

AMR HAMDY

Kibernetinio saugumo inžinierius | Įsiskverbimo testuotojas | CTO

Kairas, Egiptas • Pilietybė: Egipto • +20 100 021 7809 • amrhamdyhefny@gmail.com

LinkedIn: linkedin.com/in/amrhamdyadrian • GitHub: github.com/angixblack

PROFESINĖ SANTRAUKA

Kibernetinio saugumo inžinierius, turintis **daugiau nei 5 metų** puolamojo saugumo patirties: nuo 2021 m. savarankiškai tiria pažeidžiamumus „bug bounty“ programose, o Egipte ir Jungtiniuose Arabų Emyratuose dirbo įsiskverbimo testavimo, taikomųjų programų saugumo ir inžinerinių komandų vadovavimo srityse. Specializuojasi žiniatinklio programų, REST API ir tinklų įsiskverbimo testavime; turi didelę patirtį nustatant, patvirtinant ir šalinant OWASP Top 10 pažeidžiamumus (XSS, SQL injekcijas, IDOR, pažeistą autentifikaciją, prieigos kontrolės ir verslo logikos spragas). Šiuo metu – arabiškos daugiakanalės SaaS platformos **Tawwan CTO**, anksčiau – techninis vadovas, kūręs dirbtinio intelekto ir skaitmeninės ekspertizės produktus bei diegęs saugaus programinės įrangos kūrimo ciklą (Secure SDLC). Atvirojo kodo puolamojo saugumo įrankių autorius; turi CEH sertifikatą, baigė OffSec OSCP ir OSEP mokymus.

PROFESINĖ PATIRTIS

Vyriausiasis technologijų vadovas (CTO)

2026-06 – dabar

Tawwan (tawwan.com) — Dubajus, Jungtiniai Arabų Emyratai

- Formuoja technologijų strategiją ir architektūrą bei pats kuria Tawwan – arabišką daugiakanalę pranešimų ir komentarų automatizavimo SaaS platformą.
- Suprojektavo ir sukūrė visą platformą, įskaitant integracijas su „Meta“ ir „Google“ API bei automatizavimo procesus su dirbtiniu intelektu.
- Visame produkte taiko „secure-by-design“ principus ir užtikrina saugią autentifikaciją, autorizaciją, duomenų apsaugą, slaptųjų duomenų valdymą ir diegimą.
- Atsako už technologijų plėtros planą, infrastruktūrą ir pasirengimą paleidimui; kartu su verslo vadovais sprendžia produkto kryptį ir dalyvauja pokalbiuose su investuotojais.

Techninis vadovas (Tech Lead)

2025-09 – 2026-05

El Motahida — Kairas, Egiptas

- Vadovavo programinės įrangos kūrimo skyriui; atsakė už sudėtingų sprendimų planavimą, projektavimą ir įgyvendinimą.
- Derino komandos valdymą su praktiniu programavimu – tiesiogiai kūrė dirbtinio intelekto ir skaitmeninės ekspertizės produktų architektūrą ir kodą.
- Visuose projektuose įdiegė saugaus programavimo standartus ir struktūrizuotas kodo peržiūras; projektavo atsparias ir patikimas sistemas.
- Bendradarbiavo su kibernetinio saugumo komandomis, integruodamas saugumo kontroles į kiekvieną programinės įrangos kūrimo ciklo etapą.
- Mentoriavo programuotojus; gerino kodo kokybę, inžinerinius procesus, programų našumą ir plečiamumą.

Kibernetinio saugumo inžinierius

2025-01 – 2025-08

Aurages — Kairas, Egiptas

- Atliko klientų ir vidinių sistemų žiniatinklio programų bei REST API įsiskverbimo testus, derindamas rankinius metodus ir automatizuotą skenavimą.
- Nustatė, patvirtino ir dokumentavo kritinius pažeidžiamumus: XSS, SQL injekcijas, IDOR, pažeistą autentifikaciją, sesijų valdymo ir verslo logikos spragas.
- Automatizavo žvalgybą, skenavimą ir pažeidžiamumų patvirtinimą naudodamas Burp Suite, OWASP ZAP, Nmap ir savo sukurtus Python scenarijus.
- Rengė įsiskverbimo testų ataskaitas su CVSS rizikos įvertinimais, koncepcijos įrodymais (PoC) ir aiškiomis taisymo rekomendacijomis techninei ir vadovų auditorijai.
- Kartu su kūrėjų komandomis diegė saugaus programavimo pataisas ir pakartotiniu testavimu tikrino jų veiksmingumą.

Programinės įrangos inžinierius

2023-06 – 2024-07

Focal Point — Dubajus, Jungtiniai Arabų Emyratai

- Kaip full-stack programuotojas suprojektavo, sukūrė ir prižiūrėjo įmonės žiniatinklio platformas: individualias WordPress temas ir įskiepius, talpinimą, našumo optimizavimą ir atsargines kopijas.
- Vertino įmonės svetainių, žiniatinklio serverių ir tinklo infrastruktūros saugumą bei diegė jautrių duomenų apsaugos priemones.
- Stiprino žiniatinklio serverių ir TVS (CMS) saugumą: tvarkė prieigos kontrolę, atnaujinimus, WAF konfigūravimą, atliko failų teisių ir įskiepių auditą.
- Kartu su IT komanda nustatė pažeidžiamumų šalinimo prioritetus ir gerino bendrą saugumo būklę.

