COMPUTER SUBJECT:	BASIC NETWORK CONCEPTS
TYPE:	GROUP WORK EXERCISE/DISCUSSION
IDENTIFICATION:	SQLInjection/MC
COPYRIGHT:	*Michael Claudius & Homayoon Fayez*
LEVEL:	INTERMEDIATE
DURATION:	2 hours - 1 month
SIZE:	50 lines!!
OBJECTIVE:	Injection of login pages
REQUIREMENTS:	**Network Security Essentials**
COMMANDS:	

IDENTIFICATION: SQL-Injection/MICL&MOFA

Prolog

The IT-Security company, SmartICT is looking for smart guys/girls with hacking skills, The salary is really high but you have to prove your skills in practice. The owner, Mohammed Fayez, (mofa@securemail.com) currently busy investigating a serious intrusion in DeBeers Ltd and his young assistant, Michael Claudi, (micl@securemail.com) have setup this assignment as a test.

Facebook information

Looking at Mr. Fayez Facebook profile you discover that he has an agricultural farm here in Denmark growing various traditional vegetables like carrots, peas, potatoes, tomatoes and so on. He is very found of these vegetables especially cucumber.

The Mission

You are to make a simulation of an attack on home page with a PHP-login to a backend system which is based on DB with a table with user information. The DB-server is unknown but it is probably a relational DB based on SQL.

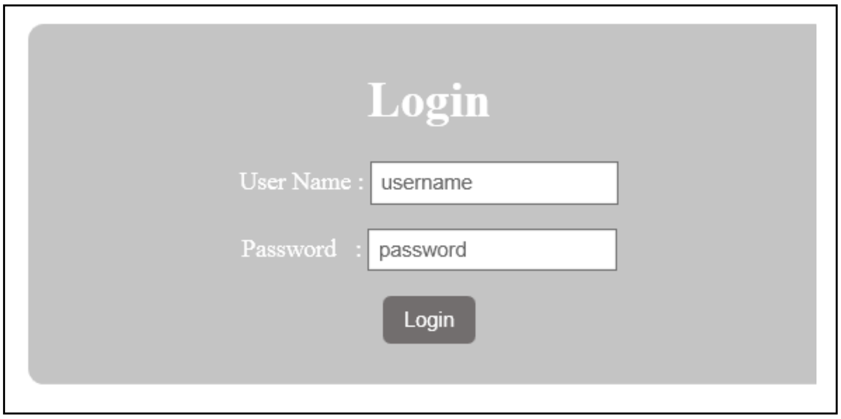
Purpose

The purpose is to find out as much as possible about the information hidden behind the link:

https://smartict.dk/sites/zealand/sqlinjection/login.php

http://www.smartict.dk/smartict/login.php (OUTDATED !Q)

where there is just one login page:



Useful links

http://www.w3schools.com/sql/sql_injection.asp;
General description

http://www.unixwiz.net/techtips/sql-injection.html; many tricks here
Tip: If you want to use ideas then copy and paste the examples into a Notepad document

Assignment 1: DB-table information

a. Prove that SQL-sentence is used to verify the user
b. Find the name of the DB server

c. Find 3 column attributes
d. Find the name of the table
e. Prove that there are more than 3 column attributes
f. Find all column attributes
g. Verify the structure of the SQL-sentence behind the stage

Assignment 2: DB-table intrusion

a. Show how to login to the system without knowing anything…
b. Guess the administrator username. Can you prove this as well?
c. Guess the administrator password
   (Normally not possible/easy requires password cracking BUT maybe tracking can used)
d. Try to insert a fake user in the system.

Assignment 3 The Net

Can you find some SQL-injection tools for hacking this site?

Assignment 4 The Net

Investigate some home pages you normally visit and test their vulnerability for SQL-Injection.
This is of course an illegal act and I have no responsibility for your actions.
Maybe its better to wait next week where we also introduce hack.me..