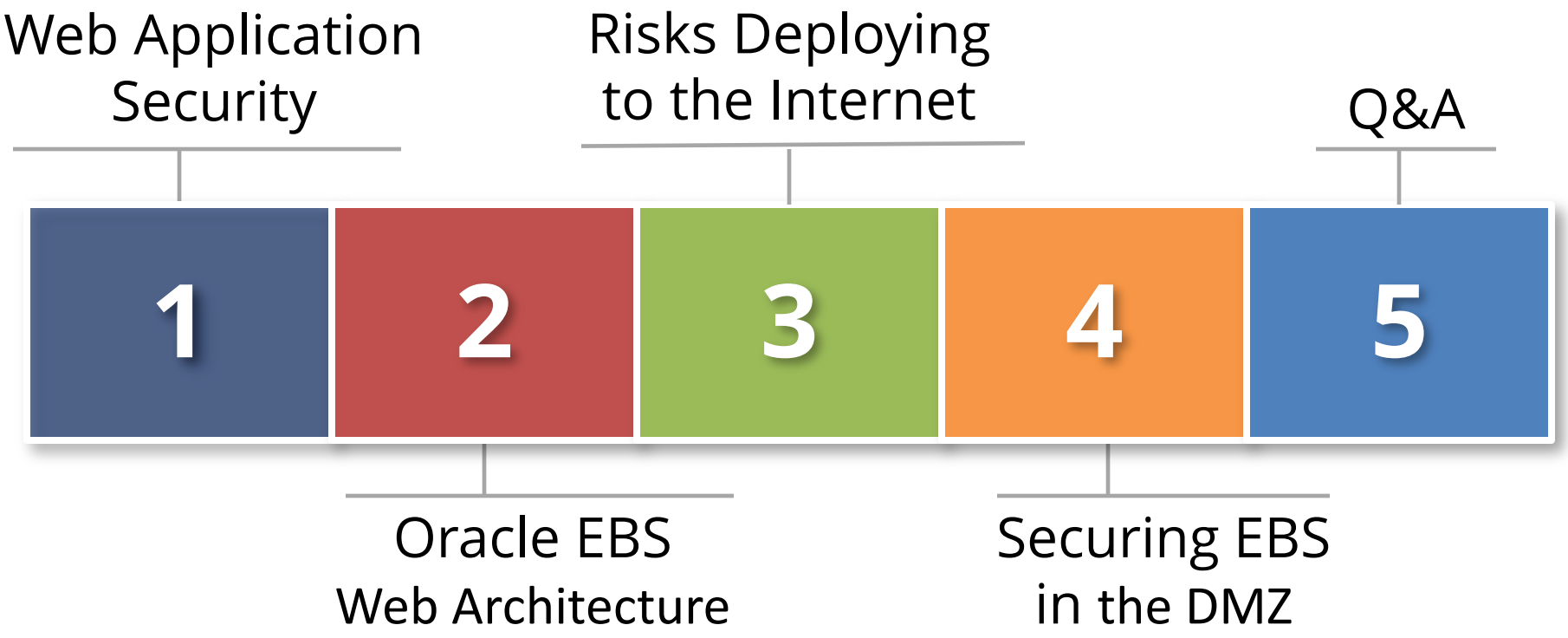
Into the Fire -
Deploying Oracle EBS to the Internet

February 2, 2012

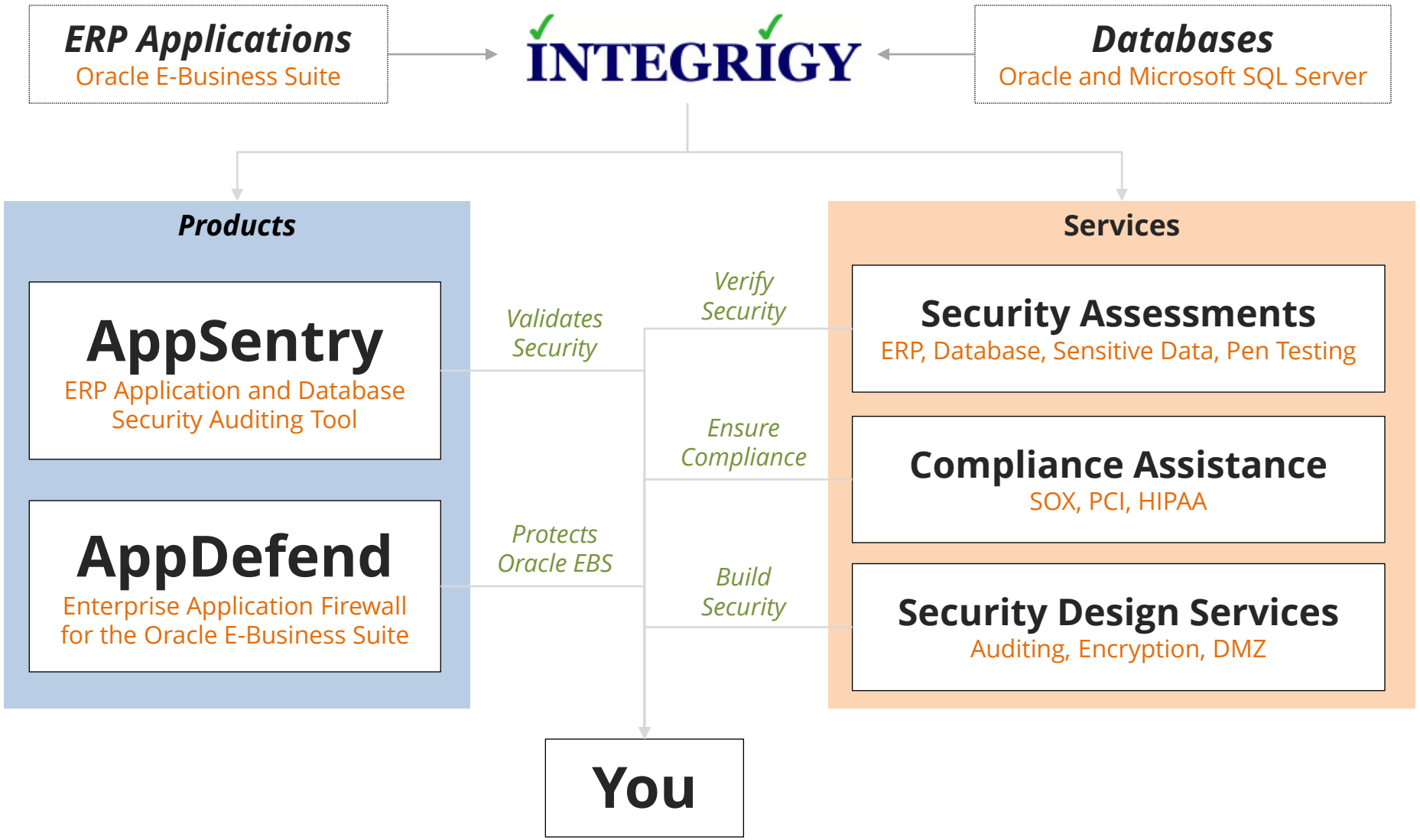
Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda


Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS in the DMZ

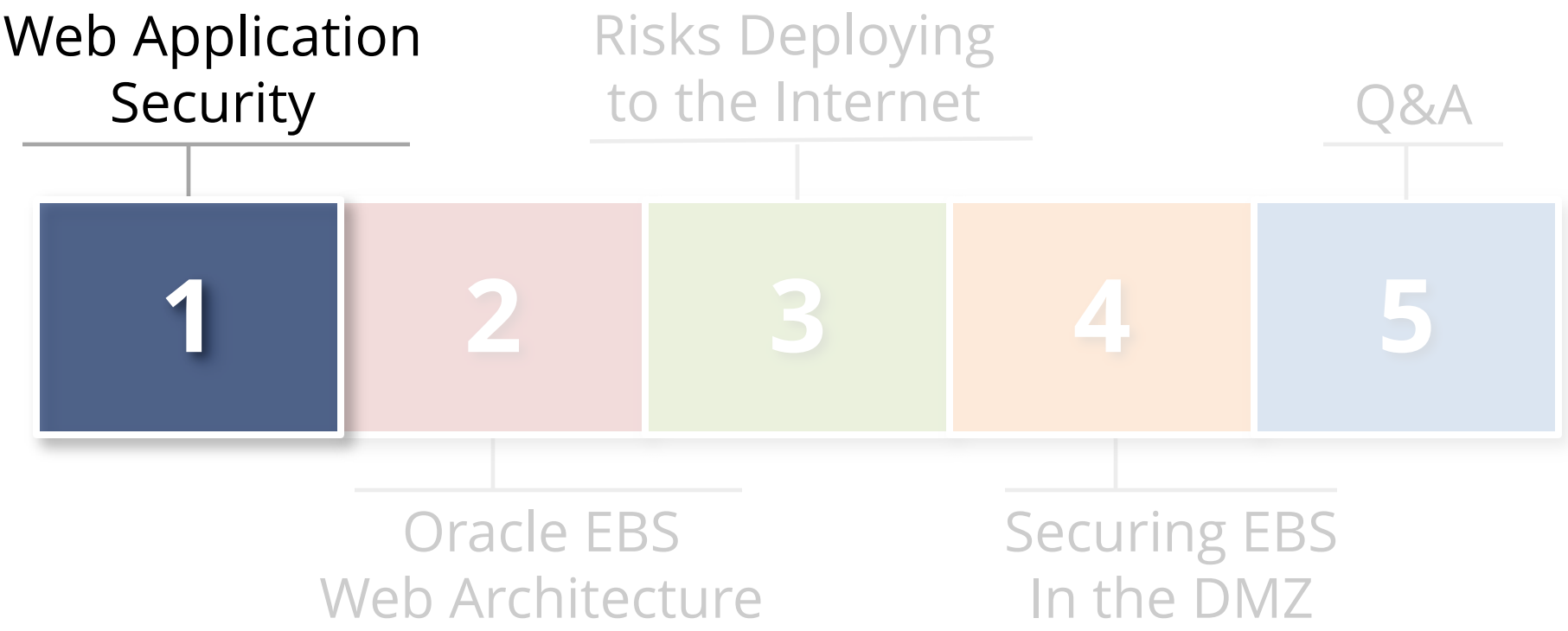
About Integrigy



Integrigy Published Security Alerts

Security Alert	Versions	Security Vulnerabilities
Critical Patch Update July 2011	11.5.10 – 12.1.x	▪ Oracle E-Business Suite security configuration issue
Critical Patch Update October 2010	11.5.10 – 12.1.x	▪ 2 Oracle E-Business Suite security weaknesses
Critical Patch Update July 2008	Oracle 11g 11.5.8 – 12.0.x	▪ 2 Issues in Oracle RDBMS Authentication ▪ 2 Oracle E-Business Suite vulnerabilities
