Oracle E-Business Suite

Web Security Vulnerabilities Examined

June 22, 2016

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation
Agenda

1. Web Application Security
2. Oracle EBS DMZ Implementation
3. Vulnerabilities Examined
4. Oracle EBS DMZ Implementation
5. Q&A
About Integirigy

**Products**

- **AppSentry**
  ERP Application and Database Security Auditing Tool

- **AppDefend**
  Enterprise Application Firewall for the Oracle E-Business Suite

**Services**

- **Security Assessments**
  ERP, Database, Sensitive Data, Pen Testing

- **Compliance Assistance**
  SOX, PCI, HIPAA

- **Security Design Services**
  Auditing, Encryption, DMZ

---

**ERP Applications**
Oracle E-Business Suite

**Databases**
Oracle and Microsoft SQL Server

---

You
Agenda

1. Oracle EBS
2. Web Application Security
3. Vulnerabilities Examined
4. Oracle EBS DMZ Implementation
5. Q&A
Oracle EBS installs all modules (250+) and all web pages for every application server.

All web pages access the database using the **APPS** database account.
- Oracle EBS installs all modules (250+) and **all web pages** for every application server
- All web pages access the database using the **APPS** database account
OWASP Top 10 – 2013 Edition

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Control
A8: Cross Site Request Forgery (CRSF)
A9: Using Known Vulnerable Components
A10: Unvalidated Redirects and Forwards

http://www.owasp.org/index.php/Top_10
The Web Application Security Consortium (WASC) has developed the **WASC Threat Classification** to “clarify and organize the threats to the security of a web site.”

### Attacks
- Abuse of Functionality
- Brute Force
- Buffer Overflow
- Content Spoofing
- Credential/Session Prediction
- Cross-Site Scripting
- Cross-Site Request Forgery
- Denial of Service
- Fingerprinting
- Format String
- HTTP Response Smuggling
- HTTP Response Splitting
- HTTP Request Smuggling
- HTTP Request Splitting
- Integer Overflows
- LDAP Injection
- Mail Command Injection
- Null Byte Injection
- OS Commanding
- Path Traversal
- Predictable Resource Location
- Remote File Inclusion (RFI)
- Routing Detour
- Session Fixation
- SOAP Array Abuse
- SSI Injection
- SQL Injection
- URL Redirector Abuse
- XPath Injection
- XML Attribute Blowup
- XML External Entities
- XML Entity Expansion
- XML Injection
- XQuery Injection

### Weaknesses
- Application Misconfiguration
- Directory Indexing
- Improper File System Permissions
- Improper Input Handling
- Improper Output Handling
- Information Leakage
- Insecure Indexing
- Insufficient Anti-automation
- Insufficient Authentication
- Insufficient Authorization
- Insufficient Password Recovery
- Insufficient Process Validation
- Insufficient Session Expiration
- Insufficient Transport Layer Protection
- Server Misconfiguration

[http://www.webappsec.org](http://www.webappsec.org)
Attacker modifies URL with extra SQL


Oracle EBS executes appends SQL to the SQL statement being executed

- SQL executed as APPS database account
- Example changes any application account password

This vulnerability was patched as part of Oracle Security Alert #32
Cross Site Scripting (XSS) Illustrated

A. Attacker enters malicious JavaScript into job application description field to for example automatically approve resume

B. HR Manager opens job application in Oracle and script executes in browser

C. Script calls an Oracle EBS URL in a hidden frame to execute some EBS functionality
Cross Site Scripting – Sample Attacks

<script>alert(0)</script>
<img src="x:x" onerror="alert(0)">
<iframe src="javascript:alert(0)"
<object data="javascript:alert(0)"
<IMG SRC=/ onerror="alert(String.fromCharCode(88,83,83))"></img>
<isindex type=image src=1 onerror=alert(0)>
<img src=x:alert(alt) onerror=eval(src) alt=0>
with(document)alert(cookie)
eval(document.referrer.slice(10));
(É=[Å=[],µ=!Å+Å][µ[È=~++Å])+(Ø+Å) [Ç=!!Å+µ,²=Ç[Å]+Ç[+!Å,Å]+²]())
[µ[Å]+µ[Å+Å]+Ç[Æ]+²](Å)
</a onmousemove="alert(1)"
data:text/html,<script>alert(0)</script>
%C0%BCscript%C0%BEalert(1)%C0%BC/script%C0%BE
<ScRIPT x src=//0x.lv?
Cross Site Scripting References

**OWASP Evasion Cheat Sheet**
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

**OWASP XSS Reference**
https://www.owasp.org/index.php/Cross-Site_Scripting

**WSC Script Mapping Project**
http://www.webappsec.org/projects/scriptmapping
Oracle E-Business Suite security vulnerabilities fixed between January 2005 and April 2016
Oracle EBS Web Vulnerabilities Fixed

