



**THE OWASP ENTERPRISE SECURITY API  
(ESAPI)**



# ESAPI Mission

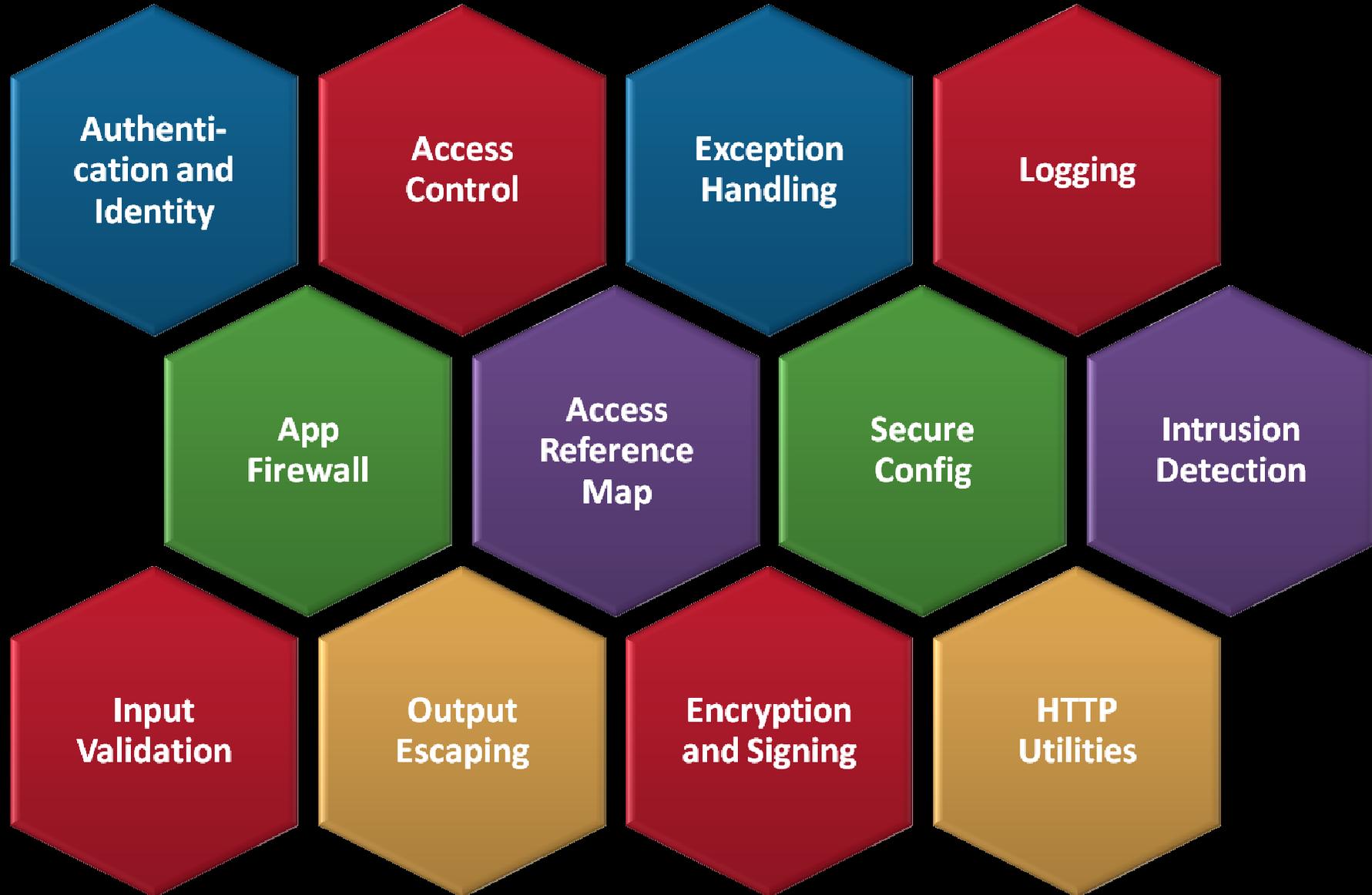
To ensure that  
strong simple security  
controls are available to  
every developer  
in every environment



