Application Security

As Assessment

Pt Penetration Testing

Cr Code Review

Determine the effectiveness of your applications' security controls and train your development team in secure coding with Trustwave's application security solutions.

For organizations that need to evaluate the security of Web applications or train their development staff on secure coding and development practices

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses throughout the world. Trustwave analyzes, protects and validates an organization's data management infrastructure - from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multi-lingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

A Analyze P Protect V Validate

For more information about Trustwave's Elements of Compliance and Data Security please visit: www.trustwave.com

A Growing Threat to Sensitive Data: Insecure Applications

Poorly coded applications put organizations at risk. A large amount of confidential consumer information lies within the application layer as more and more organizations develop applications to streamline internal processes and improve the customer experience. However, without making security an inherent part of the Software Development Life Cycle (SDLC), the risk associated with insecure applications far outweighs these gains in efficiency and customer satisfaction.

Trustwave's full suite of application security solutions delivered by an expert team of application specialists ensures that your application is tested and reviewed thoroughly. The application security team uses manual processes to test and review applications according to your needs. The result is specific guidance that can significantly improve the security of your applications. Traditional application testing with automated tools provides generic results that do little to combat the rapidly changing landscape of security exploits.

Application Penetration Testing

An application penetration test simulates an attack against an application to determine the effectiveness of its security controls. Performed by Trustwave's application security experts, the manual testing process probes an application much more thoroughly than automated assessment tools that can produce generic responses and excessive false positives. By thoroughly testing an application from a variety of authenticated- and unauthenticated-user perspectives, the Trustwave application penetration testing service highlights risks posed by exploitable vulnerabilities.

Trustwave application penetration tests evaluate an application's vulnerability to all known application exploits including but not limited to:

- Arbitrary Code Execution
- Input Validation
    - Cross-Site Scripting
    - SQL Injection
    - Buffer Overflows
- Authentication Bypass
- Input Tampering
    - URL Manipulation
    - Hidden Variable Manipulation
    - Cookie Modification

The intention of Trustwave's application penetration testing methodology is to demonstrate existing, exploitable vulnerabilities within an application that can lead to the compromise of critical data. Clients receive the results in a detailed deliverable including both tactical and strategic recommendations. The simulated attack aids clients in pinpointing flaws and mitigating the risk of data compromise.

70 W. Madison Street, Suite 1050, Chicago, IL 60602
www.trustwave.com
1.888.878.7817

Trustwave® Information Security & Compliance

Why SpiderLabs is the Best Choice

SpiderLabs services and delivery are backed by a full portfolio of information security resources:

Expertise

The SpiderLabs team consists of some of the top information security professionals in the world. With career experience ranging from corporate information security to security research and federal and local law enforcement, our staff possesses the background and dedication necessary to stay ahead of the technical, legal, and management issues affecting your organization's information security.

Experience

SpiderLabs has performed hundreds of forensic investigations and application security tests and thousands of ethical hacking exercises for a client list that includes Fortune 500 companies, small to mid-sized businesses, government security agencies and law enforcement agencies.

Certification

Trustwave is certified by the National Security Agency (NSA), the agency responsible for assessing the US government's information security posture. We are also authorized by all major credit card brands to conduct investigations of compromised merchants and processors.

Facilities

SpiderLabs maintains the most advanced application and hardware testing facility in the industry.

Safety

SpiderLabs works closely with clients to ensure that all of its services are performed with strict confidentiality and rigorous legal oversight.

SpiderLabs℠

Trustwave can perform thorough penetration tests of any application including but not limited to:

- Web-Based Applications—Web application interfaces are convenient, but an increase in risk accompanies this ease of use. Trustwave's application penetration testing service consists of a comprehensive test of the entire Web application and its supporting environment.

- Thin-Client Applications—Thin-client applications run on the client machine but are primarily used to convey data from a central server, where the majority of processing and data controls are handled. Using Trustwave's experts to conduct testing of thin-client applications provides clients with a comprehensive test of the thin-client environment.

- Thick-Client Applications—Thick-client applications run almost exclusively on the client machine, and server relationships are used only for storage or communication. Limited or no reliance on a server does not eliminate the risk of data compromise.

Application Code Review

Custom applications require custom security. During the Trustwave application code review, our application security experts manually inspect all relevant application source code to pinpoint deficiencies in security controls and identify development errors that violate best practices or may lead to vulnerabilities.
A Trustwave application code review examines all aspects of an application's security at the source-code level. In addition, the review includes an evaluation of the tools and commercial applications used to create and run the front- and back-end services.

Trustwave's analysis will evaluate your application for vulnerabilities including but not limited to:

- Improper Buffer Checking
- Unintended Operations
- Input Validation
  - SQL Injection
  - Command Redirection
  - Insecure Automatic Data Inclusion
- Dynamic Content Creation Issues
- Secure Code Signing
- Improper Cryptography
- Unexpected Failure Conditions

The code review culminates in an exhaustive report that details specific areas of application code that need repair in order to maintain a secure system. Trustwave's manual review ensures that your developers receive actionable, prescriptive information specific to your application rather than generic information provided by automated tools.

Specifically, Trustwave will provide a report for each reviewed application that will explain:

- Specific application and version tested
- Components of review performed on the application
- Assessment of the effectiveness of existing controls in terms of design and operating effectiveness
- Testing documentation
- Application risks identified
- Application security risk mitigation recommendations based on reviews
- Overall risk-level rating of the application
- Discussion of the review activities performed to arrive at the overall rating

Secure Developer Training

Trustwave provides a customized training class to an organization's developers based upon industry best practices and the results of the actual reviews performed. This service, Secure Developer Training, has been found to be more effective in mitigating future coding errors because developers are trained on examples taken from their own applications.

Trustwave can provide one to three days of client-site training tailored to fit the client's application development environment. Ideally, the training session follows an application code review or application penetration test engagement so that specific examples from those engagements can be included within the training class. This way the client's staff learns from real-world and business-relevant coding problems and can put their knowledge to use immediately.