Projekt: Erstellen und Validieren von IT-Sicherheitsdemos

Prof. Dr. Kappes

Winter-Semester 2021/2022 Projekt Bachelor

Einführungs-Tasks

In den ersten beiden Wochen sollen Einführungstasks bearbeitet werden. Dazu soll eine kleine Präsentation erstellt werden mit etwa einer Folie pro Thema. Zur Einarbeitung sollen *SQL-Injection*-Methoden erarbeitet werden.

1. Beschäftigen Sie sich mit Containern und Virtualisierung. Richten Sie sich eine Virtuelle Maschine mit Kali-Linux ein. Starten Sie den `hello-world` Docker-Container. Wie unterscheiden sich Container von Virtuellen Maschinen?
2. Geben Sie einen Überblick über die SQL-Sprache. Was ist die Data Definition Language? Was ist die Data Manipulation Language? Welche Alternativen zu SQL-Datenbanken gibt es?
3. Richten Sie sich eine SQL-Datenbank in einem Docker-Container ein (bspw. MySQL oder Postgres). Richten Sie sich ein Schema ein und befüllen es mit Beispiel-Daten.
4. Bauen Sie eine kleine Web-Anwendung mit einer einzigen Seite. Anforderungen:
   - Nutzer können ihre eigenen Einträge in der Datenbank in einer HTML-Tabelle sehen.
   - Über ein Formular mit einem Textfeld können die gezeigten Einträge weiter gefiltert werden. Die Filterung *muss* von einer SQL-Abfrage durchgeführt werden.
   - Über ein Formular können Nutzer neue Einträge hinzufügen.

   Technologie und Sprache auf dem Backend ist beliebig, aber benutzen Sie kein Object-Relational Mapping (ORM).
5. Erklären Sie das Prinzip von SQL-Injection. Zeigen Sie Beispiele.

6. Passen Sie Ihr Web-Backend so an dass es anfällig für SQL-Injection ist. Demonstrieren Sie dabei Angriffe:
    - Setzen Sie SQL-Injection beim Filtern ein um auf Einträge anderer Nutzer zuzugreifen.
    - Setzen Sie SQL-Injection beim Einfügen ein um Einträge für andere Nutzer anzulegen. Hinweis: Die Datenbank-Abfrage muss dafür mehrere SQL-Statements erlauben, in Python bspw. mittels `executescript()`.
    - Setzen Sie SQL-Injection beim Einfügen neuer Einträge ein um Einträge zu löschen.
7. Erklären Sie mögliche Verteidungs-Techniken gegen SQL-Injection.
8. Passen Sie Ihr Web-Backend wieder an sodass es gegen SQL-Injection abgesichert ist. Demonstrieren Sie dass die bisherigen Angriffe nicht mehr funktionieren.
9. Schreiben Sie eine kurze Anleitung (ca. 2 Seiten) anhand derer die Leser SQL-Injection besser verstehen können. Gestalten Sie die Anleitung verständlich, bspw. durch den geeigneten Einsatz von Abbildungen, Links und Referenzen. In der Anleitung soll die Zielsetzung, der Aufbau und die Installation Ihrer Demo klar werden.
10. Erklären Sie das Scrum-Framework.

Relevante Literatur

SQL-Injection wird in vielzähligen Büchern und Artikeln behandelt, bspw.:

- *SQL Injection Attacks and Defense* von Justin Clarke. 2009, Elsevier.
- *The Web Application Hacker's Handbook* von Dafydd Stuttard. 2011, Wiley.
- *A classification of SQL-injection attacks and countermeasures* von William Halfond, Jeremy Viegas und Alessandro Orso. Erschienen in *Proceedings of the IEEE international symposium on secure software engineering. Vol. 1*. 2006, IEEE.
- *SQL-Injection* in der PHP-Dokumentation. https://www.php.net/manual/de/security.database.sql-injection.php
- *Scrum Guide*. https://scrumguides.org/

Kontakt-Information

Email: kappes@fb2.fra-uas.de
johannes.bouche@fb2.fra-uas.de
lukas.atkinson@fb2.fra-uas.de