INTEGRIGY

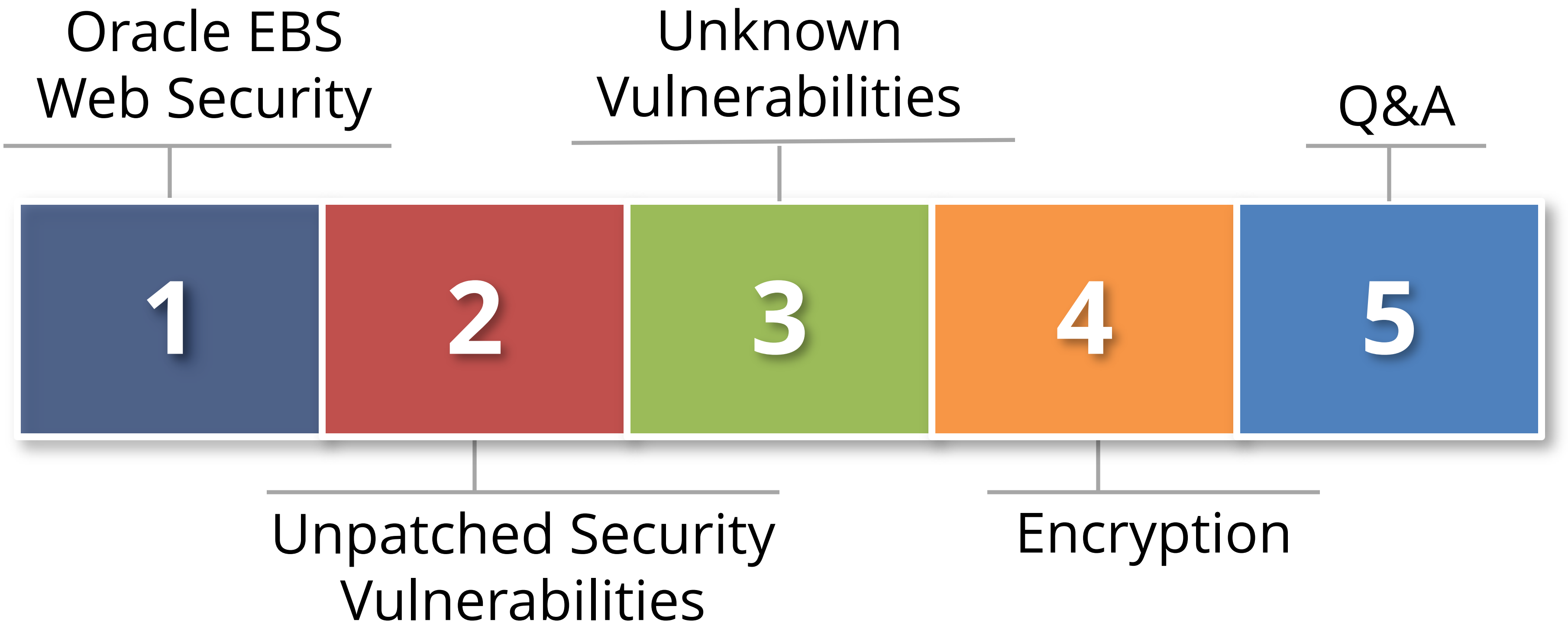
Out of the Fire - Adding Layers of Protection When Deploying Oracle EBS to the Internet

March 8, 2012

Stephen Kost
Chief Technology Officer
Integrigy Corporation

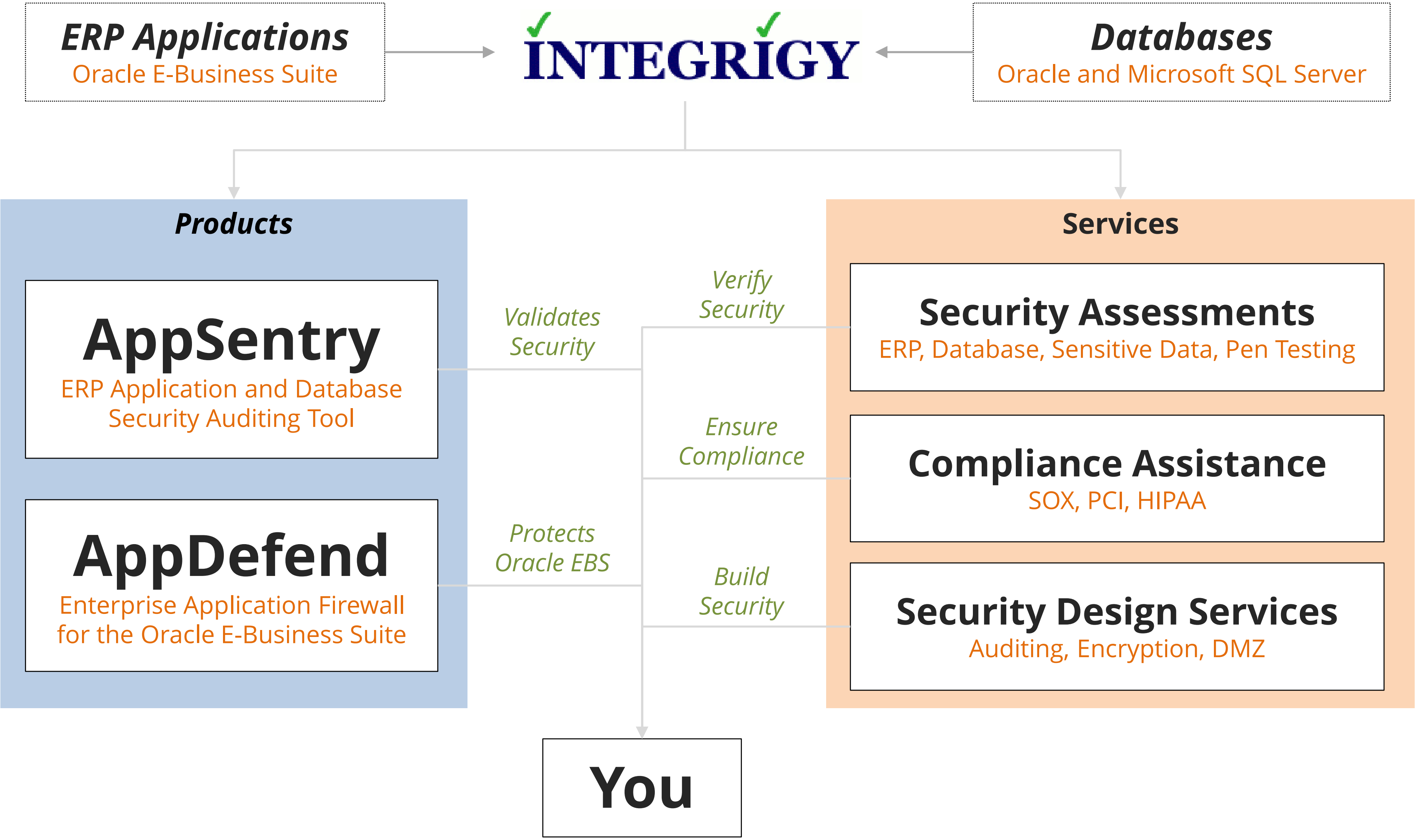
Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1. Oracle EBS Web Security
2. Unpatched Security Vulnerabilities
3. Unknown Vulnerabilities
4. Encryption
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

