MUHAMMAD BILAL ZEESHAN

Karachi | muhammadbilalzeeshan@outlook.com | +92 335-5651333 | linkedin.com/in/mbilalzeeshan
mbilalzeeshan.vercel.app | github.com/mbilalzeeshan

Education

Cambridge International A Levels **2025 – 2027 (expected)**
Homebridge by Beaconhouse, Karachi, Pakistan
Predicted grades: A A* A A | Subjects: Computer Science, Pure Mathematics, Business Studies, Physics

Cambridge O Levels **2023 – 2025**
The Froebel's School

Professional Experience

AI Security Intern **Jul 2026 – Present**
ZeroDay Reapers (Remote)

- "Break the Bot": tested 9 prompt-injection techniques against a filtered chatbot (Python + Groq API, `llama-3.3-70b-versatile`); smuggled hidden instructions into documents read by a local Ollama LLM.
- Data-poisoning experiments (label-flipping vs. backdoor attacks): 1% poisoned data drove 90%+ attack success while accuracy barely moved (97.22% to 96.94%).
- Demonstrated pickle-deserialization RCE in ML models — detection with picklescan/Fickling and SafeTensors mitigations — and published end-to-end chatbot attacks (SQL injection, command injection, reflected XSS) as a 29-page report.

SOC Analyst Intern **Jun 2026 – Aug 2026**
ITSimplera Institute

- Built a home SOC lab: Wazuh SIEM deployment (dashboard, indexer, Filebeat), pfSense firewall, Squid, ClamAV, and Syslog-NG; validated with EICAR testing, plus log analysis and incident investigation.
- Built an automated threat-intel pipeline (Wazuh → n8n webhook → Gemini AI) for severity assessment of detections.
- Mapped detections to MITRE ATT&CK; wrote custom detection rules and playbooks.

Junior Instructor **Dec 2024 – Present**
UTech Digital Education

- Taught Python to 30+ students through live coding sessions and practical projects.
- Taught cybersecurity to ∼20 students: OSINT, Google dorking, bug-bounty concepts, social engineering, and the CIA triad.
- Designed practical exercises and mentored students.

Cloud Computing Intern **Jul 2026 – Aug 2026**
Decode Labs

- Built a serverless cost-calculator API with Azure Functions (Python 3.13, Azure Functions Core Tools): POST `{"num1":10,"num2":20}` returns Sum 30.
- Hosted a static portfolio site with Azure Blob Storage static website hosting during the internship (site since migrated to Vercel); worked with Storage Accounts.
- Worked with Amazon S3, networking, and identity management across cloud workflows.

General Manager **2025 – 2026**
Homebridge Data Ninjas (school coding club)

- Coordinated the school coding club and taught Python to peers.
- Liaised with school management and club leadership on club activities.

Full Stack Development Intern **Sep 2026 – Present**
Auspify Technologies

- Recently selected; work beginning.

Technical Skills

Programming
- Python
- JavaScript/TypeScript

Web
- Next.js
- Tailwind CSS
- Supabase
- REST APIs

Cloud
- AWS
- Azure (Functions)

Systems
- Linux (Ubuntu Server, Kali)
- VirtualBox

Security
- Wazuh
- pfSense

AI/LLM APIs
- Groq
- Gemini
- Ollama

Tools
- Git/GitHub

Projects

- **AI Security Weekly Reports**
  Weekly hands-on AI-security experiments written up as public GitHub reports: prompt-injection testing ("Break the Bot"), data-poisoning experiments, pickle-deserialization RCE, and end-to-end chatbot attacks.
  GitHub Repository
- **SOC Monitoring Lab**
  Home SOC lab: Wazuh SIEM deployment (dashboard, indexer, Filebeat), pfSense firewall, custom detection rules mapped to MITRE ATT&CK, and an automated threat-intel pipeline (Wazuh $\rightarrow$ n8n $\rightarrow$ Gemini AI).
  GitHub Repository
- **Azure Serverless Cost Calculator**
  Serverless cost-calculator API built with Azure Functions (Python 3.13, Azure Functions Core Tools); deployed and tested without provisioning a traditional server.
  GitHub Repository
- **GenCode Learning**
  Early-stage education project co-founded with a partner: programming and cybersecurity courses plus freelance technical services; site in development with Next.js, TypeScript, Tailwind CSS, and Supabase.

Certifications

- Practical Linux for Hackers – CybeRace
- Cybersecurity – Google
- General Manager of Data Ninjas – Homebridge by Beaconhouse
- Python Essentials 1 & 2 – Cisco
- Introduction to Cybersecurity – Cisco
- Introduction to Cybersecurity Awareness – HP
- Effective Leadership – HP
- Generative AI with Python – UTech
- Data Science and Machine Learning with Python – UTech
- Game Development with Python – UTech
- Essentials of AI Learning Frameworks and Advanced Models – UniAthena

Languages

English (Fluent) | Urdu (Native)

References

Available upon request.