Sichere Anwendungsentwicklung für Programmierumgebungen am Beispiel von CodeOcean

Hintergrund

CodeOcean ist eine webbasierte, open-source Programmierumgebung für das Erlernen von Programmiersprachen. Die Plattform wird sowohl für Vorlesungen am HPI eingesetzt als auch für Online-Programmierkurse im Rahmen von openHPI, openSAP und mooc.house.

Während der Kurslaufzeit stellt CodeOcean dabei für über 11.000 Lernende bis zu 2,5 Millionen containerbasierte Ausführungsumgebungen pro Monat bereit, in denen die Programme der Lernenden kompiliert und unter Ressourceneinschränkungen ausgeführt werden. Ein- und Ausgaben werden dabei in Echtzeit über eine WebSocket-Verbindung zwischen der jeweiligen Ausführungsumgebung und dem beteiligten Browser ausgetauscht.

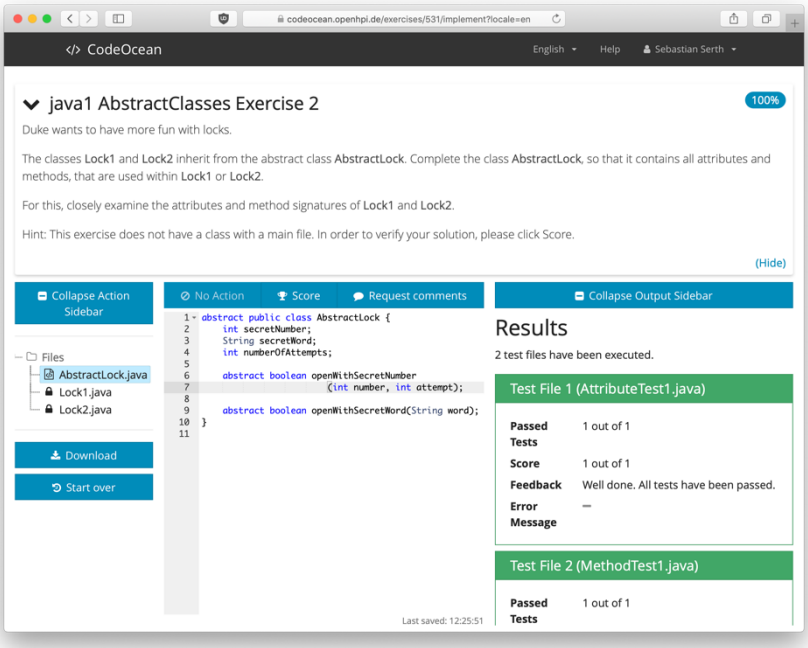

Abbildung 1: Implementierung einer vorgegebenen Programmieraufgabe aus einem Java-Kurs von openHPI in CodeOcean mit Anzeige der Testergebnisse

Aufgabenstellung

In Kooperation mit dem Berliner Unternehmen Security Research Labs (SRLabs) ist es das Ziel des Projekts, Methoden und Techniken zu untersuchen, die die Konzipierung und den Betrieb von Software in diesem Kontext ermöglichen. Durch ihren Funktionsumfang und den serverseitigen Betrieb bieten Programmierumgebungen wie CodeOcean umfangreiche Angriffsflächen, vor denen sich Betreiber schützen müssen.

Dazu zählen sowohl gängige Maßnahmen im Bereich der Webserver-Sicherheit als auch spezifische Schutzmaßnahmen im Bereich der Container-Sicherheit für die Ausführung von

fremden Quellcode auf eigenen Servern. Im Rahmen des Bachelorprojekts sollen somit einerseits mögliche Schwachstellen und Probleme identifiziert, als auch die praktische Lösung dieser betrachtet und umgesetzt werden.

Dabei sollen sowohl die Datensicherheit gesteigert als auch technische Aspekte berücksichtigt werden, die zu einem sicheren und flexibel skalierbaren Gesamtsystem führen. So soll gewährleistet werden, dass auch zukünftige Einsatzszenarien und die steigende Anzahl an Lernenden der Online-Kurse mit zusätzlichen Ressourcen versorgt werden kann. Die vorhandene Implementierung von CodeOcean stellt dabei die Ausgangsbasis der neu zu implementierenden Funktionalitäten dar. Grundsätzliche Architekturentscheidungen sowie einzelne Komponenten des Projektes sollen auf Basis der erarbeiteten Sicherheitsziele neu bewertet und Verbesserungen implementiert werden.

Die Techniken und Ansätze sollen dabei im Rahmen von CodeOcean implementiert und getestet werden. Hier ist das Ziel, bereits erfüllte Anforderungen diverser Stakeholder (wie die hohe Interaktivität, Unterstützung für diverse Programmiersprachen, Einsatz im Rahmen von mehreren Online-Kursen und -Plattformen) weiterhin abdecken zu können, während das Sicherheitslevel und die Skalierbarkeit der Gesamtapplikation erhöht wird.

Ziele

Die Ziele dieses Bachelorprojektes sind insbesondere:

(1) Erlernen von Techniken zur Analyse von bestehenden Anwendungen und Infrastrukturen.
(2) Identifikation von Techniken zur sicheren Implementierung von Web-Applikationen.
(3) Erörtern von Systemarchitekturen für Fehler-Resiliente Softwaresysteme in Bezug auf deren IT-Sicherheit.
(4) Anwendung von Aspekten für sichere Systemarchitekturen und Techniken am Beispiel von CodeOcean.

Die Ergebnisse dieses Projektes sollen im Rahmen der Bachelorarbeit sowie der Implementierung und Dokumentation von CodeOcean festgehalten sowie nach Möglichkeit produktiv eingesetzt werden. Das Projekt wird sowohl Bestandteile aus dem Security Engineering als auch dem IT-Systems Engineering beinhalten und bietet Gestaltungsspielraum für die Einbringung eigener Interessensgebiete.

Projektpartner

Security Research Labs

Security Research Labs (SRLabs)

Kontakte im HPI

Daniel Köhler	Leonard Marschke	Sebastian Serth	Prof. Dr. Christoph Meinel
H-1.13	H-1.13	H-E.34	H-1.5
daniel.koehler@hpi.de	leonard.marschke@hpi.de	sebastian.serth@hpi.de	christoph.meinel@hpi.de