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite

Protects Oracle EBS

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance
SOX, PCI, HIPAA

Build Security

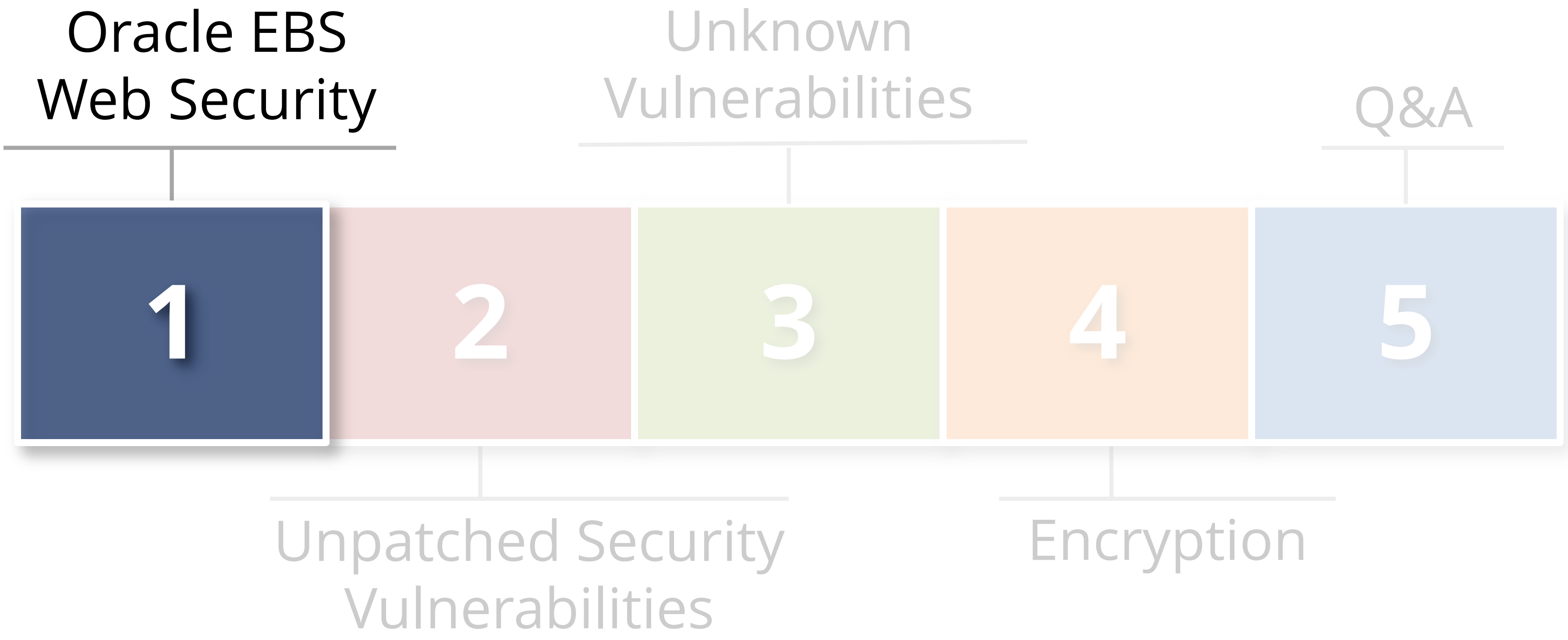
Security Design Services
Auditing, Encryption, DMZ