Nuotoliniu būdu

- Tiria žiniatinklio programų ir API pažeidžiamumus bei praneša apie juos viešose „bug bounty“ ir atsakingo atskleidimo programose.
- Daugiausia tiria CORS konfigūracijos klaidas, atvirusius peradresavimus (open redirect), XSS, IDOR, autentifikacijos ir prieigos kontrolės spragas.
- Sukūrė ir atvirojo kodo principu paskelbė žvalgybos ir aptikimo įrankius (CORSCAN, RedirXploit, Kid Recon) tyrimams išplėsti.

PROJEKTAI

- **Tawwan** — tawwan.com
Arabiška daugiakanalė pranešimų ir komentarų automatizavimo SaaS platforma. Suprojektavo, sukūrė ir jai vadovauja kaip CTO.
- **CORSCAN** — github.com/angixblack
Python įrankis, aptinkantis CORS (Cross-Origin Resource Sharing) konfigūracijos klaidas žiniatinklio programų įsiskverbimo testų metu.
- **RedirXploit** — github.com/angixblack
Automatizuotas atvirojo peradresavimo pažeidžiamumų aptikimas žiniatinklio programų vertinimams ir „bug bounty“ tyrimams.
- **Kid Recon** — github.com/angixblack
Bash įrankis, automatizuojantis žvalgybą: subdomenų paiešką, prievadų skenavimą ir technologijų nustatymą.
- **Vaizdo stebėjimo kamerų el. prekybos platforma** (baigiamasis darbas)
Suprojektavo ir sukūrė PHP/MySQL serverinę dalį: produktų katalogą, užsakymų valdymą ir saugią naudotojų autentifikaciją.

PAGRINDINĖS KOMPETENCIJOS

Puolamasis saugumas	Įsiskverbimo testavimas, pažeidžiamumų vertinimas, Red Team operacijos, priešininko imitavimas, „bug bounty“, eksploitų kūrimas, privilegijų eskalavimas, Active Directory atakos, socialinė inžinerija
Programų saugumas	Žiniatinklio ir API įsiskverbimo testavimas, OWASP Top 10, OWASP ASVS, saugaus kodo peržiūra, grėsmių modeliavimas, autentifikacijos ir autorizacijos testavimas, Secure SDLC
AI ir LLM saugumas	LLM programų saugumo testavimas, OWASP Top 10 for LLM Applications, raginimų injekcijos (prompt injection) ir „jailbreak“ atakos, AI agentų ir RAG sistemų saugumas, MITRE ATLAS
Tinklai ir infrastruktūra	Tinklų įsiskverbimo testavimas, ugniasienės, IDS/IPS, sistemų stiprinimas (hardening), Linux ir Windows administravimas, pažeidžiamumų valdymas
Ekspertizė ir žvalgyba	Skaitmeninė ekspertizė, incidentų valdymas, OSINT, kenkėjiškų programų analizė
Saugumo įrankiai	Burp Suite Professional, OWASP ZAP, Metasploit, Nmap, Nessus, Wireshark, Hydra, SQLmap, Nikto, Gobuster, Kali Linux
Programavimas	Python, Bash, JavaScript, PHP, C++, SQL, HTML/CSS
DevOps ir automatizavimas	Docker, CI/CD, Git/GitHub, Linux serveriai, MySQL, WordPress, n8n, „Meta“ ir „Google“ API
Vadovavimas	Komandos valdymas, techninė mentorystė, projektų planavimas, saugumo sąmoningumo mokymai, techninių ataskaitų rengimas, bendravimas su klientais

SERTIFIKATAI

- **Certified Ethical Hacker (CEH)** — ITI (Informacinių technologijų institutas)
- **API Penetration Testing** — APIsec University
- **Ethical Hacking Essentials (EHE)** — EC-Council
- **Penetration Testing** — American Board
- **Certificate of Experience in Hacking** — Teaching Planet Academy

PROFESINIAI MOKYMAI (BAIGTI KURSAI)

- **OffSec:** OSEP — Experienced Penetration Tester; OSCP — Certified Professional
- **INE / eLearnSecurity:** eWPTX — Web Application Penetration Tester eXtreme; eWPT — Web Application Penetration Tester; eJPTv2 — Junior Penetration Tester
- **EC-Council:** CEH v13 — Certified Ethical Hacker

IŠSILAVINIMAS

Vadybos informacinių sistemų (MIS) bakalauras

2024

Gizos institutas — Giza, Egiptas

KALBOS

Arabų: gimtoji • Anglų: profesinio darbo lygis • Lietuvių: mokosi