Critical Patch Update April 2008	12.0.x 11.5.7 – 11.5.10	▪ 8 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update July 2007	12.0.x 11.5.1 – 11.5.10	▪ 11 vulnerabilities, SQL injection, XSS, information disclosure, etc.
Critical Patch Update October 2005	11.0.x, 11.5.1 – 11.5.10	▪ Default configuration issues
Critical Patch Update July 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update April 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities ▪ Information disclosure
Critical Patch Update Jan 2005	11.5.1 – 11.5.10 11.0.x	▪ SQL injection vulnerabilities
Oracle Security Alert #68	Oracle 8i, 9i, 10g	▪ Buffer overflows ▪ Listener information leakage
Oracle Security Alert #67	11.0.x, 11.5.1 – 11.5.8	▪ 10 SQL injection vulnerabilities
Oracle Security Alert #56	11.0.x, 11.5.1 – 11.5.8	▪ Buffer overflow in FNDWRR.exe
Oracle Security Alert #55	11.5.1 – 11.5.8	▪ Multiple vulnerabilities in AOL/J Setup Test ▪ Obtain sensitive information (valid session)
Oracle Security Alert #53	10.7, 11.0.x 11.5.1 – 11.5.8	▪ No authentication in FNDFS program ▪ Retrieve any file from O/S

Agenda


Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS In the DMZ

OWASP Top 10 – 2010 Edition

- A1: Injection
- A2: Cross Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CRSF)
- A6: Security Misconfiguration
- A7: Insecure Cryptographic Storage
- A8: Failure to Restrict URL Access
- A9: Insufficient Transport Layer Protection
- 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');%20f