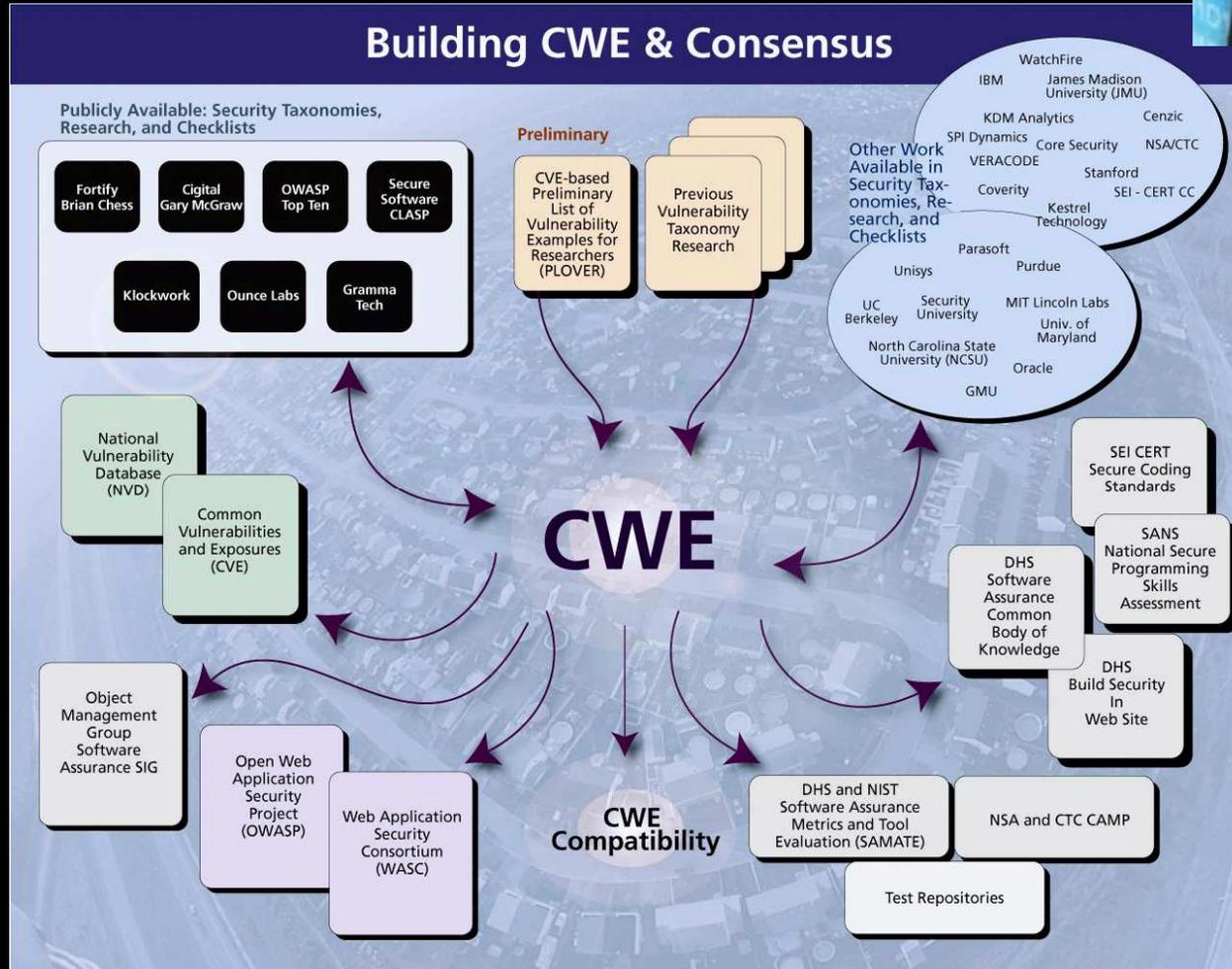
open source



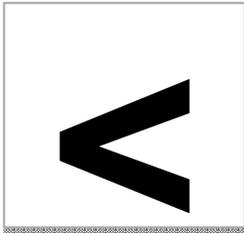
# Controls Every Application Needs



# Security Controls



Are Hard



### Percent Encoding

%3c  
%3C

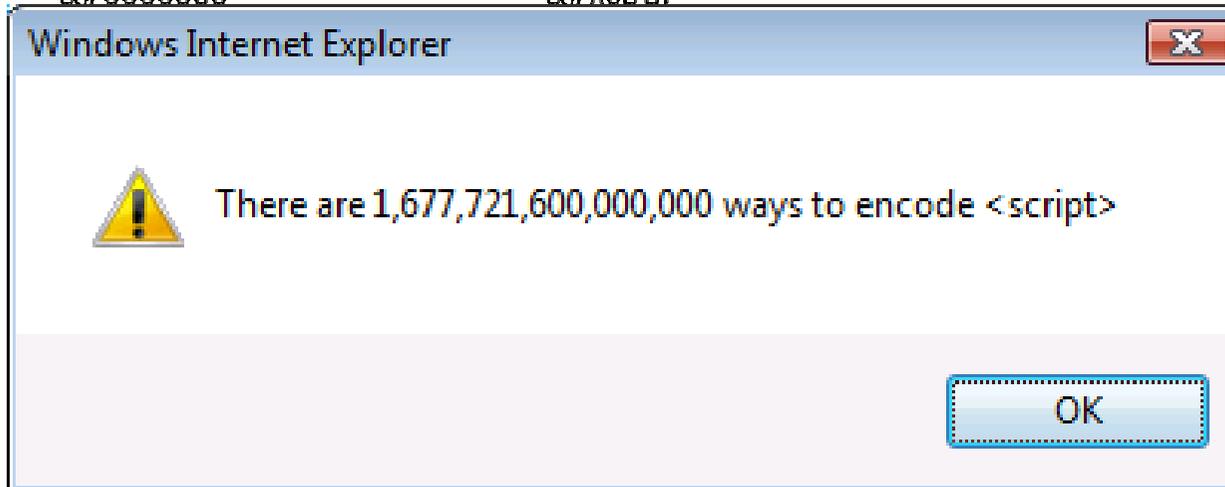
### HTML Entity Encoding

&#60  
&#060  
&#0060  
&#00060  
&#000060  
&#0000060

&#X0003c;  
&#X00003c;  
&#X000003c;  
&#x3C  
&#x03C  
&#x003C  
&#x0003C  
&#x00003C  
&#x000003C  
&#x3C;  
&#x03C;

### JavaScript Escape

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



&#x00003c;  
&#x000003c;  
&#X3c  
&#X03c  
&#X003c  
&#X0003c  
&#X00003c  
&#X000003c  
&#X3c;  
&#X03c;  
&#X003c;

&lt  
&lt  
&lt  
&lt  
&lt;  
&lt;  
&lt;  
&lt;

