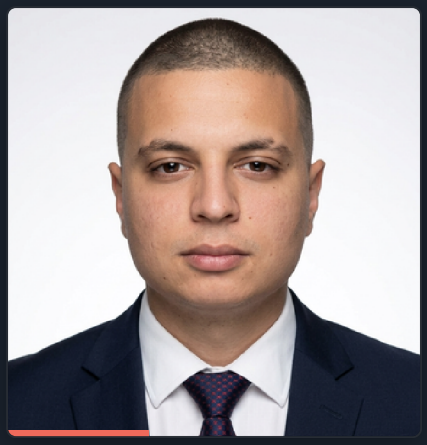

CONTACT

PHONE
+90 536 055 7280

EMAIL
altuntashalim123@gmail.com

LOCATION
Isparta, Türkiye

GITHUB
github.com/abdulhalimaltuntas

LINKEDIN
linkedin.com/in/abdulhalimaltuntas

30+	8	7
GH STARS	FORKS	TOOLS

EDUCATION

ASSOCIATE DEGREE — INFORMATION SECURITY TECHNOLOGIES
Isparta University of Applied Sciences
2025 – PRESENT

TECHNICAL SKILLS

OFFENSIVE

Web-App Pentesting · Vulnerability Assessment · Attack-Chain Development · WAF Evasion & 403 Bypass · Steganography

LANGUAGES

Go · **Python** · JavaScript · Bash

SYSTEMS

Linux · Windows Internals · Network Security · TLS / HTTP Internals

PRACTICE

Security Tool Development · Secret Detection · CI Security Gates

LANGUAGES

Turkish	NATIVE
English	B1 · INTERMEDIATE

ABDULHALIM ALTUNTAŞ

WEB APPLICATION PENTESTER

OFFENSIVE SECURITY • SECURITY TOOL DEVELOPMENT • ISPARTA, TR

00 PROFILE

Information-security student specialising in **offensive security** and **web-application vulnerability research**. I build custom tooling — a Go content-discovery engine with WAF evasion, a steganographic C2 framework, and a JavaScript-recon browser extension — to understand vulnerabilities at their root rather than relying on automated scanners. Seeking a security internship to contribute to real-world offensive operations in an international environment.

01 OPEN-SOURCE SECURITY TOOLS

Capsaicin

GO ★26 7 FORKS · MIT

Intelligent web content-discovery engine for red-teaming and bug-bounty research. Implements **JA3/JA4 TLS fingerprint spoofing** (uTLS), WAF detection across 16+ vendors, and header-injection 403 bypass. Uses **Shannon-entropy secret detection** with auto-calibrated 404 baselining to eliminate false positives; goroutine worker pool with circuit-breaking, JSON/HTML/CSV output and severity-based CI exit codes.

Chimera

GO + PYTHON RESEARCH C2

Command-and-control research framework that conceals **AES-256-GCM** traffic inside PNG images via least-significant-bit steganography. Mutual-TLS transport with timestamped anti-replay nonces, an automatic task queue, and a terminal operator console — built to study defensive evasion and detection.

JSHarvest

JAVASCRIPT · MV3 ★4

Browser extension that inventories every script on a page across **network, DOM and worker layers**, then deduplicates and classifies first- vs third-party sources. Flags missing Subresource Integrity, mixed content and failed loads; deep-scan recovers source trees from **.map** files and masks exposed secrets. Zero runtime dependencies, 77 unit tests.

Earlier tooling — **hawtsql** & **hawtxss**: Python proof-of-concept scanners for SQL-injection and XSS discovery.

02 COMPETITIONS & PROGRAMS

MAY 2026

Siber Vatan Program — SEMIFINALIST

Reached the semifinal stage of a national competitive cybersecurity program centred on operational pentesting scenarios and attack simulation.

03 REFERENCES

Furkan Şahin
CEO · PENTEGUARD
iletisim@penteguard.com
+90 507 033 5206

Serkan Özyaman
CEO · PENTEGUARD
serkanozyaman1@gmail.com