Shubham Agarwal

shubham.agarwal@cispa.de | +49(0)-1514-369-2885

EDUCATION

CISPA & UDS
PH.D. COMPUTER SCIENCE[*]
Since Mar, 2021 | Saarbrücken, DE

SAARLAND UNIVERSITY
MSc. COMPUTER SCIENCE
Feb, 2021 | Saarbrücken, DE
Cum. GPA: 1.6 / 4.0

VELLORE INSTITUTE OF TECHNOLOGY
B.TECH. COMPUTER SCIENCE
(SPEC. IN BIOINFORMATICS)
May, 2017 | Vellore, IN
Cum. GPA: 8.78 / 10.0

LINKS

Personal:// **shubh401**
GitHub:// **shubh401**
LinkedIn:// **shubhamagarwal401**

COURSEWORK

GRADUATE
Web Security
Mobile Security
Data Networks
ML in Cybersecurity
Privacy Enhancing Techniques
Artificial Intelligence

UNDERGRADUATE
Data Structures & Algorithms
Operating Systems
Data Mining & Warehousing
Software Project Management
Database Management System

SKILLS

PROGRAMMING
Over 5000 lines:
Python • JavaScript • C# • SQL
Over 1000 lines:
C++ • Java • PHP • NoSQL

OPERATING SYSTEMS
Linux (with Android) • Windows

AWARDS

- **Employee of the Quarter** - INSZoom
- **Hackathon Winner * 2** - INSZoom
- **Grant for Graduate Studies** - IMPRS

EXPERIENCE

MAX PLANCK INSTITUTE FOR INFORMATICS | STUDENT ASSISTANT - INTERNET ARCHITECTURE
Feb, 2020 - Feb, 2021 | Saarbrücken, DE
- **Technology Stack** - C++, Python & P4
- Low-level (L2/L3) topology & routing design and implementation for programmable SDNs.

SAARLAND UNIVERSITY | TEACHING ASSISTANT - SE 2019
Oct, 2019 - Mar, 2020 | Saarbrücken, DE
- Project Manager for course projects involving graduate students and third-party clients.

IT INKUBATOR (UDS) | STUDENT ASSISTANT
Jun, 2019 - Nov, 2019 | Saarbrücken, DE
- **Technology Stack** - C++ & TypeScript
- Core Library Development and Integration.

INSZOOM | PRODUCT ENGINEERING TRAINEE
Feb, 2017 – Mar, 2018 | Bangalore, IN
- **Role** - Full Stack Application Development.
- **Technology Stack** - ASP.NET MVC Framework, C#, MS SQL 2016 (Relational + Document/JSON), JavaScript frameworks.
- **Major Contributions** - Design & Implementation of Secure Authentication Module, Web Services for Routine Actions, Third-Party REST Web API Integration, Chrome Extensions, Database Design, User Interfaces and Automated Testing Modules.

RECENT PROJECTS

- **Investigation of the Impact of Manipulating Security Headers by Browser Extensions*** | Research Immersion Lab | Large-scale analysis of chrome extensions that alter security headers and quantifying associated threat.

- **Client-Side CSRF Vulnerabilities in Web Applications** | Master Thesis | Python, JavaScript, NodeJS, SQL | Large-scale analysis of top 1 million web applications to investigate Client-Side CSRF by implementing automated web framework.

- **ML Applications in Medical Diagnosis & Potential Adversarial Impacts** | ML in CyberSecurity | Python | Evaluation of various evasion & poisoning attacks on medical dataset & leveraging DC-GAN to synthesize new similar data points.

- **IPC Provenance & SELinux Extensions** | Android Security | Java, C++ | Extended IPC call-chain tracking & SELinux policies in Android middleware for fine-grained identity & access-control management over privileged resources.

PUBLICATIONS

- **First, Do No Harm: Studying the manipulation of security headers in browser extensions.** | Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2021.