%f8%80%80%80%bc  
%fc%80%80%80%80%bc

### US-ASCII

¼

### UTF-7

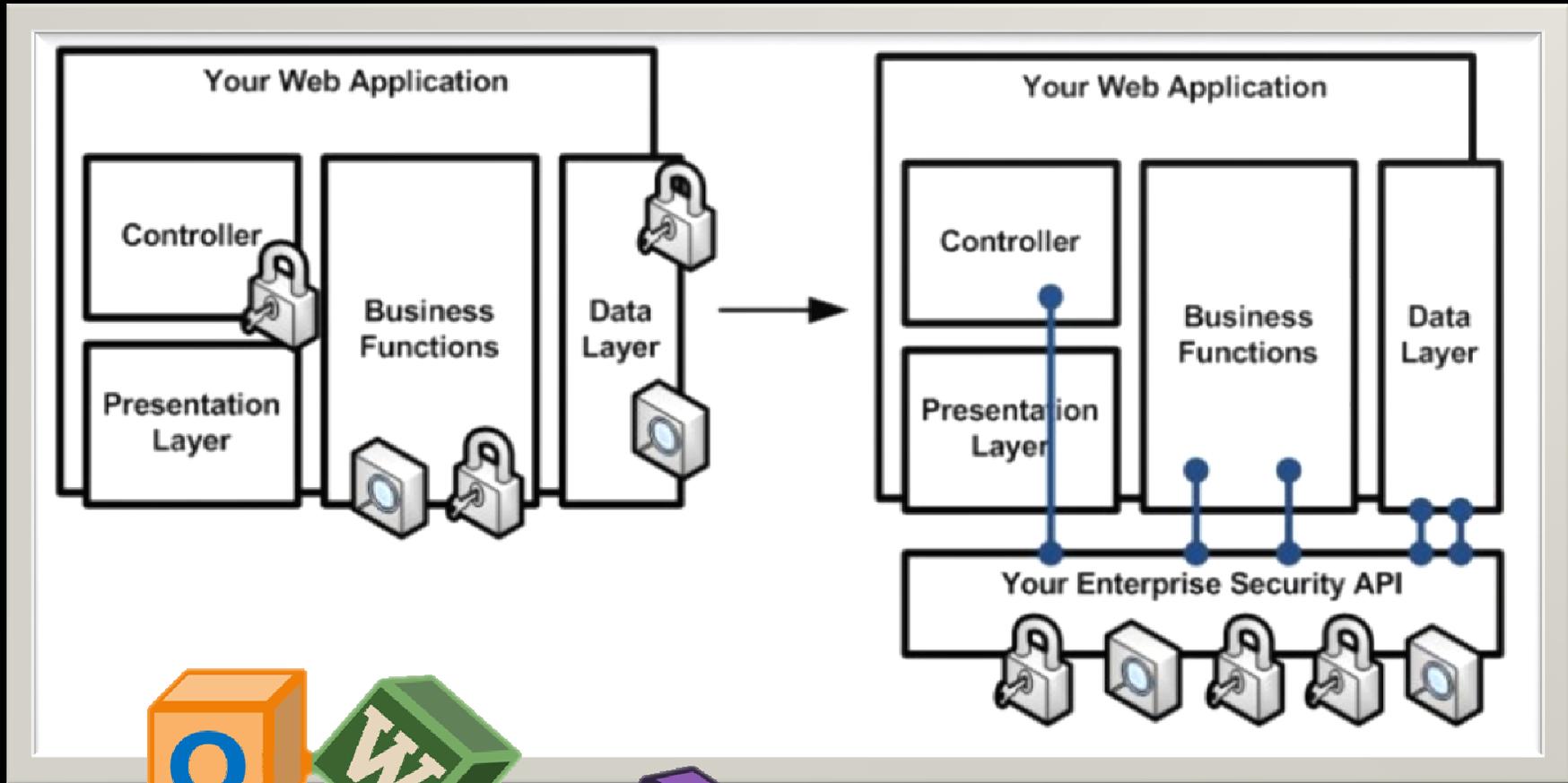
+ADw-

### Punycode

<-



Cheaper, Better, Faster



accountability

verification

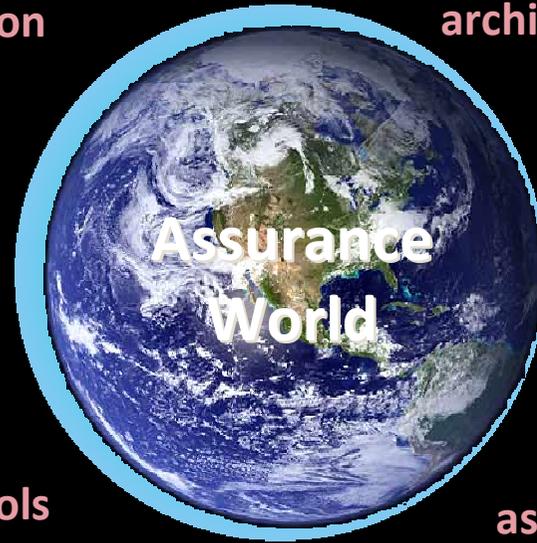
architecture

policy

visibility

patterns

metrics



controls

assurance

completeness

threats

exploits

impact

pentest

flaws

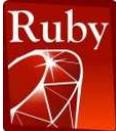
risks

attacks

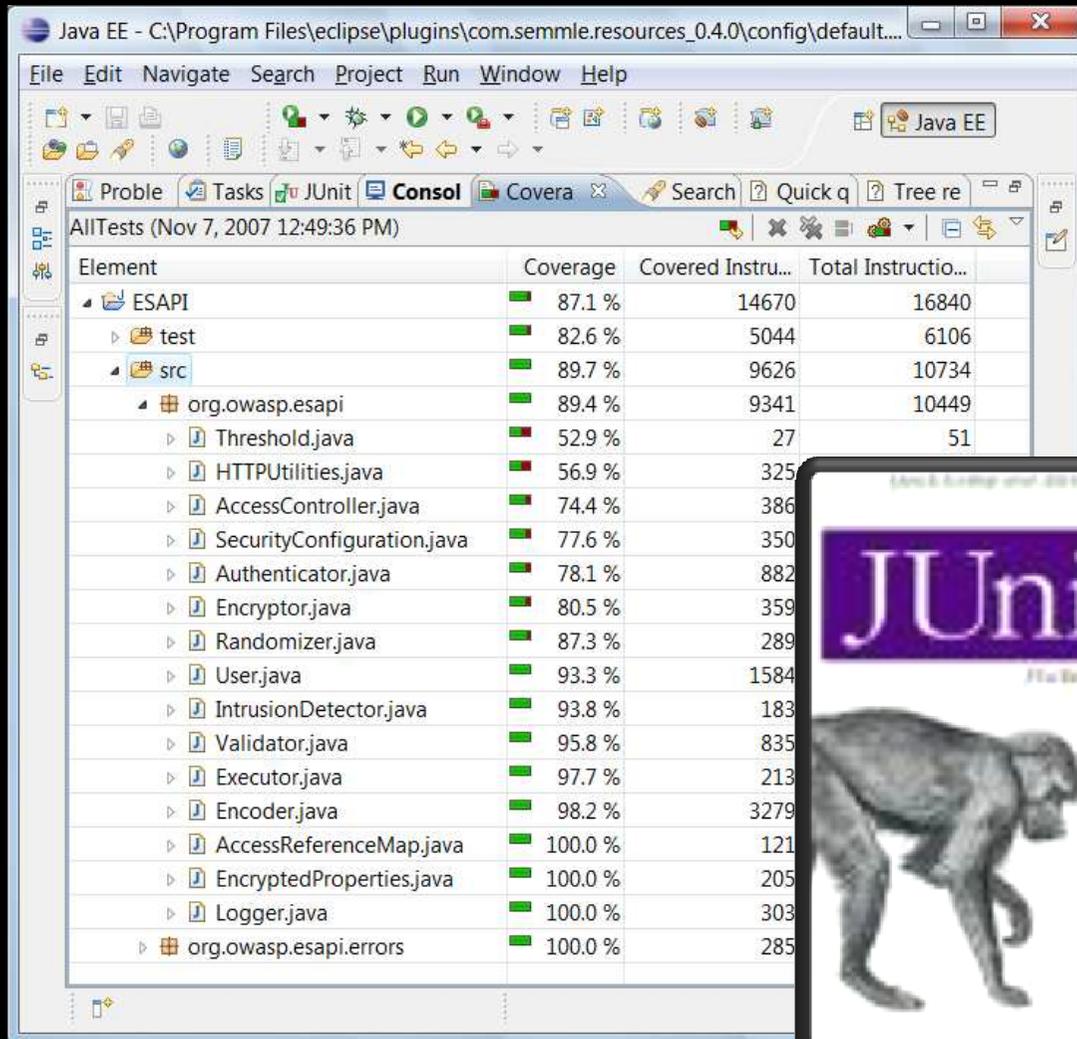
scanning



vulnerabilities

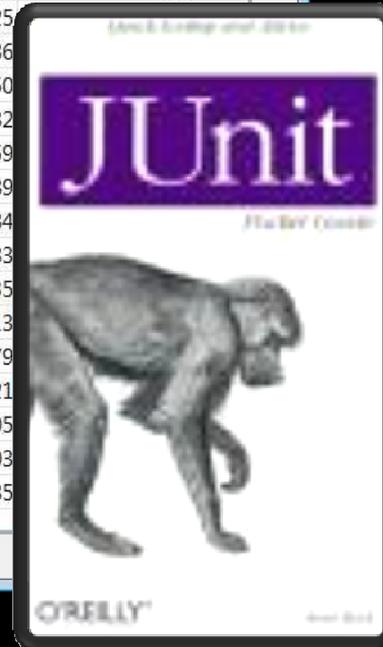
ESAPI Scorecard											
Authentication	✓	✓		✓	✓	✓					
Identity	✓	✓		✓	✓	✓					
Access Control	✓	✓	✓*	✓*	✓	✓			✓		
Input Validation	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Output Escaping	✓	✓		✓	✓	✓	✓		✓	✓	✓
Canonicalization	✓	✓		✓	✓	✓	✓		✓	✓	✓
Encryption	✓	✓	✓		✓	✓				✓	
