Osama Al-Wardi

Bremen, Germany | osamaalwardi@yahoo.com | LinkedIn

Research Interests

Agentic AI Security; Systems Security; Software Security; Access Control; Information Flow; Static and Dynamic Program Analysis; Isolation; Runtime Policy Enforcement

Education

Brandenburg University of Technology Cottbus–Senftenberg 2020–2023
M.Sc. Cyber Security, final grade: 1.9 *Cottbus, Germany*

- Master's thesis: *Design and Implementation of Taint Analysis for GraphQL-based Web Applications* (grade: 1.9).
- Research-oriented program; 124 credits completed.

Constructor University (formerly Jacobs University Bremen) 2017–2020
B.Sc. Computer Science, final grade: 2.77 *Bremen, Germany*

- Bachelor's thesis: *Performing Service Dependency Discovery on Web Application Clients*

Publications

Leen Lambers, Lucas Sakizloglou, **Osama Al-Wardi**, and Taisiya Khakharova. "Taint Analysis for Graph APIs Focusing on Broken Access Control." *International Conference on Graph Transformation (ICGT)*, LNCS 14774, pp. 180–200, 2024. DOI: 10.1007/978-3-031-64285-2_10. **EASST Best Software Science Paper Award**.

Zaid Al-Wardi and **Osama Al-Wardi**. "Recursive Ternary-Based Algorithm for Computing Prime Implicants of Multi-Output Boolean Functions." *Journal of Engineering and Sustainable Development*, 27(3), 2023. DOI: 10.31272/jeasd.27.3.2.

Research Experience

Master's Research — Static/Dynamic Taint Analysis for GraphQL 2022–2023
Software Systems Engineering, BTU Cottbus–Senftenberg

- Formalized an initial research idea into an end-to-end pipeline for analyzing broken access control and data leakage in GraphQL APIs.
- Modeled GraphQL schemas and operations using typed graphs and graph-transformation rules, then used dependency analysis to identify security-relevant source/sink operation pairs.
- Selected GitHub's GraphQL API as a real-world evaluation target, designed the experimental methodology, and implemented Python-based dynamic tests across users with different access privileges.
- Compared the approach with Schemathesis; the resulting work developed into the ICGT 2024 publication listed above.

KanAxe — AI Agents for Cyber Security 2023
Research-transfer project

- Helped develop a research-driven project exploring LLM-based agents for penetration testing, cloud security, compliance and related cyber security workflows.
- Built early LangChain-based tool-using agents that interacted with security tools, interpreted tool output, and selected subsequent actions.
- Investigated long-workflow context limitations, retrieval-based approaches, reliability of general-purpose LLMs on specialized security tasks, tool integration, and orchestration with human supervision.
- The project was developed into an application for EXIST Research Transfer, a German federal funding program for research-intensive technology-transfer projects.

Professional Experience

PROGNOST Systems GmbH 2024–Present
Cyber Security Engineer *Germany*

- Perform cyber security engineering for operational technology (OT) and industrial control systems (ICS) in industrial environments.
- Contribute to product certification projects with respect to standards and regulations such as IEC 62443-3-3, UR E27, and the EU Cyber Resilience Act (CRA).
- Conduct penetration testing, vulnerability scanning and management, authentication and authorization testing, cloud asset monitoring and code reviews.

Insentis GmbH 2022–2023
IT Security Consultant *Germany*

- Conduct penetration tests and security assessments of web applications, APIs, mobile applications, enterprise environments, and Active Directory infrastructures.
- Identify and validate vulnerabilities, analyze exploitation paths and attack surfaces, and communicate technical findings and remediation guidance to stakeholders.
- Translate hands-on assessment results into clear technical reports for engineering and security teams.

Philotech GmbH 2020–2022
Penetration Tester (Working Student) *Germany*

- Performed security testing in automotive environments, including infotainment systems.
- Investigated attack surfaces and exploitation opportunities in embedded/automotive systems.
- Contributed to autonomous-driving risk assessments and designs related to automotive security operations centers.

Teaching & Academic Experience

- **Teaching Assistant, Advanced Programming in Python**, Jacobs University Bremen — led tutorials/help sessions, supported students in labs, and graded assignments and exams.
- **Teaching Assistant, Computer Networks**, Jacobs University Bremen — explained networking concepts, assisted students during tutorials, and graded coursework.
- **Teaching Assistant, Ethical Hacking Laboratory** — supported hands-on security exercises and student learning in practical offensive-security topics.
- **Project Assistant** — contributed to porting a simulation library from JavaScript to Python.

Awards & Certifications

- **EASST Best Software Science Paper Award**, ICGT 2024.
- **Certified Azure Red Team Professional (CARTP)** by Altered Security.
- **Certified in Cybersecurity (CC)** by ISC2.

Technical Skills

Security	Web/API security, penetration testing, Active Directory security, cloud security, mobile application security, operational technology and industrial control system security, automotive systems security, vulnerability analysis, access control and authorization testing
Programming	Python, JavaScript, C/C++, Bash, PowerShell
Research Methods	Static and dynamic analysis, taint analysis, graph transformation, security testing, information-flow reasoning
Agentic Systems	LangChain, LangGraph, tool-using agents, retrieval-augmented workflows, LLM tool orchestration