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

OWASP

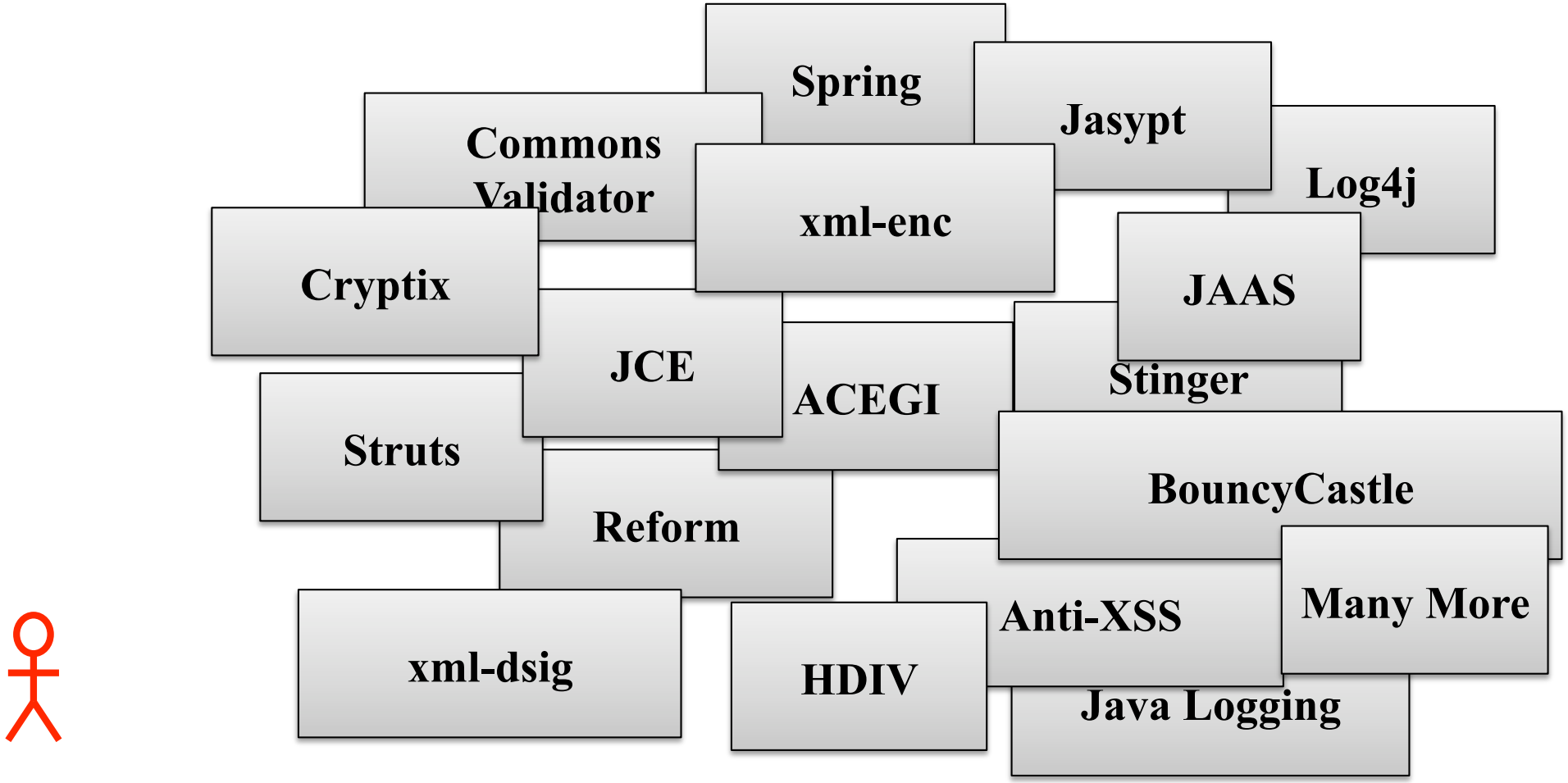
Jeff Williams
Aspect Security CEO
Volunteer Chair of OWASP
jeff.williams@aspectsecurity.com

