Soheil Khodayari

Security Researcher @CISPA | Ph.D. Candidate
Saarland, Germany
January, 1995 | soheil.khodayari@cispa.de | https://scnps.co | Soheil__K | github.com/SoheilKhodayari | linkedin.com/in/soheilkhodayari |
Google Scholar: oxIuE5wAAAAJ

Bio Overview

Soheil Khodayari is a security researcher at CISPA - center for information security in Saarland, Germany. His expertise lies in application security, penetration testing, and large-scale threat detection, utilizing a blend of static and dynamic code analysis, and machine learning. Soheil has presented and published his works on top-tier security venues like IEEE S&P, NDSS, USENIX Security, RAID, RuhrSec, Stanford SecLunch, and OWASP AppSec. His works have been honored with multiple awards, such as a distinguished paper award at the prestigious IEEE S&P '23 conference and the best applied research accolade at CSAW. On his free time, Soheil serves as the program committee of security conferences like IEEE S&P, WebConf, CCS, Euro S&P and artifact evaluation committee of USENIX and ACSAC. Finally, Soheil is the developer and maintainer of multiple open-source testing tools including `https://ja-w.me` and `https://domclob.xyz`.

Work Experience

CISPA - Helmholtz Center for Information Security GmbH *Saarbruecken, Germany*
Web Security Researcher (Full-Time) *Aug 2019 - Present*
- Security testing of Web-based applications (penetration testing, static analysis, dynamic analysis, scanners and fuzzing, machine learning)
- Security information and event management (SIEM, EDR), vulnerability assessment, threat analysis and intelligence
- Web security research and large-scale threat measurements (browser policies, JavaScript vulnerabilities, authentication/authorization)

IMDEA Software *Madrid, Spain*
Security Intern R&D (Part-Time) *Sep 2018 - Aug 2019*
- Penetration testing Web applications, threat analysis and exploit generation
- Large-scale detection and analysis of Web threats, black-box security and privacy testing, reverse engineering
- Scripting languages (JavaScript/Python), container and cloud systems (Docker, LXC, AWS, GCP).

Brooktec S.L. *Madrid, Spain*
Web Developer (Part-Time) *Sep 2018 - July 2019*
- Developed banking apps and services using GraphQL APIs on Amazon EC2 as part of the Finametrix project for Allfunds bank.
- Used Node.js/Python, Angular, React/Redux, MongoDB/PostgreSQL, GraphQL, Jenkins, Docker, AWS.

Fraunhofer IESE/AISEC *Kaiserslautern, Germany*
Security Intern R&D (Part-Time) *Feb 2018 - Aug 2018*
- Building a reusable and multi-language static analysis tool for C/C++/Java for automated code security compliance testing (see here)

IUST Cloud Computing Center *Tehran, Iran*
OpenStack Intern (Part-Time) *Dec 2016 - Aug 2017*
- Secure distributed and disaggregated computing (OpenStack, Python, bash script and AWK)
- Developed VM utilization-aware schedulers for Nova, Keystone authentication methods, resource overcommitment, and VM migration scripts

Vesta Software *Tehran, Iran*
Junior Software Developer (Part-Time) *June 2014 - Dec 2016*
- Developed web services, resource-oriented APIs and micro-service banking systems (C#, ASP.NET, Jenkins, Docker, Azure)

Education

PhD in Computer Science *Saarland, Germany*
University of Saarland (UdS) *August 2019 - April 2024 (Expected)*
- Doctoral candidate, static-dynamic security analysis of web applications at scale (Advisor: Giancarlo Pellegrino, CISPA).

Double MSc. in Computer Science *Madrid, and Kaiserslautern*
Polytechnic University of Madrid (UPM) and Technical University of Kaiserslautern (TUK) *Sep 2017 - June 2019*
- Erasmus Mundus double master degree, graduated with distinction, top student (A grade), best thesis award on XS-Leak attacks.
- Advisors: Juan Caballero (IMDEA) and Avinash Sudhodanan (Meta/Facebook).

BSc. in Computer Engineering *Tehran, Iran*
Iran University of Science and Technology (IUST) *Sep 2013 - Aug 2017*
- Graduated with honors, top student (A grade), best practical thesis on OpenStack VM scheduling and authentication.

