INTEGRIGY

# AppDefend

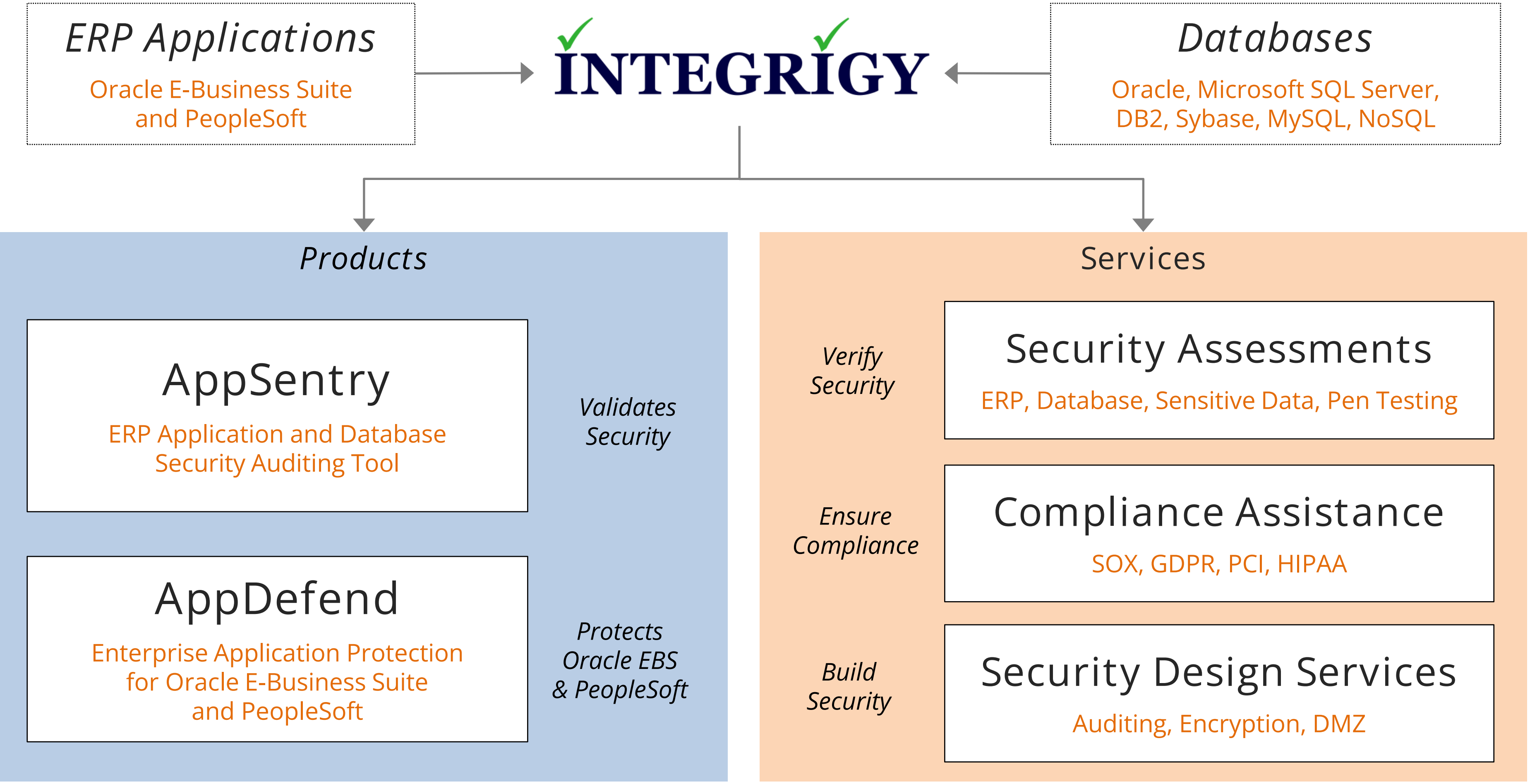
## Oracle PeopleSoft

## Enterprise Application Protection

October 2023

*mission critical applications …*
*… mission critical security*

# About Integrigy



*ERP Applications*

Oracle E-Business Suite and PeopleSoft

INTEGRIGY

*Databases*

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL, NoSQL

*Products*

AppSentry

ERP Application and Database Security Auditing Tool

*Validates Security*

AppDefend

Enterprise Application Protection for Oracle E-Business Suite and PeopleSoft

*Protects Oracle EBS & PeopleSoft*

Services

*Verify Security*

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

*Ensure Compliance*

Compliance Assistance

SOX, GDPR, PCI, HIPAA

*Build Security*

Security Design Services

Auditing, Encryption, DMZ

Integrigy Research Team

ERP Application and Database Security Research

ORACLE Gold Partner

# Agenda

1 Web Application Security

2 PeopleSoft Web Architecture

3 AppDefend Overview

4 AppDefend Benefits

5 Q & A

# Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Integrigy's products remains at the sole discretion of Integrigy.