nd_user_pkg.updateUser('operations',%20'S
EED',%20'welcome1
```

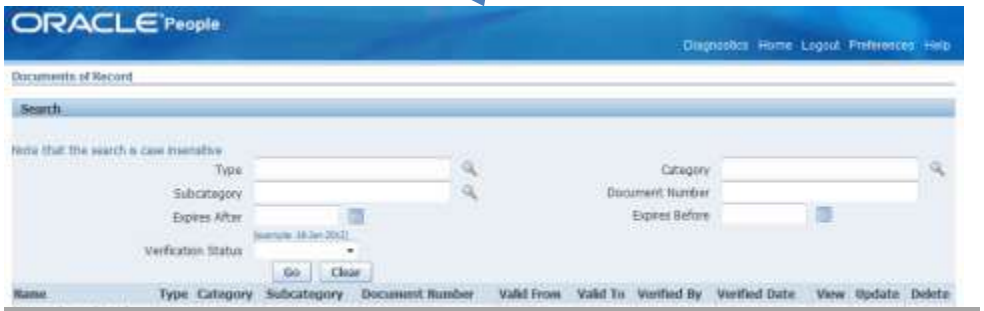
Oracle EBS executes appends SQL to the SQL statement being executed

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

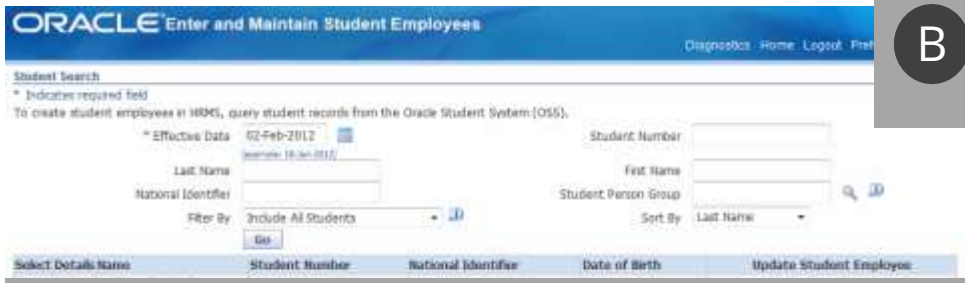
This vulnerability was patched as part of Oracle Security Alert #32

Cross Site Scripting (XSS) Illustrated

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

Oracle EBS Security Vulnerabilities

Oracle E-Business Suite security vulnerabilities fixed between January 2005 and January 2012

232

Oracle EBS Web Vulnerabilities Fixed

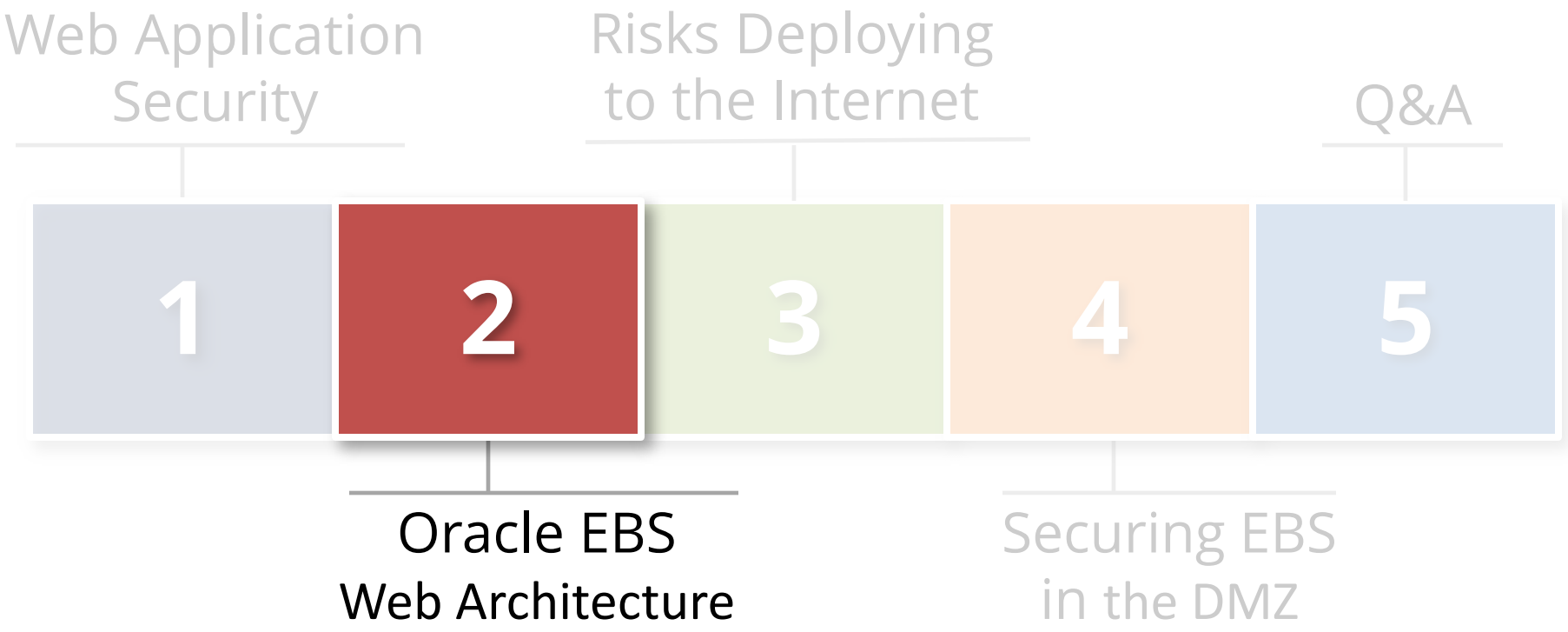
~60 SQL Injection in web pages

~70 Cross Site Scripting

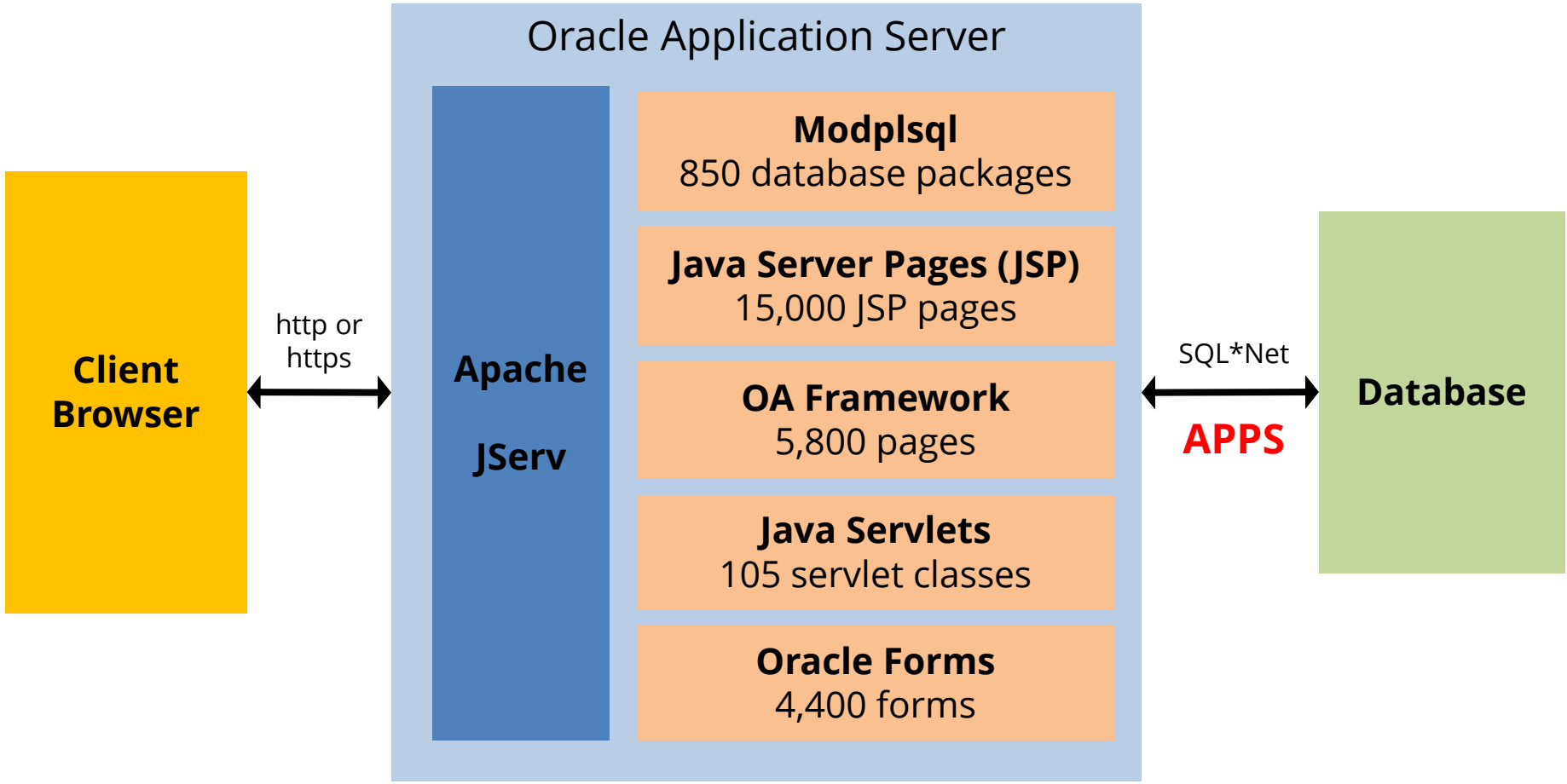
