

Studenten	Joël Schwab, Ryan Horiguchi
Examinator	Ivan Bütler
Themengebiet	Sicherheit

## Backdoors

**Einleitung:** Eine Backdoor (auch Trapdoor oder Hintertür) bezeichnet einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. In dieser Arbeit war das Ziel, sowohl Möglichkeiten von applikatorischen Backdoors zu ermitteln, als auch drei Varianten davon in einer eigenen Docker basierten Mini-Anwendung zu implementieren. Ziel von diesen mit Hintertüren versehenen Mini-Anwendungen ist es, zukünftige Security Experten damit zu beüben, damit deren Fähigkeiten hinsichtlich dem Auffinden von Backdoors geschult werden kann. Die erste Mini-Anwendung ist eine web-basierte Closed Sourced Applikation. Der Student erhält für das Finden des Backdoors keinen Zugriff auf den Quellcode. Der Student soll die Anwendung analysieren und das Backdoor finden. Für dieses Backdoor wird das Wissen von Verschlüsselungsalgorithmen benötigt. Die zweite Mini-Anwendung ist ebenfalls eine web-basierte Applikation, bei welcher der Quellcode offengelegt wird. Der Student soll im Code diverse Abhängigkeiten und Fehlimplementationen finden, um innerhalb der Mini-Anwendung administrative Rechte (Admin) zu erlangen. In der dritten Backdoor Implementation ist der Source Code der Anwendung ebenfalls öffentlich. Diesen muss der Hacker genau analysieren, um festzustellen, wie man sich ihn zu nutzen machen kann, um mehr Rechte zu vergeben, als der Entwickler geplant hat.