eCommerce
- Identified and responsibly disclosed 100+ high/critical vulnerabilities
- Achieved 98% post-remediation success rate with zero repeat vulnerabilities
- Discovered critical payment gateway vulnerabilities saving clients $500K+ in potential fraud

🔍 Bug Bounty & Research

- Verified Security Researcher on HackerOne with successful vulnerability disclosures
- Active contributor on Bugcrowd platform with accepted submissions
- Notable disclosure: Information Disclosure vulnerability in Remitly (Bug #3116964)
- Specialized findings: Auth bypass, IDOR chains, SSRF→RCE pivots, rate-limit abuse

⚙️ Automation & Tool Development

- Built UltraAPI framework reducing API testing time by 70%
- Developed automated recon systems processing 10,000+ subdomains in minutes
- Created 15+ custom offensive security tools for red team operations
- Tools adopted by 5+ security teams for daily testing workflows

📊 Platform Rankings & Recognition

- TryHackMe: Top 5% global ranking (Advanced Offensive Security)
- HackTheBox: Intermediate+ level completion
- PortSwigger Web Security Academy: Complete certification
- Maintained 5-star rating across all freelance engagements

TECHNICAL SKILLS

Security Tools & Platforms

Penetration Testing: Burp Suite Professional, Metasploit Pro, Nessus Professional, OWASP ZAP, Nikto
Network Analysis: Nmap, Wireshark, Netcat, Masscan, tcpdump
Reconnaissance: Amass, Subfinder, Assetfinder, Gobuster, Dirsearch, ffuf, nuclei, httprobe
API Testing: Postman, Insomnia, Fiddler, mitmproxy, Swagger/OpenAPI analyzers
Exploitation: Metasploit Framework, SQLmap, XSStrike, Commix, BeEF
Operating Systems: Kali Linux, ParrotOS, BlackArch, Debian, Ubuntu Server
Bug Bounty Platforms: HackerOne, Bugcrowd, Synack Red Team, Intigriti

Programming & Development

Languages: JavaScript/Node.js, Python 3, Bash/Shell scripting, PowerShell (basic)
Frameworks: Express.js, React.js, Next.js, Flask
Automation: Puppeteer, Playwright, Selenium, Beautiful Soup, Requests
DevOps: Docker, Docker Compose, Git/GitHub, CI/CD basics, Jenkins
Databases: MongoDB, MySQL, PostgreSQL, Redis, SQLite
API Development: REST APIs, GraphQL, WebSocket, gRPC

Vulnerability Expertise

API Security: Broken Authentication, BOLA/IDOR, Mass Assignment, Rate-limit bypass, Excessive Data Exposure, Security Misconfiguration
Web Application: XSS (Stored/Reflected/DOM), SQL Injection, SSRF, XXE, CSRF, LFI/RFI, SSTI, Command Injection, Deserialization attacks
Authentication: JWT manipulation, OAuth 2.0 flow abuse, Session fixation, Cookie poisoning, 2FA bypass
Infrastructure: Privilege escalation, Lateral movement, Container escape, Subdomain takeover, CORS misconfiguration
Business Logic: Payment manipulation, Race conditions, Workflow bypass, Price manipulation, Privilege escalation through features

---

PROFESSIONAL EXPERIENCE

🔥 Offensive Security Engineer (Independent Consultant)

2017 – Present | Remote | Multiple Client Engagements

Specialized in red team engagements, API security assessments, and offensive security automation for mid-to-large organizations across fintech, SaaS, healthcare, and eCommerce sectors.

🎯 Red Team & Penetration Testing

- Conducted 50+ full-scope penetration tests across web applications, APIs, cloud infrastructure, and mobile backends
- Executed red team simulations using MITRE ATT&CK framework techniques for realistic threat modeling
- Identified 100+ high/critical findings including authentication bypass, chained IDOR exploitation, SSRF→RCE pivots, and payment gateway abuse vectors
- Delivered executive-level reports with CVSS scoring, business impact analysis, and detailed remediation roadmaps
- Maintained 98% post-remediation success rate with clients successfully patching all critical findings within SLA
- Performed security retesting and validation to ensure permanent vulnerability resolution

🔍 Bug Bounty Research & Responsible Disclosure

- Active security researcher on HackerOne and Bugcrowd with verified vulnerability discoveries
- Discovered critical vulnerability in Remitly payment platform (Bug #3116964) - Information Disclosure leading to potential account takeover
- Specialized in payment gateway security testing: OTP bypass, transaction manipulation, callback abuse
- Expertise in finding API-specific vulnerabilities: Broken Object Level Authorization (BOLA), Mass Assignment, Excessive Data Exposure
- Collaborated with security teams for responsible disclosure and remediation guidance