modified by app@iki.fi

The OWASP Foundation
http://www.owasp.org


الله
يارب
علي
علي
الغلي

The Challenge…



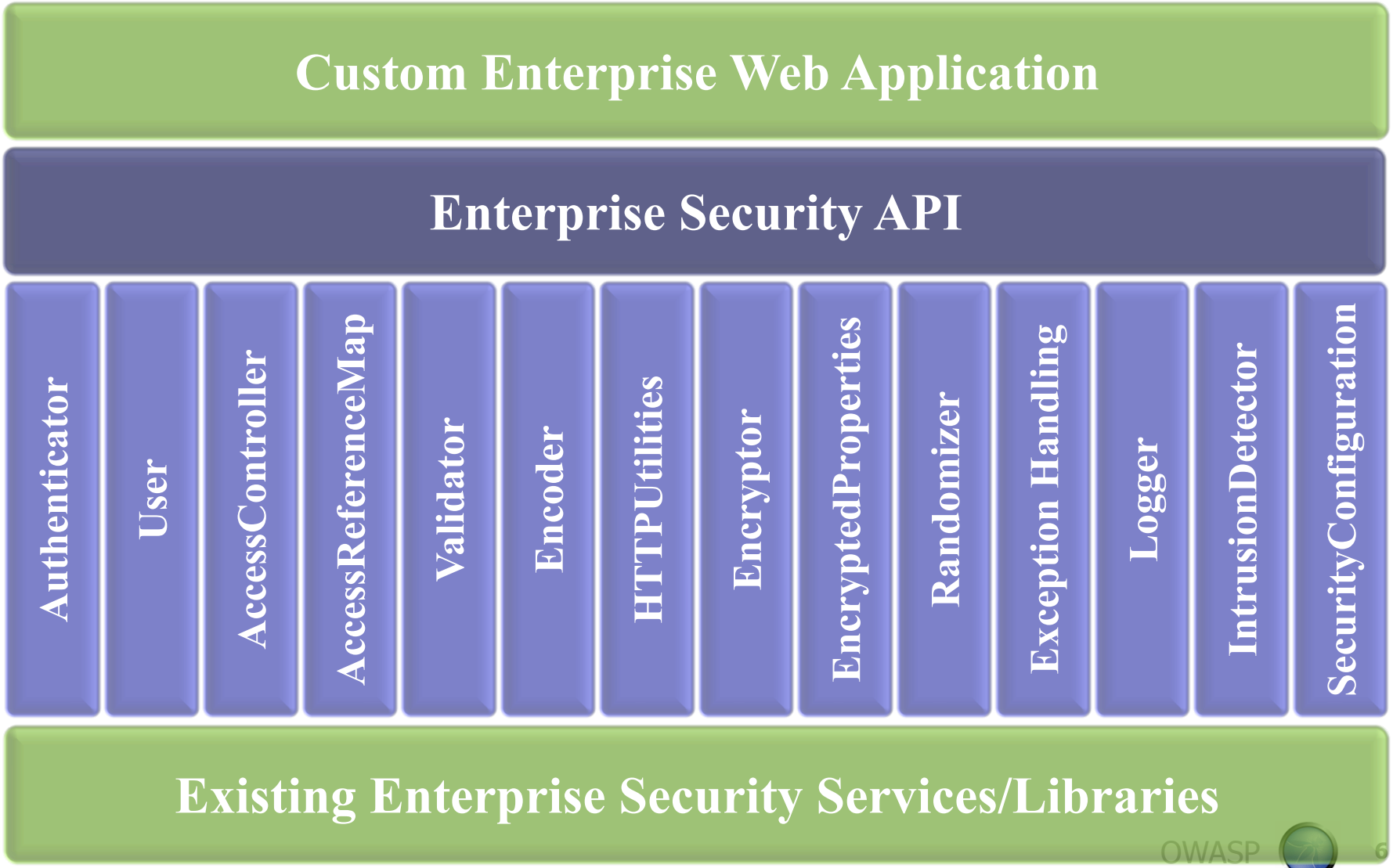
Philosophy

- 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



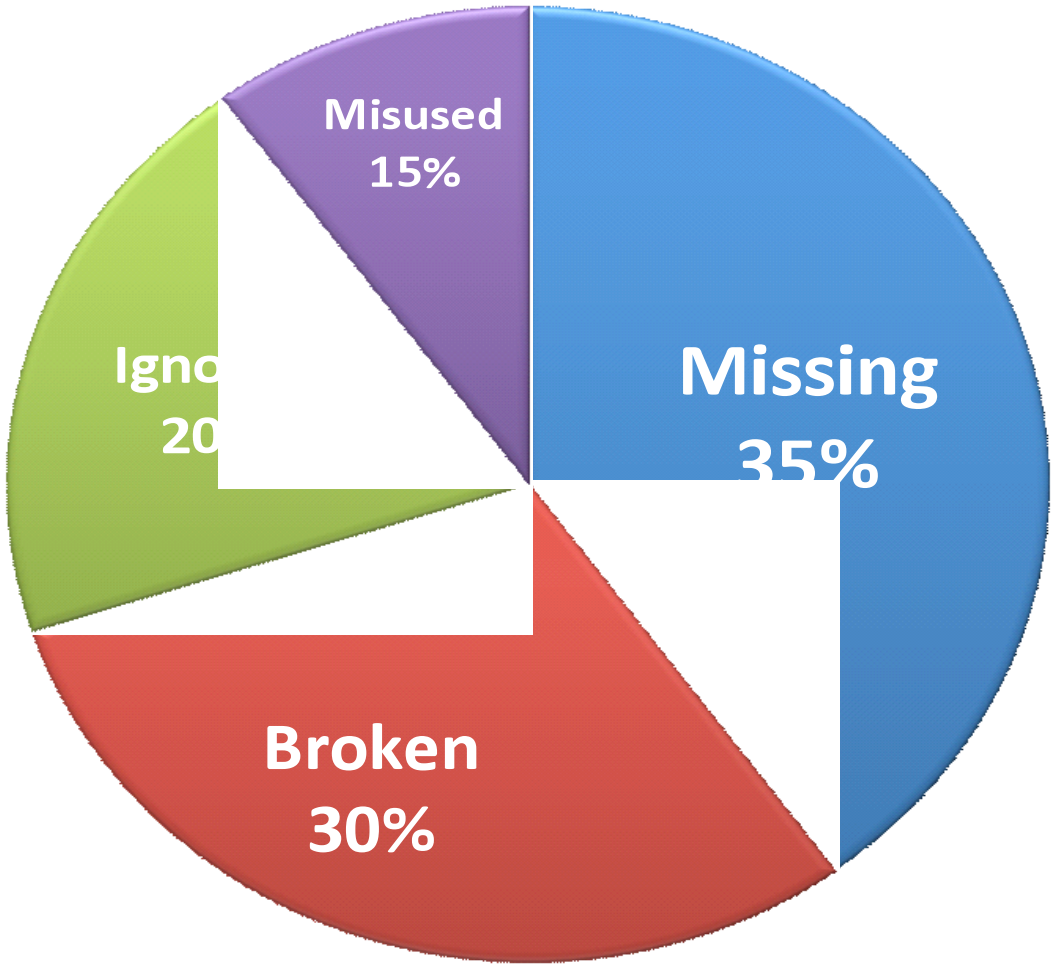
Create Your ESAPI Implementation

- 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



Web Escaping and Encoding

<

Percent Encoding
%3c
%3C

HTML Entity Encoding
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
<
<
<
<
<
<
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
<
<
<
<
<
<
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
