WRITE UP FOR

3ATAR

Contact :
contact@cybercohesion.com

APAC / JAPAN / INDIA / MIDDLE EAST / AFRICA / SOUTH AMERICA

Scenario :

- **FIRST:**

bypass balance for order.php (use jwt) :

- **bypass balance checks with a jwt vulnerability with the help of enumeration.**
- **The participant should decode the military-grade js obfuscated script in «a11.js» file.**

```php
    // PROCESS HERE
    include "includes/api.php";
    $validation_data = (array) jwt_decodeData($encrypted_token);

    if ($validation_data === false) {
        // Handle invalid JWT token
        http_response_code(400);
        decide_the_shame("Error Trail", 5);
        header("Location: mol_7anout.php");
        die();
    }

    // Check if the data in $_POST is the same as the one in the JWT decoded data
    if ($_POST['product_id'] !== $validation_data['product_id'] ||
//        $_POST['price'] !== $validation_data['price'] ||
        $_POST['name'] !== $validation_data['name'] ||
        $_POST['email'] !== $validation_data['email'] ||
        $_POST['address'] !== $validation_data['address'] ||
        $_POST['city'] !== $validation_data['city']) {
        http_response_code(400);
        decide_the_shame("Mind Games", 5);
        header("Location: mol_7anout.php");
        die();
    }


    // check price
    $balance = $_SESSION['balance'] ?? 0;
    if ($balance < $validation_data['price']) {
        http_response_code(400);
        decide_the_shame('The Missing Piece', 5);
        header("Location: mol_7anout.php");
        die();
    }

    $_SESSION['thanks_for_ordering'] = "NOICE_BRUH";
    header("Location: thanks.php");
    die();
```

Answer :

Cyber_Cohesion{glazah_bayetsa_a_ruky_deelayut}

Scenario :

- **SECOND:**

wall of shame calculations giving either random or correct flags based on attacker attempts :

- **if the participant has been detected more then 50 times he will be getting a dummy flag else the correct flag.**

```
$detected_count = $stmt->fetch()["detected"];

if ($detected_count >= 50) {

    include "includes/fncs.php";
    $flag = "Cyber_Cohesion{".generateRandomString(50)."}"; //FAKE FLAG

}else{

    $flag = "Cyber_Cohesion{G14BqLVwdOLHR3qAIjbAWPssPo6hOxeJeViNfZ6xcxIrmHyPya}"; //REAL FLAG

}
```

Answer :

Cyber_Cohesion{G14BqLVwdOLHR3qAIjbAWPssPo6hOxeJeViNfZ6xcxIrmHyPya}

WARZONE

AND THAT WAS IT

for 3ATAR !