



Don't Write Your Own Security Code – The Enterprise Security API Project

OWASP

Jeff Williams

Aspect Security CEO

Volunteer Chair of OWASP

jeff.williams@aspectsecurity.com

modified by app@iki.fi

Copyright © 2009 - The OWASP Foundation

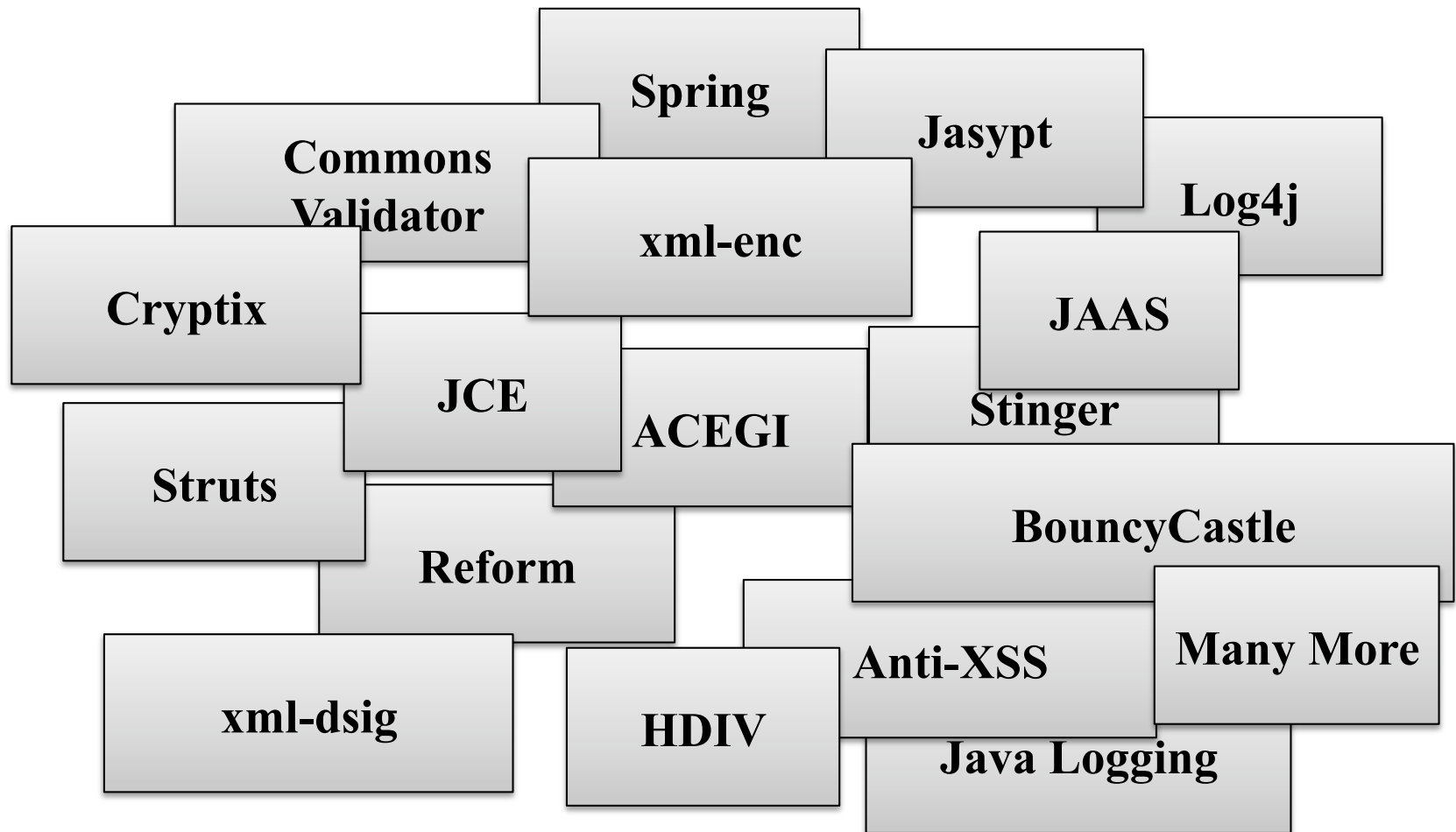
This work is available under the Creative Commons SA 3.0 license

The OWASP Foundation

<http://www.owasp.org>



The Challenge...