Publications

- **Soheil Khodayari**, Thomas Barber, and Giancarlo Pellegrino, "The Great Request Robbery: An Empirical Study of Client-side Request Hijacking Vulnerabilities on the Web," Proceedings of 45th IEEE Symposium on Security and Privacy, **2024**. [Link].
- **Soheil Khodayari** and Giancarlo Pellegrino, "It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses," Proceedings of 44th IEEE Symposium on Security and Privacy, **2023**. [Link].
- **Soheil Khodayari** and Giancarlo Pellegrino, "The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies," Proceedings of 43rd IEEE Symposium on Security and Privacy, **2022**. [Link].
- **Soheil Khodayari** and Giancarlo Pellegrino, "JAW: Studying Client-side CSRF with Hybrid Property Graphs and Declarative Traversals," Proceedings of 30th USENIX Security Symposium, **2021**. [Link].
- Xhelal Likaj, **Soheil Khodayari**, and Giancarlo Pellegrino, "Where We Stand (or Fall): An Analysis of CSRF Defenses in Web Frameworks," Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses, **2021**. [Link].
- Avinash Sudhodanan, **Soheil Khodayari**, and Juan Caballero, "Cross-Origin State Inference (COSI) Attacks: Leaking Website States through XS-Leaks", In: Network and Distributed System Security Symposium, **2020**. [Link].

Selected Talks

May 2023	**Everything You Wanted to Know About DOM Clobbering,** RuhrSec IT Conferencce	*Bochum, Germany*
Jun 2022	**Testability Pattern-driven Web Application Security and Privacy Testing,** EU Projects to Policy Seminar	*Brussels, Belgium*
Jun 2022	**Everything You Wanted to Know About Client-side CSRF (But Were Afraid to Ask),** OWASP AppSec EU	*Online Event*
May 2022	**The State of the SameSite (Cookies),** 43rd IEEE Symposium on Security and Privacy	*San Francisco, US*
Oct 2021	**Where We Stand (or Fall): An Analysis of CSRF Defenses in Web Frameworks,** 24th RAID Symposium	*San Sebastian*
Aug 2021	**Studying Client-side CSRF with Hybrid Property Graphs and Declarative Traversals,** USENIX Security	*Online Event*
Jun 2019	**A Framework for Testing Web Applications for Cross-Origin State Inference Attacks,** UPM Talk Series	*Madrid, Spain*

Security Advisories

- Large-scale vulnerability notification campaigns with the assistance of national CSIRTs.
- Identified and disclosed confirmed vulnerabilities to high-profile websites like Microsoft, PayPal, Linkedin, Amazon, Imgur, GitHub and Meetup.
- Contributions to the OWASP Cheat Sheet series (`https://cheatsheetseries.owasp.org`)

Community Services

- **Program Committee**: IEEE S&P (2024), CCS (2024), EuroS&P (2024), WWW (2024), SecWeb (2023).
- **Artifact Evaluation Committee**: Usenix Security 2023 [Link]; ACSAC 2022 [Link].
- **External Reviewer**: Usenix Security (2020-22), S&P 2022, ACSAC (2021-22), Euro S&P (2020-22), DIMVA 2020, WWW (2020-21), Asia CCS (2020-22).
- **Hiring Committee**: CISPA (2020).
- **Web Chair**: IEEE Euro S&P (2020).

Open-Source Projects

- **JAW**: JavaScript Analysis Framework, SAST/DAST, (https://ja-w.me).
- **DOMC-BT**: DOM Clobbering Browser Testing Service, (https://domclob.xyz).
- **TP-Framework**, SAST Testability Patterns Catalog (https://github.com/OWASP/www-project-testability-patterns-for-web-applications).
- **SameSite-Wiki**, Wiki for Cookie Policies (https://canopus-k.site/same-site-wiki).
- **Basta-COSI**: A scanner for detecting XS-Leak vulnerabilities (https://github.com/SoheilKhodayari/Basta-COSI).

Awards and Honors

2023	**CSAW Europe - Applied Research Accolade,** Grenoble INP - Esisar, France	*Valence*
2023	**Made it to MSRC 2023 Q2 Bug Bounty Leaderboard,** Black Hat, Microsoft Security	*Las Vegas*
2023	**Distinguishsed Paper Award,** IEEE S&P Symposium	*San Francisco*
2019	**Best MSc. Thesis Award,** Polytechnic University of Madrid	*Madrid*
2019	**Elite,** Graduated MSc. with distinguished GPA at TUK.	*Kaiserslautern*
2017	**Scholarship,** Received the prestigious Erasmus Mundus scholarship for academic excellence.	*EU*
2017	**Nomination,** Selected in IR2017 special talents framework by Sharif university of technology.	*Tehran*
2017	**Outstanding Student Award,** Awarded as an outstanding BSc. student of IUST for 4 consecutive years.	*Tehran*
2013	**Elite,** Placed in top 1% of the highly competitive nation-wide university entrance exam.	*Tehran*