# Integrigy’s Products

| | |
|---|---|
| AppSentry | Security scanner for databases, application servers, and ERP packages<br>▪ Performs advanced penetration testing and in-depth security and controls auditing<br>▪ Performs over 1,000+ audits and checks on Oracle products<br>▪ Requires no software to be installed on the target servers |
| AppDefend | Application firewall and protection system for ERP packages<br>▪ Blocks common attacks like SQL injection, session hijacking, cross site scripting, and Java deserialization<br>▪ Blocks access to unimplemented application modules and pages<br>▪ Scans all incoming web requests and outbound responses |

# Agenda

1 Web Application Security

2 PeopleSoft Web Architecture

3 AppDefend Overview

4 AppDefend Benefits

5 Q & A

# Oracle PeopleSoft Vulnerabilities

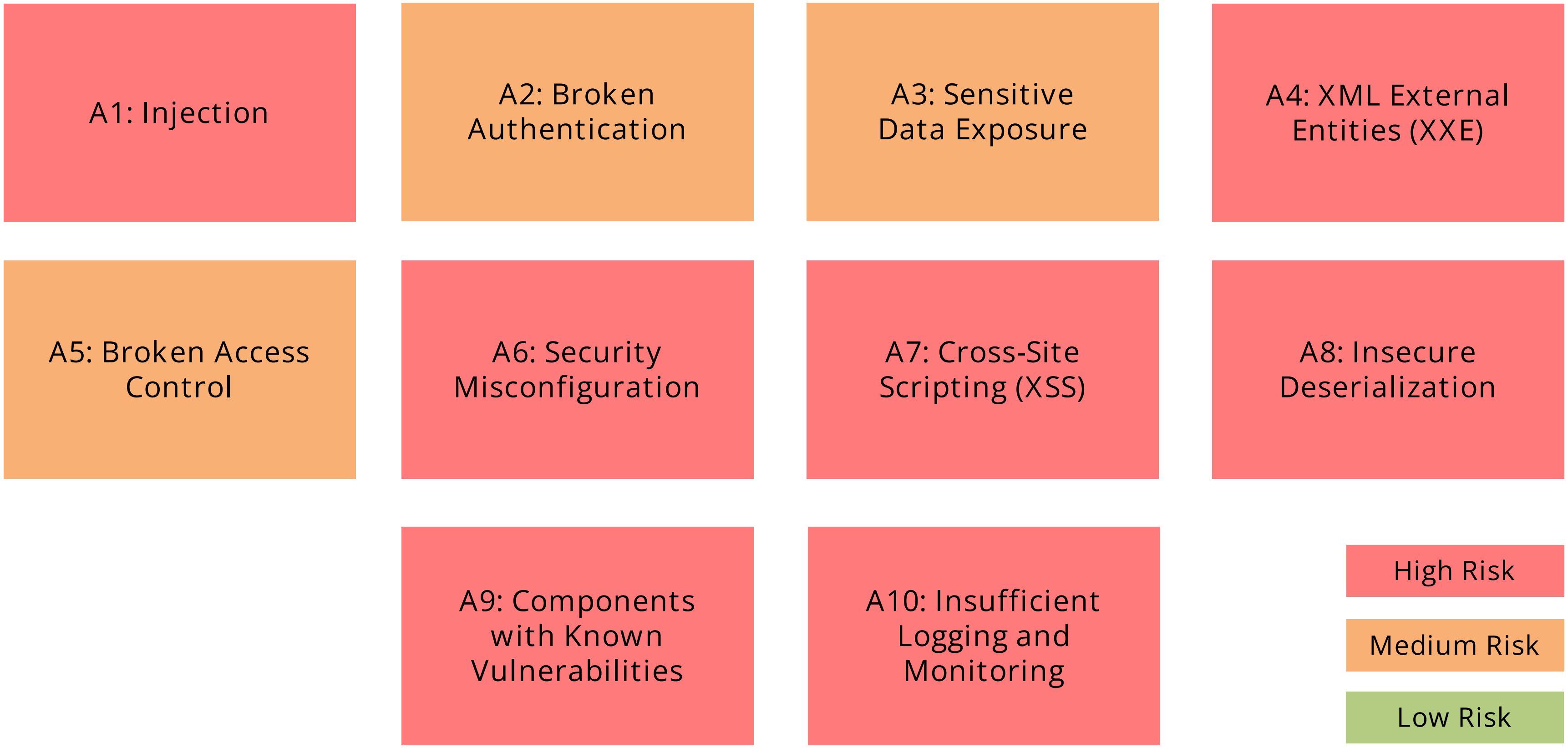
Oracle PeopleSoft
security vulnerabilities
fixed between
January 2005 and April 2021

524

# OWASP Top 10 – PeopleSoft Mapping

OWASP
Open Web Application
Security Project

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



🟥 A1: Injection

🟧 A2: Broken Authentication

🟧 A3: Sensitive Data Exposure

🟥 A4: XML External Entities (XXE)

🟧 A5: Broken Access Control

🟥 A6: Security Misconfiguration

🟥 A7: Cross-Site Scripting (XSS)

🟥 A8: Insecure Deserialization

🟥 A9: Components with Known Vulnerabilities

🟥 A10: Insufficient Logging and Monitoring

🟥 High Risk

🟧 Medium Risk

🟩 Low Risk

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

# WASC Threat Classification – PeopleSoft Mapping

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

# 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

# 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 (WAF) Shortcomings

- Must be heavily customized for Oracle EBS
  - No out of the box rules for PeopleSoft – no CPU specific rules
  - Unaware for the unique web application architecture of PeopleTools
  - Rules, application profiles, and learning must be developed, tuned, and tested by you
  - PeopleSoft is multiple web architectures resulting in additional tuning

