# PHP and MySQL E-Commerce

## PCI Compliance

PCI DSS 🡪 Payment Card Industry Data Security Standard. We do not want to store the user’s credit card information

Requirements

* Build and maintain a secure network
* Protect Cardholder Data
* Maintain a Vulnerable Management Program
* Implement Strong Access Control Measures
* Regularly Monitor and Test Networks
* Maintain an Information Security Policy

The technical difference between dedicated and collocated hosting is that the host typically owns a dedicated server whereas we typically own a collocated one.

### Payment System

Payment Processors 🡪 It is a delayed payment system that normally goes through a third-party site.

Payment Gateway 🡪 It is a real-time payment system that can be directly integrated into our own site.

Thumb Rule for Database

* Public: SELECT
* Customer: SELECT, INSERT, UPDATE
* Admin: SELECT, INSERT, UPDATE, DELETE

## Secure Transactions

Secure Sockets Layer (SSL) defines a protocol protecting data transmitted over public networks. SSL is an absolute must for e-commerce site. SSL provides encryption, decryption of data passed back and forth between the server and the client.

## Types of Attacks

### Protecting the User

**Cross-Site-Scripting**

It can be injecting JavaScript into the components of user inputs and therefore, steal the user cookies or execute code to steal the personal data. This can be easily avoided using PHP function **strip\_tags()**, this removes any HTML, JavaScript or PHP from any string

## Protecting the Site

**Denial of Service**

It attempts to connect to our simultaneously from all around the world and causing the server to be busy

**SQL Injections**

Tricking MySQL with comments. A double hyphen (--) is used in SQL to comment out the remainder of a line of SQL code.

We can use the PHP and SQL function combined function **mysqli\_real\_escape\_strings()**, it **e**scapes special characters in a string for use in an SQL statement, taking into account the current charset of the connection.

We should typecast all values that should be numeric to force them to be numbers.

**$id = (int)$\_GET[‘id]**

**Remote File Inclusion (RFI)**

The hacker attempts to get a site to include a file found on another server, PHP, when it calls fopen(), require(), include(), **LFI (Local File Inclusion)** attack is similar to RFI allows sensitive data like password to be read and displayed🡪 this can be prevented if the server do not use system() and exec() PHP functions.

**Cross-Site Request Forgeries**

A cross-site request forgery(CSRF) is an attack that attempts to cause a victim to unknowingly send arbitrary HTTP requests, usually to URLs requiring privileged access and using the existing session of the victim to determine access. We can prevent this by creating unique tokens

**$token = md5(uniqid(rand(),true))**

**$\_SERVER['HTTP\_USER\_AGENT']**

### Summary

|  |  |
| --- | --- |
| **Functions** | **Usage Reason** |
| **strip\_tags()** | Removes any HTML, JavaScript or PHP from any string |
| **mysqli\_real\_escape\_string()** | Escapes special characters from the string |
| **(int)$\_GET[‘id’]** | Typecast the numeric values |
| **$token = md5(uniqid(rand(), true))**  **$\_SERVER['HTTP\_USER\_AGENT']** | Halts unwanted arbitrary HTTP requests and prevents use of existing session |