<
<
<
<
<
<
&lt
&lT
&Lt
&LT
<
&lT;
≪
<

JavaScript Escape
\<
\x3c
\X3c
\u003c
\U003c
\x3C
\X3C
\u003C
\U003C

CSS Escape
\3c
\03c
\003c
\0003c
\00003c
\3C
\03C
\003C
\0003C
\00003C

Overlong UTF-8
%c0%bc
%e0%80%bc
%f0%80%80%bc
%f8%80%80%80%bc
%fc%80%80%80%80%bc

US-ASCII
¼

UTF-7
+ADw-

Punycode
<-

Simple Double Encoding
< --> < --> &#26;lt&#59 (double entity)
< --> %3c --> %253c (double percent)
etc...

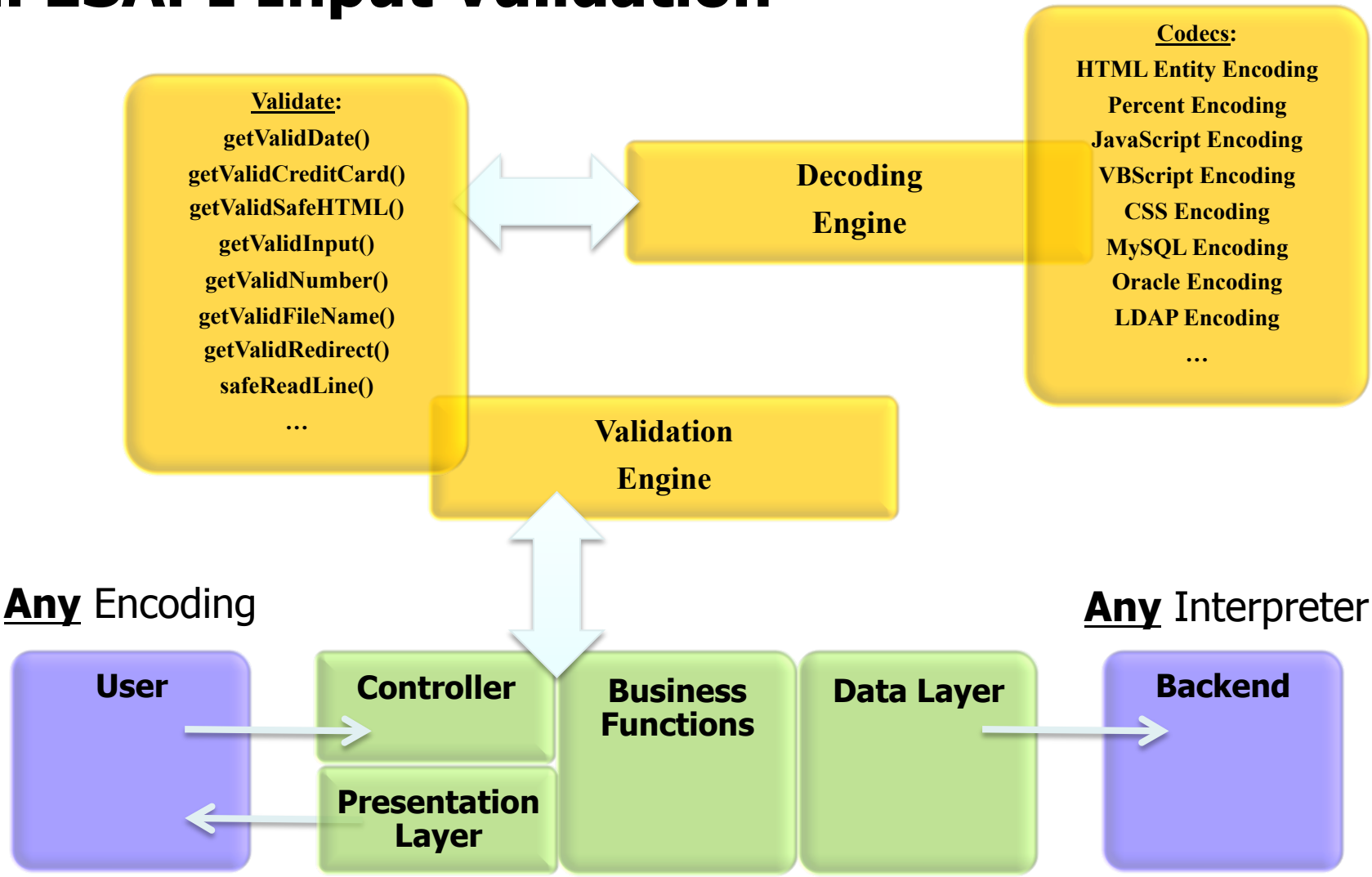
Double Encoding with Multiple Schemes
< --> < --> %26lt%3b (first entity, then percent)
< --> %26 --> &#25;26 (first percent, then entity)
etc...