~15 Authorization/Authentication

~5 Business Logic Issues

Agenda

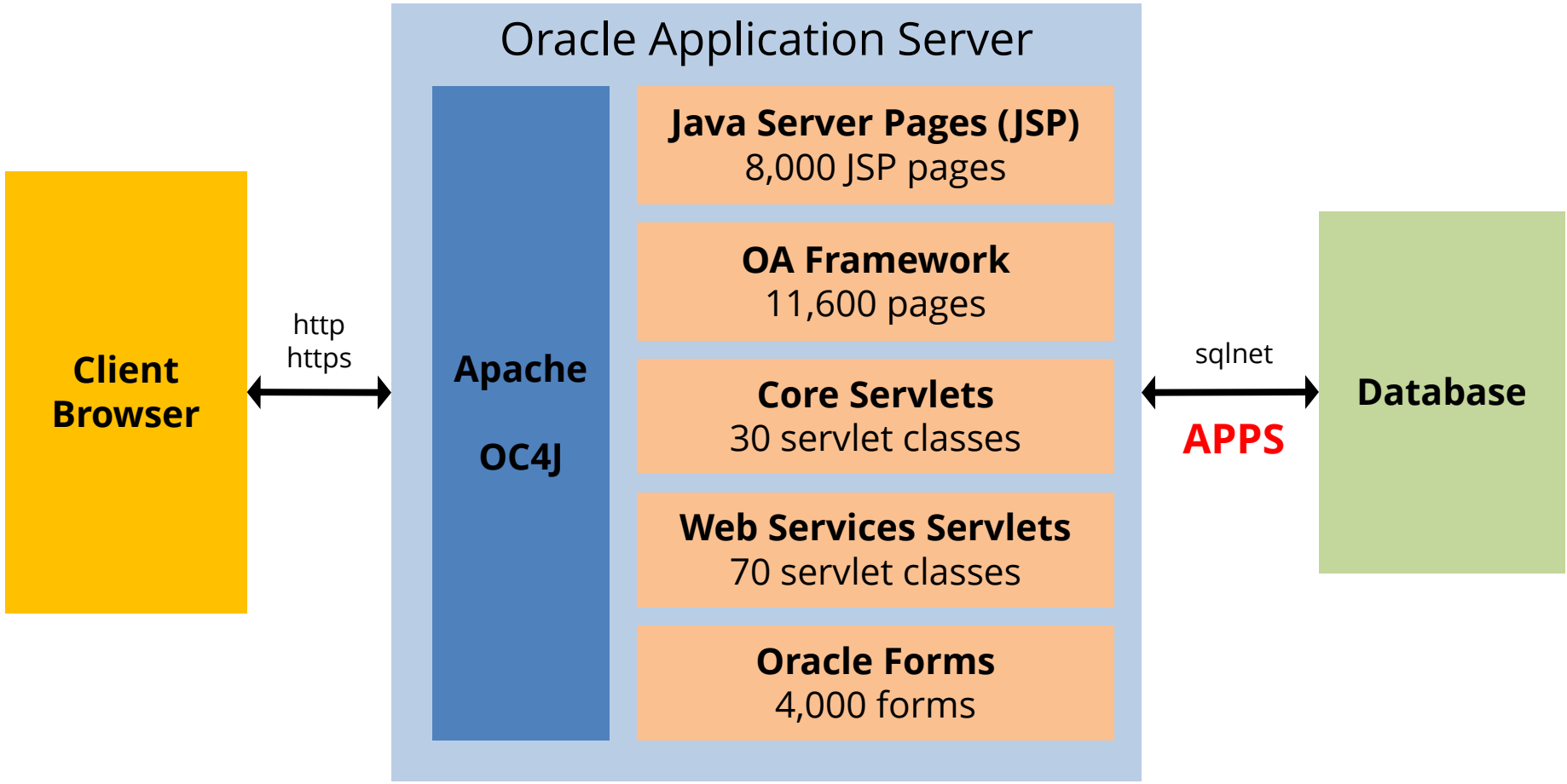

Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS in the DMZ

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 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 DMZ Certified Modules (R12)

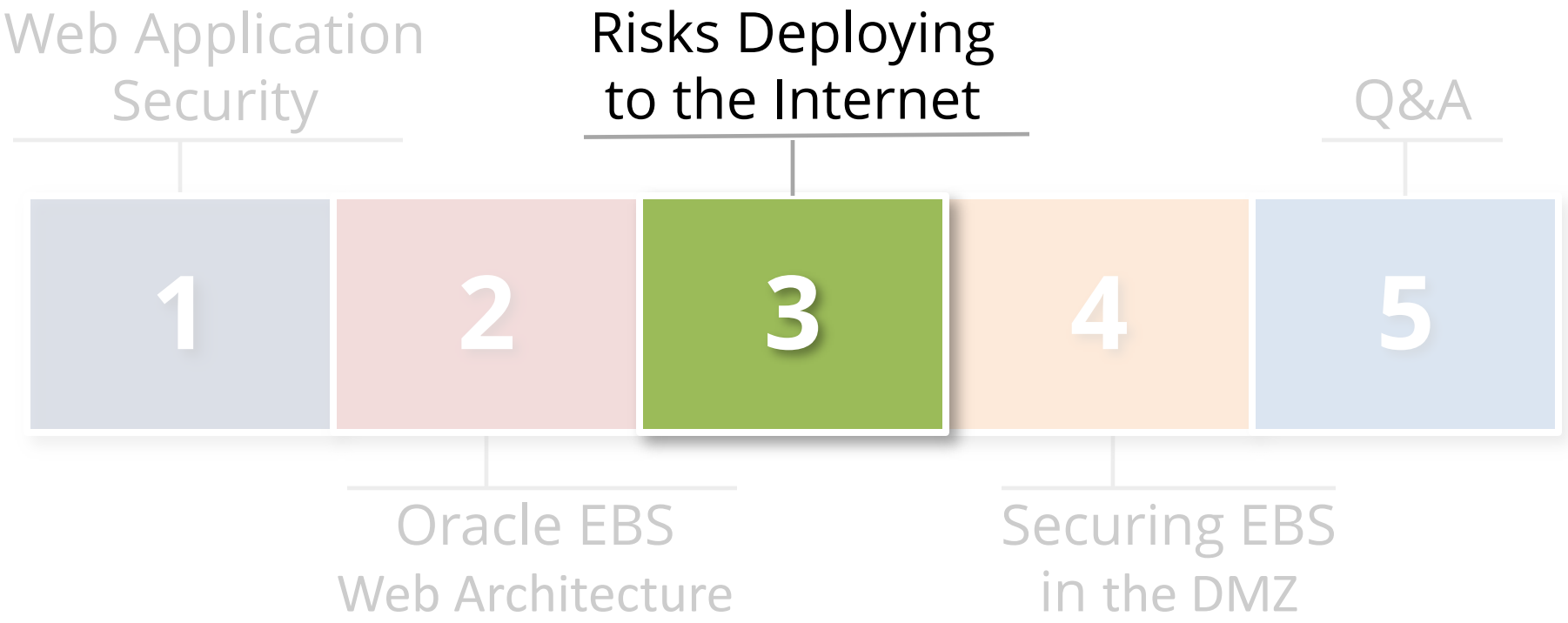
Oracle only certifies a limited set of modules for use in a DMZ

- 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)

Agenda


Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS in the DMZ

OWASP Top 10 – Oracle EBS Mapping

A1: Injection

A2: Cross Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CRSF)

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