1. <? php session\_start();
2. $token = md5(uniqid(rand(), true));
3. $agent = $\_SERVER['HTTP\_USER\_AGENT'];
4. $\_SESSION['token'] = $token;
5. $\_SESSION['agent'] = $agent;
6. setcookie('token', $token, time() + (86400 \* 30), "/");
7. setcookie('agent', $agent, time() + (86400 \* 30), "/");
8. echo "<!DOCTYPE html>";
9. echo "  <html lang = 'en'>";
10. echo "      <head>";
11. echo "          <title> Form </title>";
12. echo "          <meta charset = 'UTF-8'/>";
13. echo "          <meta name = 'viewport' content = 'width=device-width; initial-scale=1'/>";
14. echo "      </head>";
15. echo "      <body>";
16. echo "          <form method = 'post' action = 'handleForm.php'>";
17. echo "              <input type = 'hidden' name = 'token' value = '".$token."'/>";
18. echo "              <input type = 'hidden' name = 'agent' value = '".$agent."'/>";
19. echo "              <label for = 'data'> Data </label><br/>";
20. echo "              <input type = 'text' name = 'data' /><br/><br/>";
21. echo "              <input type = 'submit' name = 'submit' value = 'Confirm'/>";
22. echo "          </form>";
23. echo "      </body>";
24. echo "  </html>"; ?>
25. <? php session\_start();
26. define('DB\_USER', 'root');
27. define('DB\_PASS', '');
28. define('DB\_HOST', 'localhost');
29. define('DB\_NAME', 'ecommerce1');
30. if ($\_SERVER['REQUEST\_METHOD'] == 'POST'): if (isset($\_SESSION['token']) && isset($\_SESSION['agent'])): if (isset($\_COOKIE['token']) && isset($\_COOKIE['agent'])): if ($\_POST['submit']): if ($\_POST['token'] == $\_SESSION['token']): if ($\_POST['agent'] == $\_SESSION['agent']): if ($\_POST['token'] == $\_COOKIE['token']): if ($\_POST['agent'] == $\_COOKIE['agent']): $connection = mysqli\_connect(DB\_HOST, DB\_USER, DB\_PASS, DB\_NAME);
31. $strip = $\_POST['data'];
32. $escape = mysqli\_real\_escape\_string($connection, $strip);
33. echo "You entered: ".$escape.
34. "<br/>";
35. echo "Your token: ".$\_POST['token'].
36. "<br/>";
37. echo "Your agent: ".$\_POST['agent'].
38. "<br/>";
39. echo "Current agent: ".$\_SERVER['HTTP\_USER\_AGENT'].
40. "<br/>";
41. else :echo "Cookie Agent do not match";
42. endif;
43. else :echo "Cookie Token do not match";
44. endif;
45. else :echo "Session Agent do not match";
46. endif;
47. else :echo "Session Token do not match";
48. endif;
49. else :echo "Form did not get submitted";
50. endif;
51. else :echo "Token and Agent Cookie is not set";
52. endif;
53. else :echo "Token and Agent Session is not set!";
54. endif;
55. else :echo "It is not a post request!";
56. endif; ?>

## Database Design

The **categories**, **pages**, and **pdfs** tables 🡪 **Product Side**

**categories** table 🡪 Lists the categories into which the HTML content will be organized.

**pages** table 🡪 stores the actual HTML content 🡪 **title, description and content**

**Pages**

**title 🡪** It will be used as a **link to each page** and will also be used as the **browser’s title**

**description 🡪** Describes the page content

**content** 🡪 Stores the actual html content

**PDF**

It lists the particulars for each PDF file the site has

**Users**

This table stores a minimum amount of information about the customers. Each customer can create a username, stores their email address, a password, first name and their last name.

Enum, It represents the list of options whether administrator or member. The date\_expires

column stores the data through which their account is active.

**Orders**

This table swill stroe every that goes through PayPal, associated with the ID. Three pieces of information will be recorded: the transaction\_id, payment status, payment amount

**Primary Key**

* There can only be one primary key in a table
* In some DBMS it cannot be NULL - e.g. MySQL adds NOT NULL
* Primary Key is a unique key identifier of the record

**Unique Key**

* Can be more than one unique key in one table
* Unique key can have NULL values
* It can be a candidate key
* Unique key can be NULL and may not be unique

Primary key makes the table row unique (i.e, there cannot be 2 rows with the exact same key). We can only have 1 primary key in a database table.

Unique key makes the table column in a table row unique (i.e., no 2 table rows may have the same exact value). You can have more than 1 unique key table column (unlike primary key which means only 1 table column in the table is unique).

`backtick` allows us to use ridiculously column names in tables. Ex: **bro,so,cool,man**

**CATEGORIES**

1. CREATE TABLE categories(id SMALLINT NOT NULL AUTO\_INCREMENT, category VARCHAR(30) NOT NULL, PRIMARY KEY(id), UNIQUE KEY category(category))

**ORDERS**

1. CREATE  TABLE  orders(id  INT  UNSIGNED  NOT  NULL  AUTO\_INCREMENT,  user\_id  INT  UNSIGNED  NOT  NULL,  transaction\_id  VARCHAR(30)  NOT  NULL,  payment\_status  VARCHAR(30)  NOT  NULL,  payment\_amont  DECIMAL(6.2)  UNSIGNED  NOT  NULL,  payment\_data\_time  TIMESTAMP  NOT  NULL  DEFAULT  CURRENT  TIMESTAMP  PRIMARY  KEY(id),  KEY  user\_id(user\_id))

