INTEGRIGY

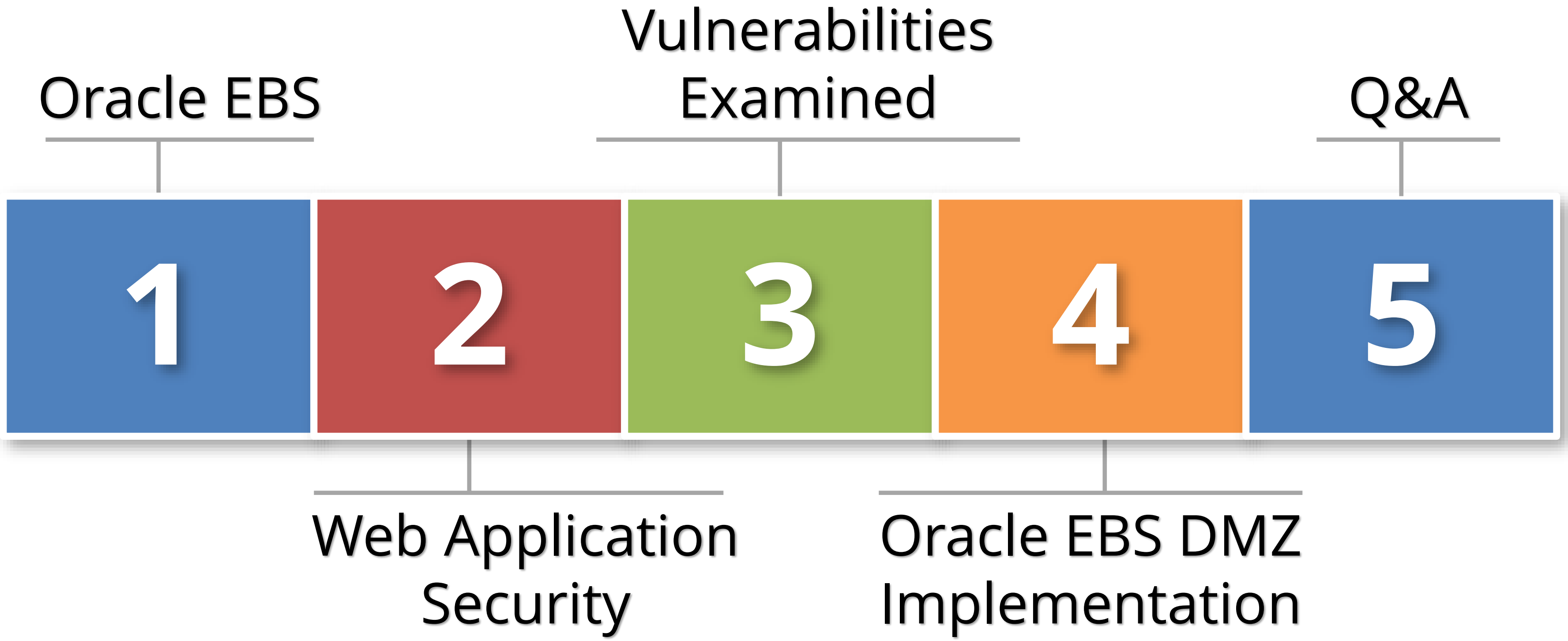
Oracle E-Business Suite
Web Security Vulnerabilities Examined

June 22, 2016

Stephen Kost
Chief Technology Officer
Integrigy Corporation

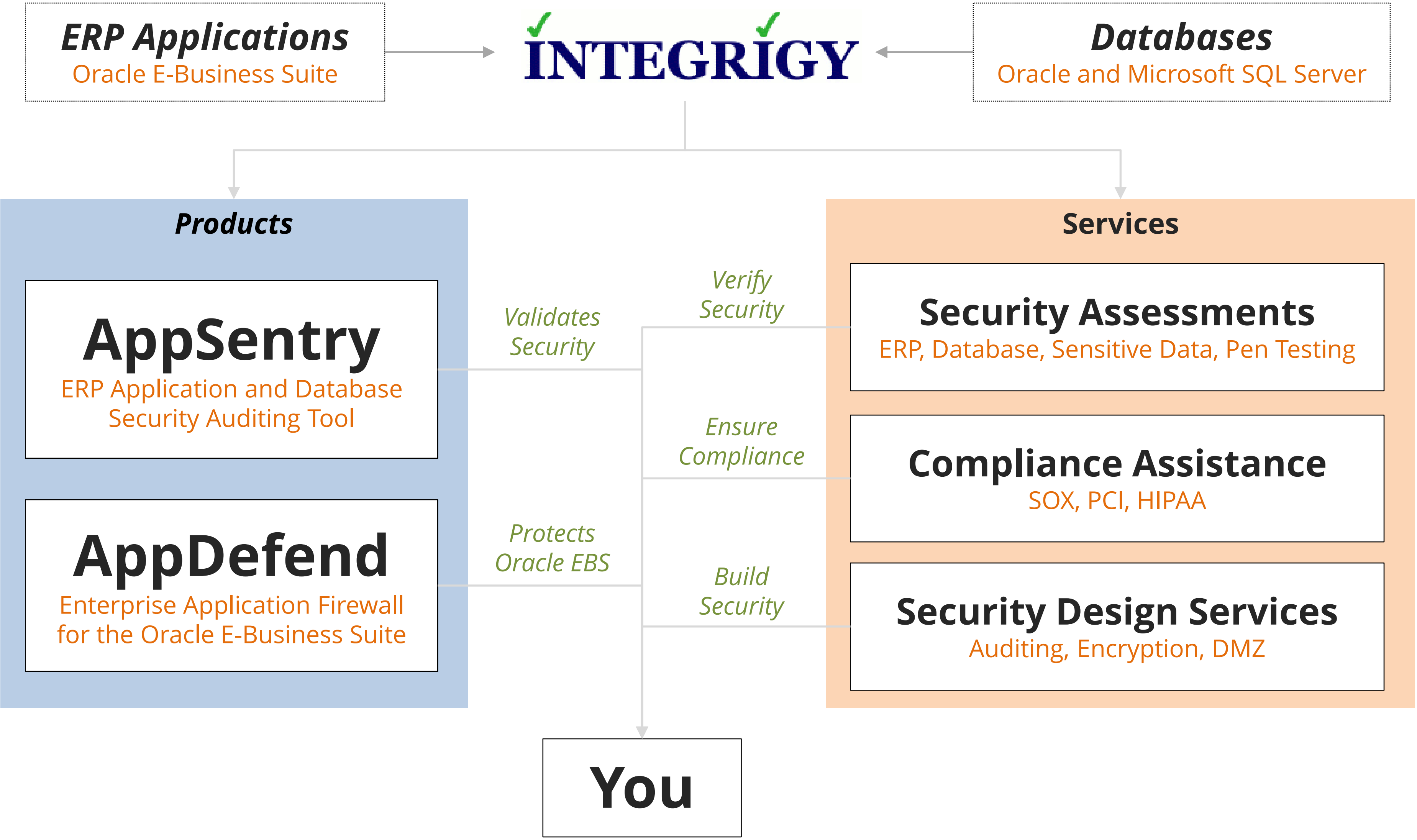
Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