Random Numbers	✓	✓	✓		✓	✓				✓	
Exceptions	✓	✓	✓		✓	✓					✓
Logging	✓	✓	✓	✓	✓	✓	✓			✓	
IntrusionDetection	✓	✓			✓	✓					
Security Config	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
App Firewall	✓										

# Assurance



The screenshot shows the Eclipse IDE interface with a code coverage report for ESAPI tests. The report is titled "AllTests (Nov 7, 2007 12:49:36 PM)" and displays a table with columns for Element, Coverage, Covered Instru..., and Total Instructio... The table lists various Java classes under the org.owasp.esapi package, along with their respective coverage percentages and instruction counts.

Element	Coverage	Covered Instru...	Total Instructio...
ESAPI	87.1 %	14670	16840
test	82.6 %	5044	6106
src	89.7 %	9626	10734
org.owasp.esapi	89.4 %	9341	10449
Threshold.java	52.9 %	27	51
HTTPUtilities.java	56.9 %	325	
AccessController.java	74.4 %	386	
SecurityConfiguration.java	77.6 %	350	
Authenticator.java	78.1 %	882	
Encryptor.java	80.5 %	359	
Randomizer.java	87.3 %	289	
User.java	93.3 %	1584	
IntrusionDetector.java	93.8 %	183	
Validator.java	95.8 %	835	
Executor.java	97.7 %	213	
Encoder.java	98.2 %	3279	
AccessReferenceMap.java	100.0 %	121	
EncryptedProperties.java	100.0 %	205	
Logger.java	100.0 %	303	
org.owasp.esapi.errors	100.0 %	285	



# Deceptively Tricky Problems for Developers

1. Input Validation and Output Encoding
2. Authentication and Identity
3. URL Access Control
4. Business Function Access Control
5. Data Layer Access Control
6. Presentation Layer Access Control
7. Errors, Logging, and Intrusion Detection
8. Encryption, Hashing, and Randomness

