Shubham Agarwal

+49-173-1728310 | agarwalshubham401@gmail.com | ap0ca1ypse.in | linkedin://shubh401 | github://shubh401

PROFILE

Post-Doctoral researcher specializing in Web security, with expertise in application security, data privacy, and large-scale vulnerability detection and analysis. I currently focus on end-to-end threat analysis of Internet applications and understanding S&P perspectives of different stakeholders. In my free time, I like to tinker around with self-hosted applications and read about human civilizations and cultural philosophies..

EDUCATION

CISPA Helmholtz Center for Information Security & Universität des Saarlandes — Saarbrücken, DE
Ph.D in Computer Science, Web Security — *March 2021 - August 2025*

Universität des Saarlandes — Saarbrücken, DE
M.Sc. in Computer Science — *April 2018 – Feb 2021*

Vellore Institute of Technology, Vellore — Vellore, IN
B.Tech. in Computer Science and Engineering (with Specialization in Bioinformatics) — July 2013 – May 2017

Technical Skills

Programming & Frameworks: Python, JavaScript/TypeScript, Node.js, C++, C#.
Operating Systems: Linux (Ubuntu, CentOS, Debian), macOS, Windows, Android.
Operations, Infrastructure & Deployment: CI/CD, Docker, Kubernetes, Grafana, Prometheus, nginx, Apache.
Security Practices: OWASP Top 10, Secure Coding Practices, Threat Modeling, Vulnerability Assessment.
Protocols & Networking: OSI/IP stack, WebSockets, SSH, SSL/TLS, OAuth.
AI & Machine Learning: PyTorch, Keras, scikit-learn, AI Agents.
Others: Automation (Playwright, Selenium, etc.), REST API frameworks (Django, Flask, etc.), GraphQL, and Git.

PUBLICATIONS

· *Ali Mustafa, Jannis Rautenstrauch, Florian Hantke**, Shubham Agarwal,** Stefano Calzavara, Ben Stock. "LEAKYLINKS: Measuring the Security and Privacy Risks of URL Scanning Services"*. In IEEE S&P 2026.·
· ***Shubham Agarwa**l,* Rafael Mrowczynski, Maria Hellenthal, Ben Stock. *"I have no idea how to make it safer": Studying Security and Privacy Mindsets of Browser Extension Developers*. In USENIX Security 2025.

· ***Shubham Agarwal***, Aurore Fass & Ben Stock**.** *Peeking through the window: Fingerprinting Browser Extensions through Page-Visible Execution Traces and Interactions***.** In *ACM CCS 2024***.**

· ***Shubham Agarwal*****.** *Helping or Hindering? How Browser Extensions Undermine Security*. In *ACM CCS 2022***.**

· ***Shubham Agarwal*** & Ben Stock**.** *First, Do No Harm: Studying the manipulation of security headers in browser extensions.* In *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2021***.**

TALKS

German OWASP Day 2025 (*Link*) — *November 2025 — Düsseldorf, DE*
German OWASP Day 2024 (*Link*) — *November 2024 — Leipzig, DE*
Ad-filtering Dev Summit 2024 (*Link*) — *October 2024* — Berlin, DE

TEACHING EXPERIENCE

The Web Security Seminar — Tutorial Assistant — Saarbrücken, DE
Graduate course Offered by CISPA & Saarland University — *2021 – 22, 2022 – 23, 2024, 2024 – 25*

Thesis Supervision *(at Universität des Saarlandes)* — Saarbrücken, DE
· *Master Thesis Title: EXterminate: Disrupting Web Extensions at Scale* — *Mar 2024 – Aug 2024*
· *Bachelor Thesis Title: Longitudinal Evolution of Electron Applications Security* — *Oct 2022 – Dec 2022*
· *Bachelor Thesis Title: Temporal Analysis of the Security of Extension Updates*

Software Engineering — Tutorial Assistant — Saarbrücken, DE
Graduate course, Offered by Chair of Software Engineering, Saarland University — *Oct 2019 – Mar 2020*

ACADEMIC SERVICES

Program Committee

- Annual Computer Security Applications Conference (ACSAC) 2026, 2025.
- RAID 2026
- The Web Conference (WWW) 2026.
- MADWeb Workshop 2023 – 2026 *(Co-located with Network and Distributed System Security Symposium)*.
- International Conference on Information Systems Security 2024.
- SecWeb Workshop 2023 *(Co-located with IEEE S&P 2023)*.

Artifact Evaluation Committee

- USENIX Security 2026, 2025 *(**Noteworthy Artifact Reviewer)*, 2024 *(**Distinguished Artifact Reviewer), 2023, 2022*.
- Network and Distributed System Security Symposium 2024.

Sub-reviewer

- IEEE S&P 2025.
- Network and Distributed System Security Symposium 2025.
- USENIX Security 2024.

WORKING EXPERIENCE

Post-Doctoral Researcher — Bochum, DE
Security & Privacy Engineering Lab (SPRING), Max Planck Institute for Security & Privacy — *Since Sep 2025*

- Full-time security and privacy researcher.
- Deployment, monitoring and maintenance of Incus/LXD node clusters used for intensive computatic
- Collaboration and management of different research projects.
  - Supervision of Bachelor/Master Thesis.

Research Assistant — Saarbrücken, DE
Internet Architecture, Max Planck Institute for Informatics — *Feb 2020 – Feb 2021*

- Helped set up an in-house SDN infrastructure - C++, P4, Python.
  - Solely implemented the tests and configured the L2 routing policies for the programmable SDN.

Part-time Developer — Saarbrücken, DE
IT Inkubator (Foldio GmbH), Universität des Saarlandes — *Jun 2019 – Nov 2019*

- Collaborated and developed core product features inside a microcontroller - C++, Python.
- Implemented the core component and integrated it with the Microbit/Calliope Mini framework.
  - Helped to set up different development and testing environments for feature rollout.

Product Engineering Trainee — Bengaluru, IN
INSZoom Technologies Private Limited (now acquired by Mitratech Holdings Inc.) — *Feb 2017 – Mar 2018*

- Worked as full-stack application engineer - C#, JavaScript Frameworks, MS SQL 2016, CosmosDB.
- Designed and developed a secure authentication module to integrate third-party reporting tool..
  - Delivered the production-ready module within 60 days with a record 0 bugs.
  - *Awarded Employee of the Quarter (Q1 2018) for leadership and execution.*
- Implemented and deployed web services for routine actions and periodic notifications.
  - *Led a team of three developers and built a highly customized notification endpoint for clients/enterprises.*
- Collaborated and built automation tools to handle immigration-related documents.
  - *Reduced the intensive manual effort of mapping PDF entries to HTML form fields by 90%.*

AWARDS & RECOGNITIONS

Full Scholarship for Master's Studies — Saarbrücken, DE
International Max Planck Research School — *Apr 2018*

Hackathon Winners * 2 — Bengaluru, IN
INSZoom Technologies Private Limited — *Jun 2017 & Dec 2018*