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

About Integrigy



ERP Applications
Oracle E-Business Suite

INTEGRIGY

Databases
Oracle and Microsoft SQL Server

Products

AppSentry
ERP Application and Database Security Auditing Tool

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Services

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

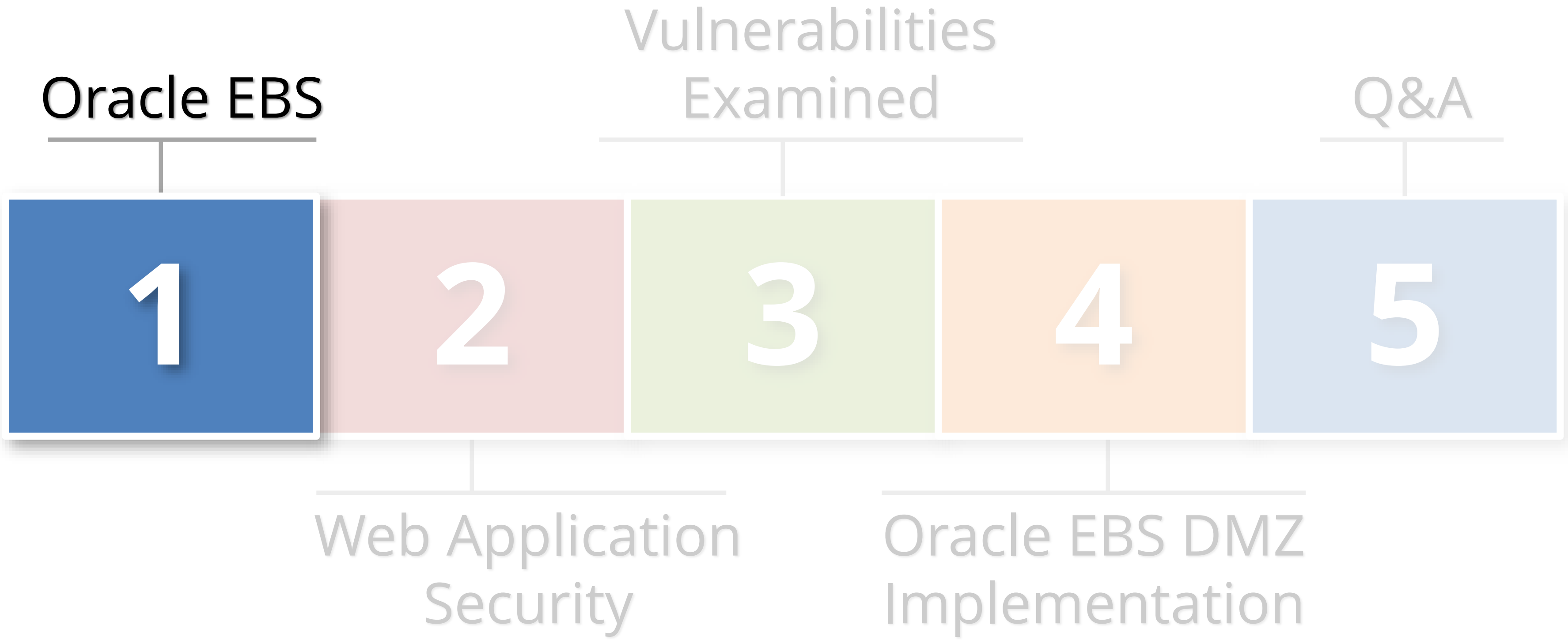
Verify Security

Ensure Compliance

Build Security

You

Agenda



1 Oracle EBS

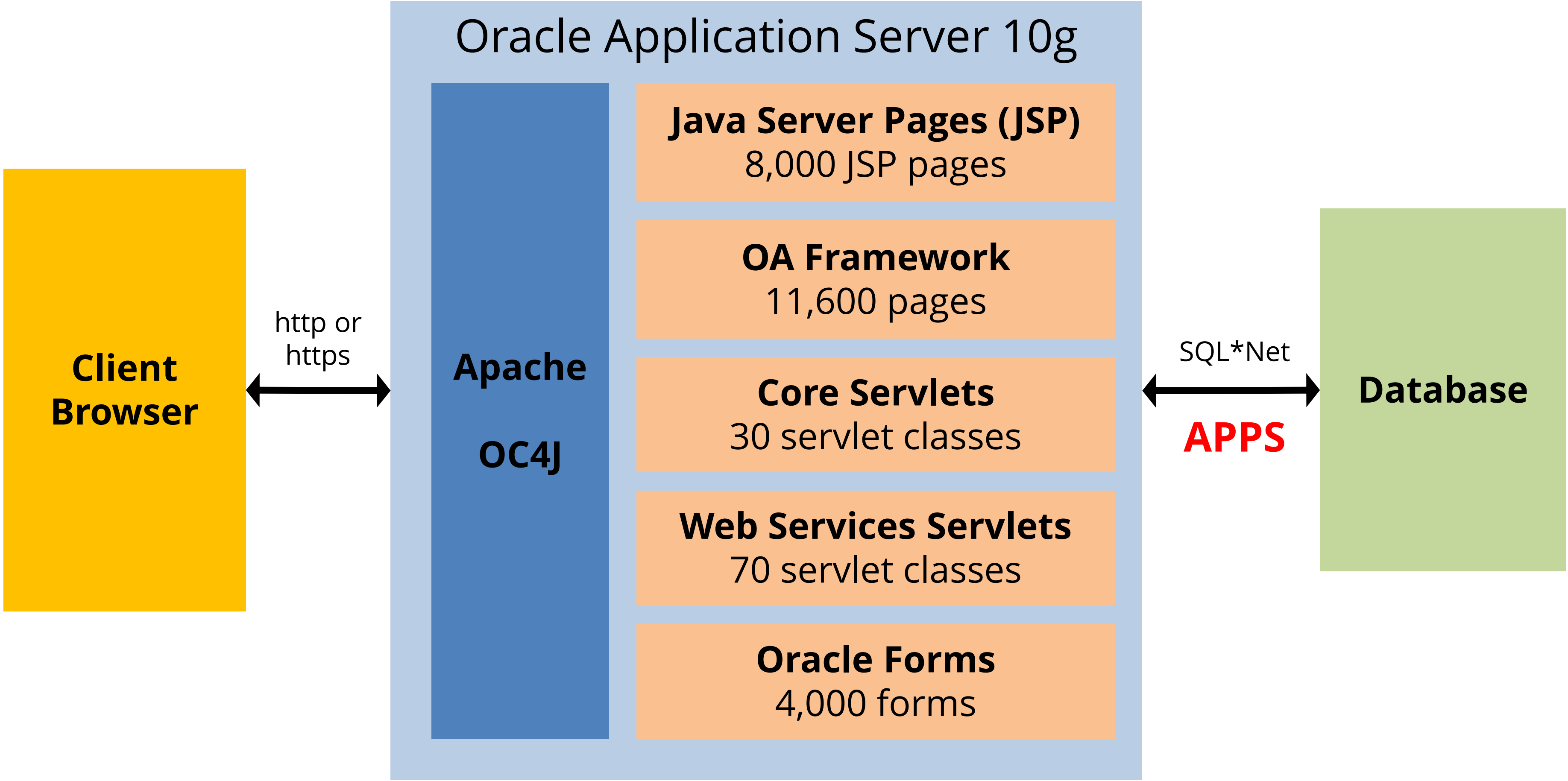
2 Web Application Security

3 Vulnerabilities Examined

4 Oracle EBS DMZ Implementation

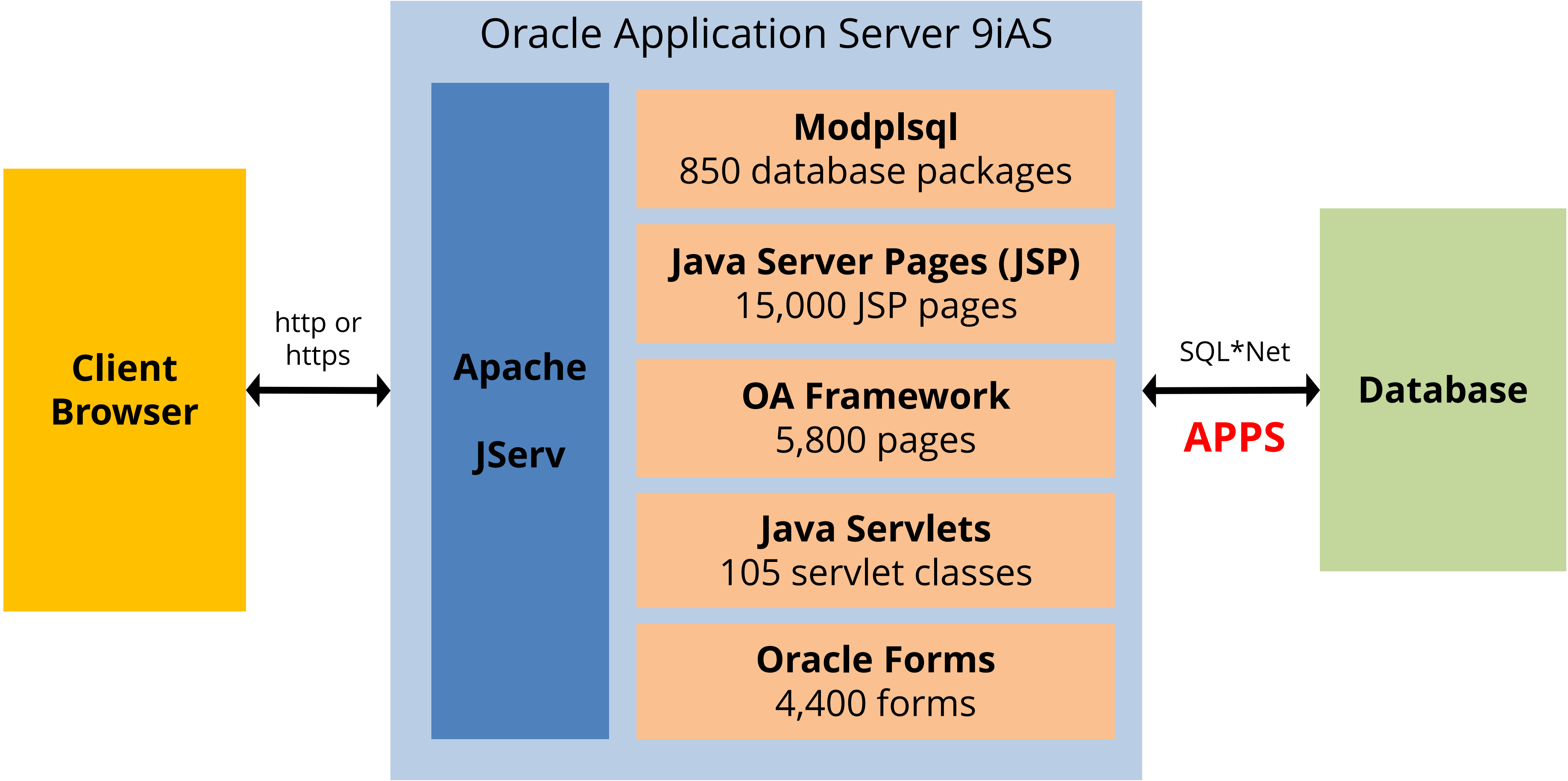
5 Q&A

Oracle EBS R12 Web Footprint



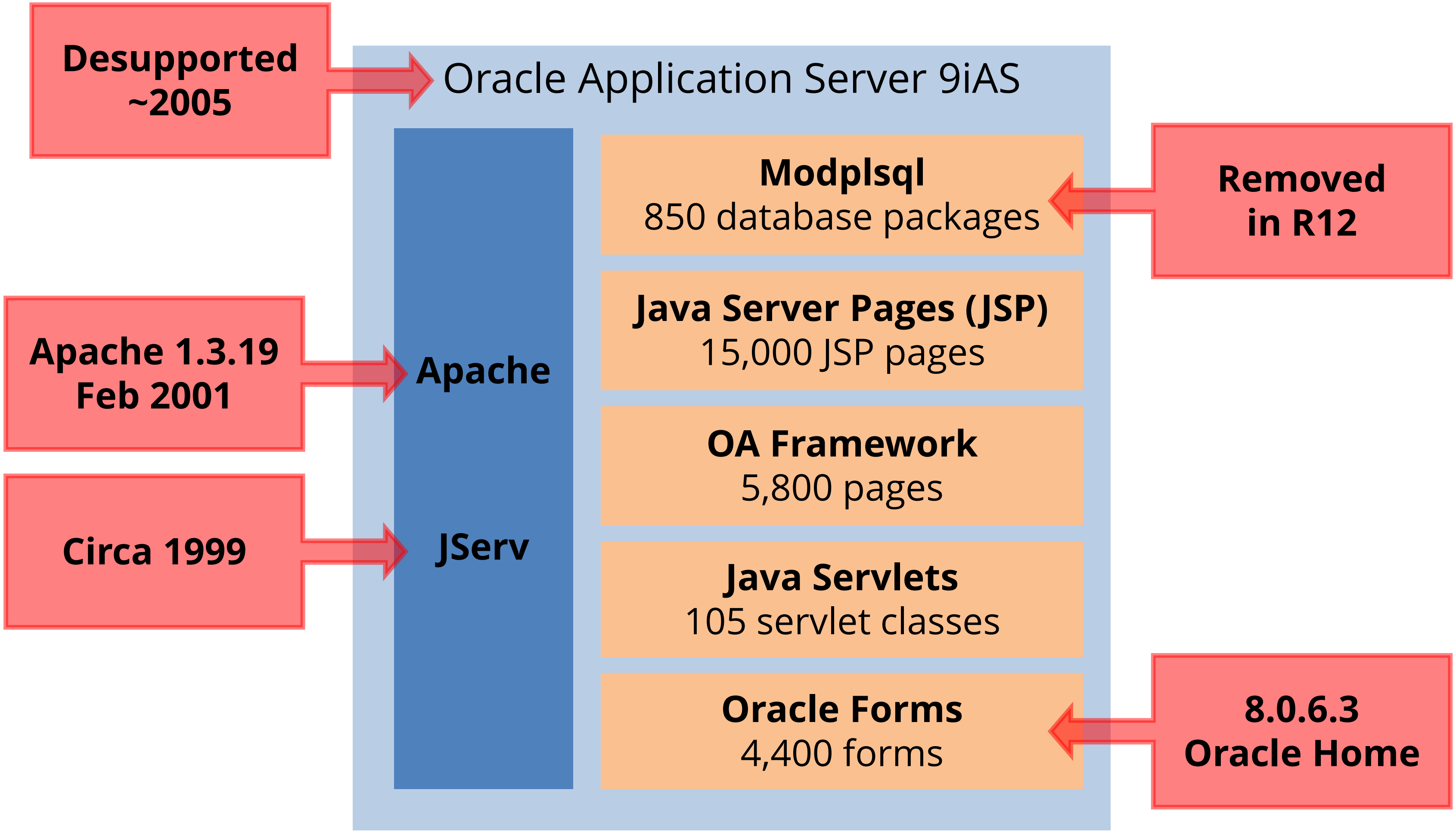
- Oracle EBS installs all modules (250+) and **all web pages** for every application server