Simple Nested Escaping
< --> %3c --> %%33%63 (nested encode percent both nibbles)
< --> %3c --> %%33c (nested encode first nibble percent)
< --> %3c --> %3%63 (nested encode second nibble percent)
< --> < --> &&108;t; (nested encode l with entity)
etc...

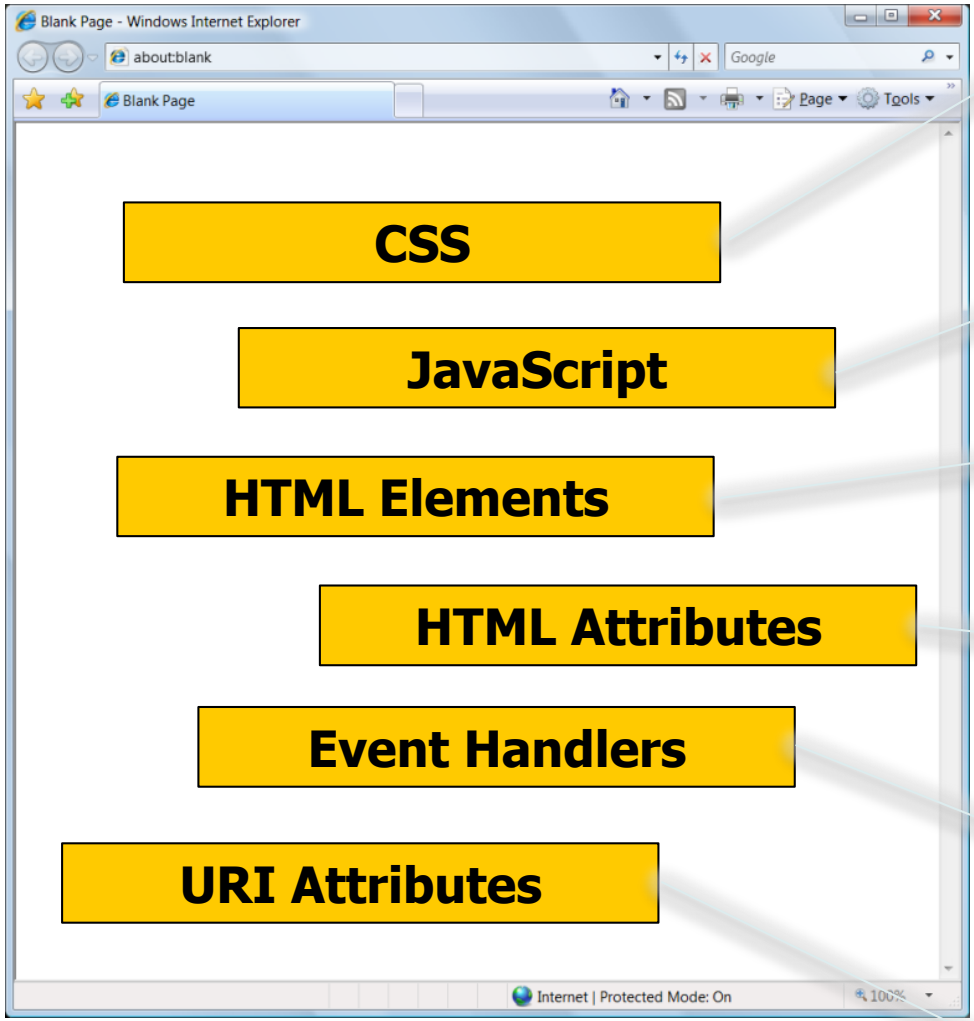
Nested Escaping with Multiple Schemes
< --> < --> &%6ct; (nested encode l with percent)
< --> %3c --> %3c (nested encode 3 with entity)
etc...

