Authenticated Web Application Security Assessment AlphaTimeHR – Authenticated Role & Authorization Testing

1. Executive Summary

A targeted authenticated security assessment was conducted against the AlphaTimeHR web application to evaluate authorization controls, role enforcement, CSRF protections, and server-side validation mechanisms.

Testing focused on verifying that lower-privileged users (Employees) cannot perform Supervisor-only actions, sensitive actions require valid CSRF tokens, server-side authorization is enforced independently of the user interface, and parameter tampering does not result in privilege escalation or data manipulation.

Overall Risk Rating: Low

2. Scope of Assessment

Included in Scope:

- Authenticated Employee and Supervisor role testing
- Manual HTTP request replay via OWASP ZAP
- Role abuse and privilege escalation validation
- Parameter tampering on time-entry endpoints
- CSRF token validation testing
- Export/report endpoint access validation
- Session enforcement validation

Scope Limitations:

- Infrastructure security (Cloudflare, hosting environment)
- Automated vulnerability scanning
- Source code review
- Authentication brute force testing

- Business logic fuzzing
- Third-party integrations (e.g., Stripe)

3. Testing Methodology

Testing was performed using authenticated browser sessions, OWASP ZAP proxy interception, manual HTTP request modification, parameter manipulation testing, CSRF token removal and alteration, and direct endpoint access attempts.

4. Authorization & Role Abuse Testing

Supervisor export endpoint replay testing confirmed proper server-side authorization enforcement.

Employee privilege escalation attempts were rejected, confirming role-based access control is enforced server-side.

5. Parameter Tampering Testing

Clock-in and clock-out endpoints were tested with modified, invalid, and missing CSRF tokens.

All tampered requests were rejected with 403 Forbidden responses.

Conclusion: Server-side validation and CSRF enforcement confirmed.

6. CSRF Protection Validation

Altered and removed CSRF tokens resulted in proper 403 Forbidden responses.

Conclusion: CSRF protection is properly implemented and enforced.

7. Session Enforcement

Sensitive endpoints require authenticated sessions. Unauthorized requests are redirected or denied without data leakage.

8. Severity Definitions

- Critical – Direct unauthorized data access or system compromise
- High – Significant data exposure or authorization bypass
- Medium – Limited data exposure or control weakness
- Low – Minor misconfigurations or informational issues
- Informational – Observations with no security impact

9. Final Assessment Conclusion

The authenticated role and authorization testing phase is complete. No Critical, High, or Medium severity findings were identified within the defined scope.

The AlphaTimeHR application demonstrates proper server-side role enforcement, effective CSRF protection, and strong session validation.