Security testing research techniques for SAP

Opportunity for a 6-month internship

Security Research @ SAP Labs France
Sophia-Antipolis – France

Maintaining security is a constantly shifting task, and we need to respond with continuous learning and research. The portfolio of SAP Security Research contains those topics that we believe are most important for SAP's security future.
SAP's vision to secure business is built on 3 ideals: **Zero-Vulnerability**, to harden the software by eliminating vulnerabilities, **Defensible Application**, to enable the software to identify and prevent attacks, and **Zero-Knowledge**, to make any theft of data useless through encryption.
Considering these aspects, SAP Security Research covers the following focal areas: Anonymization for Big Data, Secure Internet of Things, Software security analysis, Open-source analysis, Deceptive application, Applied cryptography, Quantum technology, and Machine Learning as enabler for the next generation of security.

Security Research proposes a 6-month internship in its Sophia-Antipolis offices (Mougins, France).

INTERNSHIP TOPIC

The increasingly large number of vulnerabilities that affect web-based applications has severe consequences. Attackers rely on these flaws to routinely compromise millions of web sites, steal personal and financial data, and penetrate private infrastructures.

To mitigate the Web's security problems many techniques and tools have been developed over the years. The three major approaches to identify vulnerabilities are SAST (static application security testing), DAST (dynamic application security testing) and IAST (Interactive application security testing). SAST requires the source code of the application while DAST and IAST require the application to be up-and-running and ready for passive/active testing. All the three approaches feature pro and cons. In general, SAST is subject to false positives (report attacks that are not real attacks) while DAST to false negatives (miss real attacks). IAST features almost zero false positives, but it requires complete ownership of the testing landscape in which IAST agents must be deployed to monitor the execution of the application and the coverage of the analysis depends on the available functional tests as well as on the available techniques to amplify this coverage.

We at SAP Security Research have been working on DAST techniques to detect vulnerabilities such as logic flaws [NDSS2016] and CSRF [EuroSP2017]. These techniques have been further developed and experimented internally at SAP to reach a more mature status. Fuzzing could be used to increase the effectiveness of these techniques. In this internship, we aim to further progress our techniques and to integrate them within best-suited penetration test frameworks (e.g., OWASP ZAP) to enable broader adoption, possibly also outside SAP.

More specifically, the goals of the internship are as follows:

- Understanding the SAP development process
- Understanding SAST, DAST, and IAST approaches (possibly experiencing with concrete tools/techniques)
- Studying challenging vulnerabilities (e.g., CSRF and logic flaws)
- Investigating existing and novel solutions to detect these vulnerabilities a high degree of automation
- Contributing to the development of our testing framework at SAP, also by integrating these solutions within best-suited frameworks (e.g., OWASP ZAP)
- Assessing this framework against real world SAP and non-SAP scenarios
- Support SAP internal users toward the consumption of this framework
- Documenting the developed software and the overall activities

Bibliography:

- [NDSS2016]: Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications. A. Sudhodanan, A. Armando, R. Carbone, L. Compagna. NDSS 2016.

- [EuroSP2017]: Large-Scale Analysis & Detection of Authentication Cross-Site Request Forgeries. A. Sudhodanan, R. Carbone, L. Compagna, N. Dolgin, A. Armando, U. Morelli. Euro S&P 2017.

We expect that 30% of time will be dedicated to research activities, and 70% to development and experiments.

CANDIDATE PROFILE

- University Level: Last year of MSc and behind
- Good skills in modelling, analysis and programming (Python, Java)
- Good skills in web technologies (HTTP, HTTPS, server/client-side programming language)
- Security background
- Fluency in English (working languages)
- Good oral and written communication skills

INTERNSHIP CONTEXT

SAP

Founded in 1972, SAP has grown to become the world's leading provider of business software solutions. SAP is market leader in enterprise application software. The company is also the fastest-growing major database company. Globally, more than 77% of all business transactions worldwide touch an SAP software system. With more than 347.000 customers in more than 180 countries, SAP includes subsidiaries in all major countries. SAP is the world's largest inter-enterprise software company and the world's third-largest independent software supplier, overall. SAP solutions help enterprises of all sizes around the world to improve customer relationships, enhance partner collaboration and create efficiencies across their supply chains and business operations. SAP employs more than 98.600 people.

Security Research at SAP Labs France, Sophia Antipolis

Based at SAP Labs France Mougins, Security Research Sophia-Antipolis addresses the upcoming security needs, focusing on increased automation of the security life cycle and on providing innovative solutions for the security challenges in networked businesses, including cloud, services and mobile.

STANDARD INTERNSHIP PACKAGE

- *Salary*: depending on the length of the internship and your diploma.
- *Lunch*: SAP Labs France has a local cafeteria; interns contribute 2,63 €uro/lunch, like other SAP employees.
- *Holidays*: French Bank Holidays
  - January 1st; April 12th, April 13th, May 1st, May 8th, May 21st, June 1st, July 14th; August 15th, Nov 1st and 11th; December 25th
- *Travel*: no trip will be paid by SAP.
- *Accommodation*: SAP can propose an accommodation for the duration of your internship. The accommodation is subsidized by SAP: the intern pays half of the rental cost: 342€ for a 1-room apartment or 442€ for a 2-room apartment (Choice depending on the availability).

CONTACTS AND PROCEDURE

Please candidate by clicking on this link:
https://career5.successfactors.eu/sfcareer/jobreqcareer?jobId=232928&company=SAP&username=

UPLOAD (all documents must be in English):

- Your CV
- Cover letter
- Any relevant documents