ZONES™

Application Security Assessment

Assess applications, prioritize remediation, and reduce risks

While automated scanning is an important first step to identifying vulnerabilities, an application security assessment is a crucial part of software lifecycle management. To augment automated testing, Zones application security assessments include advisory services to provide an in-depth look at vulnerabilities in software.

> Assess the security posture of commercial, web, and third-party applications

> Determine if sensitive data is stored, processed, or transmitted by applications

> Remediate vulnerabilities based on risk levels to your organization

> Stay in compliance with industry regulatory requirements

Business Value

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

Zones Application Security Assessments

Steps	Professional Level	Enterprise Level	Enterprise + Level
Automated Security Scanning: Commercial scanning tools used to identify potential vulnerabilities	🛡	🛡	🛡
Report Development and Interpretation: Analyze results and remove false positives	🛡	🛡	🛡
Network Architecture Review: Review network security design and identify weaknesses		🛡	🛡
Manual Exploit Testing: Perform manual in-depth testing techniques to validate weaknesses		🛡	🛡
Security Policy Review: Review up to five security policies for gaps in procedures		🛡	🛡
Automated Security Re-Scan (within three months): Re-scan identified systems after patches are put in place			🛡
Black Box Testing: Perform system identification without prior knowledge from the client on devices			🛡

How the Process Works

> Probe, identify, and exploit vulnerabilities in systems within scope, with manual techniques and automated tools

> Attempt to escape out of the network and application boundaries of the systems within scope

> Attempt to gain unauthorized access to systems within scope and systems connected to the web applications

All security assessments will involve, but are not limited to, the following methodologies:

- Analysis of data access requirements
- Input validation
- Transport mechanism
- Error condition handling and exception management
- Business logic, functional specification, and implementation
- Site design
- Authentication
- File system traversal
- Access control and authorization
- Session management
- Source sifting
- Data confidentiality
- Encryption
- AJAX testing