SERVICE DESCRIPTION

Trustwave Application Penetration Testing (Standard)

Service Scope

The Trustwave SpiderLabs Application Penetration Test service results in an in-depth holistic review of the entire target application and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target environment. These recommendations are both actionable and advisory in nature and are presented to the customer.

The process involves methodical and expert driven testing of the target application spanning the client and server endpoints, as well as the communications channels to determine if the application is vulnerable to application layer security risks.

This level of testing helps validate the application layer security controls; the security effectiveness of software development and deployment standards by determining how resilient the application is to determined attackers.

The product of an Application Penetration Test is a report that documents the application's existing security posture, identifies specific weaknesses and vulnerabilities, and provides purpose-built exploit code examples. The detailed report tells a compelling story of risk associated with each vulnerability and makes specific recommendations for their remediation.

Benefits of an Application Penetration Test include:

- Identification of the application's exposure to security risks
- Identification of specific vulnerabilities affecting the application
- Validation and verification of existing security controls, policies, and procedures by impartial third-party experts

Vulnerability Class	Subtypes
Authentication and Authorization	• Authentication Bypass • Vertical/Horizontal Privilege Escalation • Default/Weak Passwords • Authentication Mechanisms • Login/Password Reset Controls
Session Management	• Cross-Site Request Forgery • Session Identifier Prediction

Vulnerability Class	Subtypes
	• Session Hijacking • Session Replay • Session Fixation/Trapping • Insufficient Session Expiration • Cookie Settings • Logout Mechanisms
Injection	• SQL Injection • Cross-Site Scripting • LDAP Injection • HTML Injection • XML Injection • OS Command Injection • CRLF Injection • Formula Injection • Server-Side Template Injection • Host Header Poisoning
Application Resource Handling	• Server-Side Request Forgery • Path Traversal • Predictable Object Identifiers • XML Entity Expansion & Attribute Blowups • Local & Remote File Inclusion • Insecure Deserialization • Data Upload/Download Capabilities • Lack of Virus Scanning • Workflow bypass
Data Protection	• Weak or Missing Encryption at Rest or in Transit • Padding Oracles • Digital Certificates • Configured Framework Methods • External References
Client-Side	• Outdated Client Software • HTML Web Storage Objects • Cross-Site Scripting • Vertical/Horizontal Privilege Escalation • Authentication Bypass
Server-Side	• Outdated Server Software • Missing Web Server Patches • Superfluous Services • Missing/Poorly Configured Security Headers • Default Content • Directory Indexing • Web Caching • Verbose Error Messages
Information Disclosure	• HTML Comments • Sensitive Information in Responses or URL • Cross-Domain Referrer Leakage • Insufficient Cache Controls

Vulnerability Class	Subtypes
	• Sensitive Information Sent to Third Parties
Bounds Checking	• Stack-Based • Heap-Based • Format String • Integer Overflow/Underflow

Trustwave will utilize varying combinations of application testing approaches. Those approaches are:

Vulnerability Scan of the Application Layer

Using the Trustwave SpiderLabs application testing suite, the entire application will be reviewed for security-related flaws. The tools will identify common application vulnerabilities within the application. Depending upon application design and source code availability, this review will occur either via an offline review of the application source code, or via live interaction with the application.

Vulnerability Scan of the Infrastructure Layer

Using the Trustwave SpiderLabs infrastructure testing suite the application's server infrastructure will be reviewed for common security vulnerabilities. The Trustwave tools will identify common infrastructure issues that may undermine the security posture of the application.

Standard Application Testing

Using our standard manual testing methodology, Trustwave SpiderLabs will manually probe and test all aspects of the application aligned with industry standards such as Application Security Verification Standard. This type of testing may be performed on any type of application (including web-based and non-web based applications). Using manual analysis of the application, Trustwave is able to provide a higher level of assurance for an application. In the event that the application supports user roles, all individual roles within the scoping definitions for each application size will be tested to ensure that logical role isolation exists.

Trustwave's methodologies are based on industry standards. Standard application penetration testing assessments cover all the necessary test classes such as those outlined in Application Security Verification Standard (ASVS). The opportunistic level provides a baseline that can be adopted by most penetration testing activities. Where possible, higher-level mandates have been adhered to that did not require a level of access outside of an application penetration testing activity. A mapping of our vulnerability classes to ASVS is provided below for clarity:

ASVS	Trustwave Vulnerability Classes
V1. Architecture, design and threat modeling	Application Mapping
V3: Session Management Verification Requirements	Session Management
V4: Access Control Verification Requirements	Authentication and Authorization / Session Management
V5: Malicious input handling verification requirements	Injection / Application Resource Handling

ASVS	Trustwave Vulnerability Classes
V6: Output encoding / escaping	Injection
V7: Cryptography at rest verification requirements	Data Protection
V8: Error handling and logging verification requirements	Server-Side / Information Disclosure
V9: Data protection verification requirements	Server-Side / Client-Side / Information Disclosure
V10: Communications security verification requirements	Data Protection
V11: HTTP security configuration verification requirements	Server-Side
V12: Security configuration verification requirements	Server-Side
V13: Malicious controls verification requirements	Not applicable to application penetration testing
V14: Internal security verification requirements	Not applicable to application penetration testing
V15: Business logic verification requirements	Application Resource Handling
V16: Files and resources verification requirements	Application Handling / Injection
V17: Mobile verification requirements	Not applicable to application penetration testing
V18: Web services verification requirements	Web Services
V19. Configuration	Server-Side