**PAGES**

1. CREATE TABLE pages(id MEDIUMINT UNSIGNED NOT NULL AUTO\_INCREMENT, category\_id SMALLINT UNSIGNED NOT NULL, title VARCHAR(100) NOT NULL, description TINYTEXT NOT NULL, content LONGTEXT NOT NULL, date\_created TIMESTAMP NOT NULL DEFAULT CURRENT\_TIMESTAMP, PRIMARY KEY(id), KEY category\_id(category\_id), KEY creation\_date(date\_created))

**PDFS**

1. CREATE TABLE pdfs(id SMALLINT UNSIGNED NOT NULL AUTO\_INCREMENT, tmp\_name CHAR(40) NOT NULL, title VARCHAR(100) NOT NULL, description TINYTEXT NOT NULL, file\_name VARCHAR(40) NOT NULL, size MEDIUMINT UNSIGNED NOT NULL, date\_created TIMESTAMP NOT NULL DEFAULT CURRENT\_TIMESTAMP, PRIMARY KEY(id), UNIQUE KEY tmp\_name(tmp\_name), KEY dat\_created(date\_created))

**USERS**

1. CREATE TABLE users(id INT UNSIGNED NOT NULL AUTO\_INCREMENT, type ENUM('memeber, admin') NOT NULL, username VARCHAR(30) NOT NULL, email VARCHAR(80) NOT NULL, pas VARBINARY(32) NOT NULL, first\_name VARCHAR(20) NOT NULL, last\_name VARCHAR(40) NOT NULL, date\_expires DATE NOT NULL, date\_created TIMESTAMP NOT NULL DEFAULT CURRENT\_TIMESTAMP, date\_modified TIMESTAMP NOT NULL DEFAULT ‘0000-00-00 00:00:00’, PRIMARY KEY(id), UNIQUE KEY username(username),
2. UNIQUE KEY email(email)))

## Server Organization

🡪 Administration Files

🡪 CSS

🡪 Vendor

🡪 Images

🡪 Media

🡪 PHP includes

🡪 JavaScript

🡪 Test

### PHP Includes

**config.inc.php 🡪** It is a script that defines the sites’ general behavior and various constants.

**footer.php 🡪** It is the half of the HTML template

**form\_functions.inc.php 🡪** It defines a function used by every form

**header.php 🡪** It is the other half of the HTML template

**login.inc.php 🡪** It handles the login process

**login\_form.inc.php 🡪** It is the login form

**mysql.inc.php 🡪** Database connection

### Database Connection

#### mysqli.inc.php

**mysqli\_set\_charset($dbc, 'utf8')**

It indicates which character set should be used for communications between PHP and the database.

1. <? php define('DB\_HOST', 'localhost');
2. define('DB\_USER', 'root');
3. define('DB\_PASS', '');
4. define('DB\_NAME', 'ecommerce1');
5. $dbc = mysqli\_connect(DB\_HOST, DB\_USER, DB\_PASS, DB\_NAME) or die("Server Denied");
6. mysql\_set\_charset($dbc, 'utf8');
8. function escape\_data($data) {
9. global $dbc;
10. return mysqli\_real\_escape\_string(trim($data), $dbc);
11. }

#### PHP Closing Tag Omitting

* Functionality Loss 🡪 Redirecting User 🡪 User payment not processed properly
* Excess Line Endings 🡪 Error in Ajax response/JSON
* Downloads in our web app may causing the app to break in the long run

Therefore, leaving an extra space or blank line after the closing tag will cause problem. When other scripts will have this file included, it will result in headers being sent to the Web browser. If the including (parent) script later attempts to send a cookie, start a session, or redirect the browser, we will get “headers already sent” error message.

### Config File

#### config.inc.php

**$\_SERVER['DOCUMENT\_ROOT']**

Get the root of each site

**Custom Error Handler**

It is useful to automatically notify the coder where the problem lies.

**set\_error\_handler("err\_handler")**

This script can declare a catch-all function that is called by PHP when an error condition occurs

**err\_handler($e\_level, $e\_message, $e\_file, $e\_line, $e\_vars)**

Error Levels

|  |  |
| --- | --- |
| 2 | Warnings |
| 8 | Notice |
| 256 | User Error |
| 512 | User Warning |
| 1024 | User Notice |
| 4096 | Recoverable Error |
| 8191 | All |

The **debug\_backtrace()** function generates a PHP back trace.