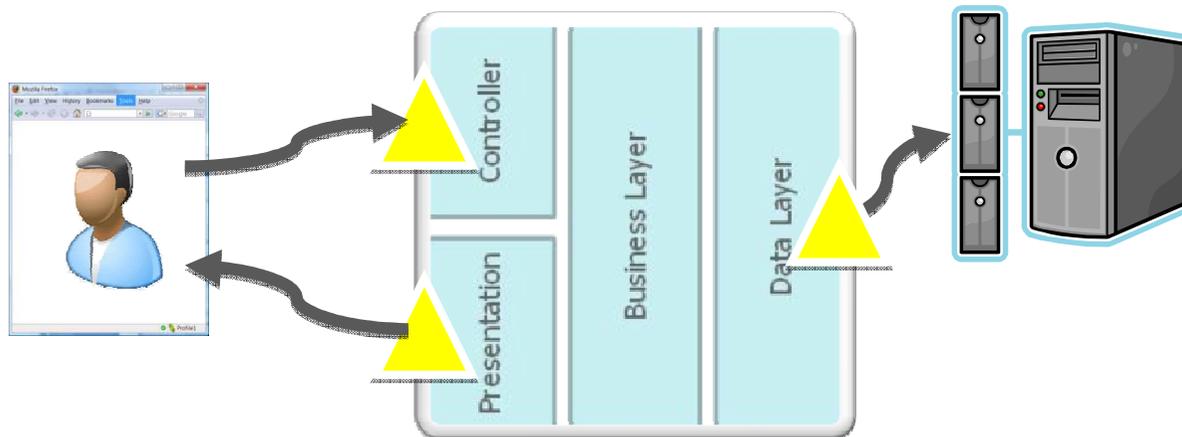
Lots more...

# Stopping Injection

Quick and Dirty

 Ad Hoc Escaping

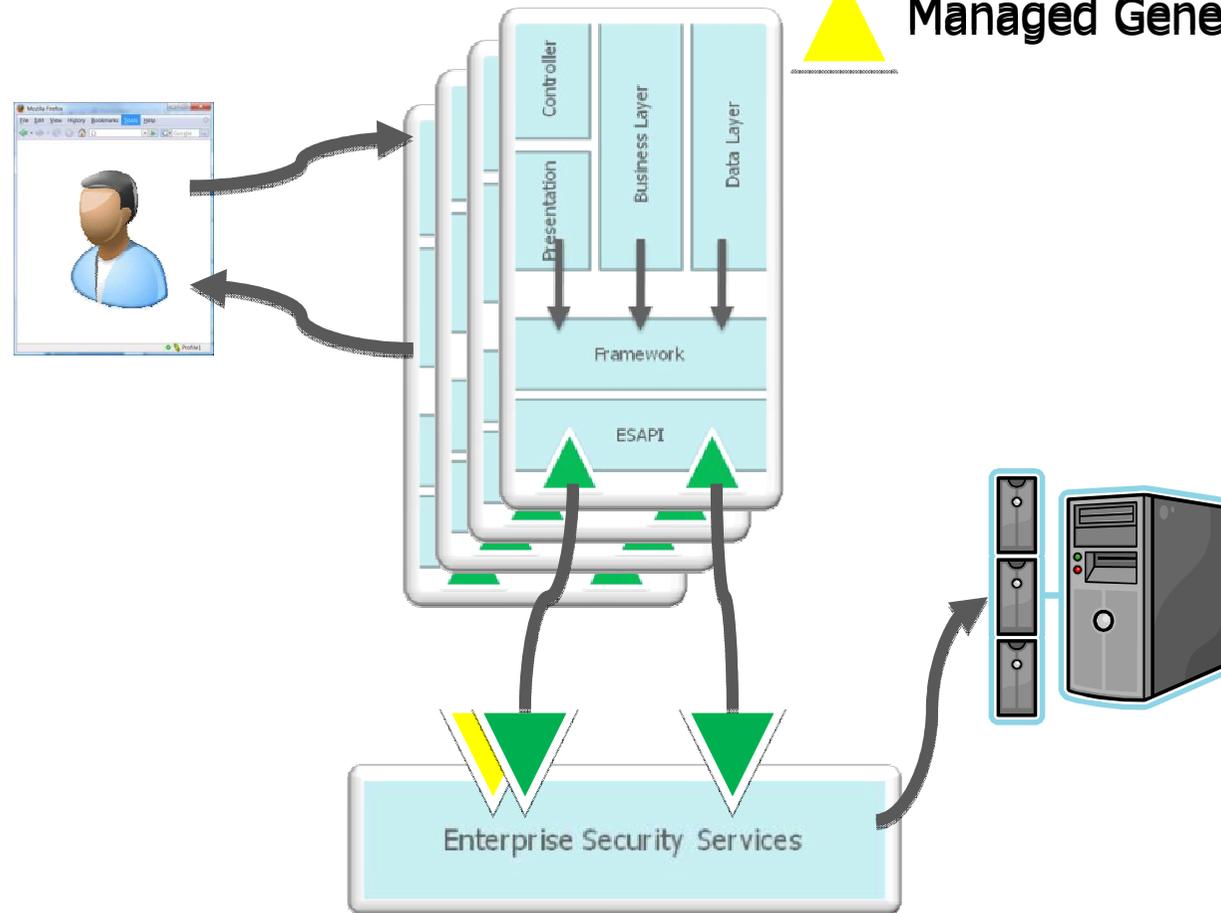
 Generic Validation



# Stopping Injection

Enterprise

- ▲ Automatic Escaping
- ▲ Managed Specific Validation
- ▲ Managed Generic Validation



The background of the slide is a dark grey color with a faint, light grey line-art illustration of a city map. A large padlock is superimposed on the right side of the map, symbolizing security. The text is centered in the upper half of the slide.