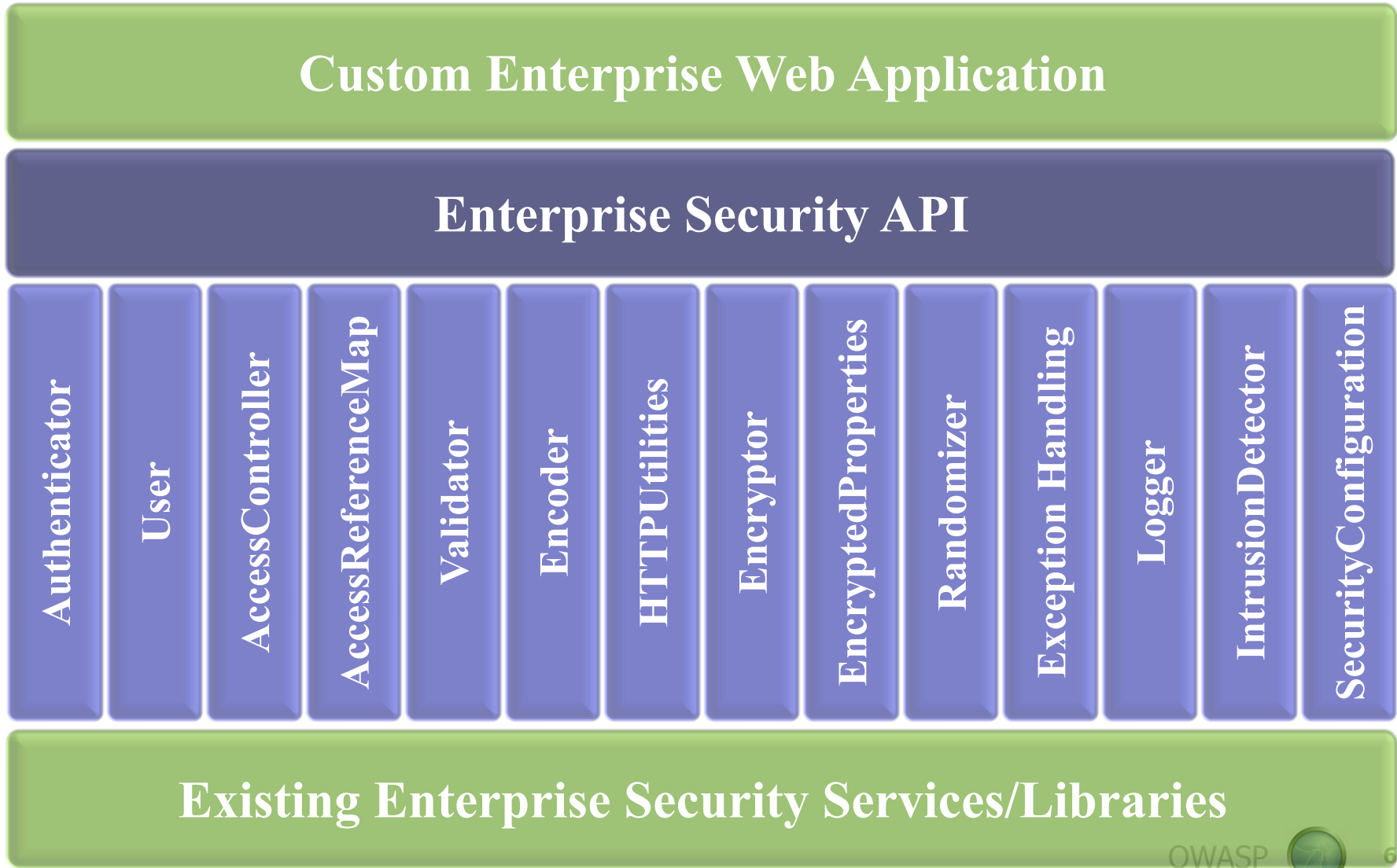
Philosophy

- Using security controls is different from building
 - ▶ All the security guidelines, courses, tutorials, websites, books, etc... are all mixed up because everyone builds their own controls
- Most developers shouldn't build security controls
 - ▶ When to use a control
 - ▶ How to use a control
 - ▶ Why to use a control (maybe)
- Most enterprises need the same set of calls

Design

- Only include methods that...
 - ▶ Are widely useful and focus on the most risky areas
- Designed to be simple to understand and use
 - ▶ Interfaces with concrete reference implementation
 - ▶ Full documentation and usage examples
- Same basic API across common platforms
 - ▶ Java EE, .NET, PHP, others?
 - ▶ Useful to Rich Internet Applications?

