# Source Code Review Exercise (Kira Kimhan)

For each sample of vulnerable code below write in actual or pseudo code to mitigate the vulnerability.

# **Brute Force Source**

|  |
| --- |
| <?php  if( isset( $\_GET['Login'] ) ) {  $user = $\_GET['username'];    $pass = $\_GET['password'];  $pass = md5($pass);  $qry = "SELECT \* FROM `users` WHERE user='$user' AND password='$pass';";  $result = mysql\_query( $qry ) or die( '<pre>' . mysql\_error() . '</pre>' );  if( $result && mysql\_num\_rows( $result ) == 1 ) {  // Get users details  $i=0; // Bug fix.  $avatar = mysql\_result( $result, $i, "avatar" );  // Login Successful  echo "<p>Welcome to the password protected area " . $user . "</p>";  echo '<img src="' . $avatar . '" />';  } else {  //Login failed  echo "<pre><br>Username and/or password incorrect.</pre>";  }  mysql\_close();  }  ?> |

# **Command Execution Source**

|  |
| --- |
| <?php  if( isset( $\_POST[ 'submit' ] ) ) {  $target = $\_REQUEST[ 'ip' ];  // Determine OS and execute the ping command.  if (stristr(php\_uname('s'), 'Windows NT')) {    $cmd = shell\_exec( 'ping ' . $target );  echo '<pre>'.$cmd.'</pre>';    } else {    $cmd = shell\_exec( 'ping -c 3 ' . $target );  echo '<pre>'.$cmd.'</pre>';    }    }  ?> |

# **SQL Injection (Blind) Source**

|  |
| --- |
| <?php  if (isset($\_GET['Submit'])) {    // Retrieve data    $id = $\_GET['id'];  $getid = "SELECT first\_name, last\_name FROM users WHERE user\_id = '$id'";  $result = mysql\_query($getid); // Removed 'or die' to suppres mysql errors  $num = @mysql\_numrows($result); // The '@' character suppresses errors making the injection 'blind'  $i = 0;  while ($i < $num) {  $first = mysql\_result($result,$i,"first\_name");  $last = mysql\_result($result,$i,"last\_name");    echo '<pre>';  echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;  echo '</pre>';  $i++;  }  }  ?> |

# **File Upload Source**

|  |
| --- |
| <?php  if (isset($\_POST['Upload'])) {  $target\_path = DVWA\_WEB\_PAGE\_TO\_ROOT."hackable/uploads/";  $target\_path = $target\_path . basename( $\_FILES['uploaded']['name']);  if(!move\_uploaded\_file($\_FILES['uploaded']['tmp\_name'], $target\_path)) {    echo '<pre>';  echo 'Your image was not uploaded.';  echo '</pre>';    } else {    echo '<pre>';  echo $target\_path . ' succesfully uploaded!';  echo '</pre>';    }  }  ?> |

# **Reflected XSS Source**

|  |
| --- |
| <?php  if(!array\_key\_exists ("name", $\_GET) || $\_GET['name'] == NULL || $\_GET['name'] == ''){  $isempty = true;  } else {    echo '<pre>';  echo 'Hello ' . $\_GET['name'];  echo '</pre>';    }  ?> |