Soheil Khodayari

Web Security Researcher

Metzer-Str 65, 66117 Saarbruecken, Germany

January, 1995 | soheil.khodayari@cispa.de | https://scnps.co | Soheil__K | github.com/SoheilKhodayari

| linkedin.com/in/soheilkhodayari | Soheil__K | Google Scholar

Bio Overview

Soheil Khodayari is a PhD candidate at CISPA, Germany, researching in the area of Web security and privacy testing, and Internet measurements. Soheil has presented and published his works on top tier security venues like IEEE S&P, NDSS, USENIX Security, Stanford SecLunch, and OWASP AppSec. He also serves as the AE PC of security conferences like USENIX and ACSAC. Among his contributions, Soheil proposed the first taxonomy and detection of XS-leaks, one of the first studies about client-side CSRF, SameSite cookies, DOM Clobbering and other client-side vulnerabilities.

Work Experience

CISPA GmbH - Helmholtz Center for Information Security

Saarbruecken, Germany

Web Security Researcher (Full-Time)

Aug 2019 - Present

- Security analysis of Web-based applications & penetration testing.
- Developing new automated security and privacy analysis tools and techniques (SAST, DAST, HAST, and IAST).
- **Tech Stack:** Python/JS/Java, SAST engines (CodeQL, Joern), DAST & browser automation (Selenium/Puppeteer/Playwright, Chrome CDP, Firefox Foxhound, BrowserStack), DBs (PostgreSQL, MongoDB, Cypher/Neo4j), Git, CI/CD, Containers & cloud (Docker, LXC, AWS, GCP).

IMDEA Software

Madrid, Spain

Security Intern R&D (Part-Time)

Sep 2018 - Aug 2019

- Penetration testing web applications; black-box security/privacy analysis and threat modeling
- Building and improving in-house tools to detect cross-origin vulnerabilities
- **Tech Stack:** Python/Django/JS, DAST & browser automation (Selenium), container and cloud systems (Docker, AWS).

Brooktec S.L.

Madrid, Spain

Web Developer (Part-Time)

Sep 2018 - July 2019

- Developing banking apps and services with GraphQL APIs on Amazon EC2 (Finametrix DQR project, Allfunds bank).
- **Tech Stack:** 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)
- **Tech Stack:** Java, Docker, and CPGs.

IUST Cloud Computing Center

Tehran, Iran

OpenStack Intern (Part-Time)

Dec 2016 - Aug 2017

- Developing Nova utilization-aware schedulers, Keystone authentication methods, resource overcommitment, and instance migration scripts.
- **Tech Stack:** Python, OpenStack, bash script and AWK.

Vesta Software

Tehran, Iran

Junior Software Developer (Part-Time)

June 2014 - Dec 2016

- Developed Web services, resource-oriented and micro-service baning systems.
- **Tech Stack:** C#/ASP.NET, SQL Server, Jenkins, Docker, Microsoft Azure.

Education

PhD in Computer Science

Saarland, Germany

University of Saarland (UdS)

August 2019 - Present

- Doctoral candidate, static-dynamic security analysis of web applications at scale (Advisor: Giancarlo Pellegrino).

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, best thesis award on XS-Leak attacks.
- Advisors: Juan Caballero and Avinash Sudhodanan.

BSc. in Computer Engineering

Tehran, Iran

Iran University of Science and Technology (IUST)

Sep 2013 - Aug 2017

- Graduated with honors, top student, best practical thesis on OpenStack VM scheduling and authentication.

Selected Talks

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: Studying the Usage, Effectiveness, and Adequacy of 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 International Symposium on Research in Attacks, Intrusions and Defenses	*San Sebastian, Spain*
Aug 2021	**Studying Client-side CSRF with Hybrid Property Graphs and Declarative Traversals,** USENIX Security	*Online Event*
Feb 2021	**JAW: Client-side CSRF,** Stanford SecLunch, Standford University	*Online Event*
Jun 2019	**A Framework for Testing Web Applications for Cross-Origin State Inference Attacks,** UPM Talk Series	*Madrid, Spain*

Publications

- It's (DOM) Clobbering Time: Attack Techniques, Prevalence, and Defenses. In **IEEE SP '23**. [Link]
- The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies. In **IEEE SP '22**. [Link]
- Where We Stand (or Fall): An Analysis of CSRF Defenses in Web Frameworks. In **RAID '21**. [Link]
- JAW: Studying Client-side CSRF with Hybrid Property Graphs and Declarative Traversals. In **USENIX Security '21**. [Link]
- Cross-Origin State Inference (COSI) Attacks: Leaking Website States through XS-Leaks. In **NDSS '20**. [Link]

Security Advisories

- Large-scale vulnerability notification campaigns with the assistance of national CSIRTs.
- Disclosed confirmed vulnerabilities to high-profile websites including PayPal, Linkedin, Amazon, Imgur, GitHub and Meetup.
- Contributions to the OWASP Cheat Sheet series.
- Patches to popular open-source libraries, like the DOMPurify sanitizer.

Community Services

- **Web Chair**: 5th IEEE European Symposium on Security and Privacy, 2020. [Link]
- **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 hiring committee 2020.

Open-Source Projects

DOMC-BT: DOM Clobbering Browser Testing

https://domclob.xyz

- An open-source (mobile and desktop) browser testing service against DOM Clobbering markups. [GitHub], [Demo]

JAW: JavaScript Analysis Framework

https://ja-w.me

- A static-dynamic security analysis framework for client-side JavaScript for the detection of taint-style vulnerabilities. [GitHub]

Basta-COSI

https://elastest.eu

- A tool to detect cross-site information leakage vulnerabilities (DAST), released as a part of the ElasTest Security Service (ESS). [GitHub]

SameSite Cookies Wiki

https://canopus-k.site/same-site-wiki

- An online service gathering cross-site attacks that can bypass SameSite cookie policies with PoCs. [GitHub]

Awards and Honors

2019	**Elite,** Best MSc. thesis award at UPM.	*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*