You

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



Oracle EBS Web Security

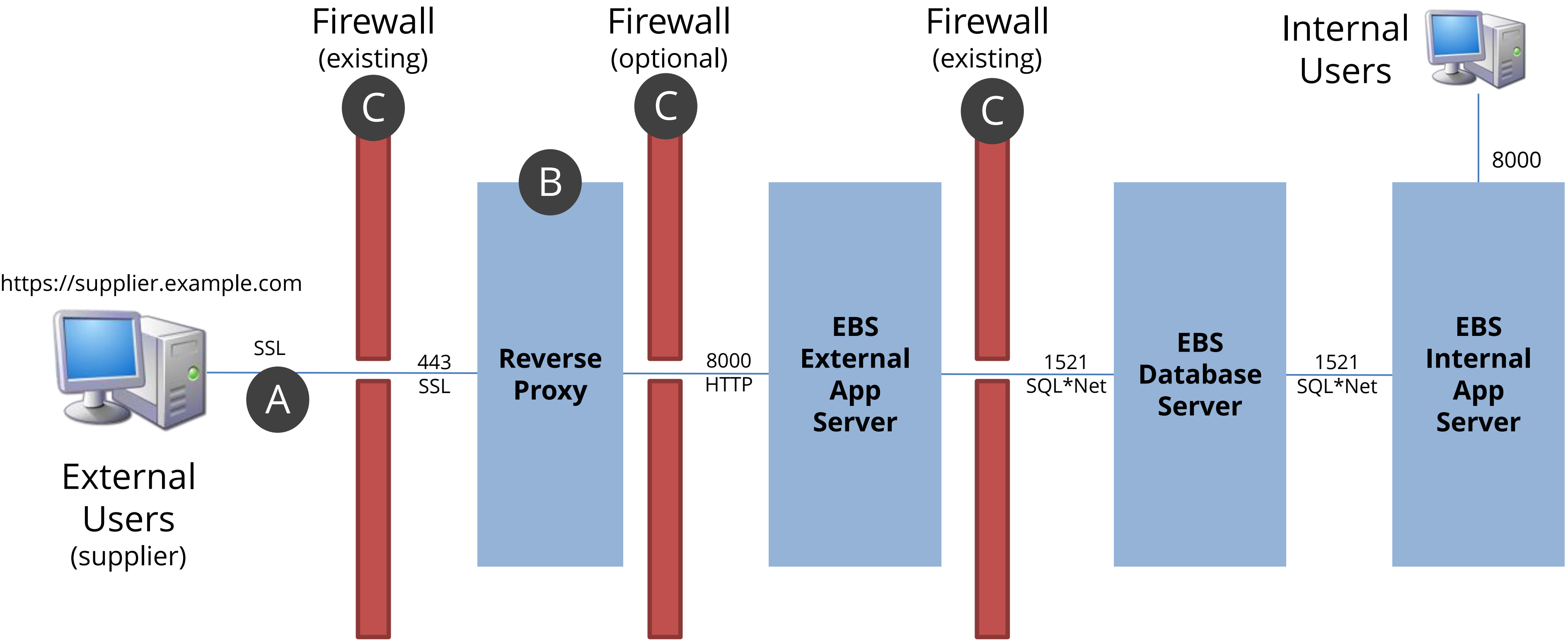
Unpatched Security Vulnerabilities

Unknown Vulnerabilities

Encryption

Q&A

EBS DMZ Architecture

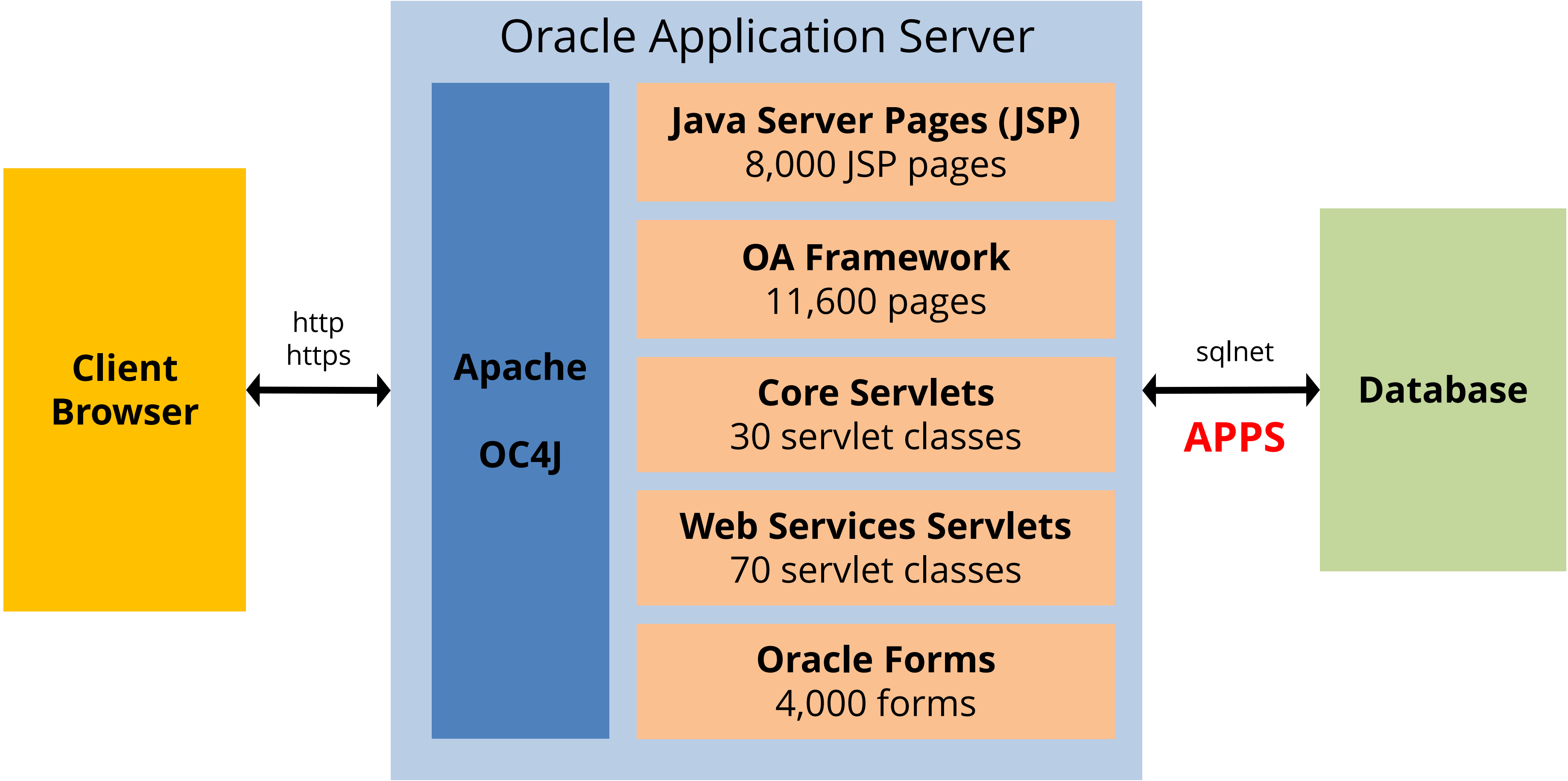


A **HTTPS/SSL** should always be used otherwise passwords and data are sent in the clear.