- All web pages access the database using the **APPS** database account

Oracle EBS 11i Web Footprint



- 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 11i Web Footprint



Desupported ~2005

Oracle Application Server 9iAS

Apache

JServ

Modplsql
850 database packages

Java Server Pages (JSP)
15,000 JSP pages

OA Framework
5,800 pages

Java Servlets
105 servlet classes

Oracle Forms
4,400 forms

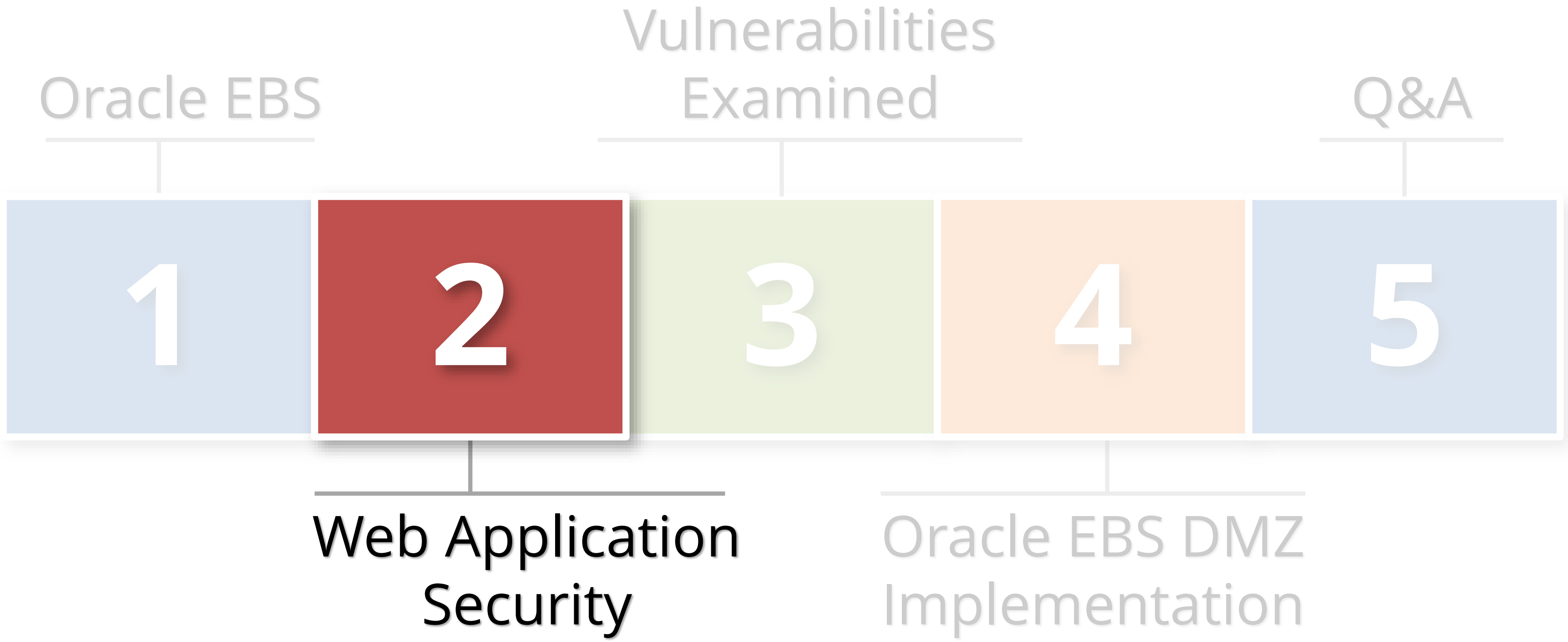
Removed in R12

Apache 1.3.19 Feb 2001

Circa 1999

8.0.6.3 Oracle Home

Agenda



Oracle EBS

Vulnerabilities Examined

Q&A

1

2

3

4

5

Web Application Security

Oracle EBS DMZ Implementation

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
- A8: 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

OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

WASC Threat Classification v2.0

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

SQL Injection Explained

Attacker modifies URL with extra SQL

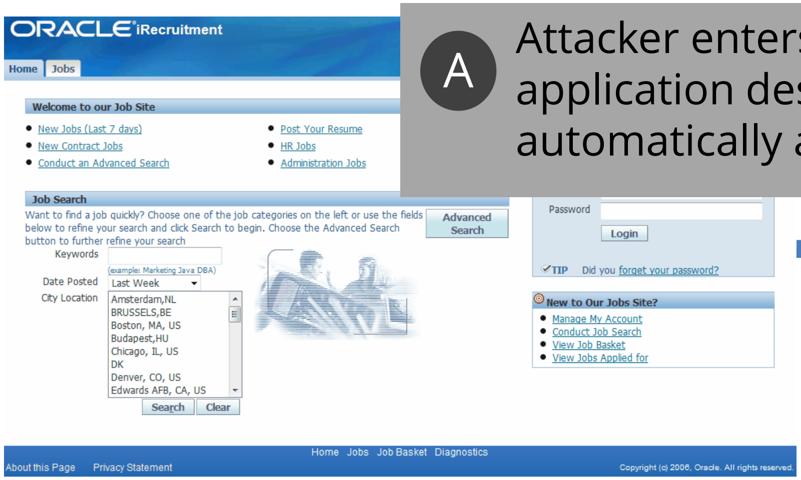
```
http://<server>/pls/VIS/fnd_gfm.dispatch?
p_path=fnd_help.get/US/fnd/@search');%20
fnd_user_pkg.updateUser('operations',%20'
SEED',%20'welcome1
```

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



ORACLE iRecruitment

Home | Jobs

Welcome to our Job Site

- New Jobs (Last 7 days)
- New Contract Jobs
- Conduct an Advanced Search
- Post Your Resume
- HR Jobs
- Administration Jobs

Job Search

Want to find a job quickly? Choose one of the job categories on the left or use the fields below to refine your search and click Search to begin. Choose the Advanced Search button to further refine your search

Advanced Search

Keywords
(example: Marketing Java DBA)

Date Posted: Last Week

City Location: Amsterdam,NL
BRUSSELS,BE
Boston, MA, US
Budapest,HU
Chicago, IL, US
DK
Denver, CO, US
Edwards AFB, CA, US

Search | Clear

Password

Login

✓TIP Did you forget your password?

New to Our Jobs Site?

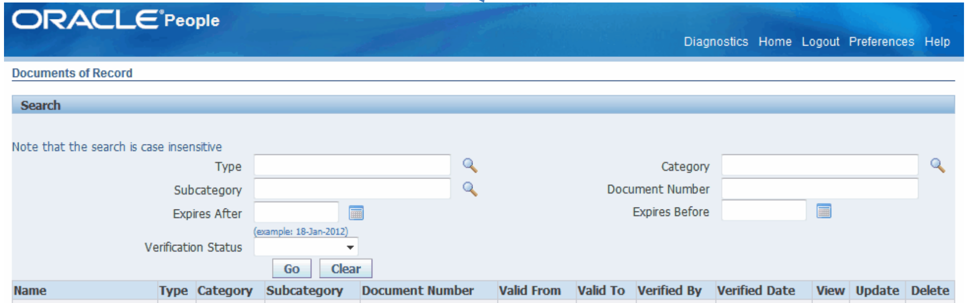
- Manage My Account
- Conduct Job Search
- View Job Basket
- View Jobs Applied for

Home Jobs Job Basket Diagnostics

About this Page Privacy Statement

Copyright (c) 2006, Oracle. All rights reserved.

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



ORACLE People

Diagnostics Home Logout Preferences Help

Documents of Record

Search

Note that the search is case insensitive

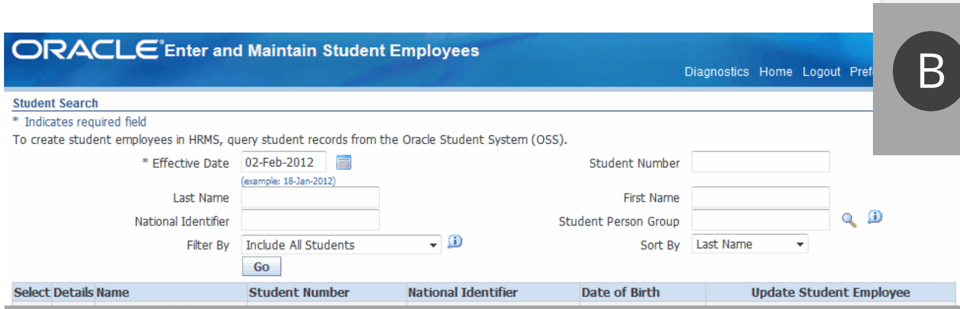
Type
Subcategory
Expires After
(example: 18-Jan-2012)
Verification Status

Category
Document Number
Expires Before

Go | Clear

Name	Type	Category	Subcategory	Document Number	Valid From	Valid To	Verified By	Verified Date	View	Update	Delete

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



ORACLE Enter and Maintain Student Employees

Diagnostics Home Logout Pref

Student Search

* Indicates required field

To create student employees in HRMS, query student records from the Oracle Student System (OSS).

* Effective Date: 02-Feb-2012
(example: 18-Jan-2012)

Last Name

National Identifier

Filter By: Include All Students

Go

Student Number

First Name

Student Person Group

Sort By: Last Name

Select	Details	Name	Student Number	National Identifier	Date of Birth	Update Student Employee

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]+({}+Å) [Ç=!!Å+µ,ª=Ç[Å]+Ç[+!Å],Å]+ª])()
[µ[Å]+µ[Å+Å]+Ç[È]+ª](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 EBS Security Vulnerabilities

Oracle E-Business Suite security vulnerabilities fixed between January 2005 and April 2016

416

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
- 🟥 A8: 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

🟥 High Risk

🟧 Medium Risk

🟩 Low Risk

OWASP
The Open Web Application Security Project
http://www.owasp.org

WASC TC – Oracle EBS Mapping

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

High Risk * Medium Risk * Low Risk * No Risk

Oracle Product Lifetime Support Model

Premier	▪ Five years from release ▪ Security patches and Critical Patch Updates
Extended	▪ Three years additional ▪ Security patches and Critical Patch Updates ▪ Additional annual fee
Sustaining (desupport)	▪ **NO security patches** ▪ **NO Critical Patch Updates** ▪ Indefinite as long as pay annual maintenance ▪ Requires a minimum patch level – usually the terminal patchset or set of patches