~120 SQL Injection in web pages
~105 Cross Site Scripting
~35 Authorization/Authentication
~20 Business Logic Issues
OWASP Top 10 – Oracle EBS Mapping

A1: Injection
A2: Broken Authentication and Session Management
A3: Cross Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Control
A8: Cross Site Request Forgery (CRSF)
A9: Using Known Vulnerable Components
A10: Unvalidated Redirects and Forwards
Attacks
Abuse of Functionality
Brute Force
Buffer Overflow
Content Spoofing
Credential/Session Prediction
Cross-Site Scripting
Cross-Site Request Forgery
Denial of Service
Fingerprinting
Format String
HTTP Response Smuggling
HTTP Response Splitting
HTTP Request Smuggling
HTTP Request Splitting
Integer Overflows
LDAP Injection
Mail Command Injection
Null Byte Injection
OS Commanding
Path Traversal
Predictable Resource Location
Remote File Inclusion (RFI)
Routing Detour
Session Fixation
SOAP Array Abuse
SSI Injection
SQL Injection
URL Redirector Abuse
XPath Injection
XML Attribute Blowup
XML External Entities
XML Entity Expansion
XML Injection
XQuery Injection

Weaknesses
Application Misconfiguration
Directory Indexing
Improper File System Permissions
Improper Input Handling
Improper Output Handling
Information Leakage
Insecure Indexing
Insufficient Anti-automation
Insufficient Authentication
Insufficient Authorization
Insufficient Password Recovery
Insufficient Process Validation
Insufficient Session Process Validation
Insufficient Transport Layer Protection
Server Misconfiguration

http://www.webappsec.org

High Risk * Medium Risk * Low Risk * No Risk
## Oracle Product Lifetime Support Model

| Premier          | Five years from release  
<table>
<thead>
<tr>
<th></th>
<th>Security patches and Critical Patch Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extended</td>
<td>Three years additional</td>
</tr>
<tr>
<td></td>
<td>Security patches and Critical Patch Updates</td>
</tr>
<tr>
<td></td>
<td>Additional annual fee</td>
</tr>
<tr>
<td>Sustaining (desupport)</td>
<td>NO security patches</td>
</tr>
<tr>
<td></td>
<td>NO Critical Patch Updates</td>
</tr>
<tr>
<td></td>
<td>Indefinite as long as pay annual maintenance</td>
</tr>
<tr>
<td></td>
<td>Requires a minimum patch level – usually the terminal patchset or set of patches</td>
</tr>
</tbody>
</table>

# Oracle E-Business Suite Version Support

<table>
<thead>
<tr>
<th>Version</th>
<th>Premier Support End Date</th>
<th>Extended Support End Date (1)</th>
<th>CPU Support End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBS 12.2</td>
<td>September 2023</td>
<td>TBD</td>
<td>TBD</td>
</tr>
<tr>
<td>EBS 12.1</td>
<td>December 2016</td>
<td>December 2021</td>
<td>October 2021</td>
</tr>
<tr>
<td>EBS 12.0</td>
<td>January 2012</td>
<td>January 2015</td>
<td>January 2015</td>
</tr>
<tr>
<td>EBS 11.5.10</td>
<td>November 2010</td>
<td>November 2013</td>
<td>January 2016 (2, 3)</td>
</tr>
<tr>
<td>EBS 11.5.9</td>
<td>June 2008</td>
<td>N/A</td>
<td>July 2008</td>
</tr>
<tr>
<td>EBS 11.5.8</td>
<td>November 2007</td>
<td>N/A</td>
<td>October 2007</td>
</tr>
<tr>
<td>EBS 11.5.7</td>
<td>May 2007</td>
<td>N/A</td>
<td>April 2007</td>
</tr>
</tbody>
</table>

1. Extended support requires a minimum baseline patch level – see MOS Note ID 1195034.1.
2. After January 2016, CPUs are available for customers with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through January 2016 provides CPUs.
<table>
<thead>
<tr>
<th>Version</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 12.2    | - EBS 12.2.3  
          | - R12.AD.C.DELTA.7                              |
| 12.1    | - Basically 12.1.3    
          | - Application Server 10.1.3.5                    |
| 12.0    | - EBS 12.0.6    
          | - Application Server 10.1.2.3 & 10.1.3.5         
          | - Java 6                                         |
| 11.5.10 | - ATG RUP 6 or ATG RUP 7                         |

EBS Cumulative Vulnerabilities per Version

- **11.5.9** No Support
- **11.5.10** RUP 6 Required
- **11.5.10.2** Minimum Baseline Required
- **12.0.x** Desupport

Line Graph:
- Blue: 11.5.9
- Red: 11.5.10
- Green: 11.5.10.2
- Purple: 12.0.x

Graph shows cumulative vulnerabilities per version from Jan-08 to Jan-16.
Inherent Risks with Package Software

Structure and vulnerabilities within the application are well known and documented.

