CS456 Assignment 3: Web Security

Gavin Stankovsky

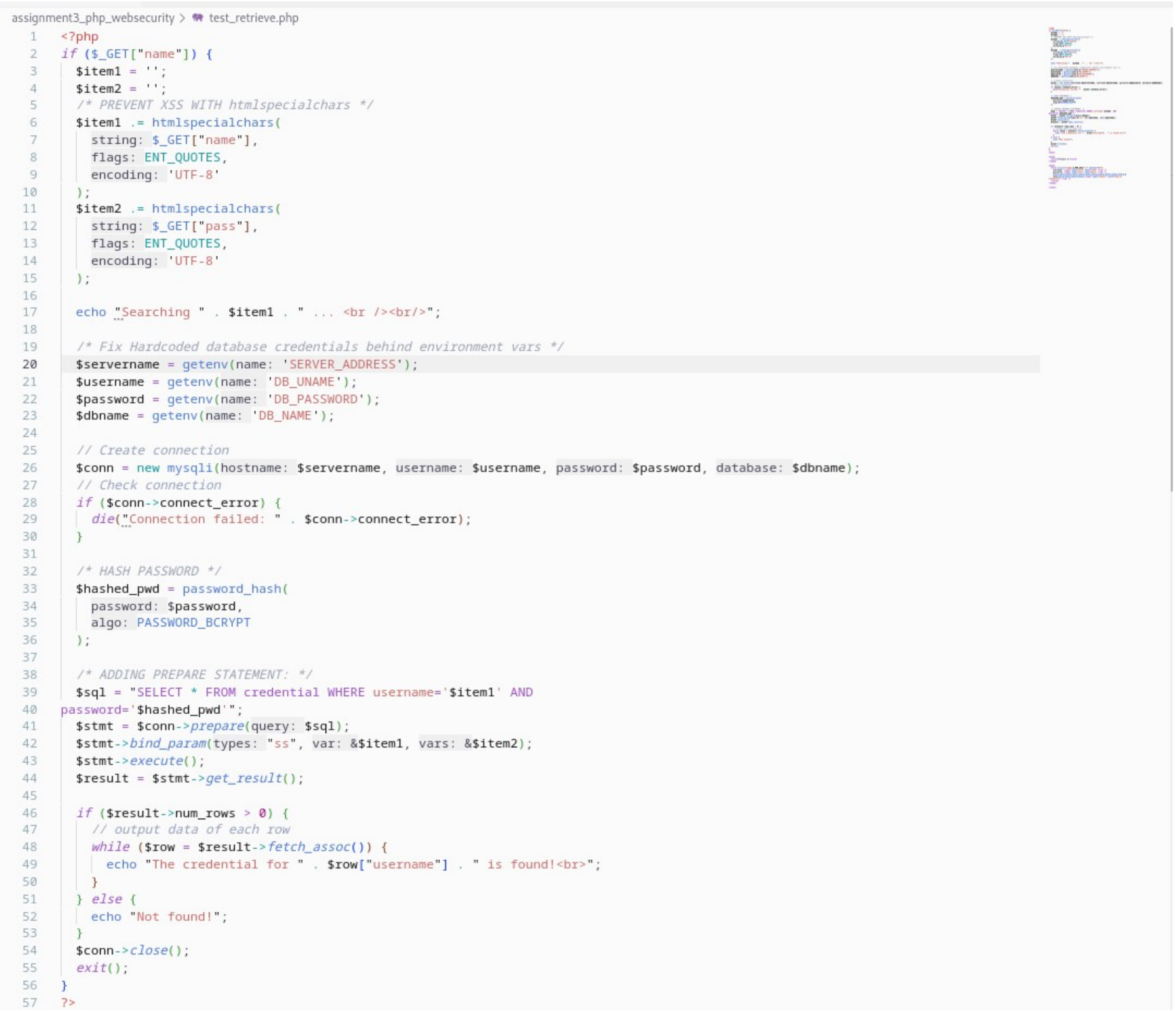
Vulnerabilities:

1. No prepared statements for input to the sql query. User input is directly executed in the query.
2. User input is inserted into the html document directly, allows XSS attacks.
3. Database credentials are hard-coded in the php file.
4. Passwords are stored as plain text in database.

Fixes:

1. Use a prepared statement for executing sql queries, prevents against SQL Injections.
2. Sanitize user input for escape characters using htmlspecialchars(), prevents XSS.
3. Store database credentials in environment variables on privileged device/account.
4. Password should be compared to hashed version stored in database (test_add.php would be hashing and storing so I simulated that here).

Amended Source Code:



assignment3_php_websecurity > test_retrieve.php

```php
<?php
if ($_GET["name"]) {
  $item1 = '';
  $item2 = '';
  /* PREVENT XSS WITH htmlspecialchars */
  $item1 .= htmlspecialchars(
    string: $_GET["name"],
    flags: ENT_QUOTES,
    encoding: 'UTF-8'
  );
  $item2 .= htmlspecialchars(
    string: $_GET["pass"],
    flags: ENT_QUOTES,
    encoding: 'UTF-8'
  );

  echo "Searching " . $item1 . " ... <br /><br/>";

  /* Fix Hardcoded database credentials behind environment vars */
  $servername = getenv(name: 'SERVER_ADDRESS');
  $username = getenv(name: 'DB_UNAME');
  $password = getenv(name: 'DB_PASSWORD');
  $dbname = getenv(name: 'DB_NAME');

  // Create connection
  $conn = new mysqli(hostname: $servername, username: $username, password: $password, database: $dbname);
  // Check connection
  if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
  }

  /* HASH PASSWORD */
  $hashed_pwd = password_hash(
    password: $password,
    algo: PASSWORD_BCRYPT
  );

  /* ADDING PREPARE STATEMENT: */
  $sql = "SELECT * FROM credential WHERE username='$item1' AND
password='$hashed_pwd'";
  $stmt = $conn->prepare(query: $sql);
  $stmt->bind_param(types: "ss", var: &$item1, vars: &$item2);
  $stmt->execute();
  $result = $stmt->get_result();

  if ($result->num_rows > 0) {
    // output data of each row
    while ($row = $result->fetch_assoc()) {
      echo "The credential for " . $row["username"] . " is found!<br>";
    }
  } else {
    echo "Not found!";
  }
  $conn->close();
  exit();
}
?>
```