Greybox Privilege Escalation via IDOR

(**Anonymized Case Study**)

Vulnerability Type

Insecure Direct Object Reference (IDOR) with Privilege Escalation

Assessment Type

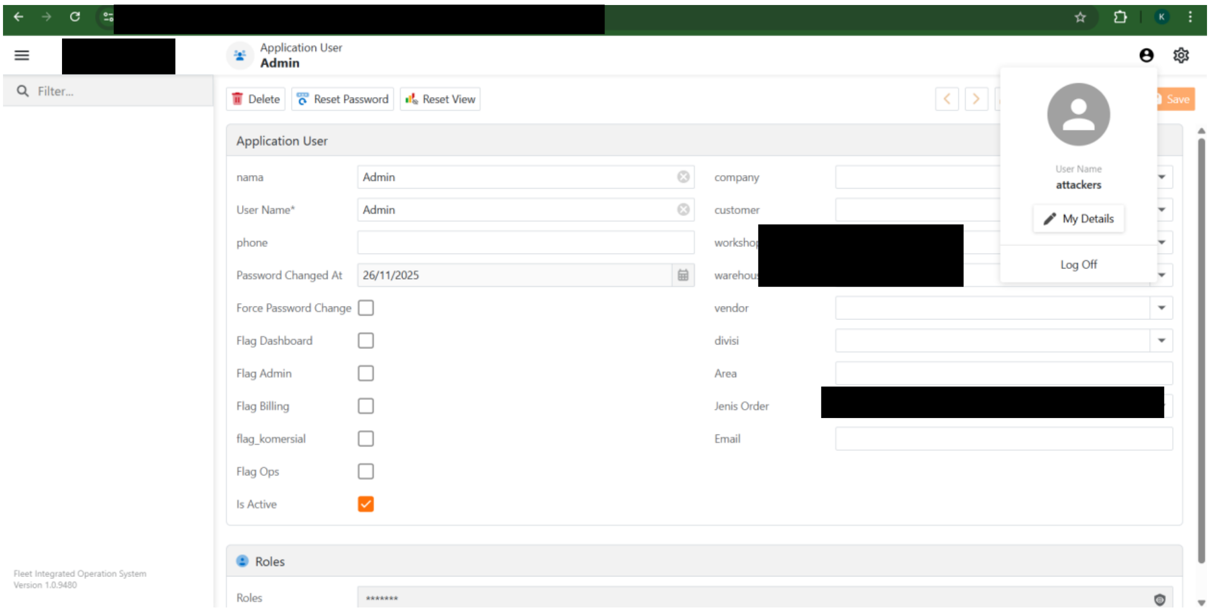
Greybox Security Assessment (Low-Privilege Account)

Summary

During an authorized greybox security assessment, a privilege escalation vulnerability was identified in a role-based web application. Starting from a low-privileged registered user account, improper authorization enforcement allowed access to administrative functionalities.

The issue enabled unauthorized execution of high-privilege actions due to missing role validation across multiple application workflows.

Evidence (Sanitized)



Application User
Admin

User Name
attackers

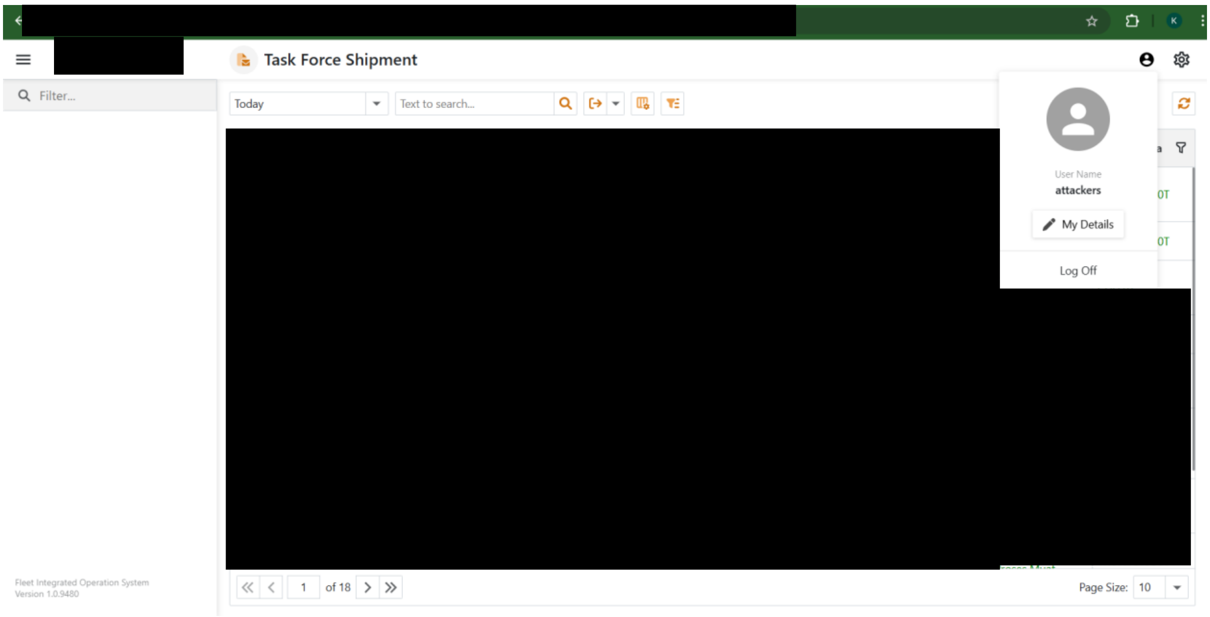
Application User

nama	Admin	company	
User Name*	Admin	customer	
phone		worksho	[redacted]
Password Changed At	26/11/2025	warehou	
Force Password Change	☐	vendor	
Flag Dashboard	☐	divisi	
Flag Admin	☐	Area	
Flag Billing	☐	Jenis Order	[redacted]
flag_komersial	☐	Email	
Flag Ops	☐		
Is Active	☑		

Roles

Roles	*******

Fleet Integrated Operation System
Version 1.0.9480


[redacted]
[redacted]
[redacted]

Under controlled testing conditions, a low-privileged user account was able to:

- Access administrative execution flows not intended for the assigned role
- Perform **create, modify, and delete operations** on privileged resources
- Trigger **password reset actions** affecting higher-privilege accounts
- Interact with internal management modules due to missing authorization checks

The root cause was identified as **inconsistent authorization validation** across sequential request execution paths, allowing privilege escalation through predictable object references and execution order manipulation.

No sensitive data was extracted, and no production disruption occurred during testing.

Risk Assessment

If exploited by a malicious actor, this vulnerability could result in:

- Full administrative account takeover
- Unauthorized modification or deletion of critical system data
- Abuse of privileged workflows
- Compromise of business operations and trust boundaries
- Regulatory and compliance exposure

Due to the ability to escalate privileges from a low-level account, this issue was classified as **High to Critical risk**, depending on deployment context.

Root Cause Analysis (High-Level)

- Missing role validation on sensitive endpoints
- Trust placed on client-side or sequential execution order
- Predictable object identifiers
- Lack of centralized authorization enforcement

Recommendations

- Enforce **server-side authorization checks** on every privileged action
- Validate user roles independently per request
- Apply **deny-by-default** access control policies
- Use non-predictable identifiers for sensitive objects
- Implement centralized authorization middleware
- Conduct regular privilege escalation testing

Security Takeaway

This finding highlights the importance of enforcing authorization consistently across all execution paths, particularly in systems with layered roles and complex workflows. Greybox testing proved effective in identifying privilege escalation risks that may not be detected through blackbox testing alone.