- An attacker knows exactly what to expect and how the application is structured
- No probing or reconnaissance of the application is required
- Fatal attack can be one URL
- Allows for easy automated attacks
<table>
<thead>
<tr>
<th>Vuln #</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-0545</td>
<td>Customer Intel</td>
<td>HTTP</td>
<td>Data Issues</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**CVSS VERSION 2.0 RISK**

<table>
<thead>
<tr>
<th>Base Score</th>
<th>Access Vector</th>
<th>Access Complexity</th>
<th>Authentication</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Last Affected Patch set (per Supported Release)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4</td>
<td>Network</td>
<td>Low</td>
<td>None</td>
<td>Partial+</td>
<td>Partial+</td>
<td>None</td>
<td>11.5.10.2 12.0.x 12.1.x 12.2.x</td>
</tr>
</tbody>
</table>

**Description:**

SQL injection in the JSP page biccfgd2.jsp allowing execution of arbitrary SQL as the APPS user.
CVE-2016-0545 Demonstration

See video at https://youtu.be/KpT-9jRk3BA
<table>
<thead>
<tr>
<th>Vuln #</th>
<th>Component</th>
<th>Protocol</th>
<th>Package and/or Privilege Required</th>
<th>Remote Exploit without Auth.?</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-0507</td>
<td>iReceivables</td>
<td>HTTP</td>
<td>AR Web Util</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### CVSS VERSION 2.0 RISK

<table>
<thead>
<tr>
<th>Base Score</th>
<th>Access Vector</th>
<th>Access Complexity</th>
<th>Authentication</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Last Affected Patch set (per Supported Release)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Network</td>
<td>Med</td>
<td>None</td>
<td>None</td>
<td>Partial</td>
<td>None</td>
<td>11.5.10.2</td>
</tr>
</tbody>
</table>

Cross-site scripting (XSS) vulnerability in a modplsql database package.
CVE-2016-0507 Demonstration

See video at https://youtu.be/KpT-9jRk3BA
## Oracle EBS Vulnerabilities – January 2016

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Oracle EBS Versions</th>
<th>Vulnerability Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2016-0525</td>
<td>11.5.10.2</td>
<td>Module: <strong>Oracle Universal Work Queue (IEU)</strong>&lt;br&gt;Sub-Component: <strong>Work Provider Administration</strong>&lt;br&gt;Type: <strong>SQL Injection</strong>&lt;br&gt;Remotely Exploitable without Authentication: <strong>Yes</strong>&lt;br&gt;CVSS Metric: <strong>6.4</strong>&lt;br&gt;URL Firewall: <strong>Blocked</strong>&lt;br&gt;A SQL injection vulnerability in a common JSP page included in 70 IEU JSP pages.</td>
</tr>
<tr>
<td>CVE-2016-0553</td>
<td>11.5.10.2</td>
<td>Module: <strong>Oracle E-Business Intelligence</strong>&lt;br&gt;Sub-Component: <strong>Definition</strong>&lt;br&gt;Type: <strong>Arbitrary File Access</strong>&lt;br&gt;Remotely Exploitable without Authentication: <strong>Yes</strong>&lt;br&gt;CVSS Metric: <strong>6.4</strong>&lt;br&gt;URL Firewall: <strong>Blocked</strong>&lt;br&gt;This vulnerability allows arbitrary read access to application server files.</td>
</tr>
</tbody>
</table>
An XML External Entity (XXE) injection vulnerability in a Configurator servlet. An attacker can pass an entity definition which will be processed by the XML parser. This entity definition may point to an external server, local file, etc. The primary attack vector in an Oracle EBS environment is the ability to access URLs external to the application, which appear to be from the Oracle EBS application server. May be possible to read arbitrary files from the application server.

This servlet is allowed in the URL Firewall section “IBE (iStore) with CZ”.
## Oracle EBS Vulnerabilities – January 2016

<table>
<thead>
<tr>
<th>CVE ID</th>
<th>Oracle EBS Versions</th>
<th>Vulnerability Information</th>
</tr>
</thead>
</table>
| CVE-2016-0532| 11.5.10.2 12.0.1-12.0.6 12.1.1-12.1.3 12.2.3-12.2.4 | Module: Oracle **CRM Technical Foundation**  
Sub-Component: **Security Assignments**  
Type: **Unauthorized Access to Data**  
Remotely Exploitable without Authentication: **Yes**  
CVSS Metric: **6.4**  
URL Firewall: **Blocked**  
A vulnerability in CRM Technical Foundations that allows an unauthenticated user access to view and potentially change application security authorizations. |
Agenda

1. Oracle EBS
2. Web Application Security
3. Vulnerabilities Examined
4. Oracle EBS DMZ Implementation
5. Q&A
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided Metalink Note must be followed.

