Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Εργαστήριο 2 – Επιθέσεις SQL Injection

Προετοιμασία

1. Αποσυμπιέστε το zip αρχείο που περιέχει το *xampp* (http://www.apachefriends.org/download.php?xampp-win32-1.6.8.zip)
2. Αποσυμπιέστε τα αρχεία στο *acme_bank.zip* στο .../xamp/htdocs (Το αρχείο αυτό βρίσκεται στην προσωπική σελίδα του διδάσκοντα).
3. Βεβαιωθείτε ότι οι apache και mysql servers έχουν εκκινηθεί σωστά.

Δημιουργία βάσης

1. Μέσω του *phpmyadmin*, δημιουργείστε βάση και πίνακα με τα ακόλουθα στοιχεία:

   όνομα βάσης : **acmeBank**
   πίνακας : **customer**
   πεδία customer : - ***fullname*** (varchar 20)
   - ***balance*** (int)
   - ***accno*** (int)
   - ***username*** (varchar 20)
   - ***password*** (varchar 20)

2. Εισάγετε στη βάση τουλάχιστον τρεις (3) εγγραφές.

Επίθεση SQL Injection

1. Εκτελέστε SQL injection ώστε να αποκτήσετε πρόσβαση στα στοιχεία ενός πελάτη, παρακάμπτοντας το συνθηματικό πρόσβασης.

   περιγραφή:

2. Εκτελέστε SQL injection ώστε να αποκτήσετε πρόσβαση στα στοιχεία όλων των πελατών της βάσης, με μία μόνο απόπειρα πρόσβασης.

   περιγραφή:

3. Αφαιρέστε τη συνάρτηση *stipslashes*() από τον κώδικα php που περιέχεται στο αρχείο *bank.php* και επαναλάβετε τις παραπάνω επιθέσεις. Είναι εφικτή η επίθεση sql injection;

   Παρατηρήσεις: