AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Secured Unauthorized API Access:
Business Workflow System for Fintech

01

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Project Initiation and Scoping

Upon formal engagement, detailed scoping discussions with key stakeholders of the India-based Fintech organization, Ampcus Cyber helped comprehensively to outline the organization's application workflow and role-based access model. This phase focused on identifying critical business processes, particularly those involving multi-level approvals for asset management (e.g., asset allocation, replacement, and handover).

The primary objective of the assessment was to evaluate whether the application properly enforces authorization controls across different user roles and prevents unauthorized access to sensitive workflow operations. Testing was conducted from the perspective of a low-privileged user interacting with exposed application endpoints.

Due to the sensitive nature of the engagement, the client's identity and application specifics remain confidential.

Overview:

The assessment focused on the application's role-based workflow system:

Application Workflow Architecture:

- Multi-level approval system involving roles such as Employee, Manager, IT, CTO and HR.
- Workflow actions include request creation, approval, rejection, and status updates.
- Backend APIs exposed for workflow state transitions (approve/reject/update).

Key Observations:

- Role-specific endpoints were directly accessible via API calls.
- Authorization enforcement relied heavily on frontend/UI restrictions rather than backend validation.
- Certain sensitive endpoints were accessible without authentication tokens (session cookies).

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Assessment Methodology and Execution

The exploitation phase was conducted using a structured approach simulating a malicious insider or external attacker.

Reconnaissance and Workflow Analysis

Initial interaction with the application UI revealed a structured approval workflow with restricted actions for higher-privileged roles. Using an intercepting proxy, all API calls related to workflow transitions were captured and analyzed.

Endpoint Enumeration and Role Mapping

Captured requests identified distinct endpoints responsible for:

- Approving requests
- Rejecting requests
- Updating request status

These endpoints were assumed to be restricted to specific roles (Manager, IT, HR).

Authorization Bypass Testing

By replaying intercepted requests using a lower-privileged employee account, it was observed that:

- Role-restricted endpoints could be invoked successfully.
- No server-side validation existed to verify user role permissions.

Further testing revealed:

- These endpoints could also be executed **without including any valid session cookie,** indicating a complete lack of authentication enforcement.

Privilege Escalation via Direct API Invocation

Using tools such as Burp Suite Intruder:

- Multiple approval/rejection actions were automated.
- A low-privileged user successfully performed actions reserved for managerial roles.

This demonstrated a clear **vertical privilege escalation** vulnerability.

Workflow Integrity Violation (State Manipulation)

The application UI enforced a restriction where once a request was approved or rejected, it could not be modified further.

However:

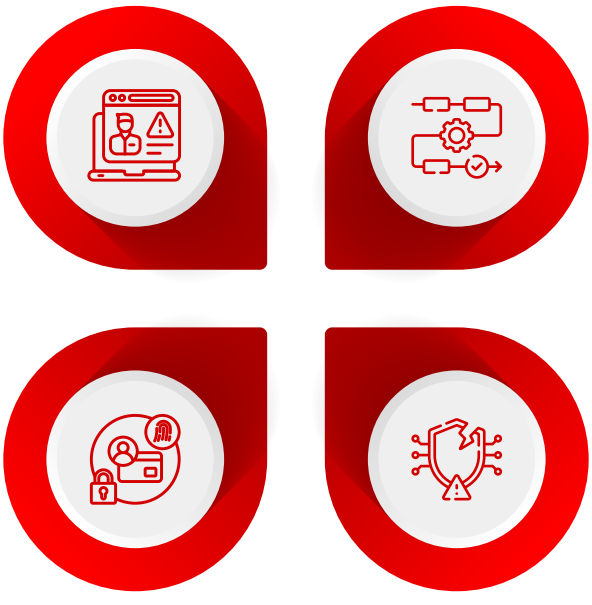
- By crafting direct **PUT requests** to the backend endpoint, previously finalized requests could be altered.
- Attackers could change the status of already approved/rejected requests arbitrarily.

This bypassed critical business logic controls and compromised workflow integrity.

Exploitation Impact Validation

The following impacts were successfully demonstrated:

Unauthorized approval/rejection of asset requests



Manipulation of finalized workflow states

Execution of privileged actions without authentication

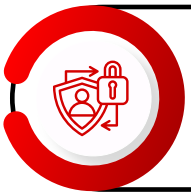
Automation of attacks at scale using Intruder

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

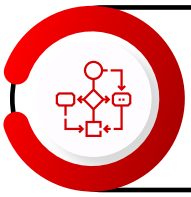
Business Impact

This vulnerability introduces severe security and business risks:

Privilege Escalation:
Low-privileged users can perform high-privileged operations (Manager/IT/HR actions).



Authentication Bypass:
Critical endpoints accessible without valid session tokens.



Workflow Compromise:
Integrity of approval processes is completely broken.

Fraud and Abuse Risk:
Attackers can approve unauthorized asset allocations or manipulate records.

Audit Failure:
Logs and approvals can no longer be trusted as legitimate.

Mass Exploitation:
Automated attacks can manipulate multiple requests simultaneously.

Overall, this results in a **complete breakdown of role-based access control (RBAC)** and trust boundaries within the application.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Remediation Support and Recommendations

01 Enforce Server-Side Authorization
Implement strict role-based access control (RBAC) checks on all sensitive endpoints. Ensure that each request is validated against the user's role and permissions on the backend.

02 Mandatory Authentication Validation
Ensure all endpoints require valid session tokens or authentication headers. Reject any unauthenticated requests.

03 Workflow State Validation
Implement server-side checks to prevent modification of finalized requests (approved/rejected). Enforce immutable state transitions.

04 Principle of Least Privilege
Ensure users can only access actions explicitly permitted for their role. Avoid exposing privileged endpoints unnecessarily.

05 Access Control Hardening
Use centralized authorization middleware to validate every request consistently across all endpoints.

06 Logging and Monitoring
Log all workflow actions with user identity, role, and timestamp. Implement alerts for anomalous actions (e.g., role mismatch).

07 Rate Limiting and Abuse Prevention
Apply rate limiting and anomaly detection to prevent automated exploitation using tools like Intruder.

08 Security Testing Integration
Incorporate authorization testing into SDLC pipelines, including automated tests for BFLA scenarios.

AMPCUS CYBER
INTELLIGENT CYBERSECURITY DELIVERED

Remediation Validation

Post-remediation validation should confirm:

- Unauthorized roles cannot access privileged endpoints
- All endpoints reject unauthenticated requests
- Workflow state transitions are strictly enforced
- Attempts to tamper with finalized requests are blocked

Conclusion

This assessment highlights a critical failure in enforcing server-side authorization controls, resulting in Broken Function Level Authorization and privilege escalation. The ability to invoke privileged APIs without authentication and manipulate workflow states demonstrates a complete compromise of application trust boundaries.

The issue underscores the importance of implementing robust backend authorization mechanisms rather than relying solely on frontend restrictions. Following remediation, the organization significantly improved its access control posture and ensured that critical business workflows are protected against unauthorized manipulation.

India
601-609A, 6th Floor, Beta Block, Sigma Soft Tech Park, Varthur Kodi, Whitefield, Bangalore, Karnataka - 560066.

USA
14900 Conference Center Dr, Suite # 500, Chantilly, VA 20151.

UAE
Office 306, Building A6, Dubai Digital Park, Dubai Silicon Oasis, Dubai.

Philippines
19th floor Exxa Tower, Bridgetowne, E.Rodriguez Jr. Ave cor C5 Road, Ugong Norte, Quezon City.

www.ampcuscyber.com

letsconnect@ampcuscyber.com