Architecture Overview



Create Your ESAPI Implementation

■ Your Security Services

- ▶ Wrap your existing libraries and services
- ▶ Extend and customize your ESAPI implementation
- ▶ Fill in gaps with the reference implementation

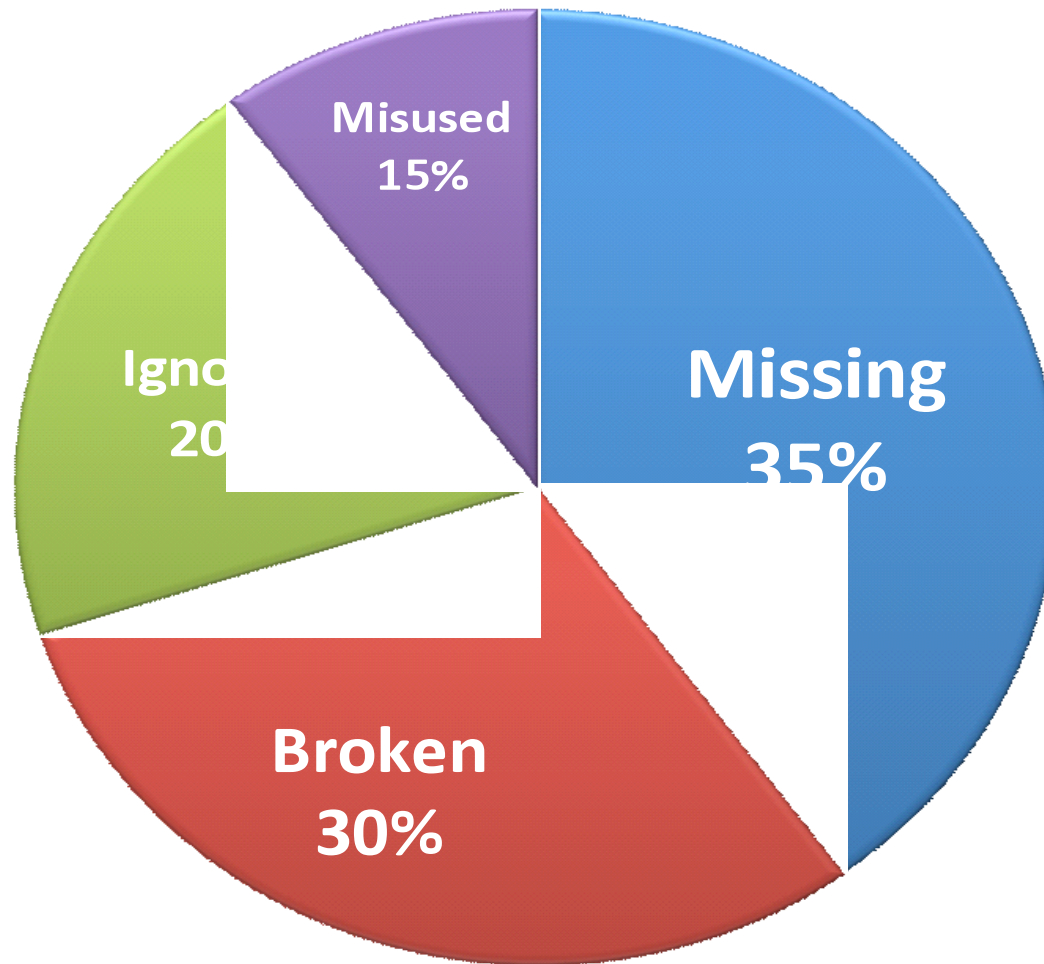
■ Your Coding Guideline

- ▶ Tailor the ESAPI coding guidelines
- ▶ Retrofit ESAPI patterns to existing code

