

**Integrigy Consulting**

# **Oracle Security Services Application Security Assessment**

The logo for Integrigy, featuring the word "INTEGRIGY" in a bold, blue, serif font. Above the 'I' and 'Y' are green checkmarks.

# Integrigy Overview

- **Integrigy Corporation specializes in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. Integrigy Consulting offers security assessment services for leading databases and ERP/CRM.**
  
- **Corporate Details**
  - Founded December 2001
  - Privately Held
  - Based in Chicago, Illinois

# Integrigy Background

- **Extensive experience with Oracle**
  - Founded by former Big-6 consultants with significant experience on Oracle implementations in Fortune 500 companies
  - Founders recognized a major gap in all implementations – little or no security auditing done on projects
  - Integrigy has found more security bugs in Oracle Applications than anyone else inside or outside of Oracle
- **Both an ERP/CRM company and a security company**
  - Products developed to support and enhance an ERP/CRM implementation – Integrigy understands the issues and risks challenging large ERP/CRM implementations
  - Integrigy bridges the gap between applications, databases, and security

# Integrigy Security Alerts

Security Alert	Versions	Security Vulnerabilities
<b>Critical Patch Update July 2008</b>	Oracle 11g 11.5.8 – 12.0.x	<ul style="list-style-type: none"> <li>2 Issues in Oracle RDBMS Authentication</li> <li>2 Oracle E-Business Suite vulnerabilities</li> </ul>
<b>Critical Patch Update April 2008</b>	12.0.x 11.5.7 – 11.5.10	<ul style="list-style-type: none"> <li>8 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update July 2007</b>	12.0.x 11.5.1 – 11.5.10	<ul style="list-style-type: none"> <li>11 vulnerabilities, SQL injection, XSS, information disclosure, etc.</li> </ul>
<b>Critical Patch Update October 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>Default configuration issues</li> </ul>
<b>Critical Patch Update July 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> <li>Information disclosure</li> </ul>
<b>Critical Patch Update April 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> <li>Information disclosure</li> </ul>
<b>Critical Patch Update Jan 2005</b>	11.5.1 – 11.5.10 11.0.x	<ul style="list-style-type: none"> <li>SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #68</b>	Oracle 8i, 9i, 10g	<ul style="list-style-type: none"> <li>Buffer overflows</li> <li>Listener information leakage</li> </ul>
<b>Oracle Security Alert #67</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>10 SQL injection vulnerabilities</li> </ul>
<b>Oracle Security Alert #56</b>	11.5.1 – 11.5.8 11.0.x	<ul style="list-style-type: none"> <li>Buffer overflow in FNDWRR.exe</li> </ul>
<b>Oracle Security Alert #55</b>	11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>Multiple vulnerabilities in AOL/J Setup Test</li> <li>Obtain sensitive information (valid session)</li> </ul>
<b>Oracle Security Alert #53</b>	10.7, 11.0.x 11.5.1 – 11.5.8	<ul style="list-style-type: none"> <li>No authentication in FNDFS program</li> <li>Retrieve any file from O/S</li> </ul>

# Application Security Assessment Overview

- **The goal of the application security assessment is to identify security issues and weaknesses in the Oracle Applications production technical environment as it is installed, configured, maintained, and used**
- **The assessment is a quantifiable, consistent, and thorough review of the state of the application and infrastructure security at a point in time**
  - Findings will be reflective of the current state of security
- **The deliverable is an actionable list of recommendations that will provide a foundation for a secure environment**

# Assessment Assumptions

- **Goal is to improve security, can't make it perfect**
- **Security is a cost/benefit proposition**
  - Balance security objectives with operational realities
- **Internal threat is greater than external threat**
  - Insider knowledge and understanding of Oracle Applications is far greater and more dangerous
- **Perimeter network is secure**
  - Internal network is insecure
- **Undisclosed security holes exist in Oracle Applications**
  - Both known and unknown security bugs must be addressed

# Assessment Critical Success Factors

- **Complete**
  - The assessment must be broad and deep in order to review the entire technology stack and application
- **Accurate**
  - All the information and recommendations must be precise and correct to allow for a rapid and thorough implementation of those recommendations
- **Applicable**
  - With the multitude of versions, modules, and configurations of Oracle Applications, the assessment must focus not only on the current state of the application but also address future patches, upgrades, and configuration changes.
- **Effective**
  - Changes to the configuration and installation must be supported and work with minimal effort and change.
- **Efficient**
  - The recommendations must be able to be implemented in a cost effective and timely manner.

# Assessment Phases

- **Phase 1 – Planning and Information Gathering**
  - Review of documentation
  - Interviews with key IT resources
- **Phase 2 – Testing**
  - Test/QA instance is analyzed first, then production
  - Automated scanning
  - Manually testing
  - Review of customizations
- **Phase 3 – Analysis and Reporting**
  - Review and correlation of data and findings
  - Development of report

# Technical Scope

- **Oracle Applications Production Environment**
  - Web servers, forms servers, concurrent manager servers, and database servers
- **Oracle Applications Development Environments**
  - Assessed using automated tools
  - Minimal manual testing
- **Modules included in the scope of the project is only reviewed and assessed from a technical perspective**
  - Functional and business activities are not in scope.
- **Segregation of duties is only analyzed for System Administrator functions and responsibilities**
  - Not for other module responsibilities or functions (GL, AP, etc.).