Source: http://www.oracle.com/us/support/lifetime-support/index.html

Oracle E-Business Suite Version Support

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

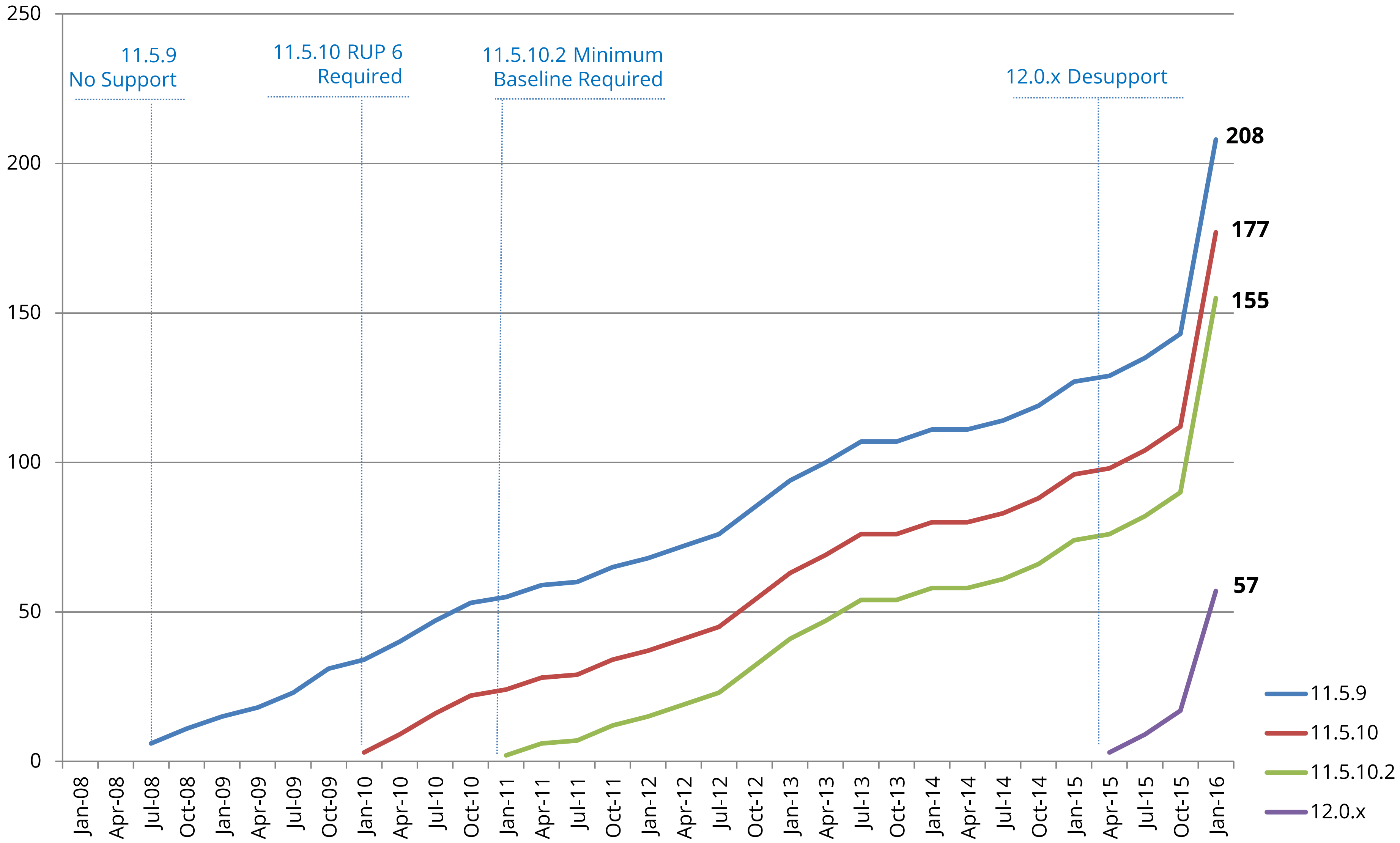
1. Extended support requires a minimum baseline patch level – see MOS Note ID 1195034.1.
2. After January 2016, CPUs are available for customers with Advanced Support Contracts.
3. 11.5.10 Sustaining support exception through January 2016 provides CPUs.

Oracle EBS Extended Support Requirements

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

Source: MOS Note ID 1195034.1 - Oracle E-Business Suite Error Correction Support Policy (V.5 – January 2015)

EBS Cumulative Vulnerabilities per Version

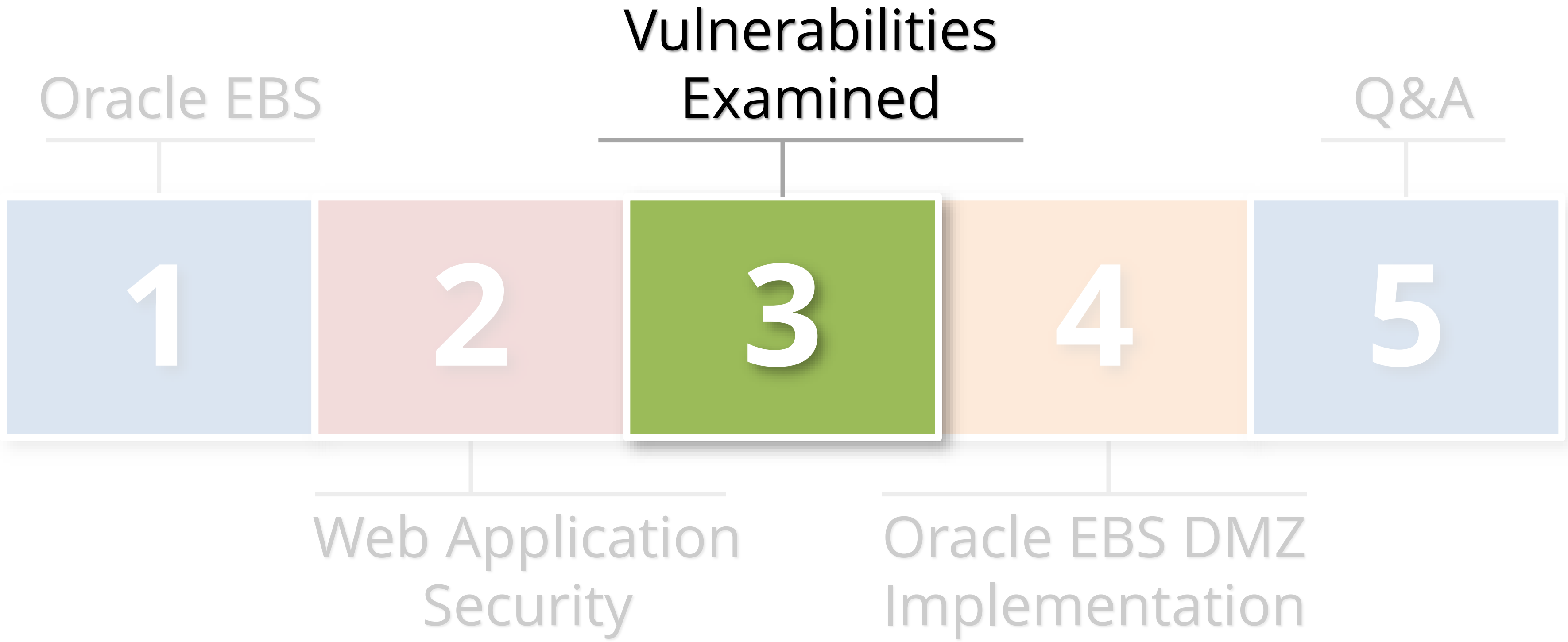


Inherent Risks with Package Software

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

Agenda



1 Oracle EBS

2 Web Application Security

3 Vulnerabilities Examined

4 Oracle EBS DMZ Implementation

5 Q&A

Oracle EBS SQL Injection – January 2016

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2016-0545	**Customer Intel**	**HTTP**	**Data Issues**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
6.4	**Network**	**Low**	**None**	**Partial+**	**Partial+**	**None**	**11.5.10.2** **12.0.x** **12.1.x** **12.2.x**

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

Oracle EBS XSS – January 2016

Vuln #	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?
CVE-2016-0507	**iReceivables**	**HTTP**	**AR Web Util**	**Yes**

CVSS VERSION 2.0 RISK							Last Affected Patch set (per Supported Release)
Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability	
4.3	**Network**	**Med**	**None**	**None**	**Partial**	**None**	**11.5.10.2**

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

CVE ID	Oracle EBS Versions	Vulnerability Information
CVE-2016-0525	11.5.10.2 12.0.1-12.0.6 12.1.1-12.1.3	Module: **Oracle Universal Work Queue (IEU)** Sub-Component: **Work Provider Administration** Type: **SQL Injection** Remotely Exploitable without Authentication: **Yes** CVSS Metric: **6.4** URL Firewall: **Blocked** A SQL injection vulnerability in a common JSP page included in 70 IEU JSP pages.
CVE-2016-0553	11.5.10.2 12.0.1-12.0.6 12.1.1-12.1.3	Module: **Oracle E-Business Intelligence** Sub-Component: **Definition** Type: **Arbitrary File Access** Remotely Exploitable without Authentication: **Yes** CVSS Metric: **6.4** URL Firewall: **Blocked** This vulnerability allows arbitrary read access to application server files.