1,677,721,600,000,000
ways to encode <script>

1. ESAPI Input Validation



HTML Execution Contexts



\any \xHH \uHHHH \000 (octal)

\specials \xHH \uHHHH

&#DD &#xHH &entity;

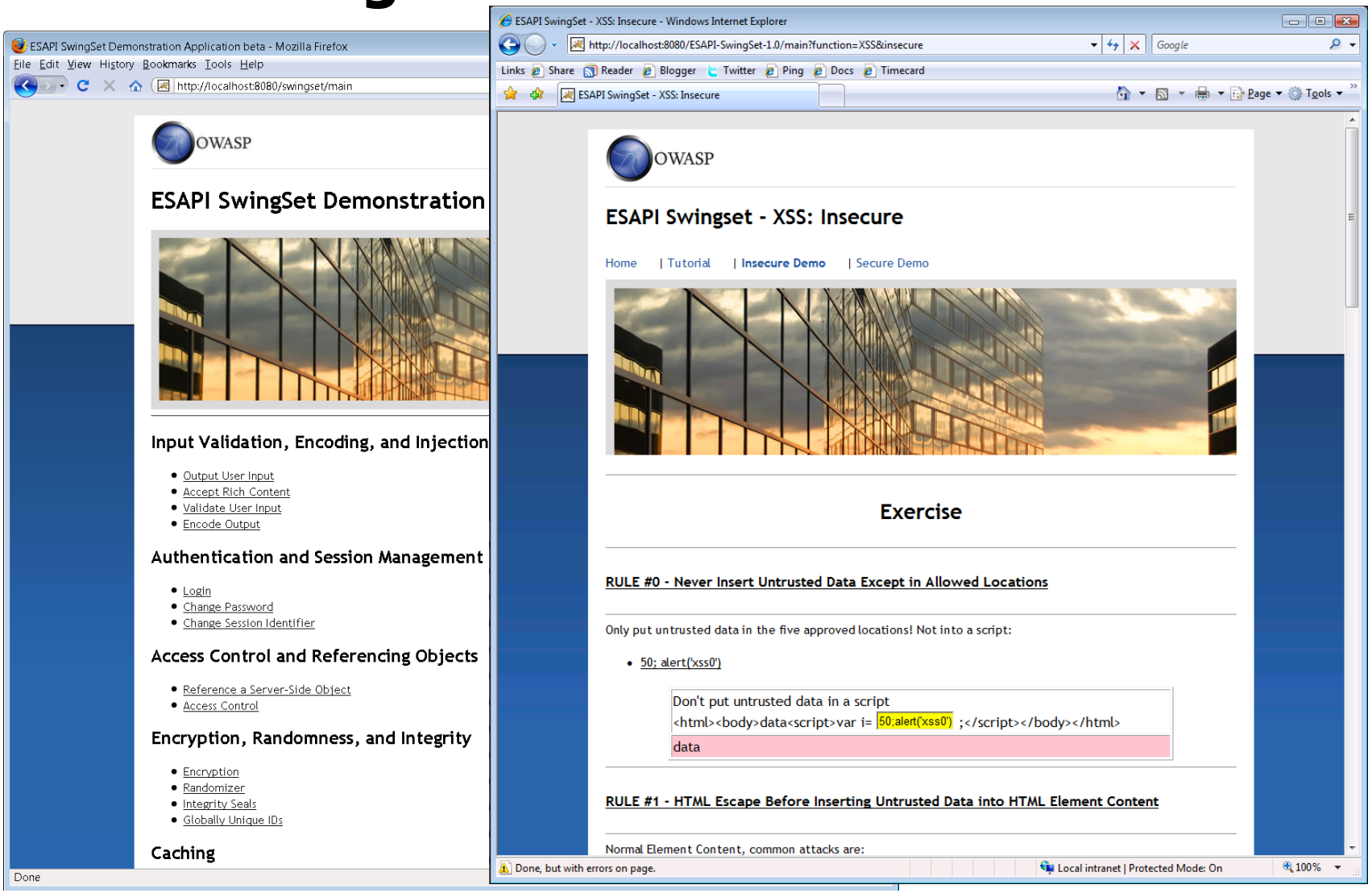