- 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

- AppDefend is complementary with an enterprise WAF solution
  - AppDefend can be stand-alone or combined with an existing WAF
  - Multiple layers of defense
  - Enterprise WAF provides general protection and eliminates “noise”
  - AppDefend provides PeopleSoft specific layer of protection

# Agenda

1 Web Application Security

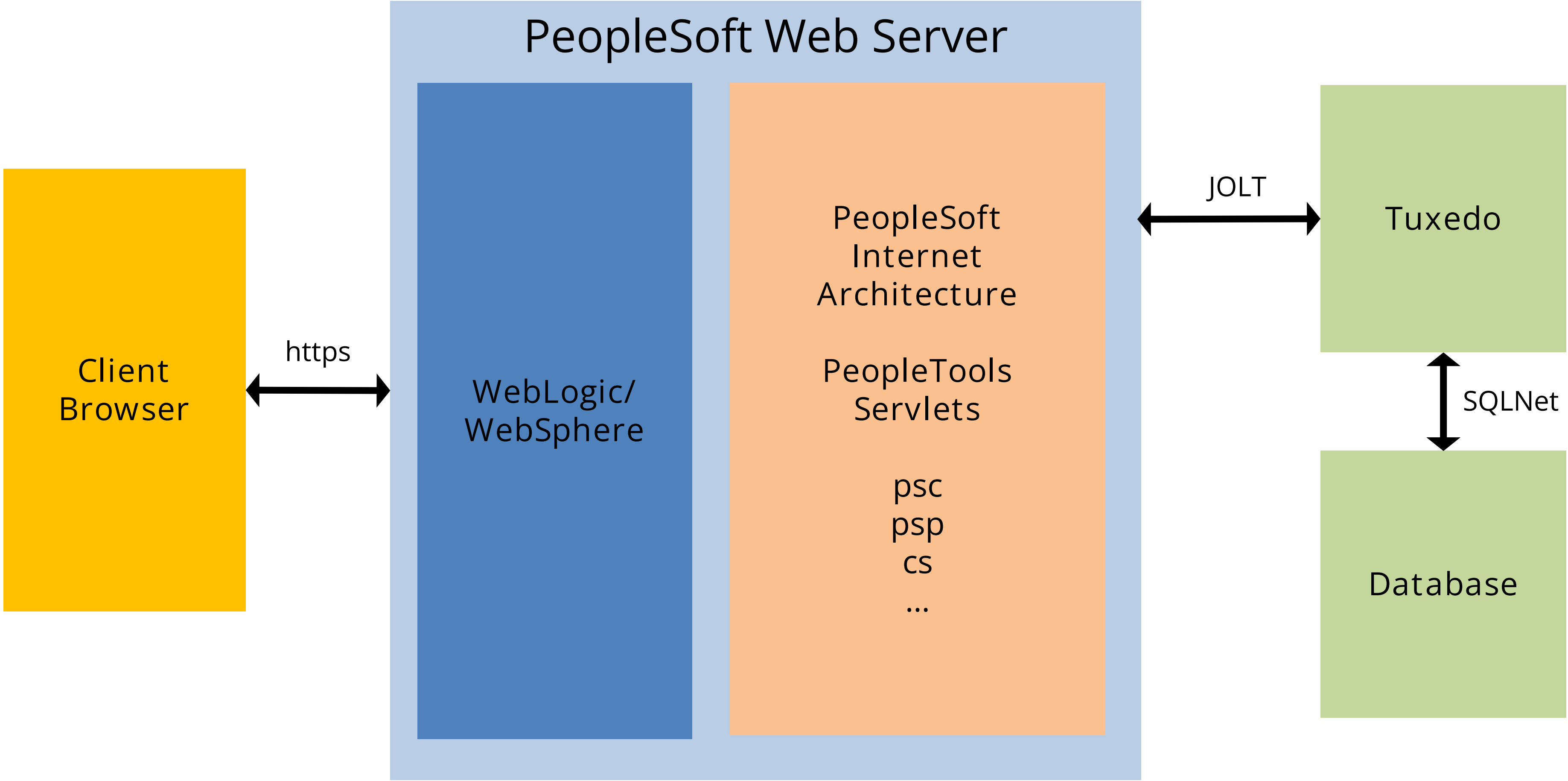
2 PeopleSoft Web Architecture

3 AppDefend Overview

4 AppDefend Benefits

5 Q & A

# PeopleSoft Web Architecture



- PeopleSoft runs as a Java application on the web server using the WebLogic/WebSphere Java container. Java servlets process inbound requests and pass the transaction to Tuxedo/JOLT for processing.

# Agenda

1 Web Application Security

2 PeopleSoft Web Architecture

3 AppDefend Overview

4 AppDefend Benefits

5 Q & A

# Integrigy AppDefend

AppDefend is an application firewall designed and optimized for Oracle PeopleSoft.