A8: Failure to Restrict URL Access

A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

High Risk

Medium Risk

Low Risk

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

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

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

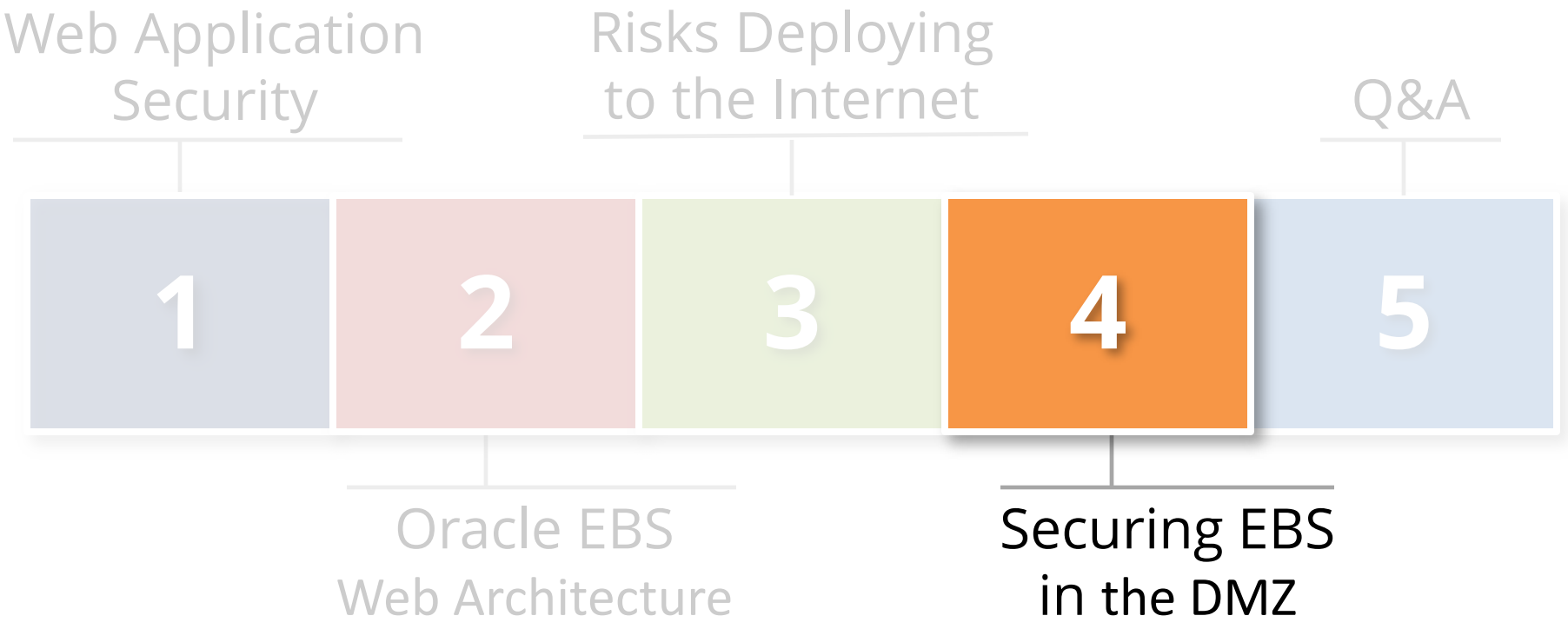
High Risk * **Medium Risk** * **Low Risk** * No Risk

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


Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS in the DMZ

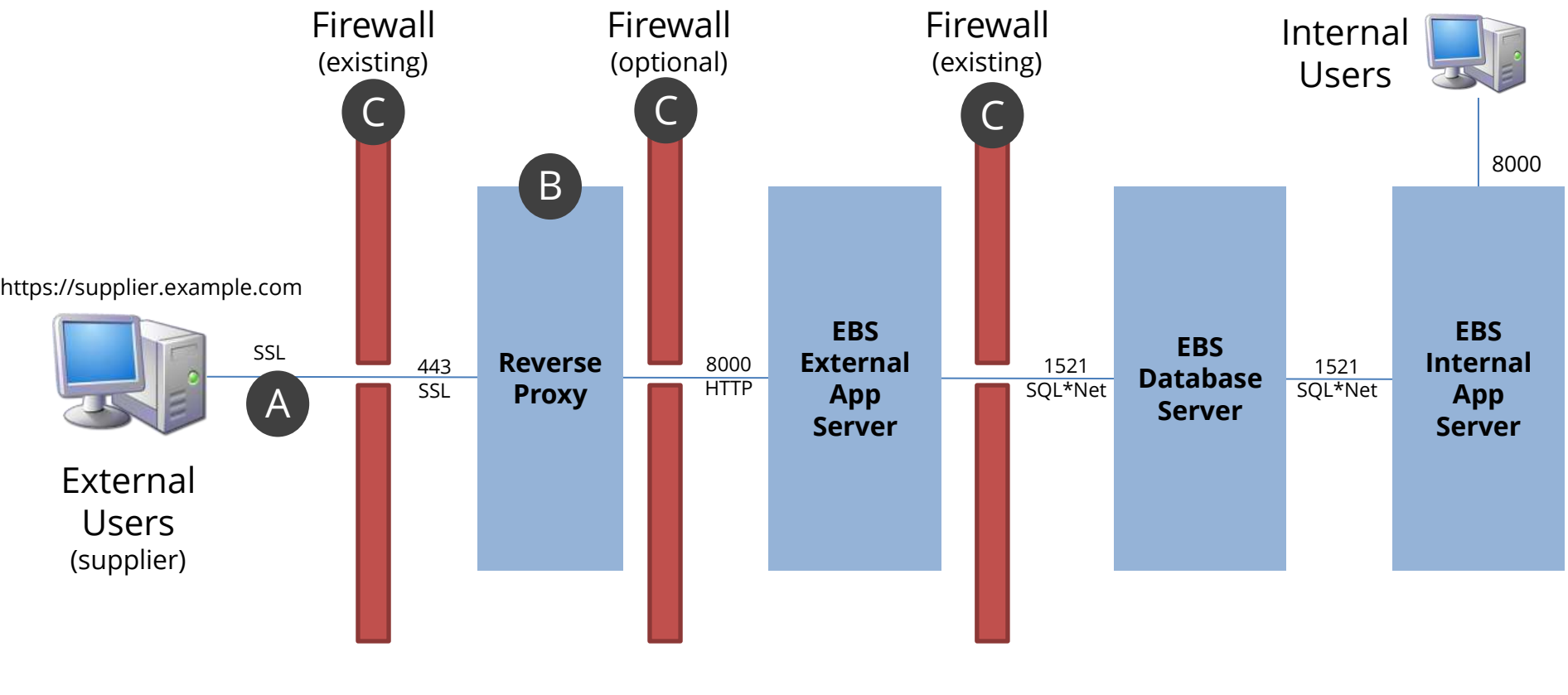
Oracle EBS DMZ Metalink Notes

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

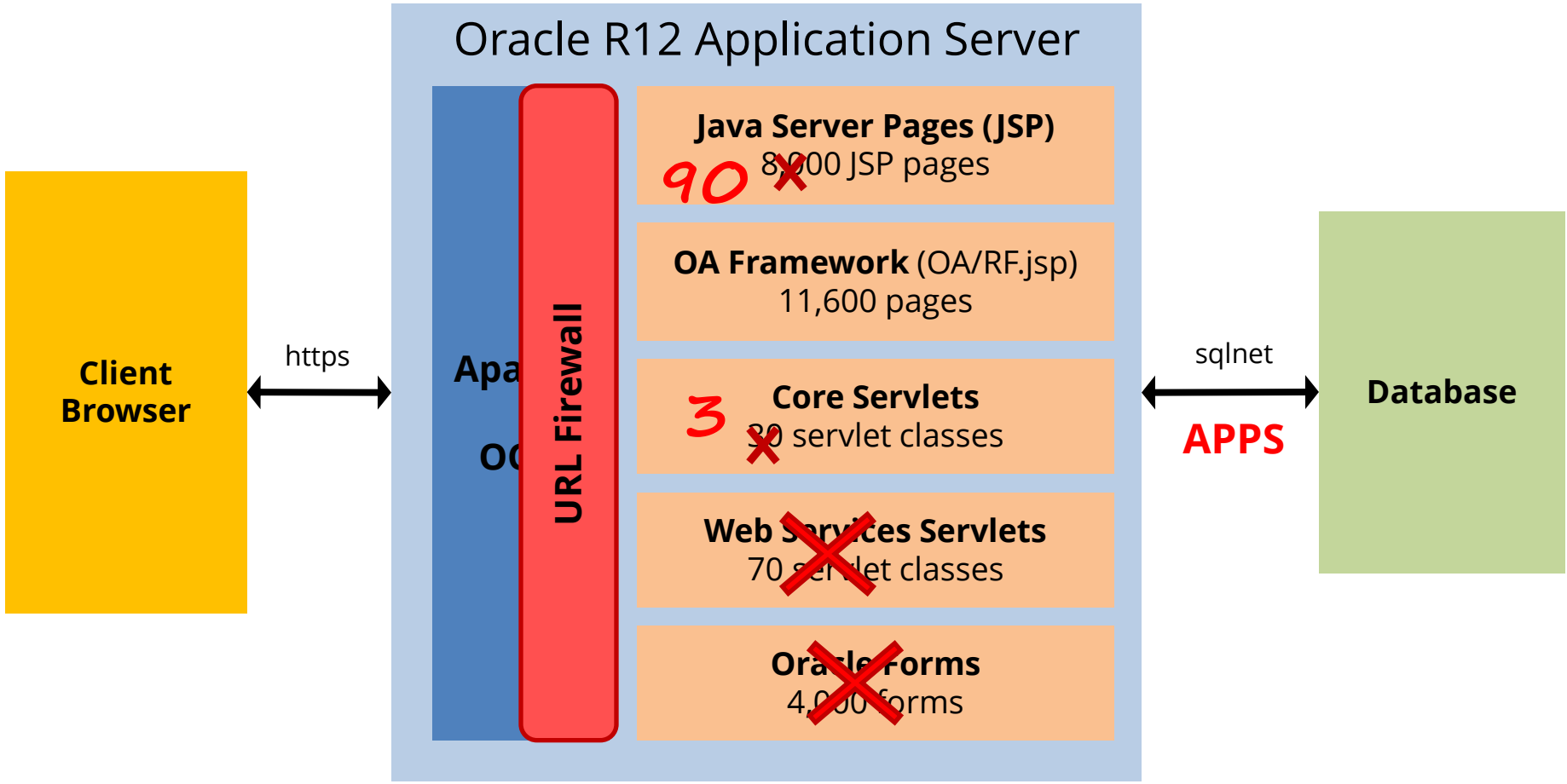


A **HTTPS/SSL** should always be used otherwise passwords and data are sent in the clear.

