Last Modified: 6 Mar 2025

Shubham Agarwal

agarwalshubham401@gmail.com | ap0ca1ypse.in | linkedin://shubh401 | github://shubh401

PROFILE

Ph.D. researcher specializing in Web security, with expertise in application security, data privacy, and large-scale vulnerability detection. My current research focuses on designing security and privacy assessment tools for client-side security in Web applications and browser extensions at scale.

EDUCATION

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

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

Languages & Frameworks: Python, JavaScript, TypeScript, Node.js, C++, C#, SQL, NoSQL.
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.
Security Tools: PortSwigger, Burp Suite, Wireshark, Metasploit, Nmap.
AI & Machine Learning: PyTorch, Pandas, Keras, scikit-learn, AI Agents & Ethics.
Others: Automation (Playwright, Selenium, etc.), REST API frameworks (Django, Flask, etc.), GraphQL and Git.

WORKING EXPERIENCE

Research Assistant — Saarbrücken, DE
Internet Architecture, Max Planck Institute for Informatics — *Feb 2020 – Feb 2021*
- Worked as a part-time student researcher to help set up an in-house SDN infrastructure - C++, P4, Python.
- Implemented the tests and configured the L2 routing policies for the programmable SDN.

Student Assistant — Saarbrücken, DE
IT Inkubator (Foldio GmbH), Universität des Saarlandes — *Jun 2019 – Nov 2019*
- Collaborated as a part-time engineer to develop core product features inside micro-controller - C++, Python.
- Implemented the core component and integrated it with the existing Microbit/Calliope Mini framework.

Product Engineering Trainee — Bengaluru, IN
INSZoom Technologies Private Limited (now acquired by Mitratech Holdings Inc.) — *Jun 2017 – Mar 2018*
- Worked as full-stack application development engineer - C#, JavaScript Frameworks, MS SQL 2016, CosmosDB.
- Designed and developed a secure authentication module and integrated a third-party dashboard-ing tool.
  - Awarded Employee of the Quarter (Q1 2018) for leadership and execution.
- Implemented and deployed web services for routine actions and periodic notifications.
- Collaborated and built automation tools as part of a team project to handle immigration-related documents.

PROJECTS

ML Applications in Medical Diagnosis & Potential Adversarial Impacts — Python, PyTorch, Keras
Machine Learning Models & Adversarial Attacks — *Nov 2020 – Jan 2021*
- Performed binary and multi-class classification on the diabetic retinopathy image dataset using CNN and GAN techniques.
- Executed multiple poisoning and evasion attack techniques on the ML model and assessed their impact.

Large-scale Measurement of Client-side CSRF Vulnerability on Web — Python, JavaScript, Postgres, Docker, Git
Web Security & Large-scale Vulnerability Assessment (Master Thesis) — *Oct 2019 – Apr 2020*
- Conducted large-scale measurement on Tranco Top 1 Million URLs to investigate the impact of persistent state on client-side and the attackers' ability to exploit for Cross-site Request Forgery (CSRF) attacks.
- Created end-to-end crawling and analysis framework by setting up CI/CD infrastructure.
- Reported vulnerabilities across 3,000 sites, highlighting significant security gaps affecting millions of users.

IPC Provenance & SELinux Extensions in Android — Linux, Android, C++, Java
Mobile Applications & Access-Control Mechanisms — *Dec 2019 – Jan 2020*

- Implemented extended IPC call chains in Android middleware to enable fine-grained identity tracking.
- Formulated SELinux policies in the Linux kernel for enhanced access-control management of sensitive resources and services.

Enterprise Autofill Assistant for Immigration-related Documents — JavaScript, REST APIs
Browser Extensions & Client-side Data Storage — *Dec 2017 – Mar 2018*

- Developed a privacy-friendly browser extension to autofill personal details on immigration documents.
- won the 1st Prize to develop a working prototype during the Hackathon.
- Extended the prototype to a cross-browser enterprise solution for customers.

PUBLICATIONS

- *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 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*

Master/Bachelor Thesis Supervision — Saarbrücken, DE
- *Master Thesis Title: EXterminate: Disrupting Web Extensions at Scale* — *Mar 2024 – Aug 2024*
- *Bachelor Thesis Title: It's not the same anymore: Temporal Analysis of the Security of Browser Extension Updates* — *Oct 2022 – Dec 2022*

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

ACADEMIC SERVICES

Program Committee
- International Conference on Information Systems Security 2024.
- MADWeb Workshop 2025, 2024, 2023 *(Co-located with Network and Distributed System Security Symposium).*
- SecWeb Workshop 2023 *(Co-located with IEEE S&P 2023).*

Artifact Evaluation Committee
- USENIX Security 2025, 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.

AWARDS & RECOGNITIONS

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

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