### Prevents Web Attacks

Detects and reacts to SQL Injection, XSS, and known application vulnerabilities

### Application Logging

Enhanced application logging for compliance requirements like PCI-DSS 10.2

### Limits PeopleSoft Pages

Flexible method to limit access to certain pages

### Protects Web Services & Mobile

Detects and reacts to attacks against native web services (SOA, SOAP, REST) and mobile applications

### Two-factor Authentication (2FA/MFA)

Enables two-factor authentication for login, user, responsibility, or function

# AppDefend PeopleSoft Support

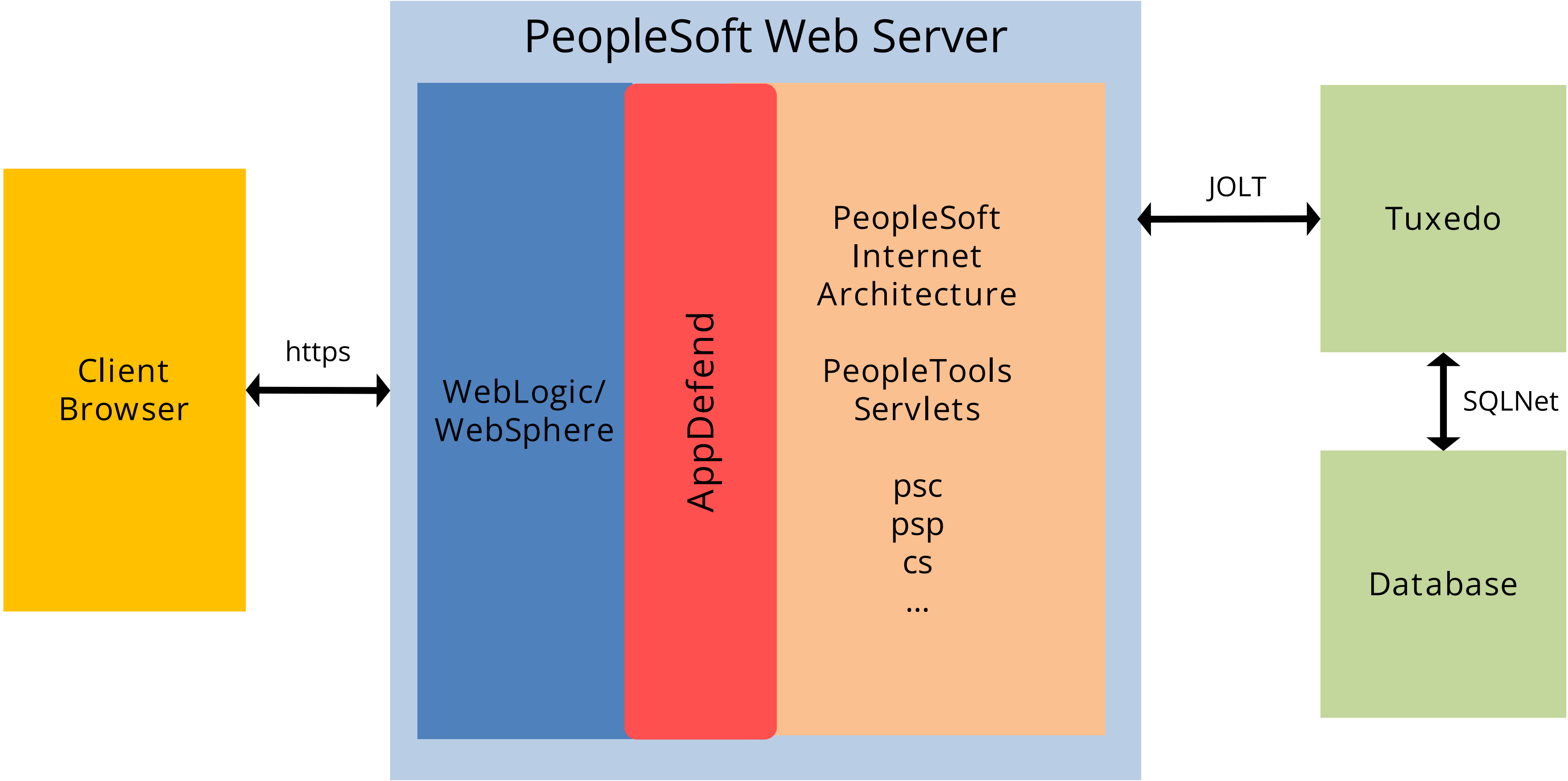
| | |
|---|---|
| Oracle PeopleSoft | ▪ 9.2<br>▪ 9.1 |
| Oracle PeopleTools | ▪ 8.50 – 8.60<br>▪ 8.50 minimum of JDK 1.6 |
| Operating Systems | Supported operating systems<br>▪ Linux x86 (Oracle Enterprise Linux; Red Hat Enterprise Linux AS/ES; SuSe)<br>▪ Sun SPARC Solaris<br>▪ Sun X64-64 Solaris<br>▪ HP PA-RISC HP/UX<br>▪ IBM AIX<br>▪ Microsoft Windows Server |

# AppDefend PeopleSoft WebSphere Support

As of February 14, 2018, Oracle has discontinued certification for WebSphere starting with PeopleTools 8.57.

- AppDefend supports WebSphere with PeopleTools 8.50 through 8.56.
- Starting with PeopleTools 8.57, AppDefend is not supported to run with WebSphere.

# AppDefend and PeopleSoft



- AppDefend runs within the WebLogic/WebSphere Java containers as a servlet filter and monitors all incoming requests and out-going responses. Being in the Java container, AppDefend can access all session state, attributes, error messages, and the database.

