Anas Hamidi

Penetration Tester | Cybersecurity Specialist

Adresse: Hauptstraße 23, 97218 Gerbrunn, Deutschland

Telefon: +4915565653303 **E-mail:** anshmaidy2000@gmail.com

LinkedIn: linkedin.com/in/anas-hmaidy

HackerOne: hackerone.com/albetisi

GEBURTSDATUM / -ORT: 06/2000 - IDLEB **STAATSANGEHÖRIGKEIT**: SYRISCH

PROFIL

Penetration Tester und Security Researcher mit über drei Jahren praktischer Erfahrung in der offensiven Sicherheit. Spezialisiert auf Web- und API-Penetrationstests mit Erfahrung in Mobile App Security, Business-Logic-Schwachstellen und sicherheitsrelevanter Automatisierung. Über 50 Schwachstellen verantwortungsvoll an internationale Unternehmen wie Canva, Pexels und Lichess gemeldet, darunter eine kritische Schwachstelle bei Canva (Belohnung 15.000 USD). Erfahren in der Integration von KI-gestützten Workflows (LLMs) zur Beschleunigung von Recon, Payload-Generierung und Code-Analyse. Strukturiert, analytisch und teamorientiert mit klarem Fokus auf nachvollziehbare technische Berichte und konkrete Mitigationsempfehlungen.

BERUFSERFAHRUNG

Selbstständiger Security Researcher / Penetration Tester

HackerOne & Bugcrowd | Februar 2023 – heute | Remote

- Durchführung realitätsnaher Web- und API-Penetrationstests aus Angreiferperspektive für internationale Plattformen.
- Identifikation und verantwortungsvolle Meldung von über 50 Schwachstellen, u. a. IDOR, XSS, SSRF, SQLi, Authentifizierungs- und Business-Logic-Fehler.
- Aufdeckung einer kritischen Sicherheitslücke bei Canva, ausgezeichnet mit einer Belohnung in Höhe von 15.000 USD.
- Platz 1 in der Hall of Fame zweier privater HackerOne-Programme (unter 50+ Researchern); Platz 9 in der Canva-Hall of Fame (unter 200+ Researchern).
- Analyse und Umgehung von Web Application Firewalls (WAFs) sowie Filter-Bypass-Techniken.
- Erstellung professioneller technischer Reports inkl. Reproduktionsschritten, Risikobewertung nach CVSS und konkreten Remediation-Empfehlungen.
- Entwicklung eigener Python- und Bash-Skripte zur Automatisierung von Recon, Schwachstellen-Triage und Datenanalyse.
- Einsatz von LLM-basierten Tools (ChatGPT, Claude) zur Unterstützung bei Recon-Automatisierung, Payload-Generierung und Quellcode-Analyse.
- Erste praktische Erfahrung im Bereich Mobile Application Pentesting (Android, OWASP MASVS).

STUDIUM

Bachelor of Science in Informationstechnik-Engineering

Universität Aleppo, Syrien | Abschluss: 2023

WICHTIGSTE ERFOLGE

- 15.000 USD Bug Bounty für eine kritische Sicherheitslücke bei Canva.
- Erzielung kontinuierlicher Bug-Bounty-Auszahlungen im fünfstelligen USD-Bereich durch systematische und nachhaltige Schwachstellenforschung.
- Platz 1 in der Hall of Fame zweier privater Bug-Bounty-Programme (HackerOne) – unter über 50 Researchern.
- Platz 9 in der Canva Bug Bounty Hall of Fame – unter über 100 Researchern.
- Anerkannte Schwachstellenmeldungen u. a. bei: Canva, Pexels, Lichess, GlanceCX, Inshur, ClassDojo.
- Über 50 verifizierte Schwachstellenberichte über HackerOne und Bugcrowd.

FÄHIGKEITEN & TOOLS

- **Web & API Security:** Burp Suite , OWASP ZAP, Metasploit (Grundlagen), Postman.
- **Schwachstellen-Scanning:** Nessus, Metasploit, Nmap
- **Exploitation & Recon:** SQLmap, FFUF, Subfinder, Amass, Nuclei
- **Mobile Pentesting:** Android (Frida-Grundlagen, APK-Analyse), OWASP MASVS
- **Methodologien:** OWASP Top 10, OWASP API Security Top 10, OWASP MASVS, SANS Top 25
- **Betriebssysteme:** Linux (Kali, Ubuntu), Windows
- **KI / Automatisierung:** Anwendung von LLMs (ChatGPT, Claude) zur Recon-Automatisierung, Payload-Generierung und Code-Analyse; Aufbau eigener Automations-Skripte
- **Soft Skills:** Analytisches und kreatives Denken, strukturierte Dokumentation, Teamfähigkeit, eigenverantwortliches Arbeiten
- Bash – fortgeschritten, Python, PHP, JavaScript - Grundkenntnisse.

WEITERBILDUNG

- PNPT (Practical Network Penetration Tester) – aktuell in Vorbereitung im Selbststudium
- Hack The Box – aktiver Member, praktische Labs (Web, Linux, Active Directory)
- TryHackMe – Hands-on Trainings im Bereich Web Security und Pentesting

FREIWILLIGENARBEIT

Technischer Leiter – ICPC Aleppo Universität 01/2023 - 02/2023

- Leitung technischer Teams bei der Organisation eines internationalen Programmierwettbewerbs

SPRACHEN

- Arabisch – Muttersprache
- Deutsch – B2 (telc zertifiziert)
- Englisch – Fließend