Oussama Draissi | Systems Security · Doctoral Researcher

oussama.draissi@protonmail.com • 0drai.xyz • oussama-draissi
0drai • 0009-0005-6065-8087 • Google Scholar

Security researcher working on **sandboxed bytecode** to raise the security of applications across diverse platforms. My specialty is memory corruption: finding it through fuzzing and program analysis, and containing it with practical, low-overhead defenses.

Personal

Date of birth: 20th April 1995

Nationality: German and Moroccan

Education

University of Duisburg-Essen
Dr.-Ing. Computer Science (in progress, expected 2027) *since 2022*
Memory-safety analysis and defenses across WebAssembly, trusted execution environments, and emerging instruction sets. Advised by Prof. Lucas Davi.

University of Duisburg-Essen
M.Sc. Software and Network Engineering *2019–2022*
Thesis: *Hunting for Memory Corruption Bugs on the Web* (grade 1.3). Large-scale fuzzing of in-the-wild WebAssembly via `wasm2c` translation.

University of Duisburg-Essen
B.Sc. Applied Computer Science (Systems Engineering) *2014–2019*
Thesis: *Evaluation of Automated Advanced Information Leak Exploitation for Memory Corruption Attacks* (grade 1.0).

Experience

Systems Security Group, University of Duisburg-Essen **Essen**
Research Scientist & Doctoral Candidate *since 2022*
- Research staff member (*Wissenschaftlicher Mitarbeiter*) on memory-safety analysis and defenses for WebAssembly, trusted execution environments, and emerging instruction sets.
- Mentor student project groups and theses; supervised 12+ Bachelor's and Master's theses in systems and software security.

Systems Security Group, University of Duisburg-Essen **Essen**
Research Assistant (Wissenschaftliche Hilfskraft) *2019–2022*
- Researched RISC-V security and trusted execution environments; wrote exploits by hand and automatically (RiscyROP).
- Built WebAssembly analysis tools to discover vulnerabilities in online systems; analyzed memory corruption on RISC-V and native systems.
- Co-designed the exploitation lab (mini-CTFs) for the *Secure Software Systems* (M.Sc.) course.

Systems Security Group, University of Duisburg-Essen **Essen**
Student Research Assistant (Studentische Hilfskraft) *2017–2019*
- One of the first hires of the newly-formed group; researched advanced memory-corruption attacks on native systems.
- Supported teaching for *Reverse Engineering* (B.Sc.) and *Secure Software Systems* (M.Sc.); wrote data-only exploits, ported them to pwntools, and reproduced artifacts of academic security papers.

Selected Publications

2026: **Bento: Fine-Grained Memory Isolation for COTS WebAssembly Binaries.**
O. Draissi, L. Davi.
The Web Conference (WWW). **CORE A***

2026: **$2B Lessons: Brigade as a Defense Against Real-World DeFi Bridge Exploits.**
P. Winkler, J.-R. Giesen, **O. Draissi**, F. Badaloni, S. Holler, C. Schneidewind, L. Davi.
International Conference on Applied Cryptography and Network Security (ACNS). **CORE B**

2025: **Wemby's Web: Hunting for Memory Corruption in WebAssembly.**
O. Draissi, T. Cloosters, D. Klein, M. Rodler, M. Musch, M. Johns, L. Davi.
ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA). **CORE A**

2023: **Fuzz on the Beach: Fuzzing Solana Smart Contracts.**
S. Smolka, J.-R. Giesen, P. Winkler, **O. Draissi**, L. Davi, G. Karame, K. Pohl.
ACM Conference on Computer and Communications Security (CCS). **CORE A***

2022: **RiscyROP: Automated Return-Oriented Programming Attacks on RISC-V and ARM64.**
T. Cloosters, D. Paaßen, J. Wang, **O. Draissi**, P. Jauernig, E. Stapf, L. Davi, et al.
International Symposium on Research in Attacks, Intrusions and Defenses (RAID). **CORE A**

Teaching & Supervision

since 2017: Teaching assistant, *Secure Software Systems* (M.Sc.).

2020/2021: Teaching assistant, *Reverse Engineering* (B.Sc.).

ongoing: Supervised **12+** Bachelor's and Master's theses in systems and software security.

Skills

Programming: Rust, Python, C, C++, JavaScript, Bash

Focus: Memory corruption, fuzzing, binary analysis & rewriting, taint analysis, exploit development, remote attestation

Platforms: WebAssembly, RISC-V, trusted execution environments (TEEs), blockchains (Solana, EVM)

Tools: AFL++, LLVM, pwntools, Ghidra, radare2, Foxhound, Docker, Git

Languages

German: Native

Arabic: Native

English: Fluent