# AppDefend Virtual Patching

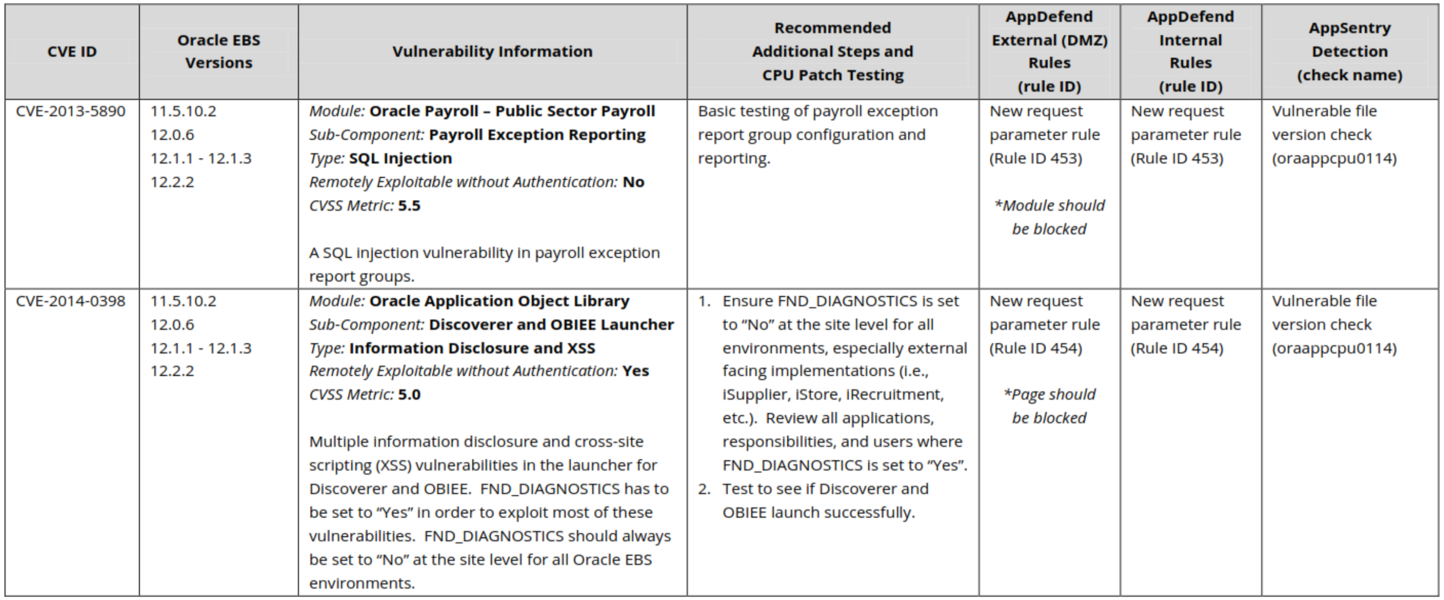
Eliminate risk and exploitation of the security bug by blocking access to the vulnerable code

- Integrigy analyzes the Oracle Critical Patch Update (CPU)
- Delivers pre-defined rules for CPU web bugs
- Rules may be at the page or field level to block known vulnerabilities
- Virtual patching for all PIA CPU patches
  - PeopleSoft patches
  - PeopleTools patches
  - WebLogic patches

# Integrigy Oracle CPU Analysis

For each quarterly Oracle CPU, Integrigy performs an analysis and updates the AppDefend rule set to include virtual patch rules for all external and internal web vulnerabilities

*Sample from Integrigy CPU Analysis*



| CVE ID | Oracle EBS Versions | Vulnerability Information | Recommended Additional Steps and CPU Patch Testing | AppDefend External (DMZ) Rules (rule ID) | AppDefend Internal Rules (rule ID) | AppSentry Detection (check name) |
|---|---|---|---|---|---|---|
| CVE-2013-5890 | 11.5.10.2<br>12.0.6<br>12.1.1 - 12.1.3<br>12.2.2 | *Module:* **Oracle Payroll – Public Sector Payroll**<br>*Sub-Component:* **Payroll Exception Reporting**<br>*Type:* **SQL Injection**<br>*Remotely Exploitable without Authentication:* **No**<br>*CVSS Metric:* **5.5**<br>A SQL injection vulnerability in payroll exception report groups. | Basic testing of payroll exception report group configuration and reporting. | New request parameter rule (Rule ID 453)<br>**Module should be blocked* | New request parameter rule (Rule ID 453) | Vulnerable file version check (oraappcpu0114) |
| CVE-2014-0398 | 11.5.10.2<br>12.0.6<br>12.1.1 - 12.1.3<br>12.2.2 | *Module:* **Oracle Application Object Library**<br>*Sub-Component:* **Discoverer and OBIEE Launcher**<br>*Type:* **Information Disclosure and XSS**<br>*Remotely Exploitable without Authentication:* **Yes**<br>*CVSS Metric:* **5.0**<br>Multiple information disclosure and cross-site scripting (XSS) vulnerabilities in the launcher for Discoverer and OBIEE. FND_DIAGNOSTICS has to be set to “Yes” in order to exploit most of these vulnerabilities. FND_DIAGNOSTICS should always be set to “No” at the site level for all Oracle EBS environments. | 1. Ensure FND_DIAGNOSTICS is set to “No” at the site level for all environments, especially external facing implementations (i.e., iSupplier, iStore, iRecruitment, etc.). Review all applications, responsibilities, and users where FND_DIAGNOSTICS is set to “Yes”.<br>2. Test to see if Discoverer and OBIEE launch successfully. | New request parameter rule (Rule ID 454)<br>**Page should be blocked* | New request parameter rule (Rule ID 454) | Vulnerable file version check (oraappcpu0114) |

