Махмуд Оуф

Junior специалист по анализу защищённости (пентест)

Бакалавр программной инженерии

КОНТАКТЫ

Email **contact@mahmoudouf.com**

LinkedIn **mahmoudadel0x01**

GitHub **mahmoud0x01**

Telegram **t.me/rdmsr**

Hack The Box **Профиль HTB**

TryHackMe **@iamkernel**

Сайт **mahmoudouf.com**

Базируется в Египте (UTC+2) · Открыт к удалённой работе и релокации по всему миру
Визовая поддержка / B2B контракт

ПРОФИЛЬ

Инженер по кибербезопасности, специализация — application security и offensive security: топ 0.55% в глобальном рейтинге Hack The Box, 20+ отметок в Bug bounty Hall of Fame на Bugcrowd (Verisign, DigitalOcean, Pinterest, Dell) за уязвимости, найденные и устранённые в продакшене. Коллеги прозвали меня Kernel за системный интерес докапываться до сути, а не оставаться на поверхности — тот же подход стоит за сертификатом CNSP (с отличием) и практическим опытом в пентесте и основах SOC на обеих сторонах — наступательной и защитной.

ОПЫТ РАБОТЫ

Стажёр — инженер-программист Фев 2025 – Июнь 2026

Национальный исследовательский Томский государственный университет

- Разработал **2 MVP + 12 диаграмм** (UML/SDLC) по полному SDLC — системное мышление для воспроизводимых находок.
- Проектировал архитектуру и документацию: требования, модели данных, интерфейсы и план тестирования.

Стажёр по инженерии безопасности 10 июля – 10 сентября 2024

Bastion Security — стажировка по инженерии безопасности

- Прошёл трек Penetration Testing & Application Security — лекции компании, CTF-задания, лабораторные работы по эксплуатации уязвимостей.
- Провёл исследовательский проект по анализу техник атак на кэширование веб-приложений.
- Вошёл в **Топ 5 из 100** во внутренних соревнованиях по пентесту и повышению привилегий.

Смотреть подтверждение → · сертификат стажировки Bastion Security

ОБРАЗОВАНИЕ

Бакалавр программной инженерии — выпуск июль 2026
Томский государственный университет
Сен 2022 – Июль 2026

ПРИЗНАНИЕ

- **Bug Bounty Hall of Fame — 20+ отметок** через Bugcrowd (**bugcrowd.com/h/mahmoud_adel**) — именные: Verisign $1,000 CSRF → захват аккаунта (DomainScope OAuth state, апр 2018), DigitalOcean (апр 2019), Pinterest и Dell (2018). **CRITICAL**
- **Соревнования и лаборатории:** внутренний CTF Bastion — **Топ 5 из 100**; Hack The Box — **Топ 0.55% Pro Hacker** (**подтверждённые бейджи**); TryHackMe — **Топ 1%** (**@iamkernel**). **VERIFIED**
- **Детекция и исследования:** SOC-лаборатория ELK — 50k+ событий, 5 правил Sigma (MITRE ATT&CK), дашборды Kibana и триаж; разбор малвари в изолированной Windows 10 VM (Sysmon/KAPE); AppArmor-защита от RCE; API и пути атак Active Directory. **LAB**

ПРАКТИЧЕСКИЕ ЛАБОРАТОРИИ И CTF-ПЛАТФОРМЫ

- **Hack The Box — подтверждённые бейджи · Топ 0.55% Pro Hacker**
- **TryHackMe — @iamkernel · Топ 1%**

СЕРТИФИКАТЫ

- **Certified Network Security Practitioner (CNSP)** — The SecOps Group · 2026 · с отличием · ID 11896945 — **Подтвердить ↗**
- **Blue Team Junior Analyst** — SecurityBlue Team · 2023 — **Подтвердить ↗**
- **Cyber Threat Intelligence** — IBM · 2023 — **Бейдж ↗**
- **Jr Penetration Tester** — TryHackMe · 2024 — **PDF ↗**

НАВЫКИ

CORE

Web/API Security, Vulnerability Assessment, Linux, Windows, TCP/IP, Privilege Escalation (lab), Burp Suite, Nmap, Python, Bash

APPLIED

OWASP, Network Security, Active Directory, Kerberos, Wireshark, BloodHound, Impacket, Docker, System Administration, Firewall, SIEM (ELK), Incident Response, MITRE ATT&CK, Cloud Security (AWS IAM)

FAMILIAR

Ghidra (lab), Metasploit (lab), Cobalt Strike (exposure), Sliver (lab), Nuclei (lab), SQLMap (lab), ffuf (lab), Malware Analysis (lab), Threat Intel (exposure), Exploit Dev (lab), Red Team (lab), YARA (lab), Sigma (lab), Suricata (lab), Splunk (lab)

ENGINEERING

JavaScript, C/C++, Assembly, SQL, Git, Presentation, Problem Solving

ЯЗЫКИ

Арабский · Родной

Английский · C2 — Профессиональный

Русский · C1 — Продвинутый

ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ

Verisign CSRF → захват аккаунта — отсутствие OAuth state → перехват Google-ссылки → устойчивый захват аккаунта и установка пароля (награда $1,000, Bug bounty Hall of Fame, апр 2018). **Разбор ↗**

AppArmor RCE Killswitch — deny /bin/** и сети → audit DENIED exec /bin/sh → allowlist-контейнмент и харденинг. **Разбор ↗**

ELK SOC Detection Engineering — 50k+ событий, 5 правил Sigma по MITRE ATT&CK, дашборды Kibana и процесс триажа. **Разбор ↗**

Всё тестирование безопасности проводилось исключительно в рамках авторизованного контура, лабораторий или ответственного раскрытия. · Рекомендации и логи проверок доступны по запросу.