Ali Sünbül

alisunbul@proton.me | github.com/xeloxa | xeloxa.netlify.app | hackpaper.netlify.app

PROJECTS

s3finder — Go, AWS, CLI

- Built a high performance AWS S3 bucket discovery CLI with intelligent name generation, concurrent workers, adaptive rate limiting, and connection pooling
- Automated certificate transparency recon, 780+ seed permutations, and AWS validation workflows to identify bucket region, ACL exposure, and sample object metadata

WP-Hunter — Python, FastAPI, Semgrep, SQLite

- Developed a passive first WordPress plugin and theme reconnaissance and static analysis platform with local dashboarding, WebSocket scan visibility, and Semgrep driven analysis
- Built offline plugin catalog sync and local query workflows for large scale version mapping, heuristic risk scoring, and instant querying through a local SQLite dataset
- Open sourced the platform and grew the repository to 40+ GitHub stars

HackPaper — Technical Writing, Security Research

- Published security writeups on TryHackMe, Hack The Box, and AWS topics, growing the site to 8,000+ visits

AWS Cloud Practitioner Notes — AWS, Technical Writing

- Published Turkish AWS Cloud Practitioner notes and exam tips derived from AWS Skill Builder content in cheat sheet format for faster review
- Published Turkish CLF C02 study notes covering IAM, networking, cost management, and Well Architected topics for exam preparation

OPEN SOURCE AND SECURITY RESEARCH

- Reported 2 high severity flaws in ExactMetrics, a WordPress analytics plugin with 1,000,000+ active installs: IDOR and improper privilege management, contributing to fixes in 9.0.3 (CVE-2026-1992, CVE-2026-1993)
- Reported 2 medium severity flaws in Gutenberg Blocks with AI by Kadence WP, a plugin with 600,000+ active installs: SSRF and unauthorized media upload affecting versions through 3.6.1 (CVE-2026-1857, CVE-2026-2633)
- Published a public exploit for CVE-2024-28397 in js2py, demonstrating sandbox escape to arbitrary code execution with modular payload generation
- Fixed a path traversal issue in craft-agents-oss and contributed the remediation upstream (#142)
- Hardened credential storage in opencode-antigravity-auth by enforcing 0600 file permissions for secrets at rest (#353)

SKILLS

Languages: Go, Python, SQL
Security: Application Security, Cloud Security, Offensive Security, OWASP Top 10, Static Analysis, Vulnerability Management, Vulnerability Research, WordPress Security
Tools: AWS, Docker, FastAPI, Git, Linux, Semgrep, SQLite, WebSockets