higordiego / **VULN-001-privilege-escalation-user-management.md** Secret

Last active 3 weeks ago

`VULN-001-privilege-escalation-user-management.md`

Affected Version:

- **Invoice System in Laravel**: 1.0

Vulnerability Information:

- **Vulnerability Type:** Broken Access Control + Privilege Escalation
- **Severity:** CRITICAL
- **Status:** Unpatched

Vulnerable Endpoint:

- `/user` (POST/PUT methods)

Vulnerability Description:

The user management flow is exposed without effective authorization controls. The `user` resource routes can be reached without admin-only middleware, and the controller accepts attacker-controlled `role` data. This allows any user to create or modify accounts with administrative privileges.

Proof of Concept (PoC):

Below is a **POST** request demonstrating arbitrary role assignment during user creation:

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

name=attacker&email=attacker@example.com&password=Password123&role=admin
```

Explanation:

This payload injects the administrative role:

```
role=admin
```

The application lacks server-side enforcement to prevent non-admin users from setting the `role` field, leading to full privilege escalation.

Impact:

- **Privilege Escalation:** Attackers can elevate their own accounts to administrator status.
- **Account Takeover:** Modification of existing users with elevated permissions.
- **Access Control:** Unauthorized access to all administrative functions.

Mitigation Recommendations:

1. **Enforce Authorization:** Protect all `/user` routes with admin-only middleware.
2. **Restrict Input:** Remove `role` from the `$fillable` array or validate it against a trusted whitelist.
3. **Use Policies:** Implement Laravel Policies to authorize user creation and updates.