" ' &#DD &#xHH

" ' \specials \xHH \uHHHH

%HH

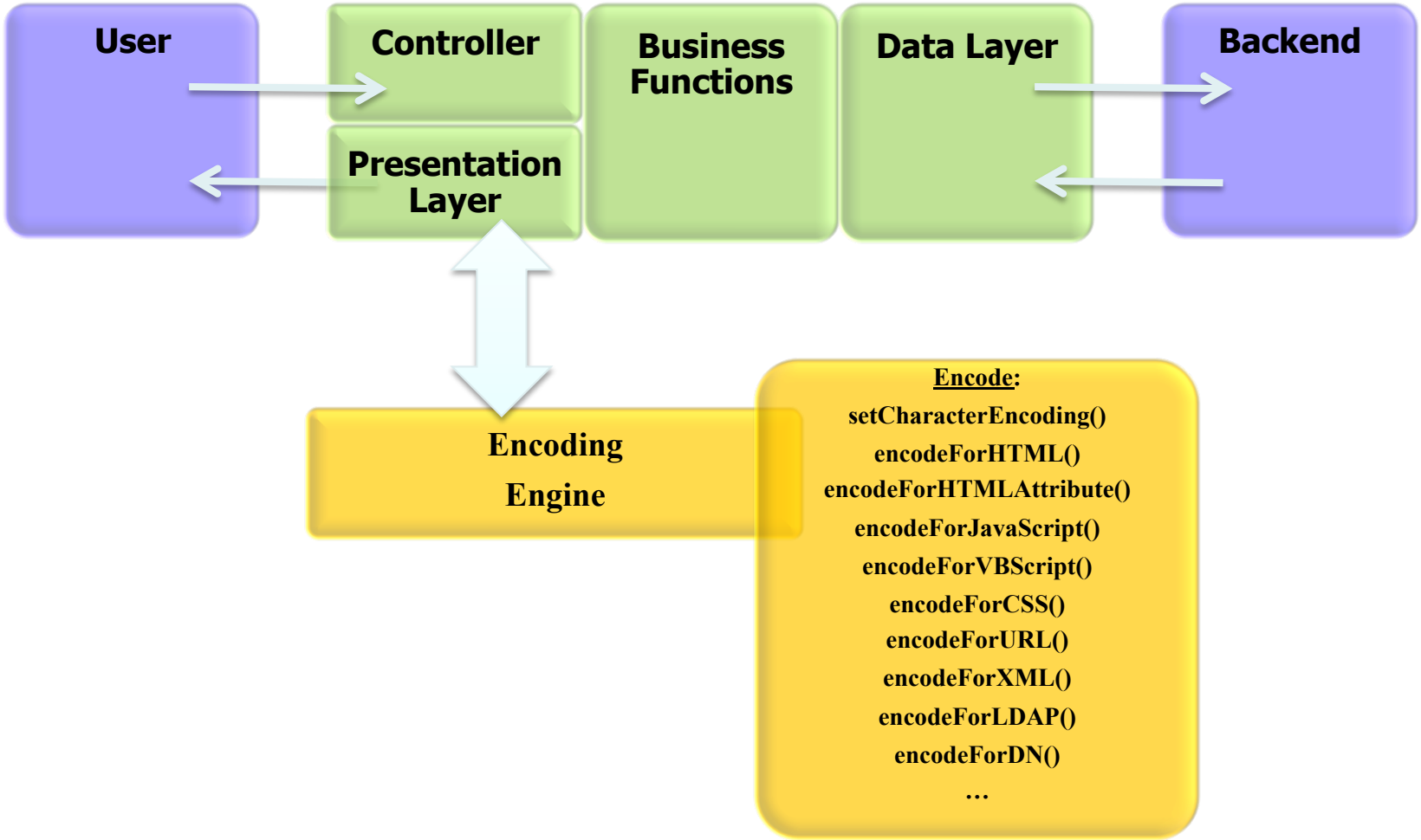
OWASP

ESAPI Swingset



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

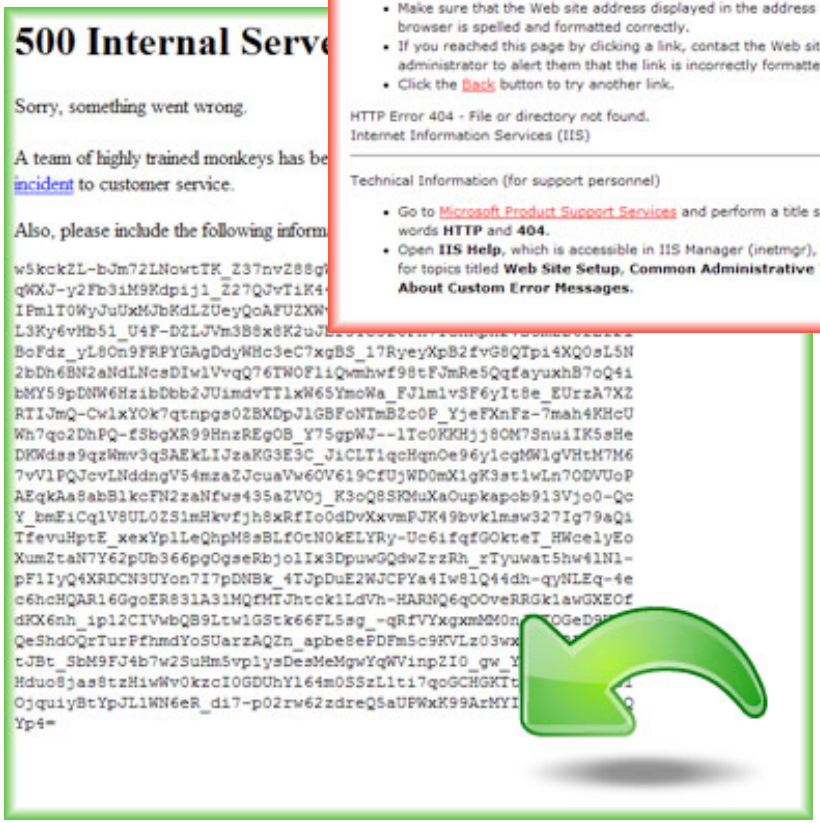
