Aryan Akbar Joyia

Islamabad, Pakistan | aryanakbarjoyia@gmail.com | LinkedIn | GitHub | Portfolio | Medium
Application Security Researcher | Web & API Penetration Tester | Vulnerability Researcher

SUMMARY

Application Security Researcher and Penetration Tester with 4+ years of independent experience identifying, validating, and responsibly disclosing high-impact vulnerabilities across web applications, REST/GraphQL APIs, and cloud environments. Consistent track record of critical findings – CVSS scores up to 9.8 – affecting global enterprises, financial platforms, and institutional systems.

Specialises in authentication bypass, broken access control (IDOR), SSRF, sensitive data exposure, and multi-stage exploitation chains. Produces reproducible proof-of-concepts and risk-based reports aligned with client risk appetite and remediation capacity. Experienced in coordinating responsible disclosure with vendor security teams across jurisdictions.

Developed custom offensive tooling and contributed research affecting organisations including Booking.com, FareHarbor, Origin Protocol, 3CX, SquareX, Shakepay, Gul Ahmed, AIOU, LUMS, and NUCES.

CORE COMPETENCIES

- Web Application Penetration Testing
- API Security Testing (REST & GraphQL)
- Authentication & Authorisation Testing
- IDOR & Broken Access Control
- SSRF & Business Logic Flaws
- OWASP Top 10 / CVSS Scoring
- Exploit Development & PoC Validation
- WAF Bypass & Evasion Techniques
- Custom Offensive Tooling (Python)
- Security Reporting & Stakeholder Communication
- Responsible Disclosure & Coordinated Triage
- Burp Suite Professional, Linux, OSINT

PROFESSIONAL EXPERIENCE

Independent Vulnerability Researcher & Penetration Tester *Feb 2022 – Present*
CyberSecOrg

- Conduct security assessments of web applications and APIs across financial services, e-commerce, telecommunications, and academic sectors.
- Identify and validate authentication bypasses, IDOR, SSRF, sensitive data exposure, and business logic flaws; produce reproducible PoCs with full exploitation chains.
- Deliver professional technical and executive reports including CVSS scoring, risk-ranked findings, and actionable remediation guidance tailored to client environments.
- Collaborate with vendor and institutional security teams throughout disclosure, triage, and remediation validation cycles.
- Developed **WAFStrike**, a custom authorisation testing framework detecting access control gaps by analysing inconsistencies between WAF filtering layers and backend enforcement logic.

Responsible Disclosure Researcher *Feb 2022 – Present*
Freelance

- Identified and disclosed vulnerabilities to technology companies and academic institutions worldwide through structured responsible disclosure programmes.
- Performed independent exploit validation, CVSS-based risk assessment, and impact communication across web, API, and access control attack surfaces.
- Supported post-disclosure remediation validation to confirm effective mitigation of reported issues.

SELECTED SECURITY RESEARCH & PROJECTS

FareHarbor – Exposed Payment Secrets *Dec 2025 | CVSS 9.4 Critical*

- Discovered hardcoded production payment credentials (Stripe, PayPal, Adyen, dLocal, FileStack) within client-side assets, exposing all authenticated users to unauthorised financial operations.
- Delivered detailed technical report through responsible disclosure; findings acknowledged and remediated.

Shakepay – API Authentication & Access Control *Oct 2025 | CVSS 9.8 Critical*

- Identified a critical API authentication weakness; developed PoC validation and communicated business impact through responsible disclosure.
- Security team acknowledged the finding; documented as accepted organisational risk.

Booking Platform – Authentication Bypass (Account Takeover) *Dec 2025 | CVSS 8.4 High*

- Identified a tracking endpoint generating trusted session tokens without credential validation, demonstrating a clear account takeover path through session escalation.
- Responsibly disclosed after confirming impact; testing halted immediately upon scope boundary identification.

Origin Protocol – Unauthenticated API Data Exposure & CORS *Dec 2025 | CVSS 8.2 High*

- Discovered production API exposing aggregated financial vault statistics without authentication; permissive CORS policy enabled cross-origin extraction by arbitrary third-party sites.
- Responsibly disclosed; findings confirmed and mitigated by the security team.

Booking.com – Session Management & CSRF Weaknesses *Dec 2025 | CVSS 7.4 High*

- Reported session ID confusion, missing CSRF protection, and absent referrer validation within the analytics tracking system during authorised bug bounty testing.
- Demonstrated practical exploitation scenarios affecting authenticated application workflows.

WordPress – Full-Scope Pentest, Administrative Compromise *Feb 2026*

- Conducted black-box assessment of a production WordPress environment behind Wordfence WAF; identified Stored XSS and LFI in the WPBakery plugin.
- Chained vulnerabilities to demonstrate administrative session hijacking and privileged access escalation; delivered executive and technical report with CVSS-rated findings.

WAFStrike – Authorisation Testing Framework *Mar – Apr 2026*

- Developed a research-grade tool for detecting IDOR, broken access control, and privilege escalation by identifying gaps between WAF filtering and backend enforcement logic.
- Designed for accuracy, reproducibility, and integration into penetration testing and bug bounty workflows.

AIOU / BigBlueButton Greenlight – Institutional Security Research *2025*

- Reported reflected XSS, static CSRF token handling, and administrative interface exposure (AIOU); identified sensitive configuration data disclosure in BigBlueButton Greenlight via coordinated responsible disclosure.

PUBLICATION

Finding Origin IPs Behind Cloudflare During Pentests *Medium, May 2026*

Research covering origin infrastructure discovery behind reverse proxies and CDN environments, including SSRF-assisted validation, backend timeout analysis, and infrastructure fingerprinting during authorised engagements.

EDUCATION

FA (Information Technology) *2026 – 2028*

Government Graduate College, Vehari, Pakistan *Flexible schedule; fully available for full-time roles*

Matriculation – Computer Science Government High School, Vehari, Pakistan

CERTIFICATIONS

Certified Ransomware Protection Officer – *EU Cyber Academy*	
Certified Network Pentester (CNP) – *The SecOps Group*	Oct 2024
Certified Network Security Practitioner (CNSP) – *The SecOps Group*	Nov 2024
Cyber Threat Management – *ENISA (EU Agency for Cybersecurity)*	Jan 2026
Cybersecurity Compliance & System Administration – *IBM iX*	Jun 2023
Vulnerability Management Foundation – *Qualys*	Sep 2024

LANGUAGES

English – Professional Working Proficiency | **Urdu** – Native | **German** – Basic