

# Web Application Test

## Compliance Overview

IT Security Compliance regulations and guidelines (GLBA, FFIEC, FDIC, NCUA, OCC, OTS) require an organization to conduct independent testing of the Information Security Program to identify vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI). Best Practices state that each organization should perform an External Penetration Test in addition to regular security assessments in order to ensure the security of their external network; this includes any web-facing applications that are exposed to risk.

## Solution Overview

The objective of the TraceSecurity Web-Application Testing service is to determine the strength of the online application security profile, and not simply 'break' or deface an application or site. The TraceSecurity Information Security Analyst (ISA) assesses the online application to identify weakness in: general architecture; session management; transport security; access control and authorization; logging; data validation; system attacks; perimeter manipulation; privacy concerns and cryptographic algorithms.

**TraceSecurity's Online Application Test will provide up-to-date security auditing for vulnerabilities such as:**

- Software Infrastructure/Design Weaknesses
- Authentication
- Session Management
- Input Validation Attacks
- Cross Site Scripting Attacks
- Script Injection Attacks
- CGI Vulnerabilities
- Cookie Theft
- User Privilege Elevation
- Web/Application Server Insecurity
- Database Vulnerabilities
- Privacy Exposures
- Logical Flaws

## Testing Requirements

- Brief training or educational introduction to the mechanics of the application
- Multiple test accounts or administrative access to create additional accounts

**The Online Application Test results are provided in an extensive report containing:**

- Immediate Notification of Critical Risks
- Executive Summary
- Business & Technical Risks/Recommendations
- Application Test Methodology  
*Information gathering, discovery, fingerprinting & enumeration, primary and secondary attack phases, and results analysis*
- Application Security Issues Listed by Risk Type and Areas of Concern
- Details & Exposure of Application Vulnerabilities
- Enumeration of Successfully Penetrated Systems
- Recommendations and Counter Measures
- Appendix Examples
- Video and/or screen image records of the application test results are available options

LEARN MORE ABOUT ONLINE APPLICATION TESTS

**Mitigating IT Security Risks  
with Penetration Tests:**

A TraceSecurity White Paper

Download at [www.tracesecurity.com](http://www.tracesecurity.com)