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 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 MOS Notes

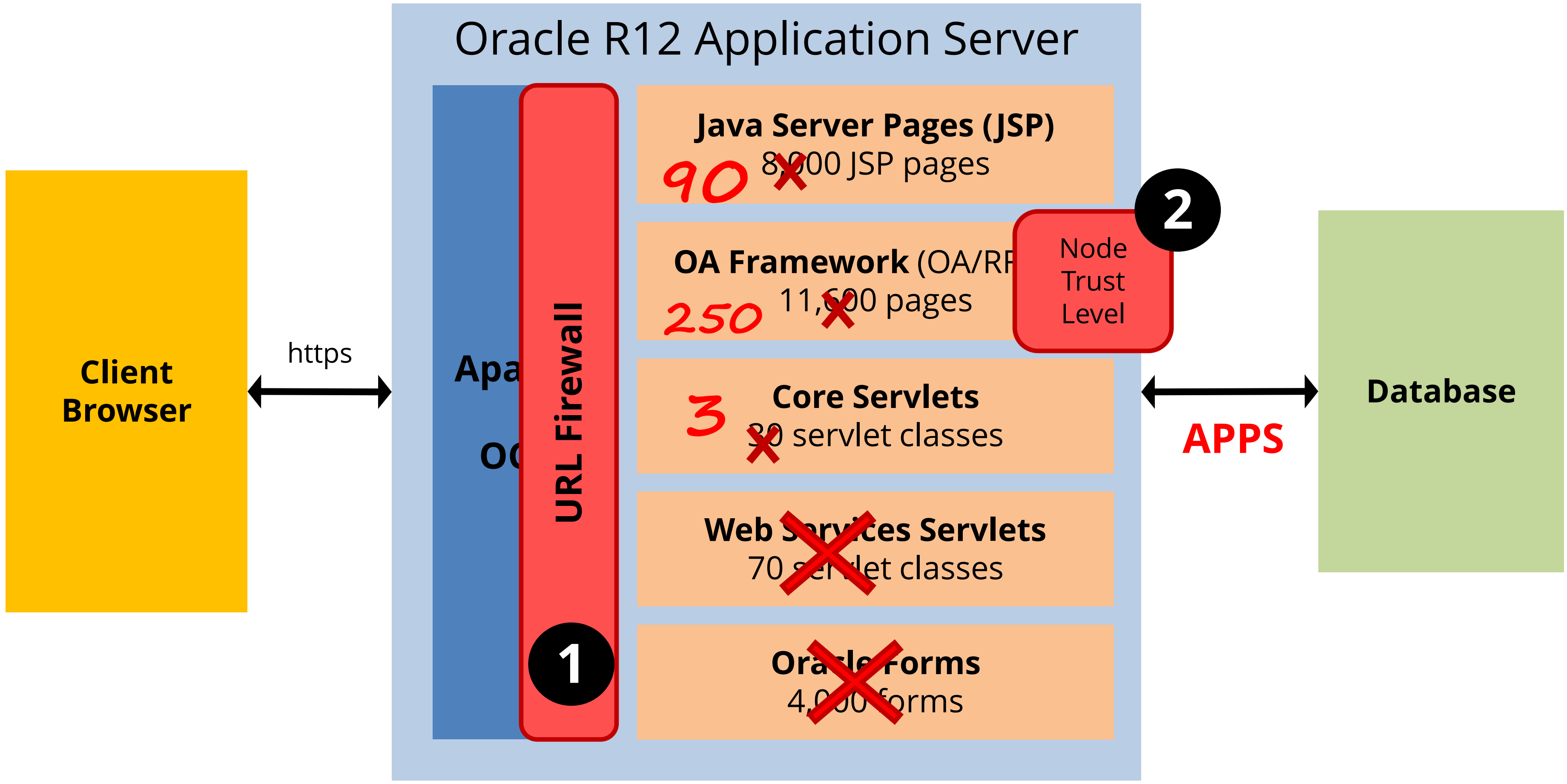
Deploying Oracle E-Business Suite in a DMZ requires a specific and detailed configuration of the application and application server. All steps in the Oracle provided MOS Note must be followed.