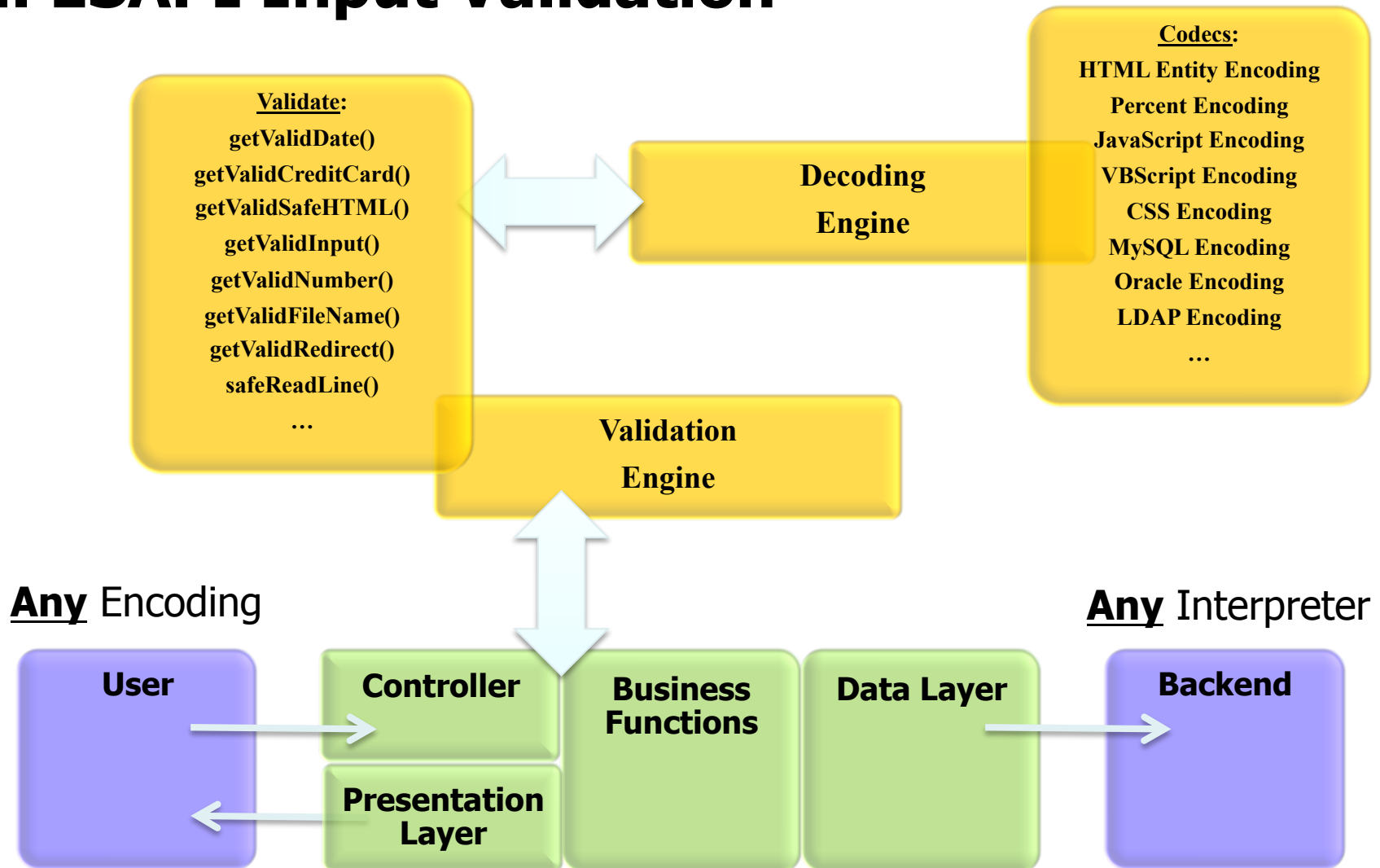
Frameworks and ESAPI

- ESAPI is NOT a framework
 - ▶ Just a collection of security functions, not “lock in”
- Frameworks already have some security
 - ▶ Controls are frequently missing, incomplete, or wrong
- ESAPI Framework Integration Project
 - ▶ We’ll share best practices for integrating
 - ▶ Hopefully, framework teams like Struts adopt ESAPI