# Deep Request Inspection™

Analyze all user provided input to identify and block malicious input

- Intelligent checking of ALL parameters, user input
- Uses best practice libraries for XSS and SQL injection detection
  - OWASP AntiSamy, Java HTML Sanitizer
  - OWASP ESAPI
- Malicious input may be detected, blocked, or sanitized

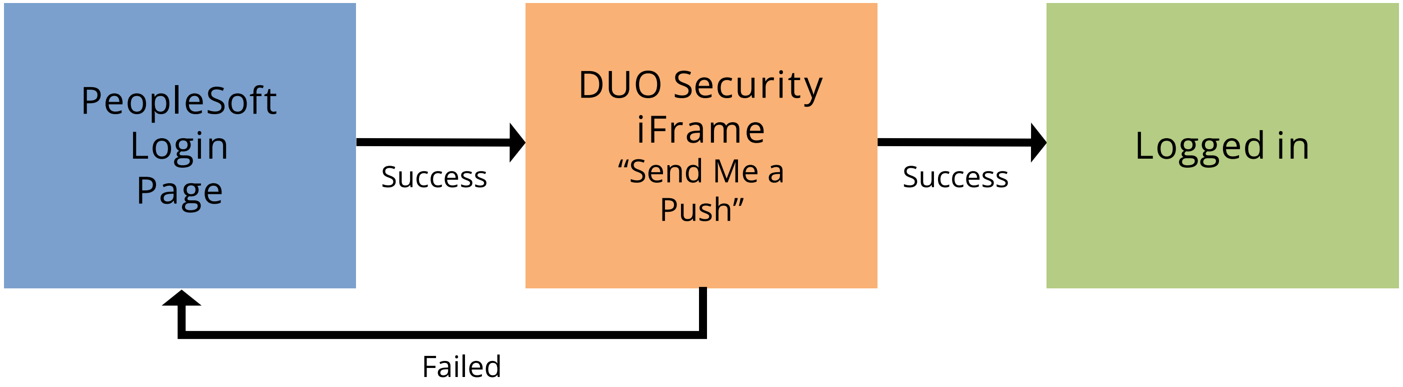
# Application Logging and Auditing

Log and audit key application and security events beyond Oracle EBS current capabilities

- Any page, action, parameter, session attribute may be logged or audited
- PCI logging includes all sessions, responsibilities, and potentially card number access through the application
- Log data can be sent to external systems such as Splunk, ElasticSearch, ArcSight, QRadar, LogRhythm, …
- Solves gaps in PeopleSoft logging

# AppDefend Adaptive Multi-Factor Authentication

AppDefend enables multi-factor authentication (MFA/2FA) for PeopleSoft using DUO Security, TOTP (Microsoft or Google Authentication), PKI Smartcards, and hardware/software tokens.



- Multi-Factor Authentication
  Enhances PeopleSoft login security by integrating with 2FA/MFA solution to provide secondary authentication

- Per Page or Role
  Require MFA when user selects or accesses specific pages, or roles through menus or directly