# Technical Scope

- **Network infrastructure associated with Oracle Applications to determine appropriateness for the Oracle implementation**
- **Operating system (Unix, Linux, Windows) installation and configuration for each server to assess the security related to Oracle Applications**
- **All Oracle Applications Modules**
  - with the following exceptions –
    - ◆ CRM Interaction Center (Call Center, Telephony, Scripting, Email Center, etc.)
    - ◆ Mobile and Palm Solutions (Field Sales, Field Service, Gateway for Mobile Devices, etc.)
    - ◆ Credit Card Processing Integration (iPayment Integration with backend systems – Cybercash, First Data Corp., etc.)
    - ◆ Industry Solutions (Automotive, Clinical, i2, etc.)
    - ◆ Data Warehousing (Clickstream Intelligence, Warehouse Builder, Data Mart Suite, etc.)

# Customization Assessment

- **All customizations assessed from a design and source code perspective**
  - interfaces
  - web customizations
  - custom forms
  - reports
- **Customization design assessed to determine any security issues inherent in the design and implementation of the customization**
- **Customization source code is reviewed to identify any potential security flaws in the implementation of the customization, which may include SQL injection, cross-site scripting, parameter tampering, information disclosure, and improper or missing authentication**

# Automated Assessment Tools

- **Integrigy AppSentry™**
  - Application security scanner designed for Oracle Applications, Oracle Application Server, and Oracle Database
  - 300+ security checks
  - Does not require any changes to the environment or software to be installed on servers – query only
  - No performance impact - Single threaded
- **Integrigy Scrutinize Suite**
  - Scrutinize/Java - Java code scanner to detect SQL injection, parameter tampering, cross site scripting
  - Scrutinize/Forms – Oracle Forms code scanner to detect SQL injection
  - Scrutinize/PLSQL – Oracle PL/SQL code scanner to detect SQL injection
- **Integrigy Intplus**
  - Capture of database information for automated and manual analysis
- **Integrigy NetScan and TNSSpy**
  - Analyzes Oracle Applications at the network level
- **Nessus**
  - Vulnerability scanner to identify OS level issues
- **Paros**
  - Web application proxy to test for issues in customizations

# Operational Security Assessment

- **Operational activities related to the Oracle Applications environment are assessed to determine if there are security or controls weaknesses**
  - Security management, auditing, monitoring and troubleshooting, change management, patching, and development are assessed for the Oracle Applications, database, application servers, and operating system
- **Operations specific to Oracle Applications are categorized into 27 domains**
  - Domains are individually assessed
  - Domains are mapped to ISO 17799, COBIT, and NIST 800-53
  - Interview questions and tests/validations for each domain are defined in the assessment methodology

# Operational Security Domains

		Oracle E-Business Suite Technical Components			
		Oracle E-Business Suite	Oracle Database	Oracle App Server	Operating System
Operational Processes	1. Security	1.1 User Management	1.3 Database Security	1.4 Network and Web	1.5 OS Security
		1.2 Segregation of Duties			
	2. Auditing	2.1 Application Auditing	2.2 Database Auditing	2.3 Web Logging	2.4 OS Auditing
	3. Monitoring + Troubleshooting	3.1 Application	3.2 Database	3.3 Web + Forms	3.4 Operating System
	4. Change Management	4.1 Object Migrations	4.3 Database Objects	4.5 Change Control	4.6 Change Control
		4.2 Application Configuration	4.4 Database Configuration		
	5. Patching	5.1 Application Patches	5.2 Database Patches	5.3 App Server Patches	5.4 OS Patches
6. Development	6.1 Application	6.2 Database	6.3 Web	6.4 Shell + File Transfer	

# Operational Assessment

- **Inspection**

- Written policies and procedures and other documentation are reviewed to ascertain what are the stated policies and procedures – **“how should it work”**

- **Collaborative Inquiry**

- Key personnel are interviewed to confirm the stated policies and procedures and management’s representations and to identify any known gaps or weaknesses – **“how do people think it works”**

- **Testing and Validation**

- For each operational domain, tests and validations are performed to determine **“how does it actually work”**

# Integrigy Contact Information

**Integrigy Corporation**  
**P.O. Box 81545**  
**Chicago, Illinois 60681**  
**888/542-4802**

**Website:** [www.integrigy.com](http://www.integrigy.com)

**Sales:** [sales@integrigy.com](mailto:sales@integrigy.com)

**Development:** [development@integrigy.com](mailto:development@integrigy.com)

**Support:** [support@integrigy.com](mailto:support@integrigy.com)

**Security Alerts:** [alerts@integrigy.com](mailto:alerts@integrigy.com)