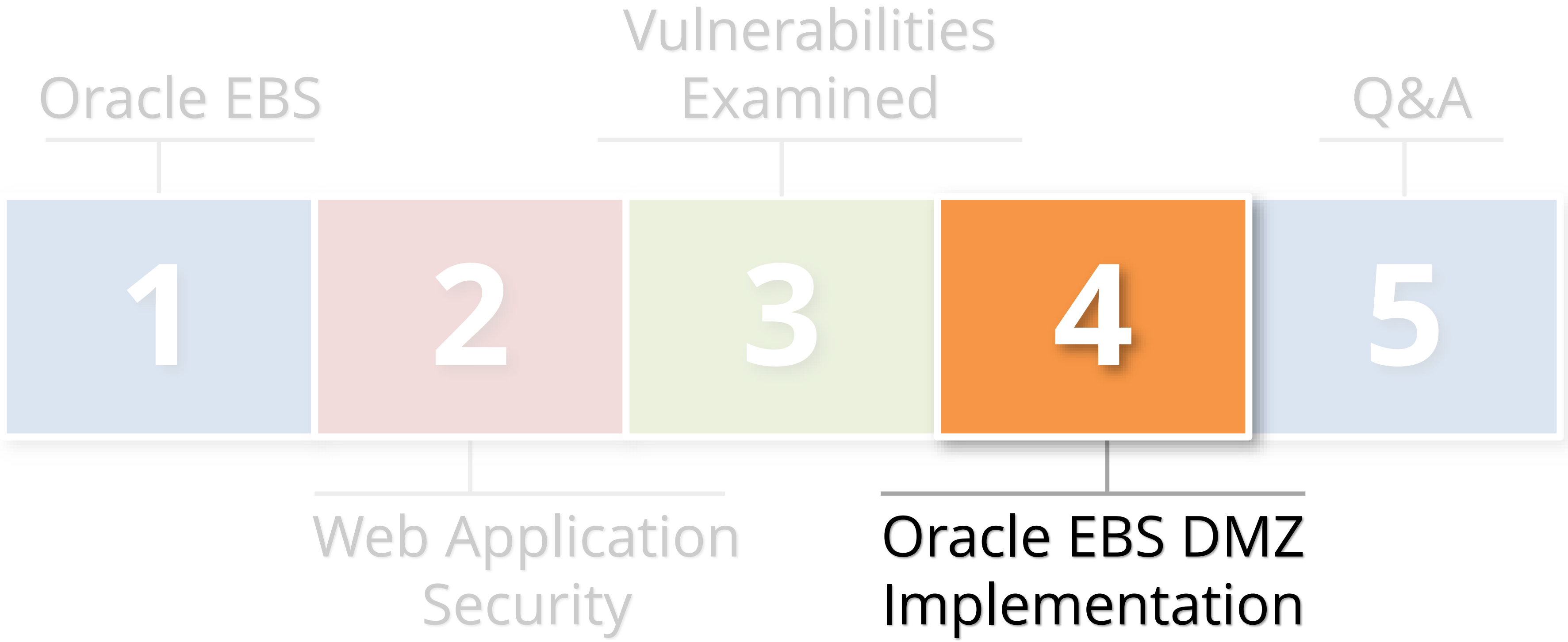
Oracle EBS Vulnerabilities – January 2016

CVE ID	Oracle EBS Versions	Vulnerability Information
CVE-2016-0541	11.5.10.2 12.0.1-12.0.6 12.1.1-12.1.3 12.2.3-12.2.5	Module: **Oracle Configurator** Sub-Component: **UI Servlet** Type: **XML External Entity (XXE)** Remotely Exploitable without Authentication: **Yes** CVSS Metric: **5.0** URL Firewall: **ALLOWED ("IBE (iStore) with CZ")** An XML External Entity (XEE) 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

CVE ID	Oracle EBS Versions	Vulnerability Information
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

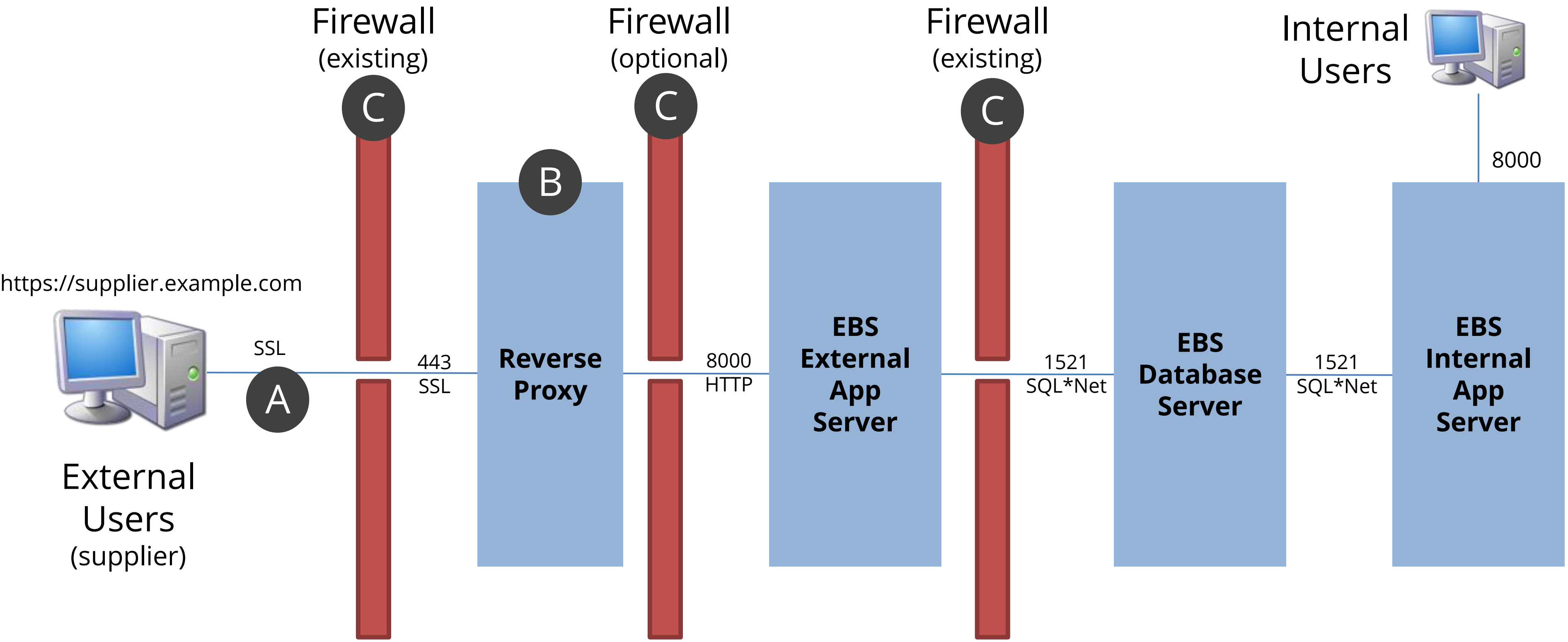
Oracle EBS DMZ Metalink Notes

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

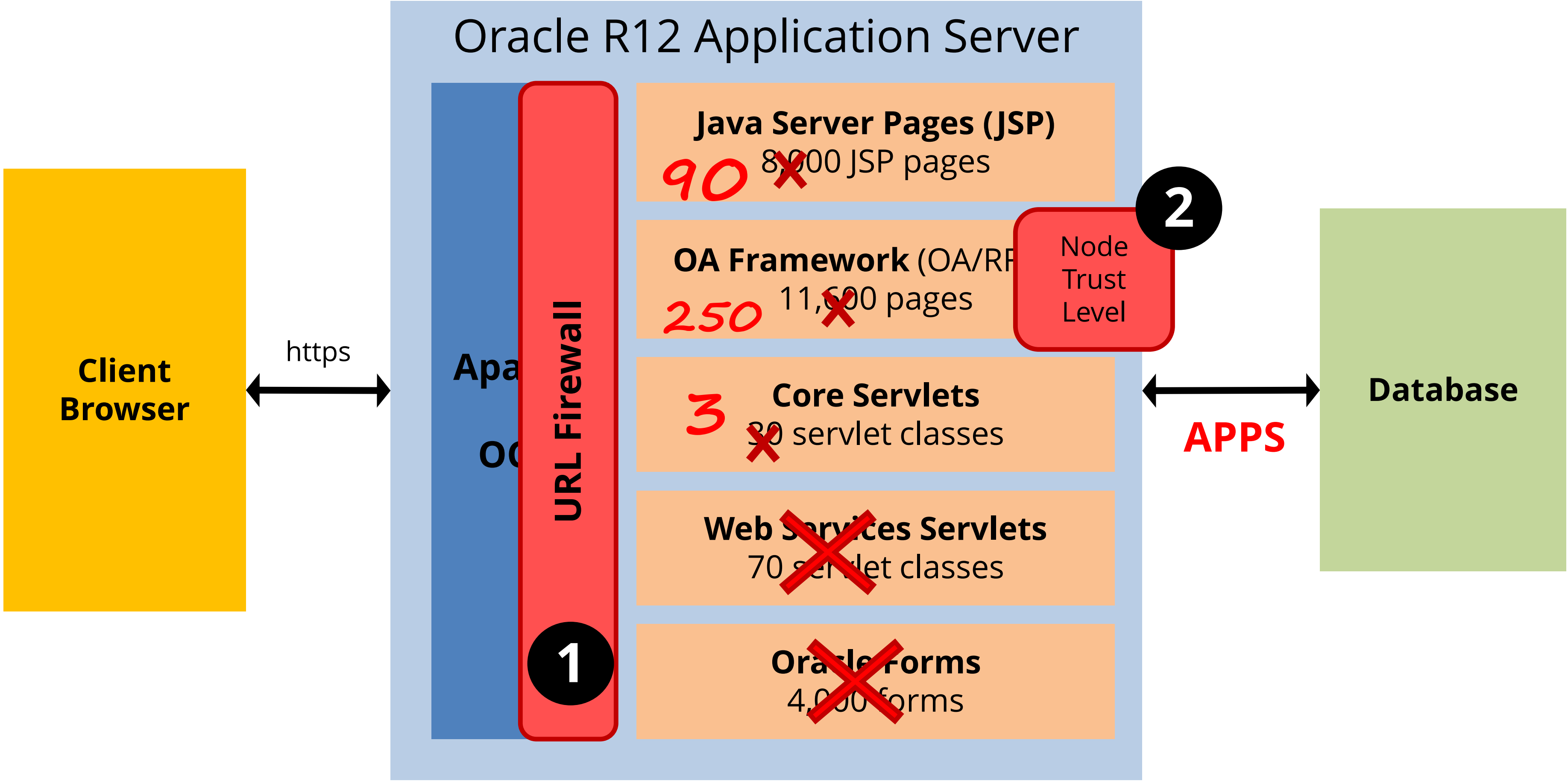


A **HTTPS/SSL** should always be used otherwise passwords and data are sent in the clear.