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

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

MOS = My Oracle Support

Oracle EBS DMZ Configuration

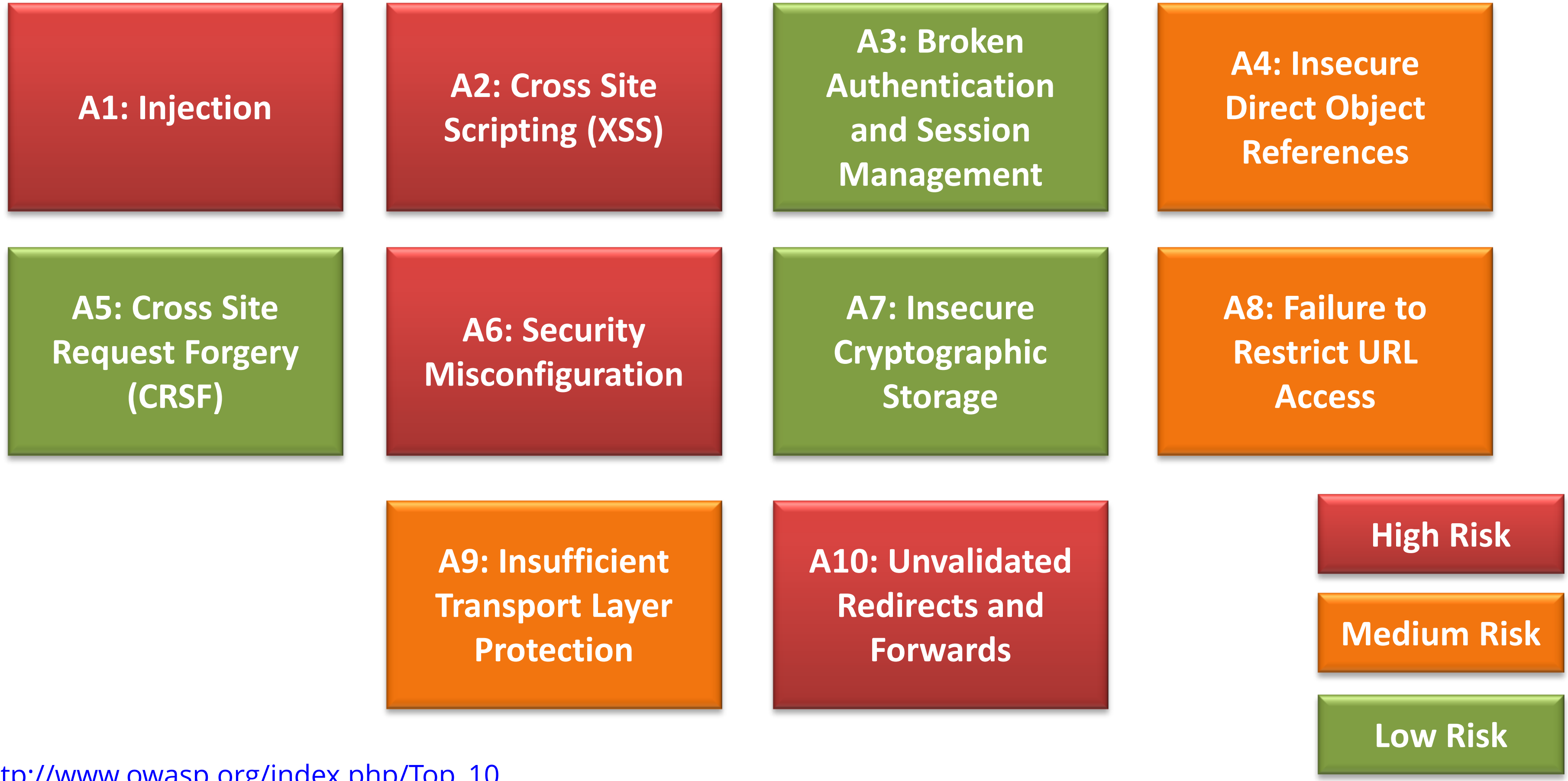


- Proper **DMZ configuration** reduces accessible pages and responsibilities to only those required for external access. Reducing the application surface area eliminates possible exploiting of vulnerabilities in non-external modules.

OWASP Top 10 – Oracle EBS Mapping

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

Ten top security risks commonly found in web applications listed by level of risk



- 🟥 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

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

WASC Threat Classification

Web Application Security Consortium

Comprehensive list of threats to the security of a web site – attacks and weaknesses

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

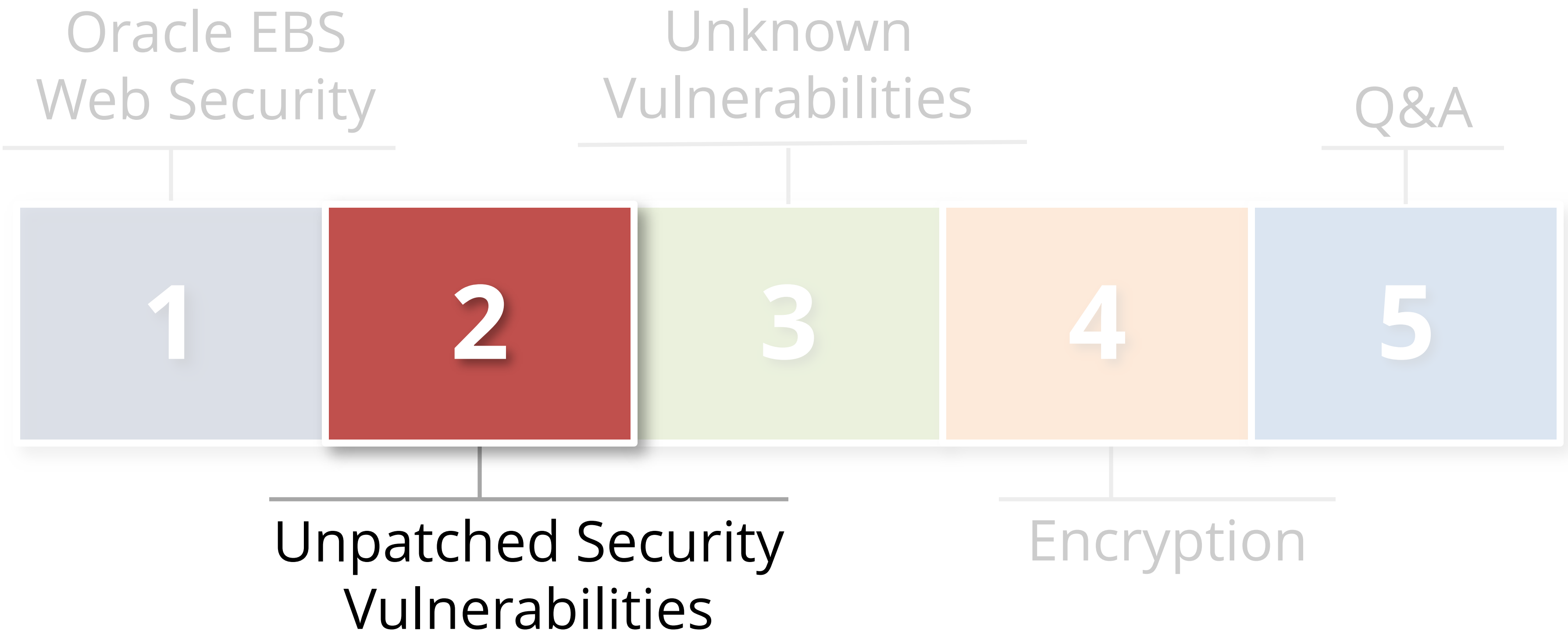
Weaknesses

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

Agenda



1 Oracle EBS Web Security

2 Unpatched Security Vulnerabilities

3 Unknown Vulnerabilities

4 Encryption

5 Q&A

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

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

Oracle Critical Patch Updates

Oracle releases security patches on a quarterly basis to fix security bugs in all Oracle products – Database, App Server, EBS