2. ESAPI Output Encoding

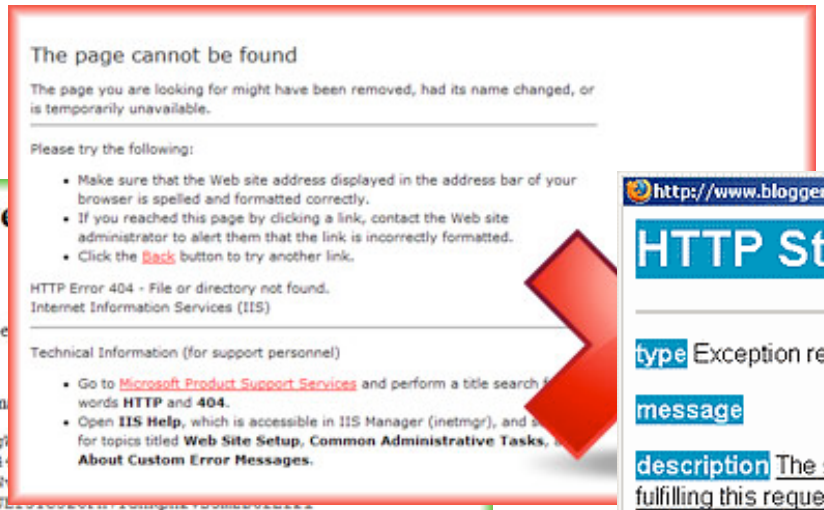


Applications Enjoy Attacks

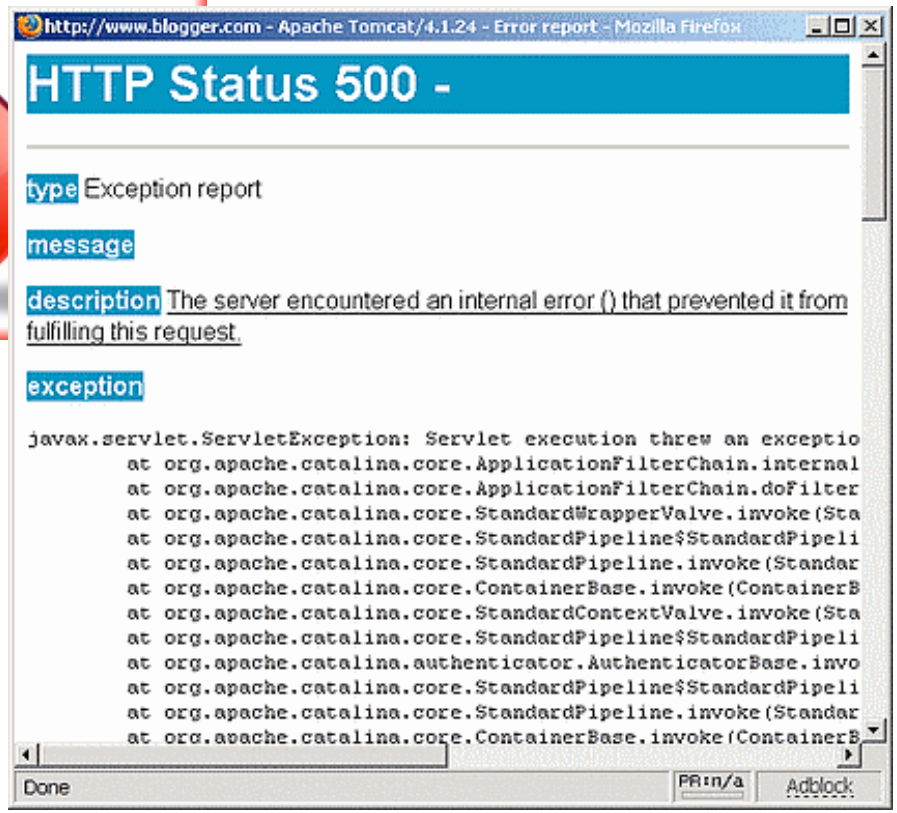
Live Search

YouTube

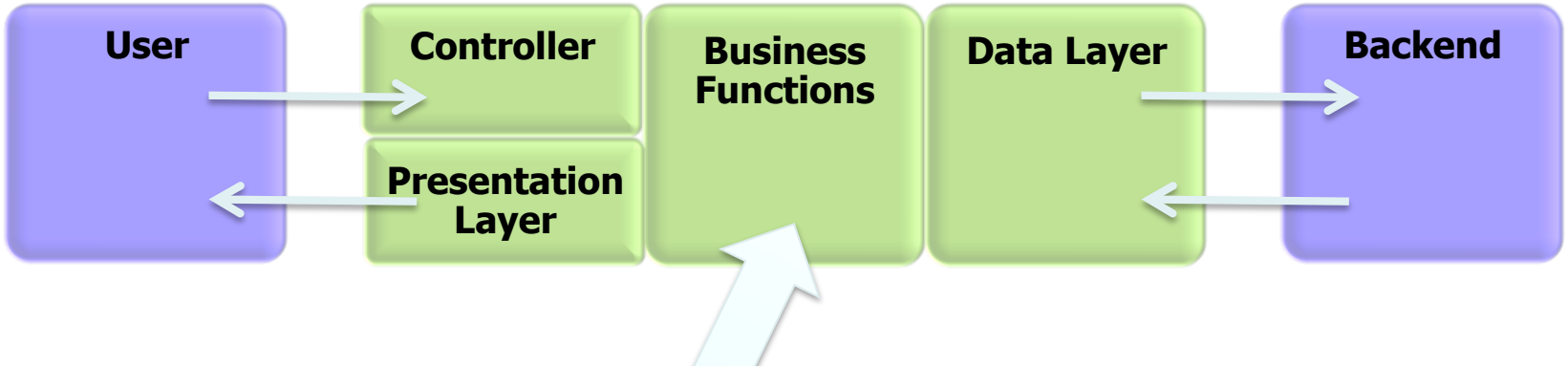




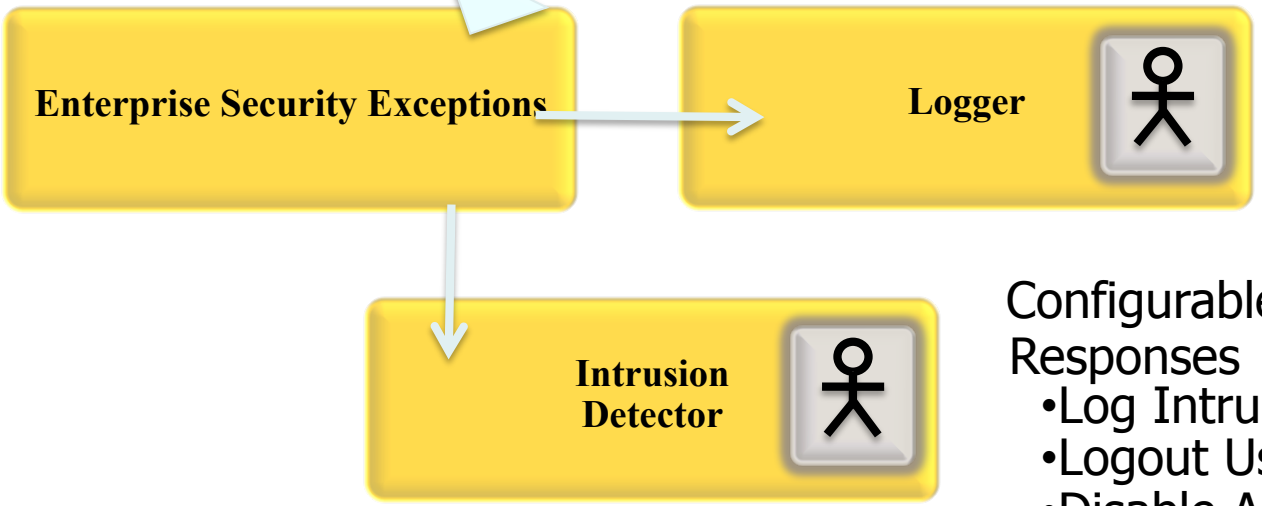