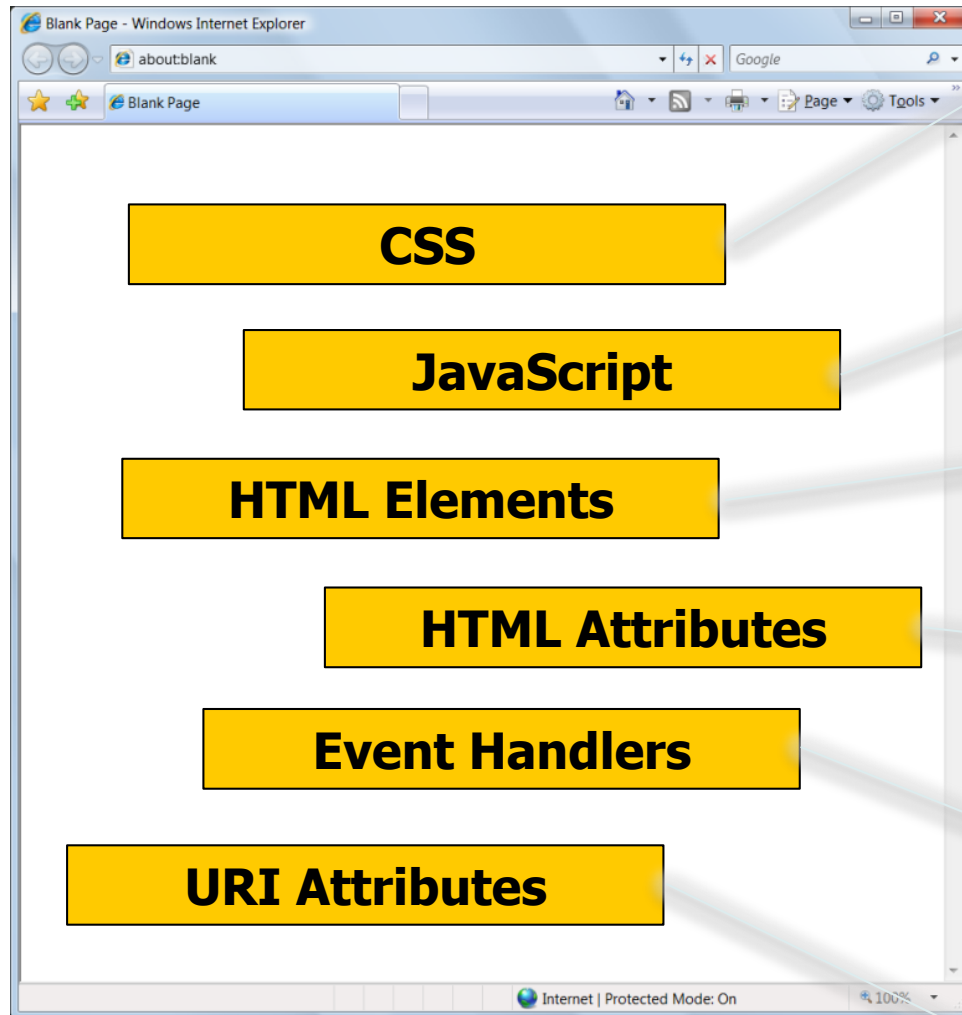
Vulnerabilities and Security Controls



1. ESAPI Input Validation



HTML Execution Contexts



`\any \xHH \uHHHH \000 (octal)`

`\specials \xHH \uHHHH`

`&#DD &#xHH &entity;`

`" ' &#DD &#xHH`

`" ' \specials \xHH \uHHHH`

`%HH`

ESAPI Swingset

The image shows two browser windows side-by-side. The left window is Mozilla Firefox displaying the ESAPI SwingSet Demonstration Application beta. The right window is Windows Internet Explorer displaying the ESAPI SwingSet - XSS: Insecure application.

ESAPI SwingSet Demonstration Application beta - Mozilla Firefox

- ESAPI SwingSet Demonstration
- Input Validation, Encoding, and Injection
 - Output User Input
 - Accept Rich Content
 - Validate User Input
 - Encode Output
- Authentication and Session Management
 - Login
 - Change Password
 - Change Session Identifier
- Access Control and Referencing Objects
 - Reference a Server-Side Object
 - Access Control
- Encryption, Randomness, and Integrity
 - Encryption
 - Randomizer
 - Integrity Seals
 - Globally Unique IDs
- Caching

ESAPI SwingSet - XSS: Insecure - Windows Internet Explorer

ESAPI Swingset - XSS: Insecure

Home | Tutorial | **Insecure Demo** | Secure Demo

Exercise

RULE #0 - Never Insert Untrusted Data Except in Allowed Locations

Only put untrusted data in the five approved locations! Not into a script:

- 50; alert('xss0')

Don't put untrusted data in a script

```
<html><body>data<script>var i= 50;alert('xss0') ;</script></body></html>
```