- **Cumulative Patches**
  Must apply large patch for all modules

- **Includes Dependencies**
  Patches often update more than just the vulnerable file

- **Upgrades Required**
  May require application upgrades (12.1.5 → 12.1.6)

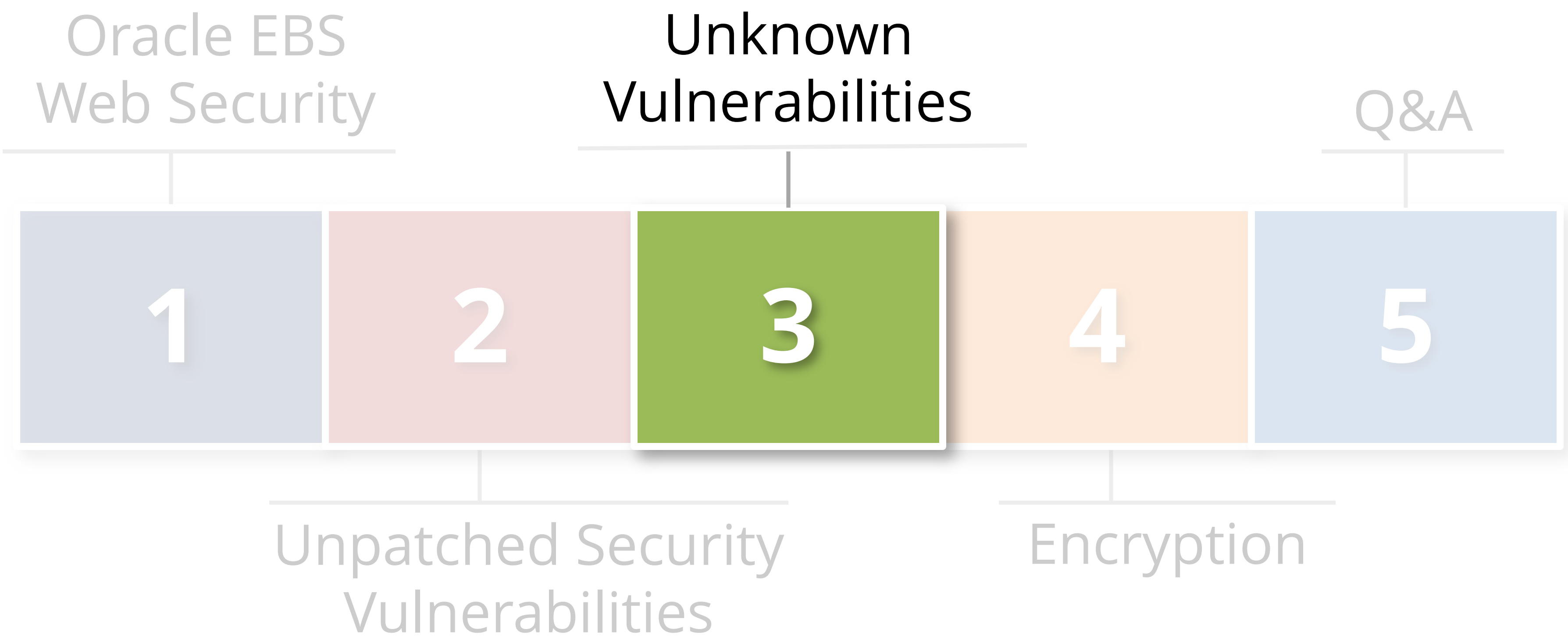
- **Testing Required**
  Patches must go through testing cycle

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

Agenda



1. Oracle EBS Web Security
2. Unpatched Security Vulnerabilities
3. Unknown Vulnerabilities
4. Encryption
5. Q&A

OWASP Top 10 – Oracle EBS Mapping

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

Ten top security risks commonly found in web applications listed by level of risk

- 🟥 A1: Injection (SQL, HTML, XML, …)
- 🟥 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

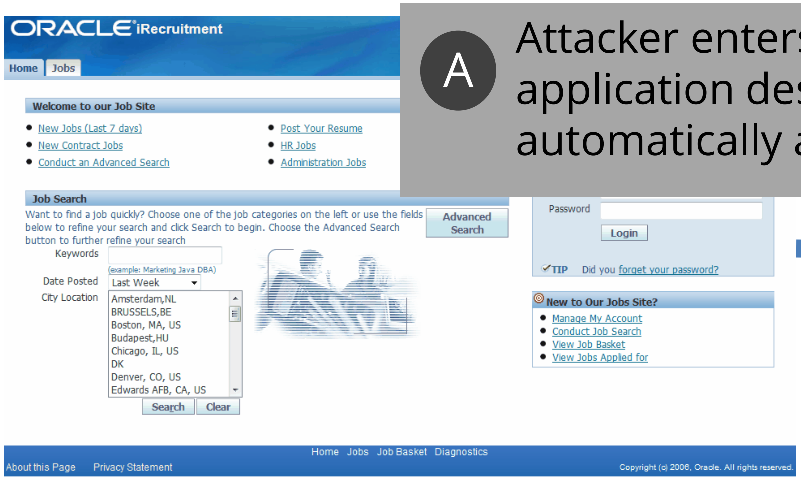
🟥 High Risk

🟧 Medium Risk

🟩 Low Risk

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

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

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 | Advanced Search

Password

Login

TIP Did you forget your password?

