SAD Project

Due April 12th 9:00am

**NOTE:**  
The application connects to the underlying database using the following user account. You are to setup this “TEST” user account on the database server before the application will create the underlying database.

$dbServername = "localhost";  
 $dbUsername = "TEST";  
 $dbPassword = "";  
 $dbName = "secureappdev";

**Deliverable:**   
You are to produce a report highlighting the following for each vulnerability:

1. The vulnerability identified with brief description
2. Actions to take in order to reproduce the vulnerability
   1. Where the vulnerability exists
   2. The type of http request (GET, POST)
   3. Vulnerable parameter / behaviour
   4. Payload / Actions to reproduce the vulnerability
3. Code fix

Vulnerability’s contained in this application to be mitigated

* Reflective XSS
* Persistent XSS
* Brute force the perimeter of the application
* Session Management
* Insecure Password Storage
* SQLi (Not covered in class yet)
* CSRF (Not covered in class yet)
* Directory Traversal (Not covered in class yet)

**Submission:**  
Please email your completed report to ***richard.butler@setu.ie***