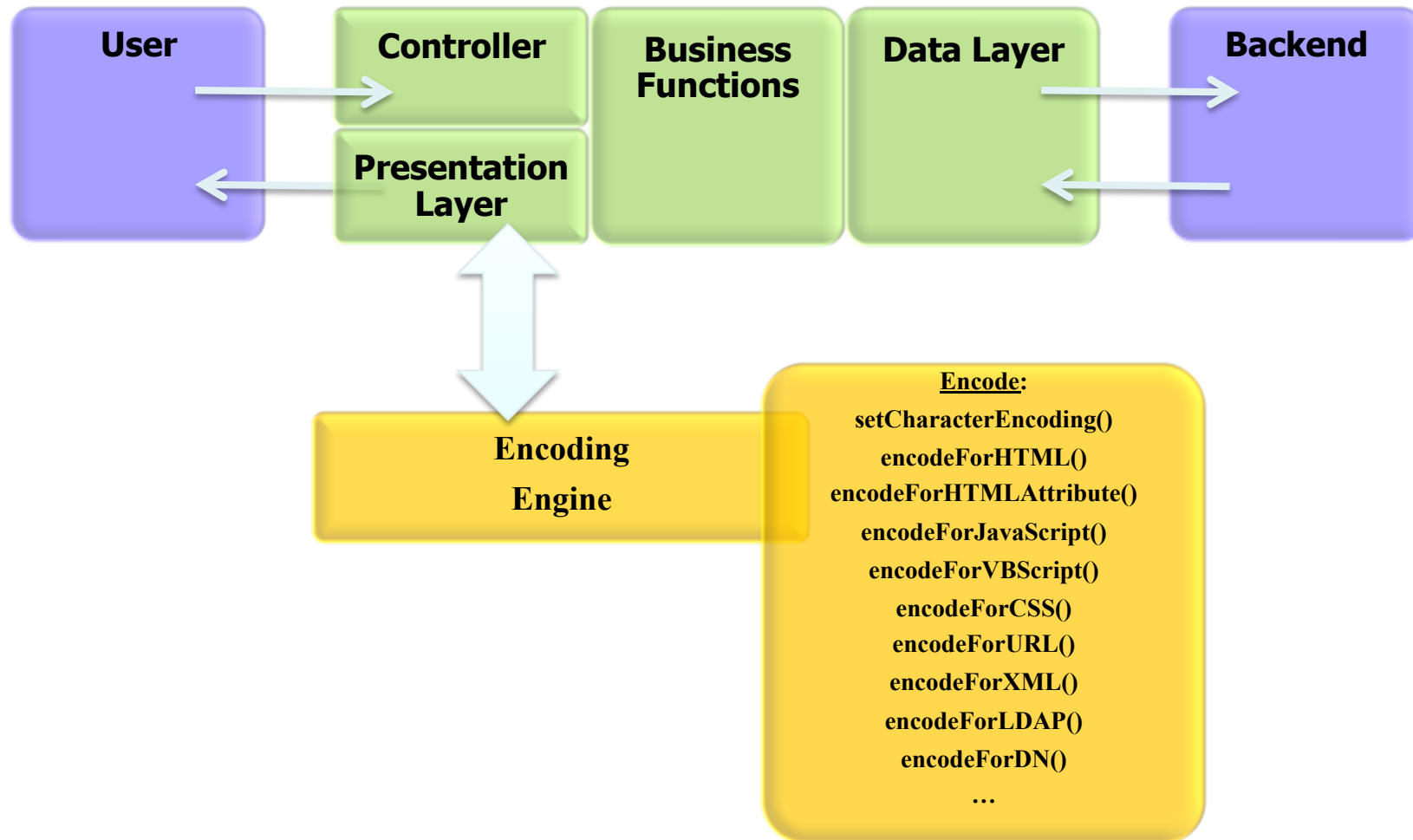
data

RULE #1 - HTML Escape Before Inserting Untrusted Data into HTML Element Content

Normal Element Content, common attacks are:

http://www.owasp.org/index.php?title=XSS_Prevention

2. ESAPI Output Encoding



Applications Enjoy Attacks

Live Search

YouTube

500 Internal Server Error

Sorry, something went wrong.

A team of highly trained monkeys has been assigned to investigate this incident to customer service.