New to Our Jobs Site?

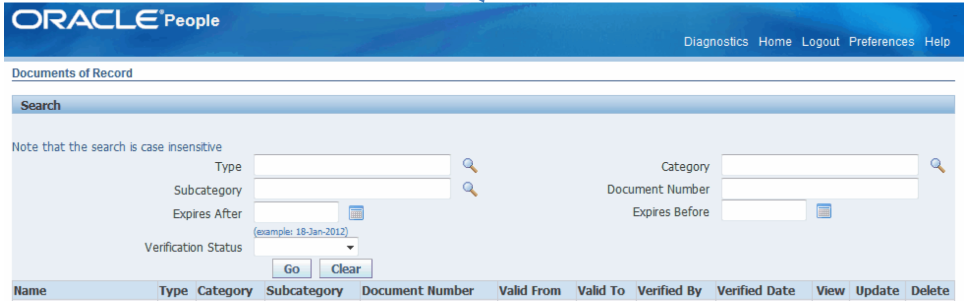
- Manage My Account
- Conduct Job Search
- View Job Basket
- View Jobs Applied for

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

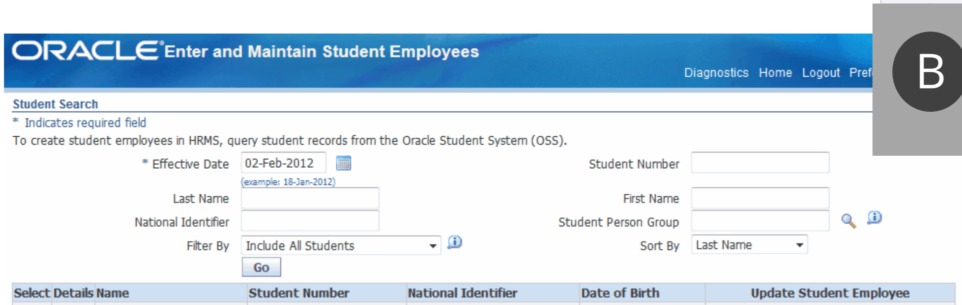
Note that the search is case insensitive

Type		Category	
Subcategory		Document Number	
Expires After	(example: 18-Jan-2012)	Expires Before	
Verification Status			

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)	Student Number	
Last Name		First Name	
National Identifier		Student Person Group	
Filter By	Include All Students	Sort By	Last Name

Go

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)">

<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

XSS Cheat Sheet

http://ha.ckers.org/xss.html

WSC Script Mapping Project

http://www.webappsec.org/projects/scriptmapping

OWASP XSS Reference

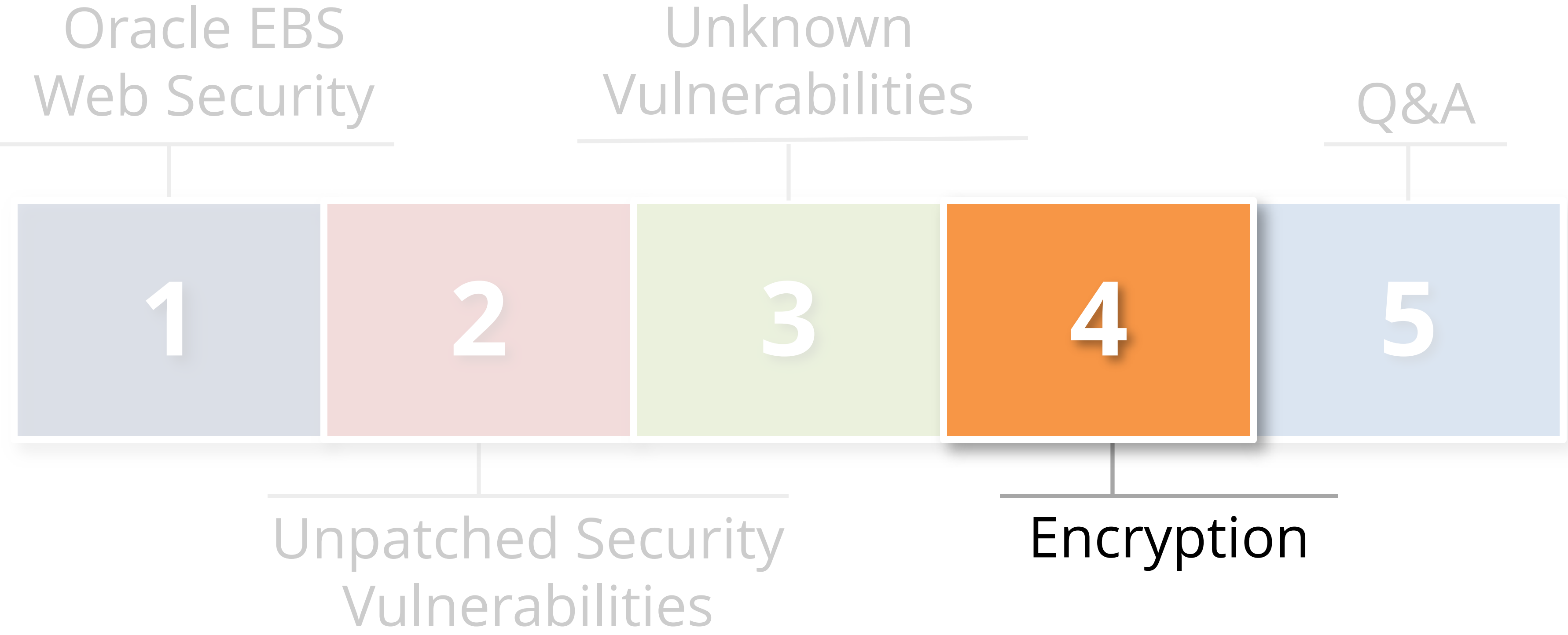
https://www.owasp.org/index.php/Cross-Site_Scripting

