# Penetration Test Summary

System: Career Automation Insights Engine

Test Date: October 2025

Tester: Internal Security Team

## Scope

- Web application (React + Supabase)
- Edge Functions (calculate-apo, search-occupations, etc.)
- Authentication (Supabase Auth)
- Database (RLS policies)

## Findings

1. Low: Missing HSTS header on some routes (fixed)
2. Low: CSP could be tightened for frame-ancestors (fixed)
3. Info: Rate limiting present but could be tuned per endpoint
4. Info: No XSS vulnerabilities found; DOMPurify in use

## Recommendations

- Enable HSTS preload
- Monitor rate limit metrics and adjust per endpoint
- Conduct annual pen-tests and update this summary

## Conclusion

No critical or high-severity vulnerabilities found. System is production-ready with standard security controls in place.

## Contact

For questions, see /responsible-ai page.