SQL Injection Attack Lab

Computer Security

Some Tips

- Debugging PHP/MySQL:
  - Original Code:

```
$sel1 = mysql_query("SELECT
ID,name,locale,lastlogin,gender FROM user
WHERE (name = '$user' OR email = '$user')
AND pass = '$pass'");
```

  - New Code:

```
$dbstr = "SELECT
ID,name,locale,lastlogin,gender FROM user
WHERE (name = '$user' OR email = '$user')
AND pass = '$pass'";
$sel1 = mysql_query($dbstr);
echo “dbstr=”.$dbstr.“, sel1=”.$sel1;
die(); // Used to terminate php script.
// Remove die() when you are sure that your
string is correct
```

Some Tips

- Debugging PHP/MySQL:
  - Open terminal and run “`mysql -u seed -pseedubuntu`”
  - Then type “`use sql_collabtive_db;`”
  - Now you can run the result of `echo $dbstr` in this program and make sure that your syntax is correct

Example

Tasks

- Task 1
  - Make sure that there is a space and a character following your ‘--’
- Task 2
  - Use http://hash.online-convert.com/sha1-generator to generate SHA1 hashes
  - Don’t forget to set the name field in the form (as this can cause a conflict in the primary keys)

Tasks

- Task 3
  - 3.1) Turn magic_quotes_gpc on and retry your earlier attacks
  - 3.2) Search the file for this line: //modified for SQL Lab and see if mysql_real_escape_string() can help

Tasks

- 3.3) Update:

```
// FROM THE SEED MANUAL,
$db = new mysqli("localhost", "root",
"seedubuntu", "sql_collabtive_db");
// Set the db query
$dbstr=“UPDATE user SET name=? WHERE
ID=?”;
// Prepare the statement
$stmt = $db->prepare($dbstr);
// Bind the parameters
$stmt->bind_param(“ss”, $name, $id);
// Run the query
$upd = $stmt->execute();
```

Tasks

- 3.3) Select:

```
// FROM THE SEED MANUAL,
$db = new mysqli("localhost", "root", "seedubuntu",
"sql_collabtive_db");
// Set the db query
$dbstr = "SELECT name,locale,gender FROM user WHERE
(name = ? OR email = ?) AND pass = ?“;
// Bind the parameters
$stmt->bind_param("sss", $user, $email, $pass);
// Run the query
$stmt->execute();
// Create a result array
$chk = array('name'=>‘temp',
'locale'=>'temp','gender'=>‘temp' );
// Bind the result of the SQL to the array
$stmt->bind_result($chk['name'],
$chk['locale'],$chk['gender']);
// Fetch the result
$stmt->fetch();
```