

SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2166 WEB APPLICATION PENETRATION TESTING

1 OVERVIEW

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

1.1 Service Summary

The purpose of Web Application Penetration Testing (the “Service”) is to identify the feasibility of an attack on a Customer’s Internet-facing web application(s) and to determine the extent of the impact of successful exploitation of that intrusion. The testing will employ intrusion analysis and testing methodologies to test the potential for Internet-based penetration of the systems. The process will mimic typical attacker techniques and actual attempts to exploit identified vulnerabilities. SilverSky consultants will meet with key members of the Customer’s staff to determine the scope and ‘rules of engagement’ for performing the testing. This includes clarifying or determining specific aspects such as the extent and depth of testing, notification requirements, and the timing of testing. The testing is performed remotely from the SilverSky offices. Typically, there is minimal interaction required of the Customer after the initial meeting.

Project Deliverables:

- Comprehensive Report

1.2 Project Summary

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

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

1.3 SilverSky Obligations:

Kick-off Meeting - Meet personnel to discuss and agree on customer goals and the rules of engagement for the project. This includes project scoping (determining the target systems to be included in the testing), testing style (authenticated vs unauthenticated and the privilege level of authentication for users provided), the timeframe for testing, the extent to which system exploits can be performed, and procedures to follow should any issues occur during the testing. Any additional precautions or provisions are also considered before testing.

Dynamic Application Security Testing (DAST) - Use automated toolsets to perform web application scanning of the targets. This includes information gathering techniques, port and service scans, fingerprinting and enumeration of systems. Once this information is gathered, dynamic web app scanning identifies potential security vulnerabilities in the web application and architectural weaknesses. DAST tools allow sophisticated scans, detecting vulnerabilities with minimal user interactions once configured with host name, crawling parameters and authentication credentials.

SilverSky Proprietary

Vulnerability Validation - SilverSky will make a best effort to manually validate findings from the application vulnerability scan. SilverSky processes and techniques for manual validation will vary significantly depending on the type of weakness identified but may include screenshots, manually verifying ports and protocols or vulnerable versions in use. SilverSky will perform testing only under the agreed-upon rules of engagement.

Analysis of Findings Phase – SilverSky will compile and analyze the data generated from the assessment tools and manual checks, and categorize vulnerabilities by severity, depending on the potential impact each can have in the affected network. This analysis is the basis for recommendations to potentially address risks associated with the vulnerabilities.

1.4 Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report composed of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after a joint review with the Customer.

Executive Summary - The executive summary summarizes the results of the assessment. It is intended for upper management and boards of directors and includes:

- Overview of assessment results
- Itemization of the risk ratings for each area reviewed during the assessment
- Key findings and recommendations

Detailed Findings - The detailed findings section describes the assessment results in detail. It is intended for management, administrators, and other operations personnel and includes:

- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Recommendations for remediation

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. In the event that the Customer requests additional services, such services will be the subject of a change request.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees and work schedules are based on the assumptions, representations and information supplied by the Customer. 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 the 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.

SilverSky Proprietary

- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky including Customer’s security policies, network diagrams, server listings, and procedures

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 who have detailed knowledge of Customer 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 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 is unable to 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 2-3 weeks, subject to project variables; comments on findings preliminary to comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
S-266-2166 Web Application Testing Tier 3	6-10 Applications. Work hours not to exceed 80
S-266-2166 Web Application Testing Tier 2	3-5 Application. Work hours not to exceed 60
S-266-2166 Web Application Testing Tier 1	1-2 Applications. Work hours not to exceed 40

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.