AURORA

Application Security Assessment

Application Security Assessment

Our Application Security Assessment is designed to meet best practices for application security. Industry regulations such as PCI, HIPAA and Red Flag require application security testing. Aurora can also assess custom-designed items such as web applications and commercial 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
- Session Management

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 application

Key value propositions include:

- Discovery of key weaknesses in the servers
- Manual and automated testing procedures
- Review of network, operating system, application and end-point security measures
- Development of key remediation recommendations
- Client specified Internet reachable systems

BUSINESS VALUE

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

FEATURES & BENEFITS

- Simulates an attacker
- Consistent and repeatable testing
- Continuously expanding vulnerability tests
- Comply with industry-driven regulatory requirement
- Fixed fee

aurorait.com
888.282.0696
info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505

AURORA

Application Security Assessment

Application Security Assessment Steps

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 5 security policies for gaps in procedures.		✓	✓
Automated Security Re-Scan (within 3 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.			✓

Ready To Get Started?

Contact us at 888-282-0696 or sales@aurorait.com to learn how Aurora Security Services can help you accomplish your specific business and IT security goals. Explore further by visiting our website at: www.aurorait.com

aurorait.com
888.282.0696
info@aurorait.com

2510 W. 237th Street | Suite 202 | Torrance, CA 90505