Deep Inspection

> *"Analyze all user provided input to identify and block malicious input"*

1. **Oracle E-Business Suite XSS Filter**
   - Limited filter – easy to bypass
2. **Web Application Firewalls**
   - Static signatures or regular expressions
   - Too expensive (CPU) to fully parse all inputs
3. **AppDefend**
   - Intelligent checking of parameters, user input
   - Uses best practice libraries – OWASP AntiSamy

Agenda


Oracle EBS Web Security
Unknown Vulnerabilities
Q&A
1
2
3
4
5
Unpatched Security Vulnerabilities
Encryption

Oracle EBS HTTP Network Traffic

```
POST
http://oa.integrigy.com:8010/OA_HTML/OA.jsp?
page=/oracle/apps/fnd/sso/login/webui/MainLo
ginPG HTTP/1.1

_AM_TX_ID_FIELD=1wcuM2LWP
_FORM=DefaultFormNameKBTL4xsJ
usernameField=SYSADMIN
passwordField=MYPASSWORD
SubmitButton%24%24unvalidated=falseI_3t5ZET
```

Using SSL Encryption

"Encrypt all end-user traffic externally as well as internally."

1. Implement SSL on Oracle EBS Application Servers
   - Use Oracle's MOS SSL Notes
   - ***Be sure to disable SSLv2 and weak ciphers***
2. Use SSL encryption and acceleration on load balancers
   - Simplifies setup and configuration
   - Removes load from application servers to load balancer with dedicated SSL encryption hardware

Oracle EBS SSL MOS Notes

Enabling SSL for Oracle E-Business Suite in a DMZ requires a complex setup because of certificates. Follow the steps for configuring SSL in the "Middle Tier."

376700.1 *Enabling SSL in Oracle E-Business Suite* ***Release 12***

123718.1 ***11i:*** *A Guide to Understanding and Implementing SSL for Oracle Applications*

MOS = My Oracle Support

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 Options

- **Reverse Proxy Server with ModSecurity with OWASP CRS**
  Open-source option on your hardware

- **Load Balancer with WAF**
  WAF, SSL termination features of many load balancers

- **Stand-alone WAF**
  Dedicated, appliance WAF

- **AppDefend**
  Distributed WAF running within application Java stack

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.

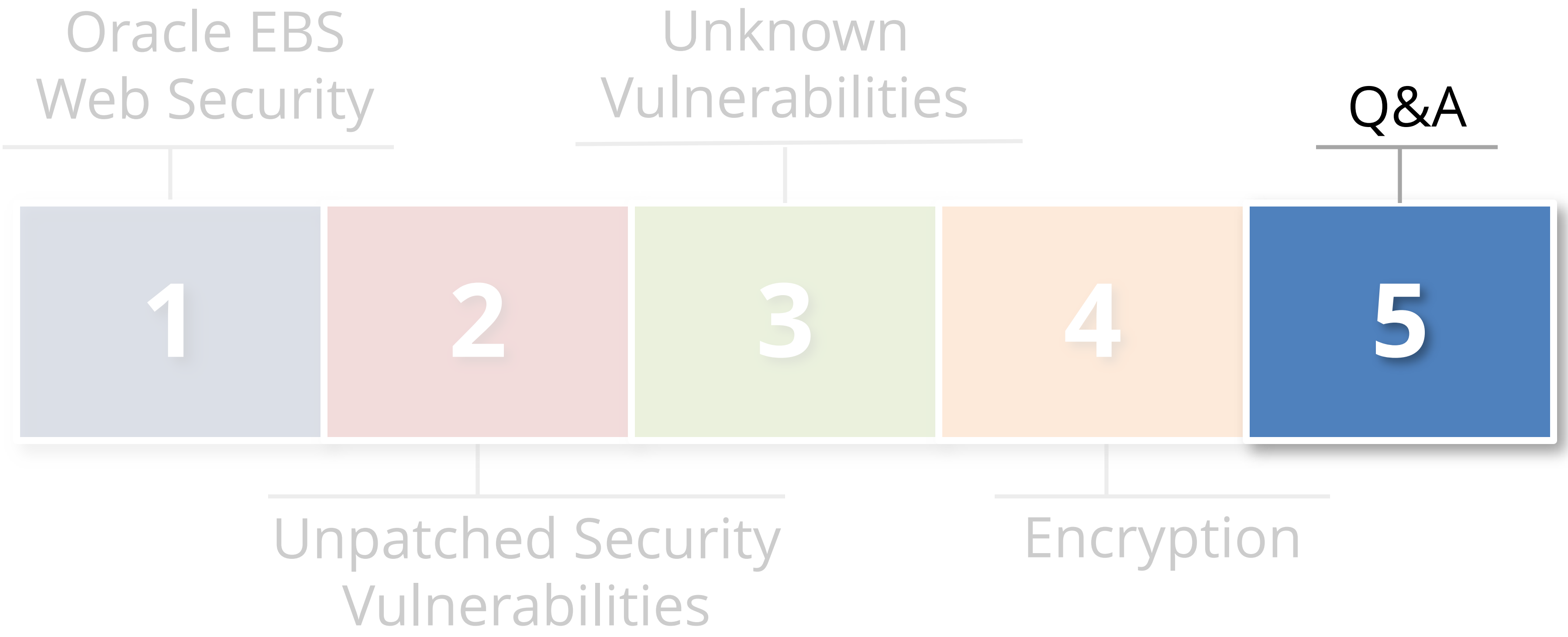
- **Prevents Web Attacks**
  Detects and reacts to SQL Injection, XSS, and known Oracle EBS vulnerabilities

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

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

- **Protects Web Services**
  Detects and reacts to attacks against native Oracle EBS web services (SOA, SOAP, REST)

Agenda



1 Oracle EBS Web Security

2 Unpatched Security Vulnerabilities

3 Unknown Vulnerabilities

4 Encryption

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**