



6421 Congress Avenue, Suite 206
Boca Raton, FL 33487-2859
561-999-5000
www.secnap.com

Contract For: {Company Name}

Consulting Project: Web Application Assessment

{Date}

Client Contact Name: {Contact Name}
Client Contact Title: {Contact Title}
Company Name: {Company Name}
Company Address: {Company Address}
Client Contact Telephone: {Phone Number}
Client Contact Email: {Email address}
External Web Application(s)
to be Assessed:
Anticipated Effort: {Insert here}
Not To Exceed: {Insert here}

Introduction

In the interest of evaluating and enhancing overall site security and further reducing the risk of attack in order to protect valuable business assets, {Company Name}, desires to contract with SECNAP Network Security to conduct web application assessments for the one above-named applications:

This project will yield valuable information and a keen understanding of current application security flaws along with recommendations for remediation. Our professionally certified consultants employ a multi-tier approach to enable you to focus on best practices for web application security:

- Detailed examination of vulnerabilities
- Assessment of application security policies and procedures
- Remediation recommendations
- Mechanisms for on-going process improvement.

The most effective solutions are usually custom-built, and airtight security demands no less. Our customized assessment is designed to address the components and variables unique to your applications, and to deliver results that will assist you in developing a seamless security policy and determining how best to deploy your most valuable resources in mitigating risk to the enterprise.

Overview of Primary Activities

Our pre-assessment consultation will identify the security lifecycle of the applications in order to facilitate precision analysis and help isolate the root causes of vulnerability.

Structured interviews with client personnel in {Company Name}, will facilitate the evaluation of security policies, practices and procedures relative to the target applications.

Leveraging a unique combination of industry-leading web application scanning technology and SECNAP security expertise and experience, application vulnerabilities will be identified in critical areas such as authentication mechanisms, session security, encryption usage and policy compliance.

This project will place a strong focus on SQL injection vulnerability detection, and will begin with penetration testing of the full site for vulnerabilities. This initial phase will look for operating system, firewall, and associated application vulnerabilities. On completion of penetration testing, intensive web application testing will be conducted.

The project deliverable will be the Web Application Assessment Report presenting site risks, threat priorities and remediation recommendations, supported by intuitive HTML reports and useful graphs and charts. Executive Summary included.

Process Outline

Web application testing will consist of a set of automated and manual tests intended to find weaknesses and vulnerabilities in the applications. Initial steps include identifying the web application layouts and locations where the greatest risks appear to reside. When the site is mapped, various attacks will be initiated to discover security gaps and vulnerabilities within the application.

A variety of fault injectors will be employed during this project. Fault injectors operate by inserting into the application certain elements that are likely to cause the application to fail. Hackers typically use these elements to probe an application for weaknesses in order to exploit it. The following fault injectors may be employed as part of this assessment:

- Windows Command Injection
- Unix Command Injection
- SQL Parser
- SQL Disclosure
- Relative Path
- Cross-Site Scripting
- Buffer Overflow
- Insecure Configuration
- Unvalidated Input
- Denial of Service

As a leading network security company, we understand the vulnerabilities that may affect today's commercial web applications and the tests required to discover and eliminate these security gaps. Following is a sampling of tests that will be conducted.

Field Vulnerabilities

This testing will determine if illegal fields can be inserted into the application and will also discover unvalidated hidden fields that could be used to extract unauthorized information from a database. Since fields may have varying degrees of confidentiality, field input validation criteria must be appropriate to the field value (e.g., zip code number validation vs. social security number validation).

Form/Page Vulnerabilities

Web applications generally combine stateful interactions with stateless protocol, where sequence is of utmost importance. This testing will verify that the application accepts input appropriate to its state, and that application development assumptions and specifications have been properly implemented.

Cross-Frame Scripting

Our synergistic assessment strategy combines the speed of automated testing with the thoroughness of manual testing. This testing will assess whether code-based safeguards have been implemented, detect gaps in Cross-Frame Scripting, and review workarounds, if any.

Broken Access Control

Testing will discover if the application allows access to restricted resources that are reserved for use by authorized users only. Tests will also attempt to access file system resources directly.

Broken Account and Session Management

Testing will assess whether the application enforces mechanisms that ensure passwords entered during account registration meet password strength criteria. Will also attempt to compromise account management by tampering with cookies.

Cross-Site Scripting (XSS) Flaws

Testing will determine if the application filters out malicious strings that could represent scripting code from an attacker.

Buffer Overflows

Tests will assess whether the web application can be made to behave improperly by injecting large volumes of characters into form input fields.

Command Injection Flaws

Testing will evaluate the application's resistance to specific command injection attacks.

