HALOCK®

WEB APPLICATION PENETRATION TEST

Protecting the leading source for data breaches.

What is a Web Application Penetration Test?

For sensitive or high value web applications, a comprehensive review is appropriate. HALOCK's approach to assessing web applications fully identifies and evaluates web application vulnerabilities. Testing is performed with knowledge of the functionality available to users and their access levels to ensure a detailed review of the application.

Why should we conduct a Web Application Penetration Test?

Custom web applications are designed to provide access to services and information. Validating if that access is used as intended requires a very specific and specialized method of testing. Because every custom application is unique, web application penetration testing is conducted to identify vulnerabilities in the underlying code that an attacker can leverage to gain unauthorized access. Most regulations governing organization security obligations specifically call out web applications as requiring this form of testing, above and beyond other internet facing assets. PCI DSS requires web application testing for those that have not used web app firewalls. Performing web application penetration testing is a critical step in ensuring the code is secure, the organization is compliant, and customers can trust their data is protected.

Why should HALOCK perform our Web Application Penetration Test?

HALOCK has the experience to best assess the security controls effectiveness for web applications. For over two decades, HALOCK has conducted thousands of successful penetration tests for companies of all sizes, across all industries.

HALOCK's dedicated penetration test team is highly **qualified**, possesses advanced certifications, and is equipped with the labs, tools, and methodologies necessary to consistently deliver quality, **accurate**, detailed, and meaningful results.

HALOCK leverages industry standard methodologies to ensure a thorough and **comprehensive** test is conducted under safe and controlled conditions. HALOCK's reports are content rich, regularly stand the scrutiny of regulatory requirements, **exceed expectations** of auditors, and frequently receive the praise of our customers. HALOCK does not simply validate automated scans. HALOCK's **expert** team discovers vulnerabilities not yet published and often not yet discovered. Exploits are pursued, documented step by step, with screen capture walkthroughs, to provide both the technical and visual **clarity** necessary to ensure corrective actions can be prioritized and remediation is **effective**.

Which web applications should we have tested?

Commercially provided web applications, especially those with minimal customization, are generally well documented through public sources for known vulnerabilities as well as the patches required to remediate those issues. Commercial applications that lack this history of testing should be considered for comprehensive web application testing as unknown (zero day) vulnerabilities may exist, but this is not common. Custom developed web applications, however, are most commonly selected for comprehensive testing. As each customer web application is unique, these public sources do not exist. Custom web applications, in particular those protecting sensitive information, should be considered for comprehensive web application penetration testing. Regulatory requirements also often dictate certain applications be tested at least annually.

While you cannot always choose ***if*** a penetration test needs to be conducted,
you ***can*** choose the provider that will deliver the results you expect.

HALOCK®

WEB APPLICATION PENETRATION TEST

A Comprehensive Testing Methodology

Information Gathering

Conducting reconnaissance activities to locate information leakage, identify the technologies utilized, map application entry and functionality, and related tasks to guide testing.

Configuration and Deploy Management Testing

Testing the configuration of underlying platform and infrastructure and identifying potential change control weaknesses such as the presence of orphaned code or code backup files.

Identity Management Testing

Verification, where appropriate, for account provisioning considerations such as user registration processes or account enumeration.

Authentication Testing

Testing for authentication related weaknesses, such as insecure authentication, default credentials, or password weaknesses.

Authoriztion Testing

Testing to validate the security of authorization controls such as privilege escalation or bypassing authorization.

Session Management Testing

An evaluation of session-related vulnerabilities such as session fixation, exposed session variables, and cross-site request forgery.

Data Validation Testing

Data validation testing including cross-site scripting, parameter tampering, SQL injection, and command injection.

Testing for Error Handling

Testing error handling issues, as they relate to security, such as analysis of Error Codes and Stack Traces.

Testing for Weak Cryptography

Testing to evaluate the effectiveness of encryption related protections such as weak SSL ciphers.

Business Logic Testing

Testing to determine if the flow or architecture of the application can be manipulated to gain access to sensitive information through flaws in business logic or application workflows.

Client-side Testing

Assessing vulnerabilities that commonalty affect the client side of the application session such as JavaScript execution, CSS injection, cross-site flashing, and clickjacking.

Deliverables

Project Plan: Prior to testing, HALOCK will develop a project plan detailing the specific plan, timing, and related considerations. This ensure all parties know what to expect throughout the execution of testing and reporting.

Penetration Test Report: The complete results of the penetration test are documented in our content rich report which includes the background, summary of findings, detailed findings, scope and methodology, and supplemental content for context and reference.

Background: An introduction of the general purpose, scope, methodology, and timing of the penetration test.

Summary of Findings: A concise overview summarizing the results at a glance, such as key critical findings requiring priority attention, system or recurring issues, and other general results.

Detailed Findings: Comprehensive results of each vulnerability, including a description of the vulnerability observed, the impact, recommendations for remediation, evidence where the vulnerability was observed, step-by-step demonstrations of exploits performed, and additional reference materials.

Scope and Methodology: A detailed recap of the specific scope of what was tested, the methodologies utilized, and related historical information necessary for audiences such as auditors to understand the specifics of the test approach.

Supplemental Content: Additional content and guidance, such as recommended post assessment activities.

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.