Also, please include the following information:

w5kck2L-bQm72LN0wtTK_Z37nvZ88g
qWxJ-y2Fb3iM9Kdp1j1_Z27QJvTiR4-
IPm1T0WyJuUxMjBkdLZUeyQoAFUZXW
L3Ky6vHb51_U4F-D2LJVm3B8x8K2uJ
BoFdz_yL8Gn9FRPYGAgDdyWHc3eC7xgBS_17RyeyXpB2fvG8QTp14XQ0eL5N
2bdh6BN2aNdLNceDIw1VvqQ76TWOFl1Qwmhwf98tFJmRe5QqfayuxhB7oQ4i
bMY59pDNW6HzibDbb2JUimdvtTlxW65YmoWa_FJlmlvSF6yIt8e_EURzA7XZ
RTIiJmQ-Cw1xYOK7qtnpqs0ZBXDpJlGBFoNtMB2e0P_YjeFXnFz-7mah4KHcU
Wh7qo2DhPQ-fSbgXR99HnzREgOB_Y75gpWJ--1Tc0KXhjj80M7SnuIK5sHe
DNWdas9qzWmv3qSAEKLIJzaKGS3E3C_JiCLT1qchqnoe96y1ogMW1gVhtM7M6
7vV1PQJevLNddngV54mzaZJcuaVw6OV619CfUjWD0mX1gK3at1wLn7ODVUoP
AEqkAa8abB1kcFN2zaNfwa435aZVoj_K3oQ8SfMuXaOupkapob913Vj0-Qc
Y_bmEiCq1V8UL0ZS1mHkvfjh8xRfIo0dDvXxvmPJK49bvklmaw327Iq79aQc
TfevuHptE_xexYp1LeQhpM8aBLf0tN0kELVry-Uc61fqfGOkteI_HWceLyEo
XumZtaN7Y62pUb366pgOgseRbjolIx3DpuwGQdwZrzRh_vTyuwt5hw41N1-
pF1IyQ4XRDCN3UYon7I7pDNBk_4TJpDuE2WJCPya4Iw8lQ44dh-qyNLEq-4e
o6hcHQAR16GqoER831A31MqTMTJhtck1LdVh-HARNQ6qOoveRRRk1awGXEOE
dFOX6nh_ip12CIVvbQB9Ltw1GStk66FL5ag_-qRfVYxgxm2M0n_0GGEDE
QeShdOqrTurPfhmdYo5UarzaQ2n_apbe8ePDM5o9KVLz03w
tJbt_SbM9FJ4b7w2SuHm5vp1yeDeaMeMgwYqWVinp210_gw_Y
Hduo8jas8tzH1wWv0kzcoIGDUhY164mOSSzL1t17qoGCHGKIt
OjquiyBtYpJL1WN6eR_d17-p02rw62zdreQ5aUFWxK99ArMYI
Yp4=

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the [Back](#) button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to [Microsoft Product Support Services](#) and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup, Common Administrative Tasks, and About Custom Error Messages**.



Blogger

http://www.blogger.com - Apache Tomcat/4.1.24 - Error report - Mozilla Firefox

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

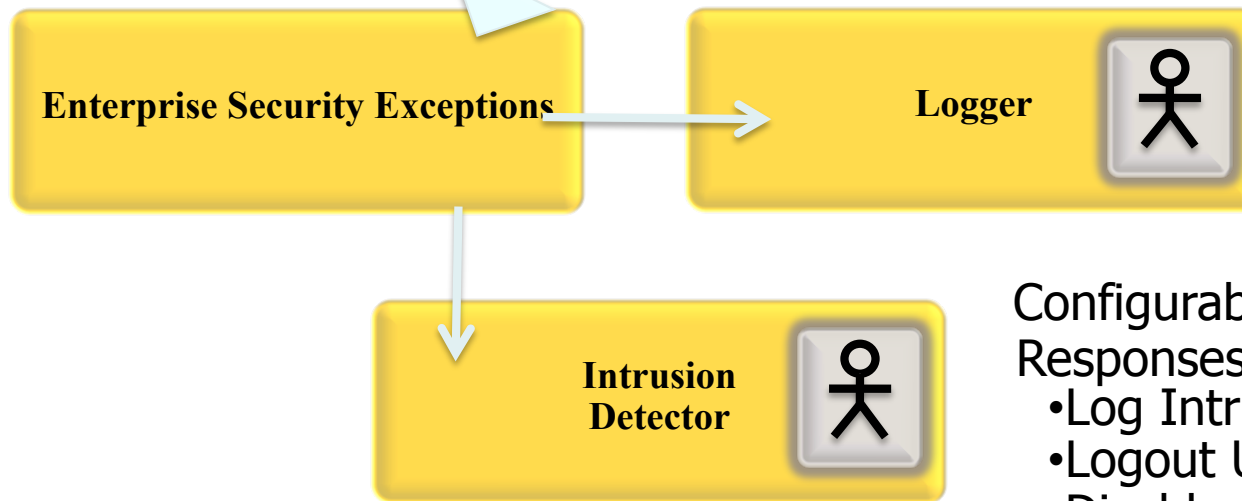
```
javax.servlet.ServletException: Servlet execution threw an exception
    at org.apache.catalina.core.ApplicationFilterChain.internal
    at org.apache.catalina.core.ApplicationFilterChain.doFilter
    at org.apache.catalina.core.StandardWrapperValve.invoke (Sta
    at org.apache.catalina.core.StandardPipeline$StandardPipeli
    at org.apache.catalina.core.StandardPipeline.invoke (Standar
    at org.apache.catalina.core.ContainerBase.invoke (ContainerB
    at org.apache.catalina.core.StandardContextValve.invoke (Sta
    at org.apache.catalina.core.StandardPipeline$StandardPipeli
    at org.apache.catalina.authenticator.AuthenticatorBase.invo
    at org.apache.catalina.core.StandardPipeline$StandardPipeli
    at org.apache.catalina.core.StandardPipeline.invoke (Standar
    at org.apache.catalina.core.ContainerBase.invoke (ContainerB
```