Error Handling Problems

Testing will evaluate error handling when invalid SQL syntax is introduced into the application, and will determine whether the application behaves appropriately when a session times out.

Inconsistent Cryptography

Testing will verify that all form data in the application is submitted via Secure Sockets Layer encryption.

Remote Administration Flaws

Testing will validate that corporate policies for administrator password strength are being enforced.

Server Misconfiguration

Testing will discover if specific web server components provide inappropriate access to content and functions that should be restricted, as well as discover if pages that should be served only via Secure Sockets Layer encryption (SSL) are also inadvertently served via non-SSL.

Potential Impacts to the Application

During the course of testing, SECNAP will necessarily take certain actions that may impact the application being tested. We recommend the Client be aware of these potential impacts, alert key stakeholders, and be prepared to take recovery actions upon completion of testing.

Form Values – During the initial, crawling phase of the assessment, all forms will be submitted and all links followed to identify the areas of the site. Bogus data will be submitted to input fields (textboxes) in order to submit data to the forms. If specific values are required in order to ensure a meaningful test, Client must supply these values in advance for inclusion as part of the test. Client should notify Intrusion Detection System administrators as to when the tests are scheduled to occur.

Administrative Interfaces – The web assessment software and scanner will attempt to locate directories and filenames, such as /admin or /test, in an attempt to discover unadvertised portions of the web application. If segments of the application allow administrative control, these areas must be identified by the Client and discussed in advance.

Database Considerations – During the attack phase, the web assessment software may submit forms multiple times as it performs input validation tests. The information submitted to the database using these forms will require removal from the database once the tests are complete. It is highly recommended that a mirrored copy of the database be created by the Client prior to the start of the assessment so that production application databases or LDAP servers can be recovered, if necessary.

Automated Actions – Some web applications perform automatic actions, such as sending an email to a support team, or performing a stored procedure when a database row is inserted. If any of these types of automated actions are possible by virtue of running a test, these items should be discussed in advance and stakeholders should be notified. In particular, if there are any “off-limit” pages that should be avoided in the application, these should be clearly identified by the Client in advance.

Application Performance – The web assessment software can generate multiple concurrent HTTP requests prior to the HTTP Response to the first queued request. If the web application has significant known limitations in this performance area, Client should disclose this in advance. In addition, as part of the test a large number of HTTP requests will be submitted with “invalid” parameters. On slower systems, this may degrade system performance or prevent system access by users during the test.

Binary Documents – The web assessment software generally ignores many binary documents commonly found in web applications such as image files, documents, etc. If there are proprietary or non-standard files that are likely to be discovered by the software, these documents should be identified by the Client in advance. Failure to do so may seriously reduce the speed and affect completion of the assessment.

Residual Files – For some tests, files will be uploaded to the Client server to determine susceptibility to this type of vulnerability on the server. If it is not possible for SECNAP to automatically delete these files as part of testing, it may be necessary for the Client to manually delete these files.

Fees and Payment Terms

Consulting Fee is payable 50% prior to engagement and the remaining 50% is due in full on delivery of the Executive Summary and draft Assessment Report.

NOTE: Additional, optional work and security equipment may be recommended to the Client based on assessment findings.

Resources Provided by Client

Client will provide all hardware, software, documentation, vendor contacts and Internet access necessary to complete work. A completed, signed SECNAP External Penetration Test authorization form is required prior to commencement of testing. Successful completion of work is dependent on availability of functional hardware, software and Internet access.

Project Overrun/Additional Consulting Services

This project estimate is based on configuration data provided by the Client and our experience with similar implementations. Many clients elect to purchase additional engineering time, beyond the original project scope, in the interest of continuity during their remediation phase or to accommodate mutually-agreed scope expansions. Additional time may be secured according to the schedule below.

Remediation Assistance	8am – 5pm Monday through Friday		After-Hours
Senior Security Engineer	\$250/hour	\$2,000/day	\$375/hour
Associate Security Engineer	\$150/hour	\$1,200/day	\$225/hour
Network Engineer	\$75/hour	\$600/day	\$115/hour

Note: Does not include \$50 per diem to cover meals and travel.

Warranty

SECNAP does not provide warranties, expressed or implied, as to the integrity or security of Client’s data or Internet access or hardware, and is not liable for any damage caused by the use of public Internet resources or by required security scans on known or unknown services or programs.

Any changes to this Statement of Work, including those which impact original estimated maximum man-hours and cost, must be mutually agreed by both parties in writing.

By signing below the Client and SECNAP concur as to scope of work and other stated terms of this engagement. We look forward to doing business with you.

For SECNAP Network Security

For Client

By (Signature)

By (Signature)

Name and Title (Print)

Name and Title (Print)

Date

Date