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

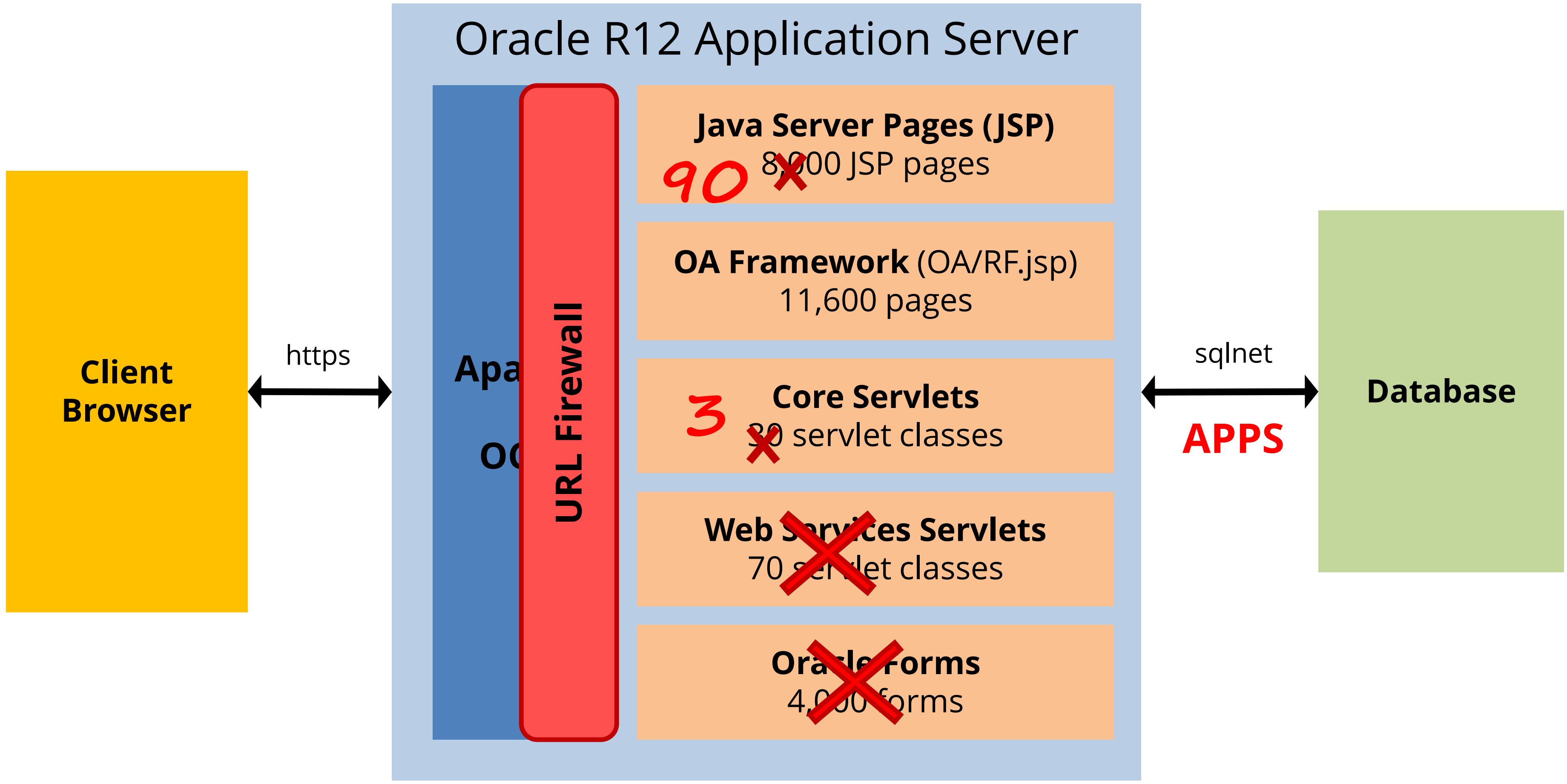
C Firewall between layers block access between layers except for explicitly defined ports.

Oracle EBS DMZ Configuration



- 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.

