# Everlytic Developer Assessment

|  |  |
| --- | --- |
| Name | Sipho Matseme |

|  |  |
| --- | --- |
| Date | 12-06-2023 |

Please complete the answers to the questions below. The assessment should take roughly 30 minutes.

### What is the difference between public, protected and private in a class definition?

|  |
| --- |
| Private members are not accessible from outside the class they are defined in |
| Protected members cannot be accessed outside the class, but can be accessed in the inherited class |
|  |

### Given this code: function doSomething(&$foo) { $bar = $foo; $foo += 1; return $foo; } $value = 3; $result = doSomething($value); echo "value: $value, result: $result"; What will be output to screen and why?

|  |
| --- |
| value: 4, result: 4 |
| both $value and $result hold the modified value of 4, which was incremented inside the doSomething() function. |
|  |

### What is wrong with this query: "SELECT \* FROM table WHERE id = $\_POST[ 'id' ]"?

|  |
| --- |
| The query you provided is susceptible to SQL injection, which is a security vulnerability. It's important to sanitize and validate user input before using it in SQL queries to prevent malicious exploitation. |
|  |
|  |
|  |

### What is the cause of this warning: 'Warning: Cannot modify header information - headers already sent', and what is a good practice to prevent it?

|  |
| --- |
| Something was sent to the browser before the PHP header() function was called |
| Place any code that modifies headers before any output is sent to the client. This means that header-related code should appear before any HTML, text, or whitespace, even before the opening <?php tag. |
|  |

### What is wrong with this code: class Foo { protected $bar; public function \_\_construct() { $this->bar = 1; } public static function doSomething() { return $this->bar; } }

|  |
| --- |
| The static doSomething method is trying to access an none static property $bar |
|  |
|  |

### Write a program that prints the numbers from 1 to 100. But for multiples of three print "Fizz" instead of the number and for the multiples of five print "Buzz". For numbers which are multiples of both three and five print "FizzBuzz".

### **What does the following code do? Explain what’s going on there.**

$date = '08/26/2003';

print preg\_replace('/([0-9]+)\/([0-9]+)\/([0-9]+)/'‚ '$2/$1/$3', $date);

|  |
| --- |
| 0-9 values will be replaced by either $2/$1/$3 |
|  |

### **Given a line of text $string, how would you write a regular expression to strip all the HTML tags from it?**

|  |
| --- |
| $strippedString = preg\_replace('/<[^>]\*>/', '', $string); |
|  |
|  |

### A palindrome is a word that reads the same backward or forward. Write a function that checks is a given word is a palindrome. Characters case should be ignored. EG. Deleveled is a palindrome and should return true as character case is ignored.

### <?php class Palindrome

### {

### public static function isPalindrome($word)

{

}

### } echo Palindrome::isPalindrome('Deleveled');

### Considering message\_text stores a combination of html and text. What security issue is prevalent in the code below and how would you fix it? <?php $messageStmt = $db->query('select message\_text from messages where message\_id = 1'); $messageStmt->execute(); $message = $messageStmt->fetch(PDO::FETCH\_OBJ); ?> <div><?php echo $message->message\_text; ?></div>

### The code is vulnerable to a Cross-Site Scripting (XSS) security issue. This occurs when user-supplied data is not properly validated or sanitized and is directly embedded in the output HTML without any escaping.

### if the message\_text column in the database contains malicious HTML or JavaScript code, it will be executed when the message is displayed on the web page. An attacker could inject code that steals sensitive information, modifies the page content, or performs other malicious actions on behalf of the user viewing the page.

### To fix this security issue, you should properly sanitize and escape the message\_text before embedding it in the HTML output by using htmlspecialchars() function,

### <div><?php echo htmlspecialchars($message->message\_text, ENT\_QUOTES, 'UTF-8'); ?></div> \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Write an inner join for the following tables

|  |
| --- |
| Select \*  From User U  INNER JOIN Address A  ON U.UserKey = A.UsrKey |
|  |

### Complete the JS function below that validates the conditions of a password: 1. The password must be greater then 7 characters 2. The first character must be a capital letter 3. The password must contain at least one number

function isPasswordValid($password) {

    var isValid = false;

    // Write you logic here

    var passw = /^(?=.\*\d)(?=.\*[A-Z]).{7,20}$/;

    if(inputtxt.value.match(passw))

    {

        alert('Correct, try another...')

        return true;

    }

        else

    {

        alert('Wrong...!')

        return false;

    }

    return isValid;

}