Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Modul Datenmanagement (DMG)

Übung DS: Datensicherheit

1. Selbststudium

☞ Lesen Sie Kapitel 3.8 aus dem Buch von Kaufmann & Meier (2016) Beantworten Sie dabei folgende Fragen:

? Was heisst Datensicherheit? Schutz vor unbefugtem Zugriff

? Welche Rolle spielen Sichten für die Datensicherheit? Dienen als Schutz von Spalten & Zeilen oder von Individualdaten durch Aggregation

? Was heisst Grant? Was heisst Grant Option? "gewähren" <- Rechte zuteilen. Grant Option erlaubt die Rechte weiterzugeben

? Was ist SQL-Injection? Wie schützt man sich davor?
SQL-Injection bedeuted, das illiegale einschliessen von SQL-Code um den erlaubten Zugriff zu umgehen.
Schutz durch: PreparedStatements oder Stored Procedures

2. Views und Grants

Gegeben ist die Ausgangslage in der Beispieldatenbank Uni auf ihrem lokalen MySQL Server. Die Professoren dürfen jeweils nur die Vorlesungen verändern (update, delete, insert), die von Kollegen mit dem gleichen Rang durchgeführt (gelesenVon) werden. Alle Professoren dürfen die Vorlesungen der Kollegen mit gleichem Rang abfragen (select). Zudem dürfen Professoren mit Rang C4 die Vorlesungen der Kollegen mit Rang C3 abfragen, aber nicht umgekehrt.

☞ Erstellen Sie pro Professor ein Benutzer mit gleichem Benutzernamen. Wählen Sie als Passwort ‚@' plus den Namen. Das Passwort müsste zuerst mit SELECT MD5(<pw>) encrypted werden
siehe Seite 2 Anhang

☞ Erstellen Sie zwei (änderbare) Sichten (updateable views), zusammen mit den entsprechenden Rechtevergaben, welche diese Anforderungen erfüllen.

➔ Alle Professoren mit Rang C4 sollen das Recht SELECT, INSERT, UPDATE und DELETE auf die View view_c4 kriegen.
```
CREATE VIEW view_c4 as SELECT * FROM professoren WHERE rang = 'C4'
GRANT SELECT INSERT UPDATE DELETE
 ON view_c4 TO professorenC4
```

➔ Zudem sollen Professoren mit Rang C4 das Recht SELECT auf die View view_c3 erhalten.
```
GRANT SELECT ON view_c3 TO professorenC4
```

➔ Alle Professoren mit Rang C3 sollen das Recht SELECT, INSERT, UPDATE und DELETE auf die View view_c3 kriegen.
```
CREATE VIEW view_c3 as SELECT * FROM professoren WHERE rang = 'C3'
GRANT SELECT INSERT UPDATE DELETE
 ON view_c3 TO professorenC3
```

Annahme: professorenCx ist die Gruppe mit professoren vom Rang x

3. SQL Injection

☞ Lösen Sie das Level 1 des SQL-Injection Hackits von gehaxelt:

http://hackit.gehaxelt.in

Dr. sc. inf. Michael Alexander Kaufmann

Dokumentieren Sie Ihr Vorgehen und ihre Lösung möglichst genau und nachvollziehbar.

- ☞ Optional: lösen Sie die Levels 2-6 des gleichen Hackits.
- ☞ Bonusaufgabe für echte Hacker: Posten Sie den String „DMG was here :)“ Red Tiger’s Hackit.

(das haben bisher noch keine Studierenden geschafft.)

Zuerst wollten wir mit einfachen Abfragen wie: 1 OR ‘1’ = ‘1 ausprobiert. Dies ohne Erfolg.
Nach etwa 10min ausprobieren haben wird dann die Lösung im Internet gesucht und durchgespielt

4. Abgabe der Übung

- ☞ Ergänzen Sie ihr Dokument mit den Namen der Teammitglieder, welche zur Lösung der Aufgabe beigetragen haben.
- ☞ Erstellen Sie ein PDF mit den Lösungen zu den Aufgaben: Übung_DS_Gruppe_<XY>.pdf
- ☞ Laden Sie die Datei als PDF auf ILIAS in den Briefkasten DS
- ☞ Abgabetermin: Siehe Semesterplan Detail (auf ILIAS > Organisatorisches)

Anhang:

Aufgabe 2:

```
CREATE ROLL Sokrates LOGIN ENCRYPTED PASSWORD ‘@Sokrates’
CREATE ROLL Russel LOGIN ENCRYPTED PASSWORD ‘@Russel’
CREATE ROLL Kopernikus LOGIN ENCRYPTED PASSWORD ‘@Kopernikus’
CREATE ROLL Popper LOGIN ENCRYPTED PASSWORD ‘@Popper’
CREATE ROLL Augustinus LOGIN ENCRYPTED PASSWORD ‘@Augustinus’
CREATE ROLL Curie LOGIN ENCRYPTED PASSWORD ‘@Curie’
CREATE ROLL Kant LOGIN ENCRYPTED PASSWORD ‘@Kant’
```