This function displays data from the code that led up to the **debug\_backtrace()** function.

Returns an array of associative arrays. The possible returned elements are:

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Description** |
| function | string | The current function name |
| line | integer | The current line number |
| file | string | The current file name |
| class | string | The current class name |
| object | object | The current object |
| type | string | The current call type. Possible calls:  Returns: "->"  - Method call  Returns: "::"  - Static method call  Returns nothing - Function call |
|  |  |
|  |  |
|  |  |
| args | array | If inside a function, it lists the functions arguments. If inside an included file, it lists the included file names |

**error\_log()**

This function sends an error message to a log, to a file, or to a mail account.

1. <? php $live = false;
2. $contact\_email = "khan.photon@gmail.com";
3. define('BASE\_URI', '/E-Commerce/includes/pdfs/');
4. define('BASE\_URL', '/E-Commerce/');
5. define('MYSQL', '/E-Commerce/includes/mysql.inc.php');
6. session\_start();
7. function my\_error\_handler($e\_number, $e\_message, $e\_file, $e\_line, $e\_vars) {
8. global $live, $contact\_email;
9. $message = "An error occured in script {$e\_file} on line {$e\_line}: \n {$e\_message}\n";
10. $message. = "<pre>".print\_r(debug\_backtrace(), 1). "</pre>\n";
11. $message. = "<pre>".print\_r($e\_vars, 1).
12. "</pre>\n";
13. if (!$live): echo "<div class = 'bgd-danger text-white error'>".nl2br($message).
14. "</div>";
15. else: error\_log($message, 1, $contact\_emails, "From:khan.photon@gmail.com");
16. endif;
17. if ($e\_number != E\_NOTICE): echo "<div class = 'bgd-danger text-white error'> A system error occurred. We apologize for the inconvenience. </div>";
18. endif;
19. return true;
20. }
21. set\_error\_handler("my\_error\_handler");

## HTML Template (Sample Non-Dynamic)

1. < !DOCTYPE html > < html lang = "en" > < head > < meta charset = "UTF-8" / > < meta name = "viewport"
2. content = "width=device-width,  initial-scale=1" / > < title > Knowledge is Power: And It Pays to Know < /title> < link rel = "stylesheet"
3. href = "../vendor/bootstrap.min.css" / > < link rel = "stylesheet"
4. href = "../CSS/style.css" / > < script src = "../vendor/jquery.min.js" > < /script> < script src = "../vendor/popper.min.js" > < /script> < script src = "../vendor/bootstrap.min.js" > < /script> < /head> < body > < div class = "row"
5. id = "wrap" > < div class = "col header text-center bg-light" > < h1 > < a href = "index.php"
6. class = "nounderline" > < code class = "text-info" > Knowledge is Power < /code> < /a> < /h1> < h2 > < code class = "text-warning" > and it pays to know < /code>  < /h2> < /div>  < /div> < div class = "row" > < nav id = "nav"
7. class = "col navbar navbar-expand-sm navbar-dark bg-dark sticky-top" > < a class = "navbar-brand"
8. href = "#" > & nbsp; < code class = "text-warning" > Code Break! < /code> < /a> < button class = "navbar-toggler"
9. type = "button"
10. data - toggle = "collapse"
11. data - target = "#collapsibleNavbar" > < span class = "navbar-toggler-icon" > < /span> < /button> < div class = "collapse navbar-collapse"
12. id = "collapsibleNavbar" > < ul class = "navbar-nav" > < li class = "nav-item active" > < a href = "index.php"
13. class = "nav-link" > < code class = "text-info" > Home < /code> < /a> < /li> < li class = "nav-item" > < a href = "about.php"
14. class = "nav-link" > < code class = "text-info" > About < /code> < /a> < /li> < li class = "nav-item" > < a href = "contact.php"
15. class = "nav-link" > < code class = "text-info" > Contact < /code> < /a> < /li>                   < li class = "nav-item" > < a href = "register.php"
16. class = "nav-link" > < code class = "text-info" > Register < /code> < /a> < /li> < /ul> < /div> < /nav> < /div> < div class = "page row" > < div class = "col content" > < /div> < /div> < /body> < /html>

