**Insecure Direct Object References (IDOR) Vulnerability Report**

Report Date: 21/08/2023

Reported by: **Amine SAJID**

Contact Email aminesajid99@gmail.com

Vulnerability Severity **Critical**

Status: [Open]

---

**Vulnerability Overview:**

An Insecure Direct Object References (IDOR) vulnerability has been identified in **moncallcenter.ma**. This vulnerability allows an attacker to access resources and perform actions that they are not authorized for by manipulating object references.

**Vulnerability Details:**

- Vulnerability Type: Insecure Direct Object References (IDOR)

- CWE Identifier: (CWE-639)

- Vulnerable Function: **/validation-profile.php**

- Affected Parameter: [email=](https://www.moncallcenter.ma/validation-profile.php?email=givatot531@dusyum.com&cle=rpa4y0u14i17082023114109) & [cle=](https://www.moncallcenter.ma/validation-profile.php?email=givatot531@dusyum.com&cle=rpa4y0u14i17082023114109)

**Steps to Reproduce:**

1. Create a new account and send the validation code to your email.

2. Click “Validate” and intercept the request.

3. Verify that **the validation link contains your email and your cle.**

4. Replace your email and cle by any other user email & cle.

5. That’s it, now you get access to any user just by knowing their email.

**Proof of Concept (PoC):**

[See: Validation\_Missconfig.mkv in attachments]

**- Impact:**

**Unauthorized Data Access:** Attackers can exploit these vulnerabilities to access data or resources that they are not authorized to access. This can lead to exposure of confidential user information, such as personal data (emails, phone number, comments...), or private documents (CV, audio records).

**Data Manipulation:** In addition to unauthorized access, attackers may also manipulate or modify data that they are not authorized to change. This can result in data corruption, fraudulent transactions, or unauthorized changes to critical system settings.

**Bypassing Authorization:** IDOR vulnerabilities can allow attackers to bypass authorization mechanisms and gain elevated privileges within a system. For example, an attacker might be able to escalate their access from a regular user to an administrator, granting them control over the entire system.

**Privacy Violation:** If an application handles user-specific data, an IDOR vulnerability could lead to privacy violations. Attackers can access private user data, violating the trust users place in the application to protect their information.

**Mitigation Steps:**

To mitigate this Insecure Direct Object References vulnerability, I recommend the following steps:

1. **Use Indirect References:**

* Avoid exposing internal identifiers or direct references to objects in URLs, parameters, or other client-side inputs.
* Instead of using identifiers, consider using a unique token or a more complex reference that cannot be easily guessed.

2. **Implement Server-Side Validation:**

* Validate user input and authorization on the server-side, even if client-side checks are in place.
* Always verify that the user has appropriate permissions for the requested action or resource.

3. **Encode and Encrypt Data:**

* If sensitive data is being transmitted or stored, ensure that it's properly encrypted to prevent unauthorized access.
* Apply proper encoding to user inputs to prevent malicious injection attempts.

**Timeline:**

- [Date]: 17/08/2023

- [Date]: Vulnerability reported to Othman Alj (Registrant Name: Gojob sarl)

- [Date]: Vulnerability acknowledged by 21/08/2023

**Acknowledgments:**

Thank you for this opportunity to assist in enhancing the security of Client's moncallcenter.ma, through this penetration testing engagement.

---

**BY Amine SAJID**