**380490.1** Oracle E-Business Suite R12 Configuration in a DMZ

**287176.1** DMZ Configuration with Oracle E-Business Suite 11i
**EBS DMZ Architecture**

External Users (supplier)

1. **Firewall (existing)**
   - A
   - HTTPS/SSL
   - SSL
   - https://supplier.example.com

2. **Reverse Proxy**
   - B
   - Firewall (optional)
   - 443 SSL
   - 8000 HTTP

3. **EBS External App Server**
   - C
   - 1521 SQL*Net

Internal Users

4. **Firewall (existing)**
   - C
   - 8000

5. **EBS Database Server**
   - 1521 SQL*Net

6. **EBS Internal App Server**

---

**A** HTTPS/SSL should always be used otherwise passwords and data are sent in the clear.

**B** A reverse proxy server should be implemented such as Apache, Blue Coat, or F5 BIG-IP.

**C** Firewall between layers block access between layers except for explicitly defined ports.
Proper DMZ configuration reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.
URL Firewall in Appendix E is absolutely mandatory. Configure using `url-fw.conf`.

A whitelist of allowed JSP pages and servlets. Allows all OA Framework pages.
Step 5.2 is set the **NODE_TRUST_LEVEL** to **EXTERNAL** for the external application server.

Step 5.3 **limits the responsibilities** accessible via the external application server.
Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.
Oracle EBS DMZ Certified Modules (R12)

Oracle only certifies a limited set of modules for use in a DMZ

- Meets DMZ architectural requirements (i.e., no forms)
- URL Firewall rules provided for the module

<table>
<thead>
<tr>
<th>iSupplier Portal (POS)</th>
<th>Oracle Transportation (FTE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Sourcing (PON)</td>
<td>Oracle Contracts Core (OKC)</td>
</tr>
<tr>
<td>Oracle Receivables (OIR)</td>
<td>Oracle Service Contracts (OKS)</td>
</tr>
<tr>
<td>iRecruitment (IRC)</td>
<td>Oracle Collaborative Planning (SCE)</td>
</tr>
<tr>
<td>Oracle Time and Labor (OTL)</td>
<td>Oracle User Management (UMX)</td>
</tr>
<tr>
<td>Oracle Learning Management (OTA)</td>
<td>Order Information Portal (ONT)</td>
</tr>
<tr>
<td>Self Service Benefits (BEN)</td>
<td>Oracle Sales for Handhelds (ASP)</td>
</tr>
<tr>
<td>Self Service Human Resources (SSHR)</td>
<td>Oracle Internet Expenses (OIE)</td>
</tr>
<tr>
<td>Oracle iSupport (IBU)</td>
<td>Oracle Performance Management (OPM)</td>
</tr>
<tr>
<td>Oracle iStore (IBE)</td>
<td>Compensation Workbench (CWB)</td>
</tr>
<tr>
<td>Oracle Marketing (AMS)</td>
<td>Oracle Payroll (PAY)</td>
</tr>
<tr>
<td>Oracle Partner Relationship Mgmt (PRM)</td>
<td>Oracle Quoting (QOT)</td>
</tr>
<tr>
<td>Oracle Survey (IES)</td>
<td>Oracle Field Service 3rd Party Portal (FSE)</td>
</tr>
</tbody>
</table>
Virtual Patching

“Eliminate risk and exploitation of the security bug by blocking access to the vulnerable code”

1. Write your own rules
   - Web Application Firewall (WAF)
   - Oracle E-Business Suite modsecurity

2. AppDefend
   - Integrigy analyzes the Critical Patch Update (CPU)
   - Delivers pre-defined rules for all CPU web bugs
Integrigy AppDefend for Oracle EBS

AppDefend is an enterprise application firewall designed and optimized for the Oracle E-Business Suite.

- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and Oracle EBS security risks

- **Virtual Patching**
  Detects and blocks known Oracle EBS security vulnerabilities

- **Limits EBS Modules**
  More flexibility and capabilities than URL firewall to identify EBS modules

- **Application Logging**
  Enhanced application logging for compliance requirements like PCI-DSS 10.2
Agenda

1. Oracle EBS
2. Web Application Security
3. Oracle EBS DMZ Implementation
4. Vulnerabilities Examined
5. Q&A
Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web: www.integrigy.com
e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog
youtube: youtube.com/integrigy