### Dynamic Template Header

**basename($\_SERVER[‘PHP\_SELF’])**

This function returns the filename from a path.

|  |  |
| --- | --- |
| **$\_SERVER[‘DOCUMENT\_ROOT’]** | **$\_SERVER[‘HTTP\_HOST’]** |
| The root directory of this site defined by the 'DocumentRoot' directive in the General Section or a section e.g.  **var/www/example**  C:/xampp/htdocs | The base URL of the host e.g.  [**www.example.com**](http://www.example.com)  localhost |

**For PHP**

If we want to include a file we cannot use **HTTP\_HOST**, we need to use **DOCUMENT\_ROOT**

include**(**$\_SERVER['DOCUMENT\_ROOT'].'/E-Commerce/includes/mysql.inc.php')

**For HTML**

**../** 🡪 means parent of the current folder

**/ 🡪** means the root folder

**./ 🡪** means the current folder

In <script> or <link> tag, we need to use

<script src = "/E-Commerce/vendor/jquery.min.js"></script>

**MAGIC Constants**

|  |  |
| --- | --- |
| \_\_LINE\_\_ | The current line number of the file. |
| \_\_FILE\_\_ | The full path and filename of the file with symlinks resolved. If used inside an include, the name of the included file is returned. |
| \_\_DIR\_\_ | The directory of the file. If used inside an include, the directory of the included file is returned. This is equivalent to dirname(\_\_FILE\_\_). This directory name does not have a trailing slash unless it is the root directory. |
| \_\_FUNCTION\_\_ | The function name. |
| \_\_CLASS\_\_ | The class name. The class name includes the namespace it was declared in (e.g. Foo\Bar). Note that as of PHP 5.4 \_\_CLASS\_\_ works also in traits. When used in a trait method, \_\_CLASS\_\_ is the name of the class the trait is used in. |
| \_\_TRAIT\_\_ | The trait name. The trait name includes the namespace it was declared in (e.g. Foo\Bar). |
| \_\_METHOD\_\_ | The class method name. |
| \_\_NAMESPACE\_\_ | The name of the current namespace. |

## HTML Template

### Header

1. < !DOCTYPE html > < html lang = "en" > < head > < meta charset = "UTF-8" / > < meta name = "viewport"
2. content = "width=device-width,  initial-scale=1" / > < title > <? php $title = isset($page\_title) ? $page\_title : "Knowledge is Power: And It Pays to Know"; ?> <? php echo $title; ?> < /title> <? php echo '<link rel = "stylesheet" href = "/E-Commerce/vendor/bootstrap.min.css" media = "screen"/>';
3. echo '<link rel = "stylesheet" href = "/E-Commerce/CSS/style.css" media = "screen"/>';
4. echo '<script src = "/E-Commerce/vendor/jquery.min.js"></script>';
5. echo '<script src = "/E-Commerce/vendor/popper.min.js"></script>';
6. echo '<script src = "/E-Commerce/vendor/bootstrap.min.js"></script>'; ?> < /head> < body > < div class = "row"
7. id = "wrap" > < div class = "col header text-center bg-light" > < h1 > < a href = "index.php"
8. class = "nounderline" > < code class = "text-info" > Knowledge is Power < /code> < /a> < /h1> < h2 > < code class = "text-warning" > and it pays to know < /code>  < /h2> < /div>  < /div> < div class = "row" > < nav id = "nav"
9. class = "col navbar navbar-expand-sm navbar-dark bg-dark sticky-top" > < a class = "navbar-brand"
10. href = "#" > & nbsp; < code class = "text-warning" > Code Break! < /code> < /a> < button class = "navbar-toggler"
11. type = "button"
12. data - toggle = "collapse"
13. data - target = "#collapsibleNavbar" > < span class = "navbar-toggler-icon" > < /span> < /button> < div class = "collapse navbar-collapse"
14. id = "collapsibleNavbar" > < ul class = "navbar-nav" > <? php $pages = ["Home" => "index.php", "About" => "about.php", "Contact" => "contact.php", "Register" => "register.php"];
15. $this\_page = basename($\_SERVER['PHP\_SELF']);
16. foreach($pages as $key => $value): if ($value == $this\_page): echo '<li class = "nav-item active">';
17. else :echo '<li class = "nav-item">';
18. endif;
19. echo '  <a href = "'.$value.
20. '" class = "nav-link">';
21. echo $key;
22. echo '  </a>';
23. echo '</li>';
24. endforeach; ?> < /ul> < /div> < /nav> < /div>