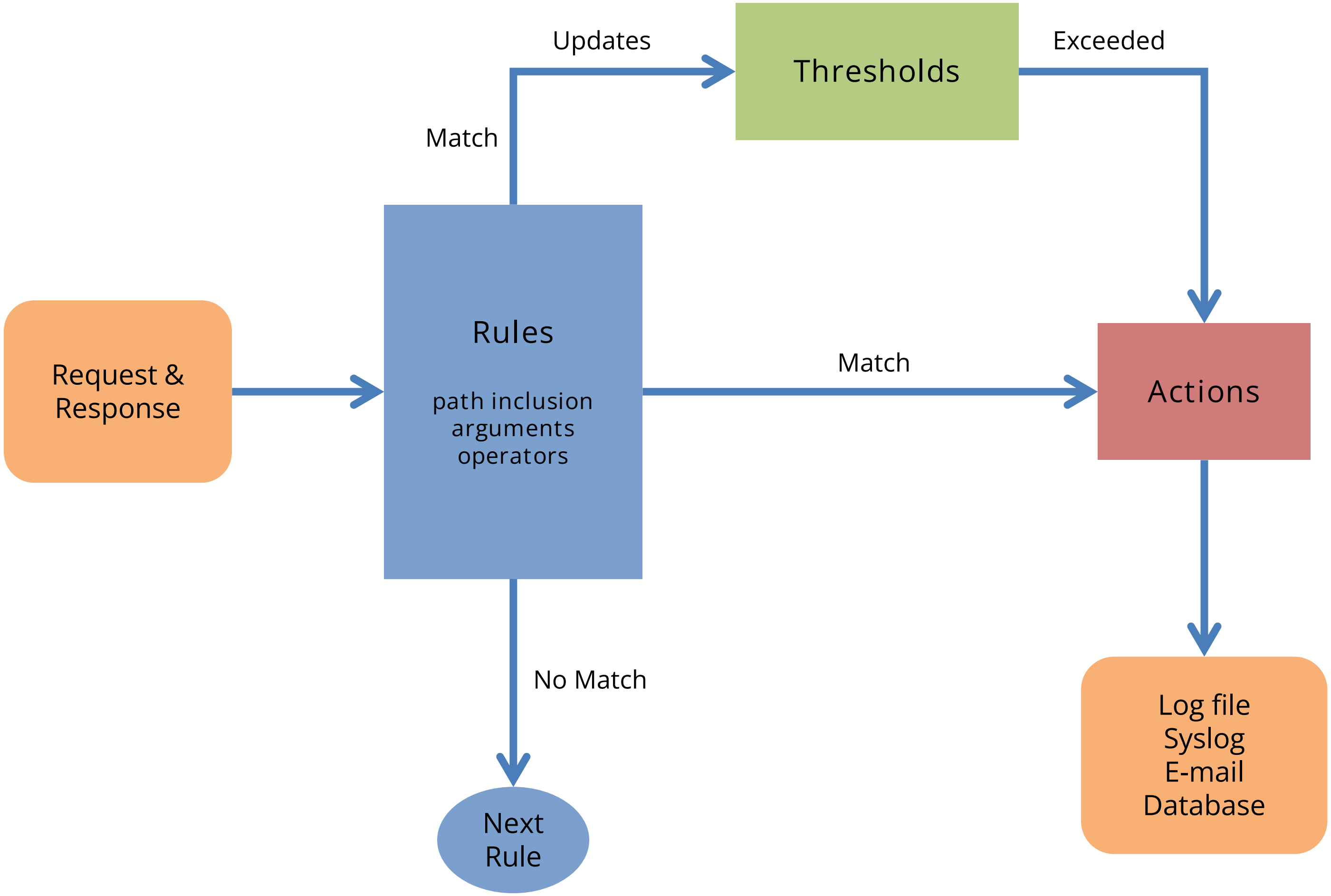
# AppDefend Features

| | |
|---|---|
| Configuration | ▪ Rules and configuration files use JSON notation<br>▪ XSS and ESAPI detection fully configurable<br>▪ Support for Single Server Domain and Multi Server Domain<br>▪ Dynamic reloading of configuration files – no restarting of the application server required |
| Logging and Alerting | ▪ Flexible formatting and destinations<br>▪ Destinations include files, syslog, e-mail, database<br>▪ Files with periodic or sized-based rotation, size limits<br>▪ Syslog with support for major logging platforms (Splunk, ArcSight, enVision, QRadar, etc.) |
| Resiliency | ▪ Fail open or closed upon internal errors<br>▪ Fail open or closed upon startup or configuration errors |

# AppDefend Installation and Updates

| | |
|---|---|
| Installation | ▪ One hour installation web sessions included with subscription – 15-minute install, 45-minute walk-through<br>▪ Download and install AppDefend binary and rules<br>▪ Customization AppDefend base configuration<br>▪ Configure filter definition<br>▪ Restart PIA web server |
| Updates | ▪ New rules and rule updates – quarterly or as needed<br>▪ Download and unzip appdefend.zip<br>▪ AppDefend dynamically reloads rules |
| Upgrades | ▪ New features and non-rule fixes – biannual or as needed<br>▪ Download and unzip appdefend.zip<br>▪ Restart PIA web server |

# AppDefend Processing



# AppDefend Arguments

AppDefend rules and alerts may use one or more of these arguments.

```
ps.user_name
ps.user_signon_name
request.attribute.<name>
request.attributes.names
request.auth_type
request.body_length
request.character_encoding
request.content_length
request.context_path
request.cookie.<name>
request.cookies.names
request.file_extension
request.file_name
request.header.<name>
request.headers.names
request.is_secure
request.line
request.local_addr
request.local_port
request.method
request.parameter.<name>
request.parameters.combined_size
request.parameters.get_names
request.parameters.get_values
request.parameters.names
request.parameters.put_names
request.parameters.put_values
request.parameters.values
request.path_info
request.path_translated
request.protocol
request.query_string
request.remote_addr
request.remote_host
request.remote_port
request.remote_user
request.scheme
request.server_name
request.server_port
request.servlet_path
request.servletcontext.<name>
request.session_id
request.uri
request.url
response.content
response.content_length
response.header.<name>
response.header.names
session.attribute.<name>
session.attributes.names
```

# AppDefend Operators

AppDefend rules can use any of these operators.

- `beginswith`
- `byterange`
- `contains`
- `notcontains`
- `endswith`
- `equals`
- `exists`
- `greater`
- `greatereq`
- `ingroup`
- `notingroup`
- `inlist`
- `notinlist`
- `ipmatch`
- `notipmatch`
- `less`
- `lesseq`
- `regex`
- `within`
- `notwithin`

# AppDefend Actions

| | |
|---|---|
| Log | Generates a log entry or alert to a file, syslog, e-mail |
| Redirect | Redirects the request to a specified full URL or relative URL for the site such as the Oracle EBS error page |
| Block | Block the request by returning the specified HTTP error code such as 403 Forbidden |
| Pause | Pause the request for the specified number of milliseconds perhaps to slow down a brute force attack |
| Sanitize | Sanitize one or all parameters and headers in the request to prevent XSS, HTML injection, or SQL injection |
| Stop | Stop the processing of all subsequent AppDefend rules.  The Stop action is useful to minimize AppDefend analyzing static request such as images, etc. |
| DoNothing | This action will do nothing as an action |