**Jeff Williams**  
**Aspect Security CEO**  
**OWASP Foundation Chair**  
**[jeff.williams@aspectsecurity.com](mailto:jeff.williams@aspectsecurity.com)**  
**<http://www.aspectsecurity.com>**  
**twitter @planetlevel**  
**410-707-1487**

**Questions?**

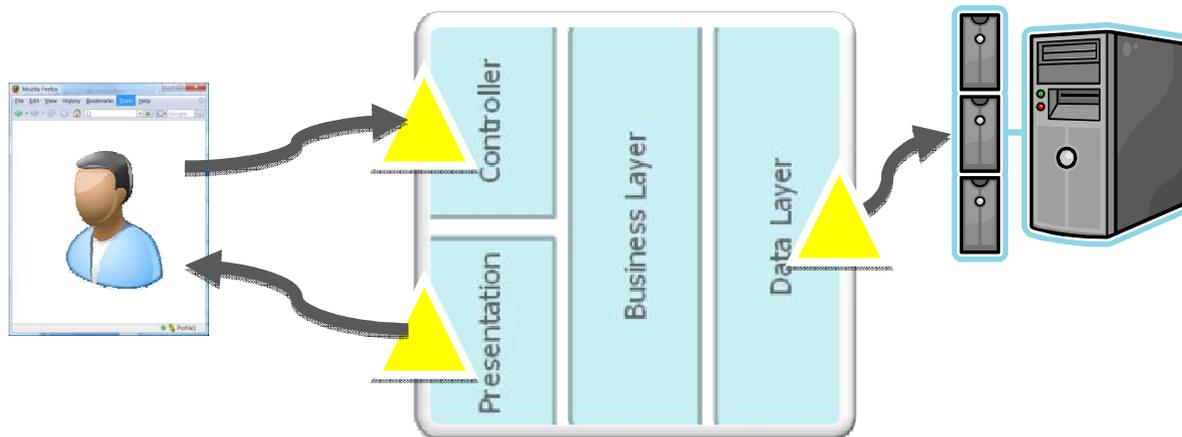