DMZ Step Appendix E – URL Firewall



Oracle R12 Application Server

Client Browser

https

Apa

OC

URL Firewall

Java Server Pages (JSP)
90 ~~8,000~~ JSP pages

OA Framework (OA/RF.jsp)
11,600 pages

Core Servlets
3 ~~30~~ servlet classes

~~**Web Services Servlets**~~
~~70 servlet classes~~

~~**Oracle Forms**~~
~~4,000 forms~~

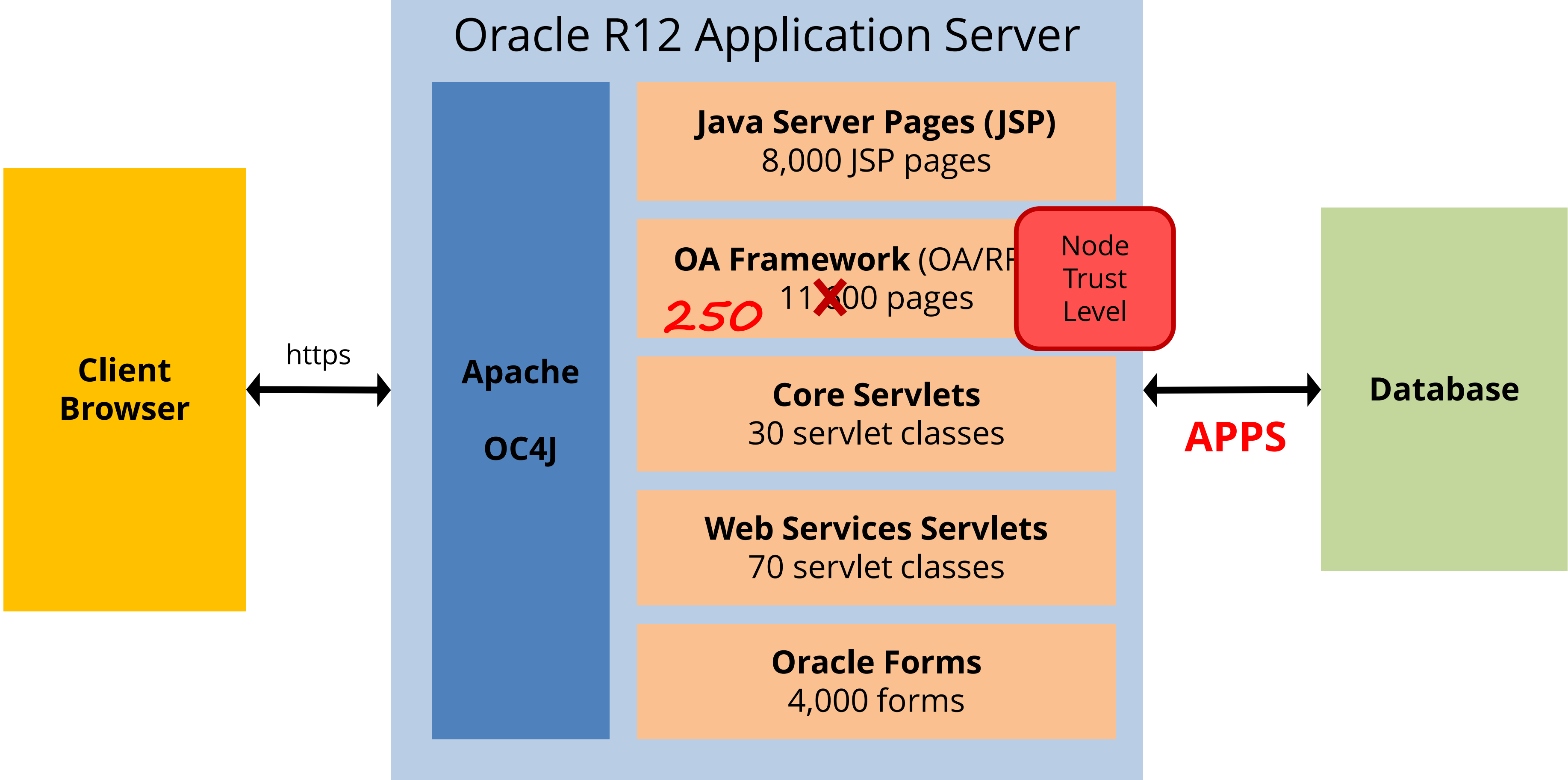
sqlnet

APPS

Database

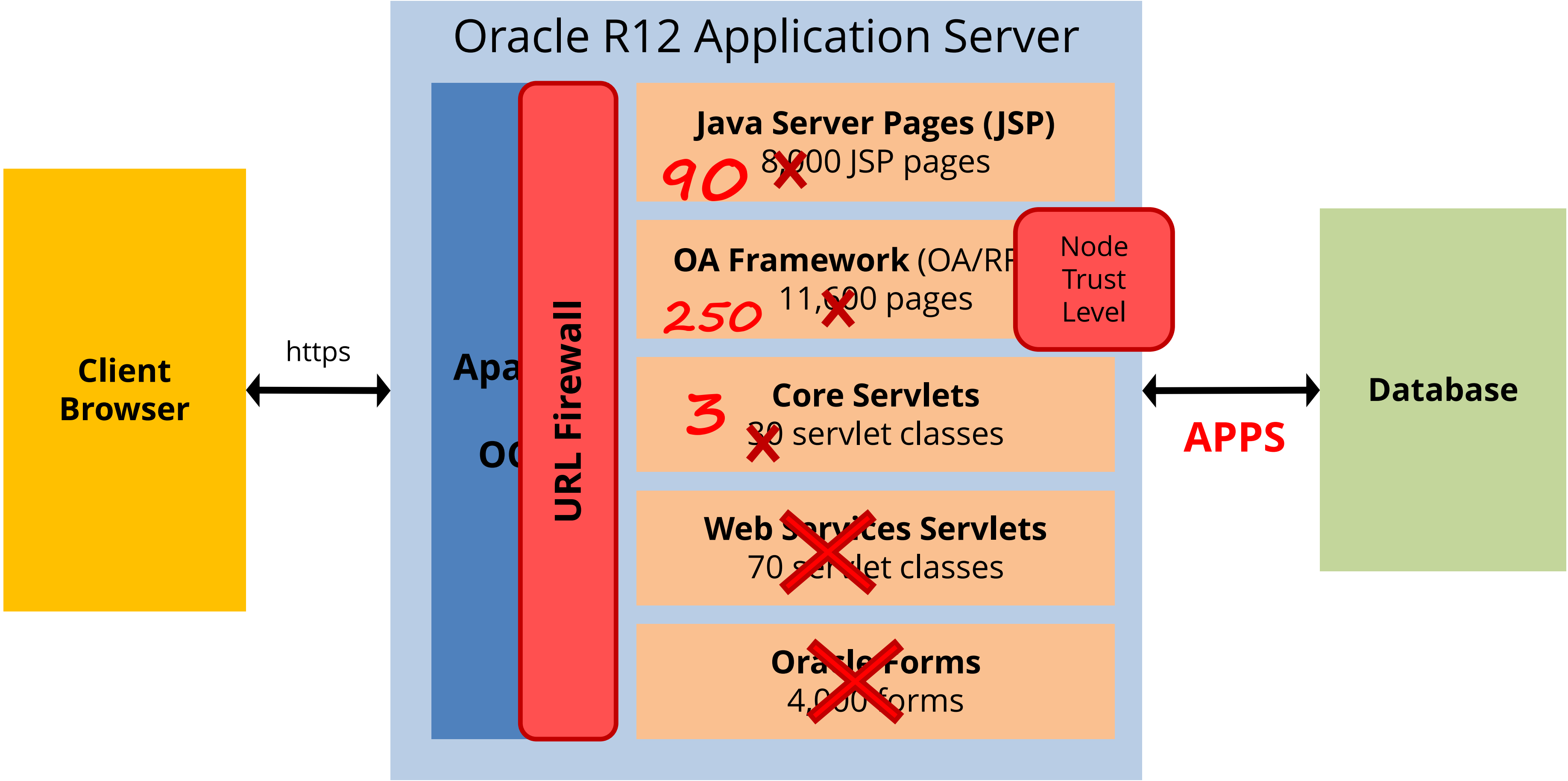
- **URL Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw.conf**.
- A **whitelist** of allowed JSP pages and servlets. Allows all OA Framework pages.

DMZ Steps 5.2 & 5.3 – Responsibilities



- 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.

DMZ Configuration



- 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

iSupplier Portal (POS)
Oracle Sourcing (PON)
Oracle Receivables (OIR)
iRecruitment (IRC)
Oracle Time and Labor (OTL)
Oracle Learning Management (OTA)
Self Service Benefits (BEN)
Self Service Human Resources (SSHR)
Oracle iSupport (IBU)
Oracle iStore (IBE)
Oracle Marketing (AMS)
Oracle Partner Relationship Mgmt (PRM)
Oracle Survey (IES)

Oracle Transportation (FTE)
Oracle Contracts Core (OKC)
Oracle Service Contracts (OKS)
Oracle Collaborative Planning (SCE)
Oracle User Management (UMX)
Order Information Portal (ONT)
Oracle Sales for Handhelds (ASP)
Oracle Internet Expenses (OIE)
Oracle Performance Management (OPM)
Compensation Workbench (CWB)
Oracle Payroll (PAY)
Oracle Quoting (QOT)
Oracle Field Service 3rd Party Portal (FSE)

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.

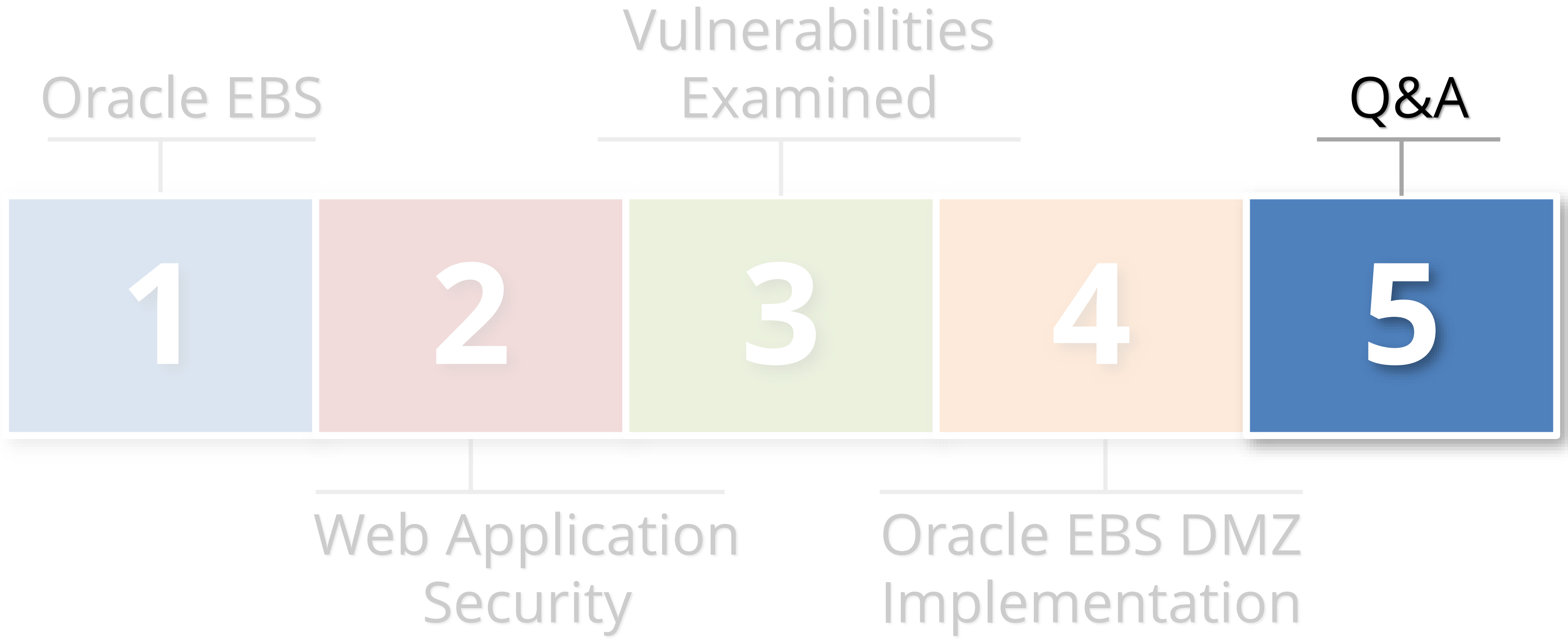
- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and Oracle EBS security risks

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

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

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

Agenda


1 Oracle EBS

2 Web Application Security

3 Vulnerabilities Examined

4 Oracle EBS DMZ Implementation

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**