⚙️ Offensive Engineering & Security Automation

- **UltraAPI Framework:** Developed advanced API security testing framework for automated endpoint enumeration, fuzzing, JWT/OAuth token abuse detection, and GraphQL introspection attacks
- **Reconnaissance Automation:** Built comprehensive OSINT and subdomain enumeration system integrating Amass, Subfinder, nuclei, and custom logic - reducing recon time by 70%
- **Session Replay & Bypass Tools:** Created sophisticated tools for testing token-based authentication systems, detecting session fixation, and automating cookie poisoning attacks
- **Browser Automation:** Designed Puppeteer-based attack simulation frameworks for testing complex multi-step workflows and single-page applications
- **Fuzzing Engine:** Developed custom fuzzing toolkit for parameter discovery, header manipulation, and input validation testing

💰 Fintech & Payment Gateway Security

- Reverse-engineered payment gateway API flows to identify vulnerabilities in OTP/PIN verification, session token handling, and transaction validation
- Conducted deep-dive security assessments on fintech platforms to identify fraud vectors, BOLA in financial APIs, parameter tampering, and race condition vulnerabilities
- Designed and implemented secure callback validation systems and webhook verification mechanisms for enterprise-grade payment simulations
- Performed PCI-DSS gap analysis and provided compliance recommendations
- Tested cryptocurrency wallets and blockchain integration security

📚 Training, Mentorship & Knowledge Sharing

- Delivered hands-on cybersecurity training sessions to 20+ development teams on secure coding practices and OWASP Top 10
- Mentored 10+ junior security researchers in ethical hacking methodologies, bug bounty hunting, and responsible disclosure
- Created comprehensive technical documentation including security testing checklists, remediation guides, and best practices
- Contributed to security community through blog posts, POC development, and tool releases
- Conducted internal "lunch and learn" sessions on emerging threats and attack techniques

---

KEY PROJECTS & OFFENSIVE TOOLS

1. UltraAPI — Advanced API Security Testing Framework

Tech Stack: Node.js, Python, Bash, REST/GraphQL
Purpose: Offensive API exploitation and comprehensive security testing

Features:

- Automated endpoint enumeration from JavaScript files, OpenAPI specs, and GraphQL introspection
- JWT/OAuth token misconfiguration detector with algorithm confusion testing
- Automated fuzzing engine for parameter discovery and input validation bypass
- BOLA/IDOR vulnerability scanner with permission matrix testing

- Rate-limit bypass techniques automation
- Mass assignment vulnerability detector
- Built specifically for red team API exploitation workflows

Impact: Adopted by 5+ security teams, reduced API testing time by 70%, discovered 30+ critical API vulnerabilities in production systems

---

2. Automated Reconnaissance & Attack Surface Mapping System

Tech Stack: Python, Bash, OSINT APIs, nuclei, Subfinder, Amass
Purpose: Comprehensive attack surface discovery and vulnerability intelligence

Features:

- Integrates multiple reconnaissance tools (Amass, Subfinder, Assetfinder, httprobe)
- Automated subdomain takeover detection
- Technology stack fingerprinting and version detection
- Generates actionable attack surface maps with prioritized targets
- Continuous monitoring mode for new asset discovery
- Webhook notifications for critical findings

Impact: Reduced manual reconnaissance time from 6+ hours to 15 minutes, discovered 500+ subdomains across client engagements, identified 25+ subdomain takeover vulnerabilities

---

3. Payment Gateway Simulation & Security Testing Suite

Tech Stack: Node.js, React.js, Express.js, MongoDB, Redis
Purpose: Security training and business logic flaw testing

Features:

- Simulates complete payment workflows: OTP/PIN verification, transaction validation, callback processing
- Implements intentionally vulnerable scenarios for security training
- Supports testing of race conditions, TOCTOU attacks, and replay attacks
- API callback abuse and webhook exploitation scenarios

- Session management and token handling security testing
- Real-time transaction monitoring dashboard

Use Cases: Used by security teams for training, penetration testing practice, and demonstrating payment vulnerabilities to stakeholders

---

4. LinkedIn Automation Bot (Security-Focused Design)

Tech Stack: Puppeteer, Node.js, Anti-Detection Techniques
Purpose: Demonstrating browser automation security implications

Features:

- Multi-step form automation with dynamic field detection
- Context-aware autofill logic with randomization
- Designed with anti-detection flow (human-like behavior simulation)
- Captcha detection and handling mechanisms
- Session management and cookie persistence
- Rate-limiting and throttling to avoid detection

Security Insights: Demonstrates security implications of automation bots, used in red team engagements to show social engineering risks

---

5. Web Application Security Scanner (Custom DAST Tool)

Tech Stack: Python, Selenium, Request Library
Purpose: Automated vulnerability detection in web applications

Features:

- Automated crawling and endpoint discovery
- XSS detection (Reflected, Stored, DOM-based)
- SQL Injection testing with various payloads
- CSRF token validation testing
- Security header analysis
- Generates detailed HTML reports with POC

---

6. Session Hijacking & Cookie Analysis Toolkit

Tech Stack: Python, Burp Suite Extensions
Purpose: Advanced session security testing

Features:

- Cookie attribute analysis (Secure, HttpOnly, SameSite)
- Session fixation vulnerability detection
- JWT decoding, validation, and algorithm confusion testing
- Session timeout testing automation
- Concurrent session testing

