1 OVERVIEW

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement that incorporates this document by reference.

1.1 Service Summary

Applications are the front door to your business — and attackers know it. Whether web-based, mobile, API-driven, or thick-client, applications frequently serve as an entry point for exploitation, lateral movement, or data theft.

Our Application Security Assessment provides a comprehensive, technology-agnostic evaluation of your application's security posture. We analyze the application, its integrations, and its underlying infrastructure, focusing on vulnerabilities, logic flaws, and misconfigurations across the full stack. The assessment is modular and can be scoped to cover one or more of the following surfaces:

- Web applications
- APIs
- Mobile apps (Android only)
- Thick clients

1.2 In-Scope Service Details

This service is tailored to your application type and deployment model. We offer coverage for:

- Public or internally hosted web and/or API apps
- Mobile binaries (Android, with or without source)
- Desktop or thick-client software with server integration
- Microservice and API-driven applications.

1.3 Scope Requirements

To scope and deliver the Assessment, we require information for the following sections. Please note that we only require information for the in-scope sections.

- List of in-scope applications
- Application type(s)
- Total number of dynamic pages
- Do your applications consume any API endpoints?
- How many API endpoints?
- Do you have any relevant documentation, such as diagrams and API collections?
- Concise summary of applications
- Out-of-scope requirements

1.4 Assessment Requirements

Typical requirements to facilitate commencement of the project will include;

1. Application URL (for the chosen environment)
2. Documentation
3. Credentials (for desired user roles)
4. Mobile application files (APK)
5. Thick client binaries
6. Relevant source code (for code-assisted engagements)

1.5 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement.

1. Kick-off Meeting
2. Application Security Testing
3. Exploitation and Vulnerability Validation
4. Analysis of Findings
5. Draft Report and Review of Initial Findings
6. Final Comprehensive Report

1.6 Methodology:

Our approach blends static analysis (where applicable), dynamic testing, and logic abuse simulation:

- Recon & Enumeration
    - Mapping application functionality and entry points
    - Identifying authentication methods, session flows, and input vectors
    - Analysis of application behavior and flow of data
    - Binary decompilation and analysis (applicable to mobile and thick applications)

- Automated & Manual Testing
    - Vulnerability scanning (e.g., OWASP Top 10, API Top 10)
    - Manual testing, validation, and chaining of findings
    - Business logic and authorization testing
    - Mobile and thick application-specific weaknesses (insecure storage, debugging flags, etc.)

- Credential & Token Abuse
    - Access control validation (IDOR, role escalation)
    - Testing JWT/session token strength and scope
    - API key and secret management review

- Exploitation & Impact Analysis
    - Proof-of-concept demonstrations
    - Replay/reuse attacks across interfaces
    - Authentication bypass, privilege escalation, and data exposure scenarios

- Strategic Recommendations

- Security findings prioritized by risk level and exploitation potential using CVSS version 4.
- Actionable and tailored remediation guidance from experienced consultants.
- Comprehensive reporting with clear visualizations of your security posture

1.7 Final Report Delivery

SilverSky will deliver a final version after a joint review with the Customer, and any changes will be addressed in the draft report.

- Comprehensive Report detailing
  - Methodology followed
  - Successful exploitation of the web application
  - Detailed recommendations for improvements

1.8 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope.

- Any web applications not identified as in-scope
- Any retesting of the application after remediations are addressed, unless specifically included in the SOW scope.
- Any testing not outlined in the in-scope testing section

If the Customer requests additional services, those services will be subject to a change request.

2 CUSTOMER OBLIGATIONS & ASSUMPTIONS

Services, fees, and work schedule are based upon the assumptions, representations, and information supplied by the Customer's fulfillment of these responsibilities is critical to the success of the engagement.

2.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize completion of key project phases, assign resources, and serve as project liaison
- **Access** - Ensure SilverSky consultants have access to key personnel and data requested
- **Resources** - Furnish SILVERSKY with Customer personnel, facilities, resources, and information, and perform tasks promptly
- **Cooperation** - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer that increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky.

2.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer's personnel with detailed knowledge of Customer's security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations, and requirements.

- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky's obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky cannot perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

3 PROJECT PARAMETERS

3.1 Project Scope

The scope of the project is based on the above description, with the additional details listed as follows:

Project Component	**Parameter(s)**
Project Start Date	Typically, within 30 days of the Effective Date
Project Duration	Approximately 1-2 weeks, subject to project variables; comments on findings preliminary to the comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
Application Security Assessment x1 Web App **S-266-2166**	Unauthenticated pentest of 1x web and 1x API
Application Security Assessment x1 Web App **S-266-2166**	Unauthenticated and authenticated pentest of 1x web and/or 1x API, using 1 user account
Application Security Assessment x1 Web App **S-266-2166**	Unauthenticated and authenticated pentest of 1x web and/or 1x API, using 2 user accounts

3.2 Location and Travel Reimbursement

The Service defined in this SOW does not require onsite participation by SilverSky staff at Customer location(s).

3.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.