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

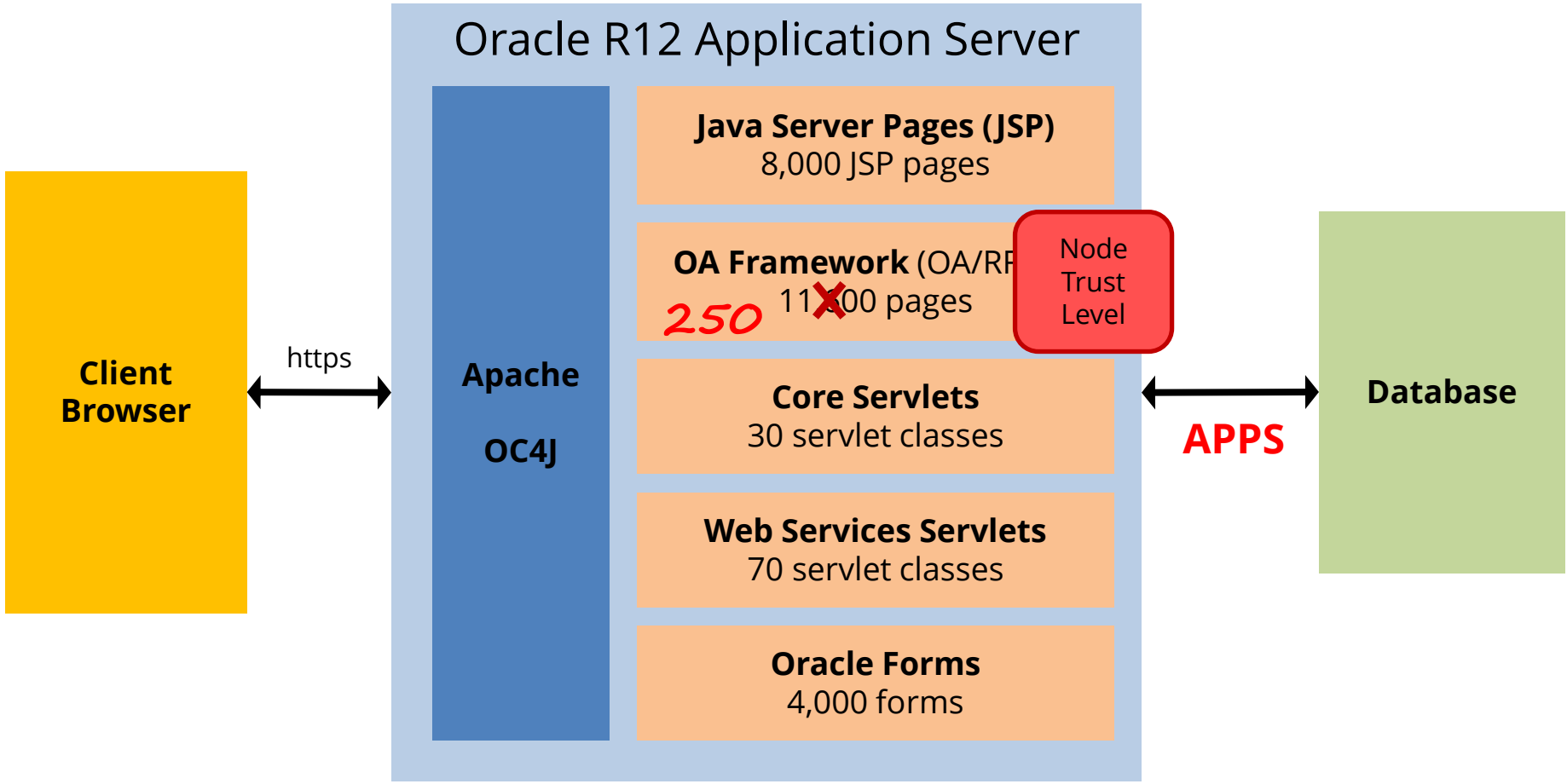
C Firewall between layers block access between layers except for explicitly defined ports.

DMZ Step Appendix E – URL Firewall



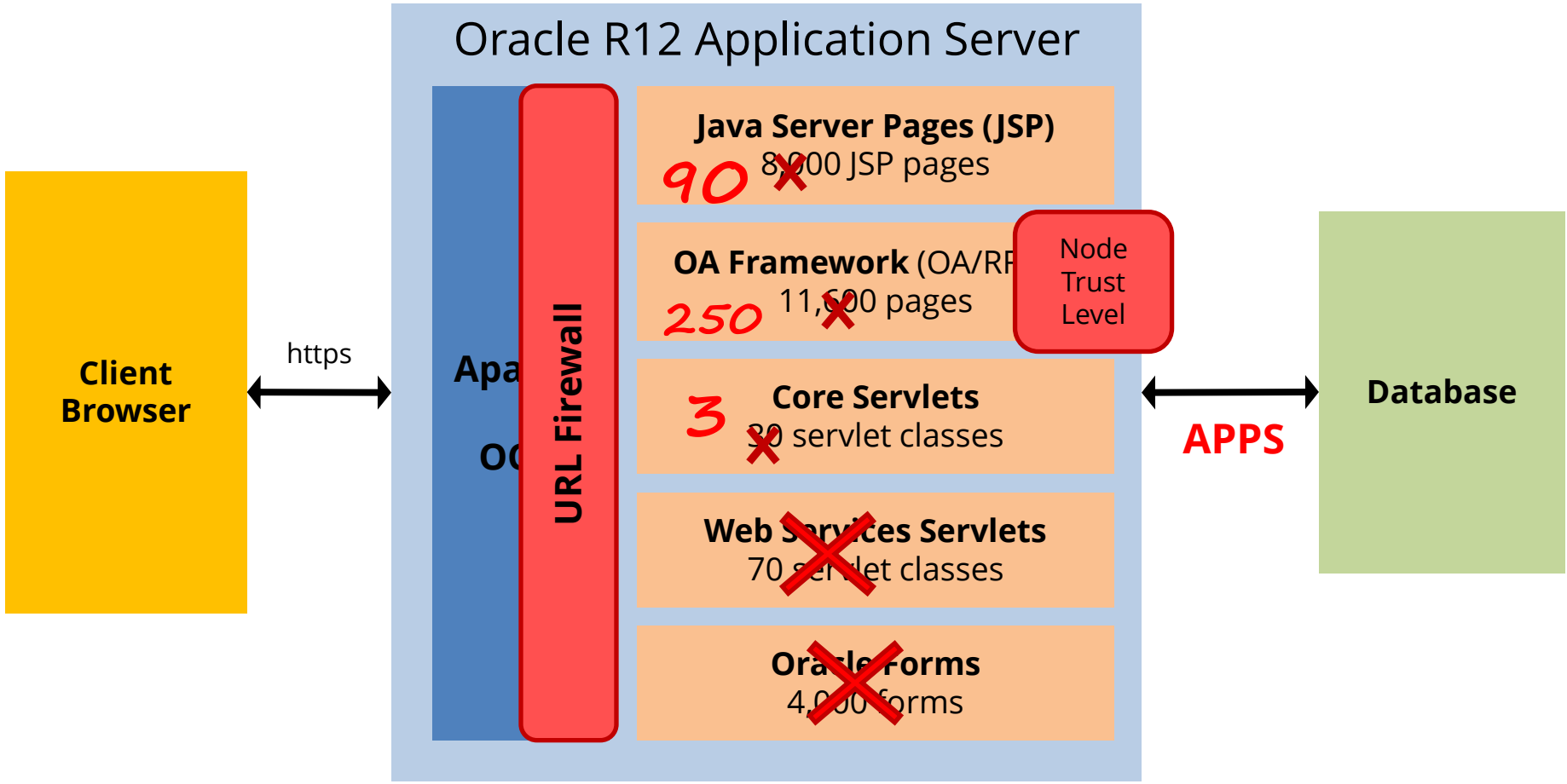
- **URL Firewall** in Appendix E is absolutely mandatory. Configure using **url_fw.conf**.
