higordiego / **VULN-002-idor-profile-takeover.md** Secret

Created 3 weeks ago

Code Revisions 1

VULN-002-idor-profile-takeover.md

Affected Version:

- **Invoice System in Laravel**: 1.0

Vulnerability Information:

- **Vulnerability Type:** Insecure Direct Object Reference (IDOR)
- **Severity:** CRITICAL
- **Status:** Unpatched

Vulnerable Endpoint:

- `/profile/{id}` (GET/POST methods)

Vulnerability Description:

The profile workflow uses a user-controlled `id` in the route and fails to verify that the requested profile belongs to the authenticated user. This allows an attacker to view or modify any user's profile data by simply changing the ID in the URL.

Proof of Concept (PoC):

Below is a **POST** request demonstrating unauthorized profile modification:

```
POST /profile/1 HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded

name=Compromised+User&email=owned@example.com
```

Explanation:

This request targets an arbitrary profile ID:

```
id=1
```

The backend updates the record associated with `id=1` without checking if it matches the current `auth()->id()`.

Impact:

- **Confidentiality:** Unauthorized access to private profile information of other users.
- **Integrity:** Potential for arbitrary modification of any user's email, name, and settings.
- **Account Takeover:** Could lead to account recovery bypass if email is modified.

Mitigation Recommendations:

1. **Bind to Auth User:** Use `auth()->user()` to resolve profile actions instead of accepting an ID from the route.
2. **Authorization Policies:** Implement a Policy to ensure `user_id` matches the authenticated session.
3. **UUIDs:** Use non-sequential identifiers to prevent easy enumeration of user profiles.