Advanced Security Testing Strategies for Web Applications

Opportunity for a 6-month internship

Security Research @ SAP Labs France
Sophia-Antipolis – France

SAP's security vision is built on 5 ideals to secure business: Defendable Application, Zero-Knowledge, Zero-Vulnerability, Security by Default, and Transparency.
SAP's security research group lays the foundation for realising the vision: The 30+ researchers of the Security Research unit focus on security engineering (e.g., the automation of the secure software development lifecycle), secure business execution (e.g., business process security and security in cloud based business applications) and secure operations (e.g., secure maintenance and support of complex and heterogeneous cloud IT landscapes).

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 two major approaches to identify vulnerabilities are static and dynamic analysis security testing, in short SAST and DAST. SAST requires the source code of the application while DAST requires the application to be up-and-running and ready for active testing. Both 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).

Though some companies are successfully reducing the number of security vulnerabilities in our code base via security testing strategies based on both SAST and DAST, there is still a big gap to close towards approaching the vision of "zero vulnerabilities". This gap is mainly caused by limitations of the tools and techniques used, in terms of (i) precision of findings (for instance, false positives reported by SAST), (ii) the lack of tool support for more challenging problems (for instance, systematic detection of XSS, CSRF, logical vulnerabilities), and (ii) the need for automated solutions for well-known problems like SQL Injection so to manage the complexity of software security analysis (for instance, the continuous emergence of new technologies and related vulnerabilities).

In the above-described context, the specific goals of the internship are as follows:

- Understanding the SAP development process
- Understanding SAST and DAST approaches as well as experiencing with concrete tools/techniques
- Studying challenging vulnerabilities (e.g., CSRF and logic flaws) and investigating solutions to detect them with a high degree of automation
- Contributing to the development of our testing framework at SAP, based on SAPUI5 technology
- Contributing to the development of our testing core engine
- Assessing our testing engine against real world SAP and non-SAP scenarios
- Support SAP internal users toward the consumption of the testing framework
- Documenting the developed software and the overall activities

Technologies/techniques involved are: Python, JavaScript, SAST/DAST tools (e.g., OWASP ZAP), and Machine Learning

We expect that 25% of time will be dedicated to research activities, and 75% to development.

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

Over the past 45 years, SAP has grown to become the world's leading provider of business software solutions. With 12 million users, 96,400 installations, and more than 1,500 partners, 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 group includes subsidiaries in over 180 countries and employs more than 84 000 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 2,40 €uro/lunch, like other SAP employees.
- *Holidays*: French Bank Holidays
    - January 1st; April 2nd, May 1st, May 8th, May 10th, May 21st, 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 send **in English** your CV, a cover letter and any relevant documents to the following persons stating the title of the Internship in the subject: [Internship Application] **Advanced Security Testing Strategies for Web Applications**.

Supervisor
Luca Compagna
luca.compagna@sap.com
Tel. +33-(0)4-9228 6495

Administrative point of contact
Sylvine Eusebi
sylvine.eusebi@sap.com
Tel. +33-(0)4-92286477