Aly Magdi *("Rony")*

Offensive Security Researcher — Web & API Security

Specialising in authentication, authorisation, and multi-tenant SaaS architecture.

Cairo, Egypt • +20 102 133 7544 • aly@alymagdi.com
alymagdi.com • LinkedIn • HackerOne

Professional Summary

Offensive security researcher specialising in web and API security, with a focus on authentication, authorisation, and tenant-isolation flaws in multi-tenant SaaS systems. I find the design-level vulnerabilities scanners miss and write reproducible reports with concrete remediation guidance.

Professional Experience

Offensive Security Researcher

Sep 2024 — Present

HackerOne & Bugcrowd — Bug Bounty Programs

Remote

- **Reported 200+ valid vulnerabilities** across HackerOne and Bugcrowd, ranking in the top 14% of researchers and earning 93+ thanks from program owners.
- **Earned top placements:** #1 on a private HackerOne program, #8 on Netflix, and top-30 on Hilton and Hostinger.
- **Credited by** Netflix, Epic Games, Sony, Mozilla, Hilton, Wells Fargo, Hostinger, and Malwarebytes for valid security findings.
- **Specialise in design-level flaws** in authentication, authorisation, and multi-tenant SaaS architecture: the kind of issues automated scanners miss but that map directly to business risk.
- **Collaborate with security teams** on retest cycles, validation, and remediation discussions across programs including Epic Games, Malwarebytes, Moveworks, Bilt, Ory, and CoinSpot.
- **Awarded a $2,600 bonus** by the Netflix Security Team for research that prompted a broader internal investigation into mail-subdomain takeover risk.
- **Write clear, reproducible reports** with concrete root-cause analysis and remediation guidance to support fast triage.

Selected Findings

[Critical] Full ATO via Password Reset Token Leaked in API Response

A password reset flow returned the reset token in the API response body, allowing full account takeover of any user given only their email address.

[Critical] Cross-Tenant Data Access via API Token Prefix Trust — Global HR Platform

A flawed token parser trusted the company ID embedded in the token string instead of resolving it from the database, giving full read and write access across tenant boundaries.

[Critical] SSRF to RCE: Container Escape on a CI/CD Platform

Escalated a blind SSRF in a webhook feature into remote code execution and container escape, demonstrating downstream CI/CD compromise potential.

[High] Unauthorised Access to All Prescription Records — Telehealth Platform

A missing member filter on a prescriptions endpoint exposed 1,352 PHI records belonging to 86 patients to any authenticated user.

Full write-ups at alymagdi.com/blog

Technical Skills

Application & API Security: Authentication and authorisation testing, OAuth and JWT analysis, broken access control, IDOR, business-logic flaws, multi-tenant SaaS isolation, REST and GraphQL API security, session and token management.

Vulnerability Classes: SSRF, RCE, injection (SQL, NoSQL, command), XSS, CSRF, file-upload abuse, race conditions, deserialisation, SSTI, dependency confusion.

Methodology: Reconnaissance and attack-surface mapping, threat modelling, grey-box testing, vulnerability assessment and triage, CVSS 4.0 scoring, responsible disclosure.

Tools: Burp Suite (primary), custom HTTP and JS analysis tooling, Postman, ffuf, nuclei, browser developer tools.

Certifications & Training

- **APIsec CASA** Certified API Security Analyst (2026)
- **API Penetration Testing** Training
- **OWASP API Security Top 10** Training
- **CVSS 4.0** Training

Education

Ain Shams University, Faculty of Al-Alsun — English Language & Literature

Languages

Arabic — Native | **English** — Fluent (Professional Working Proficiency)