IDP – AI / Machine Learning (m/f)

You are looking for an exciting and challenging IDP in a young IT-startup? You like to collect hands-on experience and take responsibility for development of our product? You are interested in the startup ecosystem and like to learn about the challenges of founding a company by working hand-in-hand with the founders? Then join our team!

Crashtest Security GmbH is a young Munich-based startup, which was founded in 2017. We offer an automated penetration test for web applications, which integrates into the agile development environment. With our service we want to revolutionize the security testing market and become the first to offer a fully automated penetration test covering the OWASP Top 10.

Possible Assignments
Evaluate with us, if the following topics can help us, to be more cost and time efficient:
• Improving existing vulnerability scanners using Machine Learning
• Recognizing similar pages (e.g. product pages, user profiles, …) and determine how they have to be scanned
• Developing a concept and a prototype to test the business logic of applications
• You have a different idea on how to improve our business using Machine Learning? Tell us about your idea and we will try to find a way to realize it.

What we are looking for...
• Master student with focus on computer science
• Knowledge in one of the following programming languages: Python or PHP
• Self-motivated, organized and driven to succeed with an entrepreneurial flair
• Work smart mentality
• Excellent written and oral communications skills in English, German is a plus

What we offer...
• A cutting-edge agile software development environment: We use Continuous Integration and Deployment to regularly release new versions of our service to the cloud (JIRA, TeamCity, Nexus, etc.)
• A scalable cloud architecture on AWS to run your components at scale (CloudFront, RDS, S3, SQS, EC2, Kubernetes, Docker, etc.)
• The startup experience: freedom to take responsibility, flexibility in the organisation of your work hours and area of responsibility, a curious and helpful team, which will support you to quickly get started with our technology stack
• We know that developers turn coffee into code, so we have a supply with coffee, spezi and beer waiting for you!
• Opportunity to continue working with us as after the IDP as an intern, working student or full-time employee

We are looking forward to receiving your application!
Please send your CV or a link to your LinkedIn-Profile to jobs@crashtest-security.com.
TUM Chair

This IDP is in cooperation with the Chair of Entrepreneurial Finance 2. Professor Reiner Braun and Sara Utmishi, Dipl-Kffr. (Univ.) will be supervising the Project. In terms of the required lecture, we recommend “Private Equity”.

(https://www.ef.wi.tum.de/fileadmin/w00bnp/www/Syllabi/Course_Syllabus_Private_Equity_WS1718.pdf)

Motivation

Security scans (e.g. penetration testing) are an integral part of a security strategy for a corporate which develops web applications. Due to the lack of internal IT security knowledge, such scans are often done by a third-party contractor. The TUM Start-up Crashtest Security offers a web application security scanner, which can be integrated into the software development lifecycle to allow continuous security scans.

A manual security scan usually costs between 1.000€ and 100.000€. The exact costs depend on the scope of the security scan. The major part of the price is the manual labour of security specialists. With an automated security scan, the price of a single scan can be reduced to a few Euros or even Cents. A major part of the price are the costs related to the operation of the security scan such as cost for server and network traffic.

In a typical web application such as an online shop, there exist multiple pages which have similar content. For example, an online shop may have the webpages /article/chair, /article/table, /article/armchair and offer hundreds or thousands of further articles. These pages are structured in the same way, share their source-code and therefore can be attacked using the same attack technique. If only one of these pages is scanned for security vulnerabilities, the result is representative for all the similar pages.

If a security scanner can detect similar pages, this can reduce the scanning cost, as only a fraction of server computation time and network traffic is used.

Methodology

A machine learning algorithm within the website spider should identify similar webpages during a security scan. It may use the site URL, the DOM of the website and further information to classify the pages. Further security scans will then only be started for one of the identified similar pages. Based on the machine learning algorithm, it will be shown how time and cost are saved compared to a traditional scan without the classification of websites.

Specification

The IDP students work includes implementing a machine learning algorithm that classifies webpages and analyse whether the implementation saves time and money for the resulting security scans. The expected result of the IDP is, to give a recommendation whether such an algorithm does save time and money and should be included in all security scans or not.