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

Industry Certifications

✅ **Certified Ethical Hacker (CEH)** — EC-Council
✅ **Offensive Security OSCP Training** (In Progress - Expected Completion: 2025)
✅ **CompTIA Network+ N10-008** — CompTIA
✅ **PortSwigger Web Security Academy** — Complete (All Labs & Certifications)
✅ **The Complete 2024 Web Development Bootcamp** — Full-Stack Development

Platform Achievements & Rankings

🏅 **TryHackMe:** Top 5% Global Ranking (Offensive Pentesting Path)
🏅 **Hack The Box:** Intermediate+ Level (Active/Retired Machine Completion)
🏅 **HackerOne:** Verified Security Researcher (Disclosed Vulnerabilities)
🏅 **Bugcrowd:** Active Bug Bounty Researcher (Accepted Submissions)
🏅 **PentesterLab:** Multiple Badge Completions

Continuous Learning

- OWASP API Security Project — Active Contributor
- SANS Cyber Security Reading Room — Regular Contributor
- Bug Bounty Reports Study — Daily Review of disclosed reports
- CTF Competitions — Regular participant (Web & Pwn categories)

EDUCATION

Bachelor of Science in Computer Science & Engineering
American International University-Bangladesh (AIUB) | **In Progress**
Focus Areas: Cybersecurity, Network Security, Cryptography, Software Engineering

Academic Excellence:

- **Secondary School Certificate (SSC):** Golden GPA 5.0
- **Higher Secondary Certificate (HSC):** Golden GPA 5.0

Self-Directed Learning:

- 6+ years of hands-on cybersecurity experience through bug bounty, CTFs, and client projects
- Completed 500+ hours of security training across multiple platforms
- Built 15+ offensive security tools and frameworks from scratch

---

RESEARCH & PUBLICATIONS

Vulnerability Disclosures

- **Remitly (HackerOne):** Information Disclosure vulnerability (Bug #3116964) - Disclosed and patched
- **Multiple Private Programs:** Authentication bypass, IDOR chains, SSRF vulnerabilities - Under responsible disclosure

Research Focus Areas

- API Security: BOLA, Mass Assignment, GraphQL vulnerabilities
- Payment Gateway Security: Transaction manipulation, race conditions, callback abuse
- Authentication Mechanisms: JWT/OAuth exploitation, 2FA bypass techniques
- Browser Automation Security: Bot detection bypass, anti-fingerprinting techniques

Community Contributions

- Published POC scripts on GitHub for educational purposes

- Contributed to OWASP testing methodologies
- Shared security findings through blog posts and technical write-ups
- Mentored aspiring security researchers through online communities

---

LANGUAGES

🌎 **Bengali:** Native/Bilingual Proficiency
🌎 **English:** Professional Working Proficiency (Technical & Business Communication)
🌎 **Japanese:** Conversational (日本語)
🌎 **Hindi:** Conversational (हिन्दी)

PROFESSIONAL PHILOSOPHY

> **"Break systems to understand them. Automate everything. Stay one step ahead."**

I am committed to advancing cybersecurity through ethical hacking, continuous learning, and knowledge sharing. My approach combines deep technical expertise with creative problem-solving to identify vulnerabilities that others miss. I believe in responsible disclosure, helping organizations build robust security postures, and staying ahead of evolving threat landscapes through constant research and adaptation.

Core Values

- **Ethics First:** Always operate within legal boundaries and responsible disclosure guidelines
- **Continuous Learning:** Technology evolves, so must our skills - daily learning is non-negotiable
- **Automation Mindset:** Automate repetitive tasks to focus on complex problem-solving
- **Knowledge Sharing:** Lift others through mentorship and community contribution
- **Client Success:** Treat every engagement as a partnership for long-term security improvement

---

AVAILABILITY & ENGAGEMENT

Current Status: ✅ Available for new projects and security assessments
Work Arrangement: Remote (Preferred) / Hybrid / On-site (International travel possible)
Time Zone: GMT+6 (Bangladesh Standard Time / Asia/Dhaka)
Response Time: Within 24 hours for inquiries
Preferred Engagement Types:

- Long-term security consultant retainers
- Comprehensive penetration testing projects
- Red team simulation exercises
- API security assessments
- Security automation tool development
- Security training and workshops

Availability Hours: Monday - Saturday, 9 AM - 11 PM GMT+6 (Flexible for international clients)

ADDITIONAL INFORMATION

Work Style & Collaboration

- Agile and adaptive to different project methodologies
- Strong documentation and reporting skills
- Comfortable with async communication (Slack, Discord, Email)
- Experience with international teams and cross-cultural collaboration
- Proficient in video conferencing (Zoom, Google Meet, Microsoft Teams)

Technical Setup

- High-speed internet (100+ Mbps) with backup connectivity
- Professional home office setup with dedicated security lab
- Multiple testing environments (VMs, cloud instances)
- Encrypted communication channels for sensitive data

Professional References

Available upon request from previous clients across fintech, healthcare, and enterprise sectors.

Last Updated: January 2025
Document Version: 2.0 Enhanced