### Body

1. < div class = "sidebar col-2 d-none d-sm-block" > < div class = "my-2" > < h4 class = "text-success bg-dark card title" > Manage Your Accounts < /h4> < ul class = "list-unstyled card" > < li > < a href = "renew.php"
2. class = "nounderline"
3. title = "Renew Your Account" > < code class = "text-secondary" > Renew Account < /code> < /a>   < /li> < li > < a href = "change\_password.php"
4. class = "nounderline"
5. title = "Change Your Password" > < code class = "text-secondary" > Change Password < /code> < /a> < /li> < li > < a href = "favorites.php"
6. class = "nounderline"
7. title = "View Your Favorites" > < code class = "text-secondary" > Favorites < /code> < /a> < /li> < li > < a href = "recommendations.php"
8. class = "nounderline"
9. title = "View Your Recommendations" > < code class = "text-secondary" > Recommendations < /code> < /a> < /li> < li > < a href = "logout.php"
10. class = "nounderline"
11. title = "Logout" > < code class = "text-secondary" > Logout < /code> < /a> < /li> < /ul> < /div> < div class = "my-2" > < h4 class = "text-info bg-dark card title" > Content < /h4> < ul class = "list-unstyled card" > <? php $dbc = mysqli\_connect("localhost", "root", "", "ecommerce1") or die("Server Denied");
12. $query = "SELECT \* FROM categories ORDER BY category";
13. $result = mysqli\_query($dbc, $query) or die("Query Denied");
14. while ($row = mysqli\_fetch\_array($result)): echo '<li>';
15. echo '  <a href = "category.php?id="'.$row['id'].
16. ' class = "nounderline" title = "'.$row['category'].
17. '">';
18. echo '      <code class = "text-secondary"> '.$row['category'].
19. ' </code>';
20. echo '  </a>  ';
21. echo '</li>';
22. endwhile; ?> < /ul> < /div> < /div> < /div>

### Footer

1. < /div> <? php
2. if (isset($\_SESSION['user\_type'])) {
3. echo '<div class = "row">';
4. echo '          <div class = "col-10"></div>';
5. echo '              <div class = "sidebar col-2 d-none d-sm-block">';
6. echo '                  <h4 class = "text-danger bg-dark card title"> Administration</h4>';
7. echo '                  <ul class = "list-unstyled card">';
8. echo '                      <li>';
9. echo '                          <a href = "add\_page.php" class = "nounderline" title = "Add a Page">';
10. echo '                              <code class = "text-secondary"> Add a Page </code>';
11. echo '                          </a>  ';
12. echo '                      </li>';
13. echo '                      <li>';
14. echo '                          <a href = "add\_pdf.php" class = "nounderline" title = "Add a PDF">';
15. echo '                              <code class = "text-secondary"> Add a PDF </code>';
16. echo '                          </a>';
17. echo '                      </li>';
18. echo '                  </ul>';
19. echo '              </div>';
20. echo '          </div>';
21. echo '      </div>';
22. } // if(!isset($\_SESSION['user\_id'])){ //   require('login\_form.inc.php'); // }
23. ?> <? php
24. if (isset($\_SESSION['user\_id'])) {
25. echo '  <div class = "row text-center">';
26. echo '              <div class = "col">';
27. echo '                  <h6> Manage Your Account </h6>';
28. echo '                  <ul class = "list-unstyled list-inline">';
29. echo '                      <li class = "list-inline-item">';
30. echo '                          <a href = "renew.php" class = "nounderline" title = "Renew Your Account">';
31. echo '                              <code> Renew Your Account </code>';
32. echo '                          </a>';
33. echo '                      </li>';
34. echo '                      <li class = "list-inline-item">';
35. echo '                          <a href = "change\_password.php" class = "nounderline" title = "Change Password">';
36. echo '                              <code> Change Password </code>';
37. echo '                          </a>';
38. echo '                      </li>';
39. echo '                      <li class = "list-inline-item">';
40. echo '                          <a href = "favorites.php" class = "nounderline" title = "View Your Favorites">';
41. echo '                              <code> Favorites </code>';
42. echo '                          </a>';
43. echo '                      </li>';
44. echo '                      <li class = "list-inline-item">';
45. echo '                          <a href = "recommentdations.php" class = "nounderline" title = "View Your Recommendations">';
46. echo '                              <code> Recommendations </code>';
47. echo '                          </a>';
48. echo '                      </li>';
49. echo '                      <li class = "list-inline-item">';
50. echo '                          <a href = "logout.php" class = "nounderline" title = "Log Out">';
51. echo '                              <code> Logout </code>';
52. echo '                          </a>';
53. echo '                      </li>';
54. echo '                  </ul> ';
55. echo '              </div>';
56. echo '  </div>';
57. } ?> < div class = "row footer navbar navbar-fixed-bottom text-center" > < div class = "col" > < a href = "site\_map.php"
58. title = "Site Map" > Site Map | < /a> < a href = "policies.php"
59. title = "Policies" > Policies | < /a> < code > & copy; <? php echo date("Y"); ?> All Rights Reserved | Designed By Photon & trade; < /code> < /div> < /div> < /body> < /html>