# Agenda

1 Web Application Security

2 PeopleSoft Web Architecture

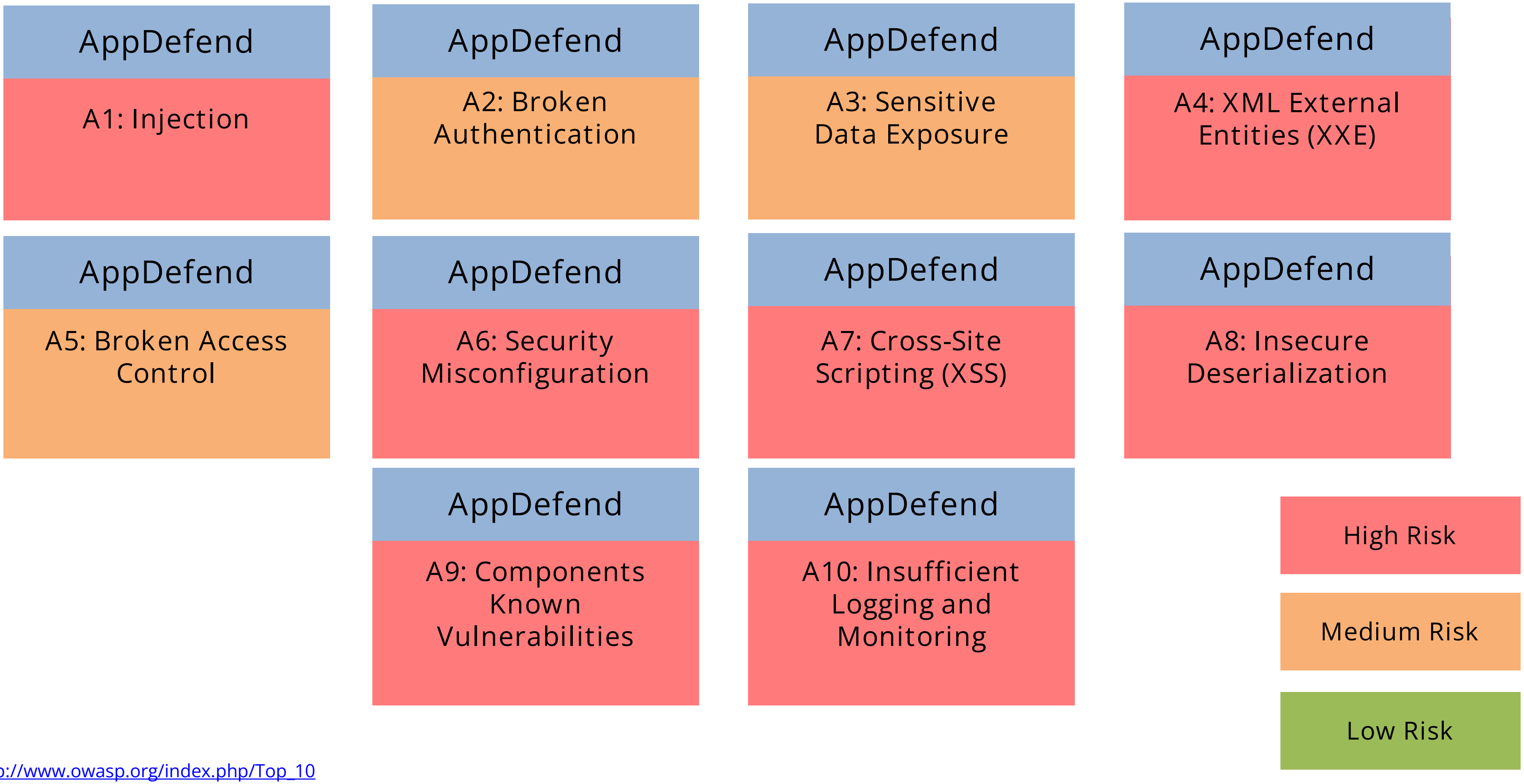
3 AppDefend Overview

4 **AppDefend Benefits**

5 Q & A

# OWASP Top 10 – AppDefend

AppDefend is the layer of defense for PeopleSoft against OWASP Top 10 security vulnerabilities.



AppDefend
🟥 A1: Injection
AppDefend
🟧 A2: Broken Authentication
AppDefend
🟧 A3: Sensitive Data Exposure
AppDefend
🟥 A4: XML External Entities (XXE)
AppDefend
🟧 A5: Broken Access Control
AppDefend
🟥 A6: Security Misconfiguration
AppDefend
🟥 A7: Cross-Site Scripting (XSS)
AppDefend
🟥 A8: Insecure Deserialization
AppDefend
🟥 A9: Components Known Vulnerabilities
AppDefend
🟥 A10: Insufficient Logging and Monitoring
🟥 High Risk
🟧 Medium Risk
🟩 Low Risk

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

# Integrigy Contact Information

Integrigy Corporation

web – www.integrigy.com

e-mail – info@integrigy.com

blog – integrigy.com/oracle-security-blog

youtube – youtube.com/integrigy