THM TECHNISCHE HOCHSCHULE MITTELHESSEN

Max Stephan

Timon Pellekoorne

MNI Mathematik, Naturwissenschaften und Informatik

Secure Software Engineering (SS 23)

14. April 2023 — Übungsblatt 1 — 1

Bitte bereiten Sie Präsentationsfolien vor, falls Sie die Aufgaben in der nächsten Übung vorzustellen möchten.

Aufgabe 1 Enkodieren Sie ihr THM Kürzel mit dem SHA3-256 Verfahren. Geben Sie anschliessend den kodierten String im Feedbacksystem ab.

Wie Sie in der Vorlesung gelernt haben, ist SHA3-256 kein sicheres Verfahren zum Hashing von Passwörtern. Recherchieren Sie ein geeignetes Verfahren, um eine Softwareanwendung auf ein neues Hash-Verfahren umzustellen. Beschreiben Sie die Migration in Ihrer Präsentation und begründen Sie, warum Sie sich für das neue Hash-Verfahren entschieden haben.

Aufgabe 2 (Verschlüsselte Datei). Laden Sie sich die mit AES-256-CBC verschlüsselte Datei (encoded.txt) für diese Aufgabe aus dem Moodlekurs herunter, knacken Sie das Passwort und entschlüsseln Sie die Datei. Geben Sie dann den entschlüsselten Inhalt im Feedbacksystem ab.

Hinweis: Schreiben Sie ein Bash-Skript, dass die üblichsten Passwörter durchprobiert. Das Passwort ist ziemlich kurz. Zum Vorab-Testen der Funktionalität des Befehls `openssl enc -d -aes-256-cbc -a -in encoded.txt -pass pass:<password>`, versuchen Sie die über Moodle erhältliche Datei `encrypted_test.txt` mit dem Passwort `secret` zu entschlüsseln.
Beachten Sie, dass `openssl` auch einen *Return-Code* von 0 liefert, obwohl das Passwort fehlerhaft ist. Schauen Sie sich die Ausgabe dieser *false-positives* an und überlegen Sie, wie Sie auch diese herausfiltern können.

Aufgabe 3 (Passwort Überprüfung). Implementieren Sie ein Programm (beliebige Sprache), das ein Passwort als Input entgegen nimmt und dieses auf seine Stärke überprüft. Nutzen Sie hierbei die in der Vorlesung vorgestellten Methoden zur Überprüfung der Passwortstärke. Hierbei dürfen Sie **keine** externe Bibliothek benutzen.

Aufgabe 4 (Gefakte Email). Verschicken Sie eine Email mit dem Absender „Guenter Schabowski <Schabowski@stasi.de>“, Absendedatum „09.11.1989 18:00:00“ und dem Subjekt: „Ups <Ihre CAS-Kennung> <Datum und Uhrzeit>“. Außerdem sollte im Plain-Body „Endlich mal Urlaub in Spanien“ stehen, im HTML-Body aber „Entschuldige Egon.“. *Hinweis:* Nutzen Sie nicht Ihr Standard-Email Programm, sondern verschicken Sie die Email z.B. über Java, PHP oder nodeJS.