### Configuration

1. <? php $live = false;
2. $contact\_email = "khan.photon@gmail.com";
3. define('BASE\_URI', $\_SERVER['DOCUMENT\_ROOT'].
4. '/E-Commerce/includes/pdfs/');
5. define('BASE\_URL', $\_SERVER['DOCUMENT\_ROOT'].
6. '/E-Commerce/');
7. define('MYSQL', $\_SERVER['DOCUMENT\_ROOT'].
8. '/E-Commerce/includes/mysql.inc.php');
9. session\_start();
11. function my\_error\_handler($e\_number, $e\_message, $e\_file, $e\_line, $e\_vars) {
12. global $live, $contact\_email;
13. $message = "An error occured in script {$e\_file} on line {$e\_line}: \n {$e\_message}\n";
14. $message. = "<pre>".print\_r(debug\_backtrace(), 1).
15. "</pre>\n";
16. $message. = "<pre>".print\_r($e\_vars, 1).
17. "</pre>\n";
18. if (!$live): echo "<div class = 'bgd-danger text-white error'>".nl2br($message).
19. "</div>";
20. else :error\_log($message, 1, $contact\_emails, "From:khan.photon@gmail.com");
21. endif;
22. if ($e\_number != E\_NOTICE): echo "<div class = 'bgd-danger text-white error'> A system error occurred. We apologize for the inconvenience. </div>";
23. endif;
24. return true;
25. }
26. set\_error\_handler("my\_error\_handler");

### Database

1. <? php define('DB\_HOST', 'localhost');
2. define('DB\_USER', 'root');
3. define('DB\_PASS', '');
4. define('DB\_NAME', 'ecommerce1');
5. $dbc = mysqli\_connect(DB\_HOST, DB\_USER, DB\_PASS, DB\_NAME) or die("Server Denied");
6. mysqli\_set\_charset($dbc, 'utf8');
8. function escape\_data($data) {
9. global $dbc;
10. return mysqli\_real\_escape\_string(trim($data), $dbc);
11. }

### Index

1. <? php require\_once("includes/config.inc.php");
2. require\_once("includes/header.php");
3. require\_once(MYSQL);
4. $\_SESSION['user\_id'] = 1;
5. $\_SESSION['user\_type'] = 'admin';
6. echo '<div class = "row page">';
7. echo '<div class = "col-10 content card border border-warning my-2">';
8. echo '<h3 class = "pl-2"> Welcome </h3>';
9. echo '  <p class = "pl-2"> Welcome to Knowledge is Power, a site dedicated to keeping you up to date';
10. echo '      on the Web security and progamming information you need know </p>';
11. echo '</div>';
12. require\_once("includes/body.php");
13. require\_once("includes/footer.php");
14. echo $\_SESSION['user\_id'];
15. echo $\_SESSION['user\_type']; ?>

## PHP Terms

**mysqli\_set\_charset($dbc, 'utf8')**

It indicates which character set should be used for communications between PHP and the database.

**$\_SERVER['DOCUMENT\_ROOT']**

Get the root of each site

**debug\_backtrace()**

This function generates a PHP back trace.

**error\_log()**

This function sends an error message to a log, to a file, or to a mail account.

**basename($\_SERVER[‘PHP\_SELF’])**

This function returns the filename from a path.