Done PR:n/a Adblock

3. Errors, Logging, and Detection

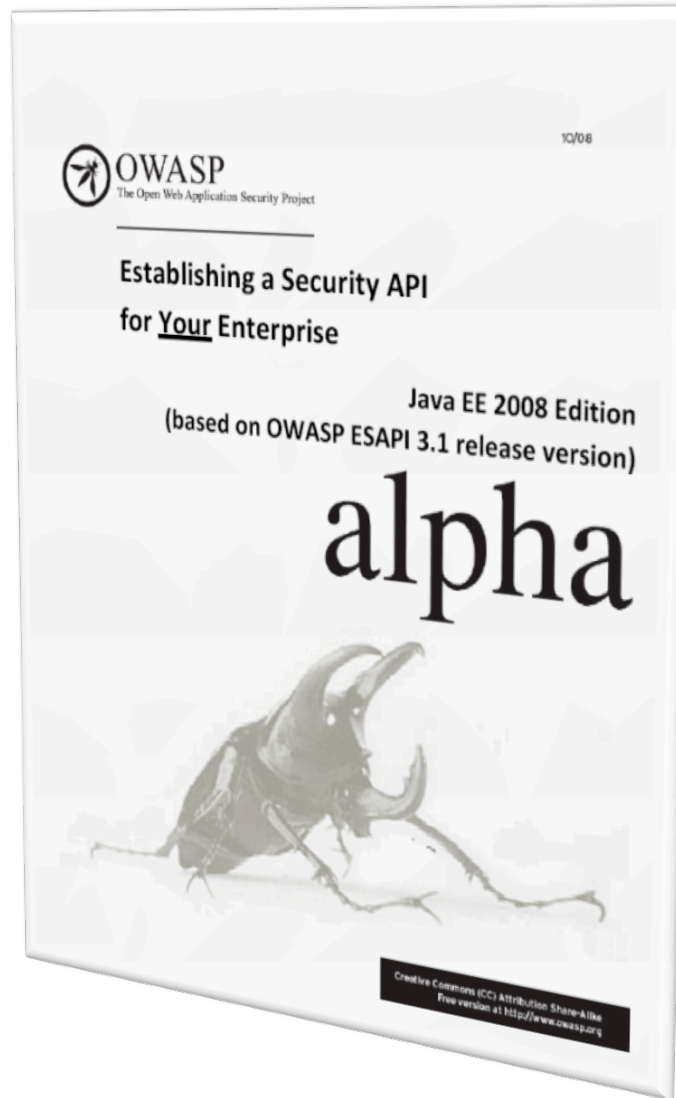


`throw new ValidationException("User message", "Log message");`



- Configurable Thresholds
Responses
- Log Intrusion
 - Logout User
 - Disable Account

ESAPI Book!



http://www.owasp.org/images/7/79/ESAPI_Book.pdf

Closing Thoughts

- I am learning an amazing amount (I thought I knew)
- An ESAPI is a key part of a balanced breakfast
 - ▶ Build rqmts, guidelines, training, tools around your ESAPI
- Secondary benefits
 - ▶ May help static analysis do better
 - ▶ Enables security upgrades across applications
 - ▶ Simplifies developer training
- Next year – experiences moving to ESAPI

Questions and Answers

- Rollout strategy?
- Integrating existing security libraries?
- Technical questions?

Contact Information:

Jeff Williams

jeff.williams@aspectsecurity.com

Work: 410-707-1487

Main: 301-604-4882