Blogger



3. Errors, Logging, and Detection

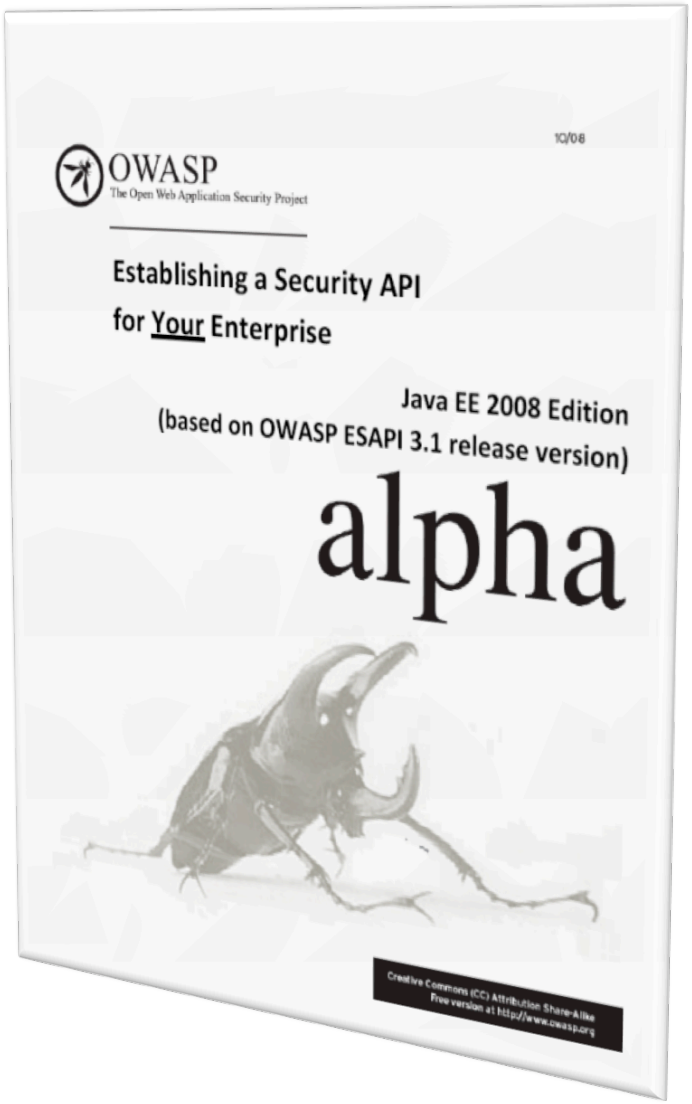


throw new ValidationException("User message", "Log message");



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