- A **whitelist** of allowed JSP pages and servlets. Allows all OA Framework pages.

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.

OWASP Top 10 – Oracle DMZ Config

A1: Injection

Oracle DMZ: Partial
A2: Cross Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CRSF)

A6: Security Misconfiguration

A7: Insecure Cryptographic Storage

Oracle DMZ: Mostly
A8: Failure to Restrict URL Access

Oracle DMZ: Complete
A9: Insufficient Transport Layer Protection

A10: Unvalidated Redirects and Forwards

High Risk

Medium Risk

Low Risk

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

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

Another Layer of Security

Web Application Firewalls (WAF) are specialized firewalls designed to detect and prevent web application attacks by analyzing the HTTP web requests.

- **Prevents common web application attacks**
  Detects and blocks SQL injection, XSS, and known vulnerabilities in widely used web applications
- **Often implemented as an appliance**
  Dedicated appliance used to protect all web applications in an organization
- **May be required for compliance such as PCI-DSS**
  PCI-DSS 2.0 requirement 6.6 requires use of a WAF or periodic reviews

Web Application Firewall Shortcomings

- **Must be heavily customized for Oracle EBS**
  Rules, application profiles, and learning must be developed, tuned, and tested by you

- **Unable to block unused Oracle EBS modules**
  Due to the complexity of the Oracle naming and design, very difficult to implement blocking of EBS modules with WAF rules

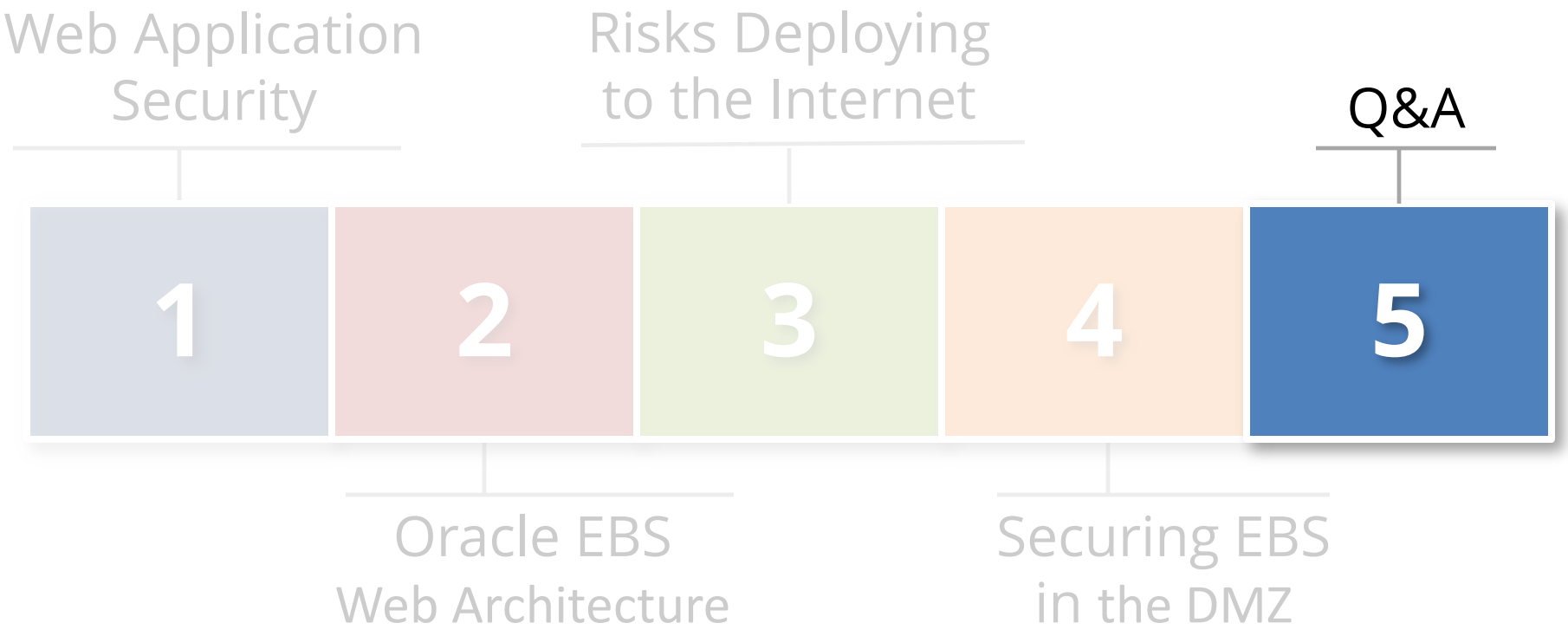
- **Significant cost, effort, and skill required to deploy**
  WAFs are usually an appliance that must be deployed and the learning curve for configuring and operating an enterprise WAF is steep

Integrigy AppDefend for R12

AppDefend is an **enterprise application firewall** designed and optimized for the Oracle E-Business Suite R12.

- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and known Oracle EBS 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
- **Protects Web Services**
  Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

Agenda


Web Application Security
Risks Deploying to the Internet
Q&A
1
2
3
4
5
Oracle EBS Web Architecture
Securing EBS in the DMZ

Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

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