SVS | Exercise 3

Task 1

1. Was ist Session Hijacking? Welche Möglichkeiten für den Angriff gibt es?
2. Die Seite https://mytuc.org/vwfx ermöglicht es einem registrierten Nutzer, die PIN-Nummer seiner Mobilfunkkarte einzusehen (z.B. Nutzername „Max“ und Passwort „Mustermann“). Finden Sie die PIN-Nummer des Nutzers „John“ heraus.

1. What is Session Hijacking? Which kind of attacks do you know?
2. The page https://mytuc.org/vwfx enables registered users to retrieve the PIN number of his mobile phone (e.g. using username *Max* and password *Mustermann*). Find out the PIN number of user *John*.

Task 2

Richten Sie eine MySQL-Datenbank[1] ein:

1. Legen Sie eine Datenbank namens {URZ Nutzername}-*svs* an. In der Datenbank legen Sie eine Tabelle namens *personen* an. Die Tabelle soll folgende Spalten enthalten:
   - id: INT, Index: PRIMARY, AUTO_INCREMENT
   - name: CHAR(20)
   - age: INT
2. Fügen Sie einige Datensätze hinzu.
3. Schreiben Sie eine SQL-Anfrage, die alle Personen zurückgibt, die *Max* heißen.
4. Erweitern Sie das Programm *personen.php* um die obere SQL-Anfrage. Platzieren Sie es in dem Dokumenten-Verzeichnis Ihres

Install a MySQL database[1]:

1. Create a database named *{URZ Nutzername}-svs*. In this database create a table named *personen*. The table should contain the following columns:
   - id: INT, Index: PRIMARY, AUTO_INCREMENT
   - name: CHAR(20)
   - age: INT
2. Add some data to the table.
3. Write an SQL query, which returns all persons, whose name is *Max*.
4. Extend the program *personen.php* to send the above query to the database. Place the

---

[1]

a) Die virtuelle Maschine aus der Übung 2 hat die Datenbank schon vorinstalliert. Mittels der Verwaltungssoftware (http://localhost/phpmyadmin, Nutzername: *root*, Passwort: *!vsruser!*) können Sie die Datenbanken einsehen und modifizieren.
b) URZ bietet ebenfalls einen Datenbankdienst an (https://www.tu-chemnitz.de/urz/db)
c) Sie können auf Ihrem System ein XAMPP Paket installieren (https://www.apachefriends.org).

a) The virtual machine from the 2nd tutorial has the database already installed. Using the management software (http://localhost/phpmyadmin, Nutzername: *root*, Passwort: *!vsruser!*) one can inspect and modify the database.
b) The university computer center (URZ) offers a database service (https://www.tu-chemnitz.de/urz/db)
c) You can install a XAMPP package on your system (https://www.apachefriends.org).

Webservers[2] und rufen Sie die Seite in dem Webbrowser auf.

5. Erweitern Sie das Programm um die Suchfunktionalität. Nur wenn ein Name eingegeben wird, sollen die dazugehörigen Daten (*id* und *age*) angezeigt werden. Verwenden Sie String-Konkatenation für den Aufbau der SQL-Anfrage.

file into the document folder of your Web server and open the page in a browser.

5. Extend the program with search functionality. Only if a name is entered, corresponding data (id and age) should be shown. Use string concatenation to build SQL query.

Task 3

Rufen Sie die Seite aus der Aufgabe 2 auf.

1. Was kann man in das Suchfeld eingeben um **alle** Personen in der Tabelle anzuzeigen?
2. Was kann man eingeben um festzustellen, ob es neben der Tabelle *personen* noch eine nicht leere Tabelle gehaelter in derselben Datenbank gibt?
3. Beantworten Sie die folgende Fragen:
   a. Welche Fehler werden bei SQL-Injection-Angriffen ausgenutzt?
   b. Welche Möglichkeiten zur Durchführung von SQL-Injection kennen Sie?
   c. Welche Schutzmechanismen gibt es dagegen?

Open the page from task 2.

1. What you can enter into the search field to find **all** persons in the table?
2. What can you enter to find out, if the current database contains a non-empty table *gehaelter*?
3. Answer the following questions:
   a. Which mistakes are exploited during SQL-Injection attacks?
   b. Which possibilities to inject SQL queries do you know?
   c. Which defense mechanisms against SQL injection exist?

Homework

Unter https://mytuc.org/yngk ist ein Formular zur Abfrage von Nutzerdaten vorhanden. Einer der registrierten Nutzer hat die Zugangsdaten „user1“, „pass1“. Finden Sie heraus, welche Nutzer es noch im System gibt.

At https://mytuc.org/yngk one can find a form to request user data based on a username and a password. One valid pair is *user1* and *pass1*. Find out, which further users exist in the table.

[2] Z.B. in dem *public_html*-Verzeichnis des URZ-Homeordners