# Stopping Injection

Quick and Dirty

 Ad Hoc Escaping

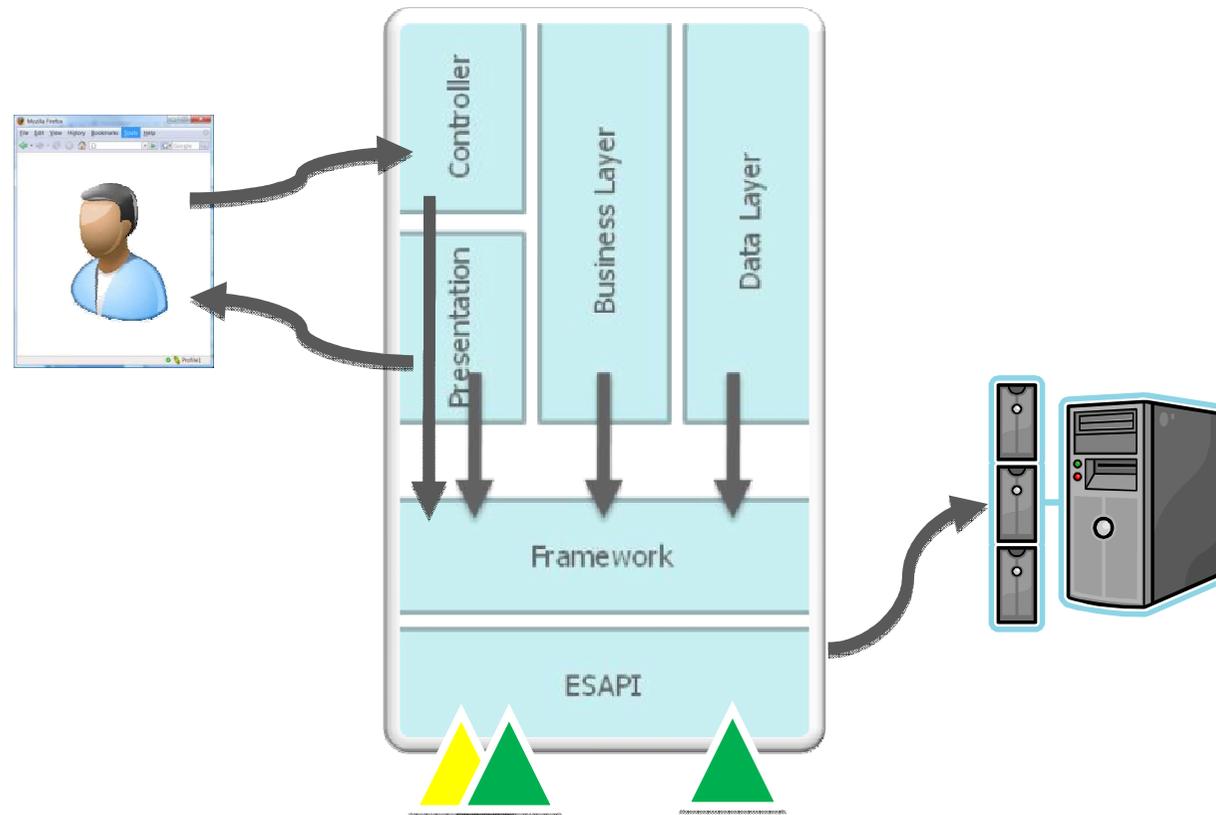
 Generic Validation



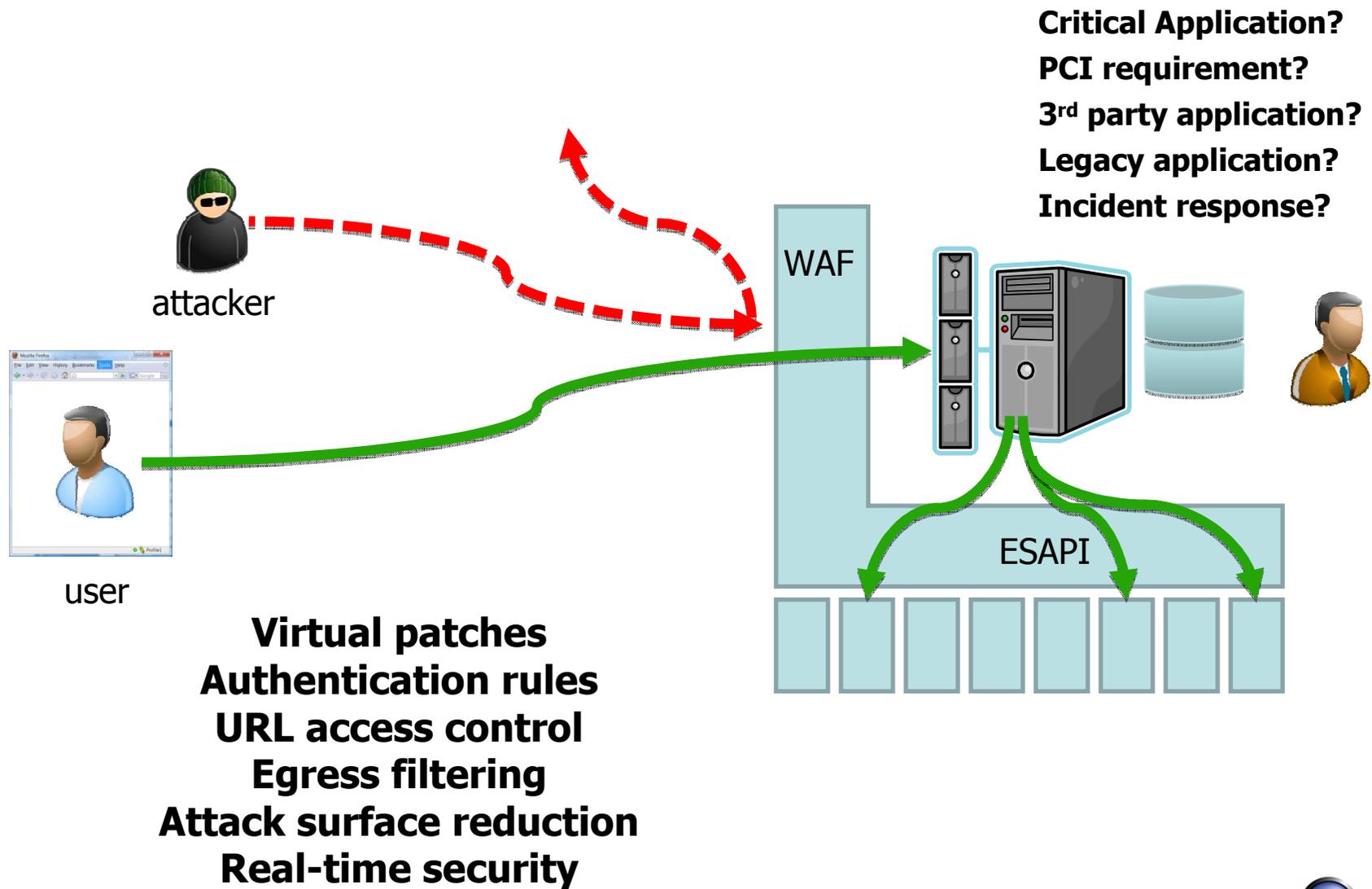
# Stopping Injection

Strong Application

- ▲ Mandatory Escaping
- ▲ Specific Validation
- ▲ Generic Validation (+can)



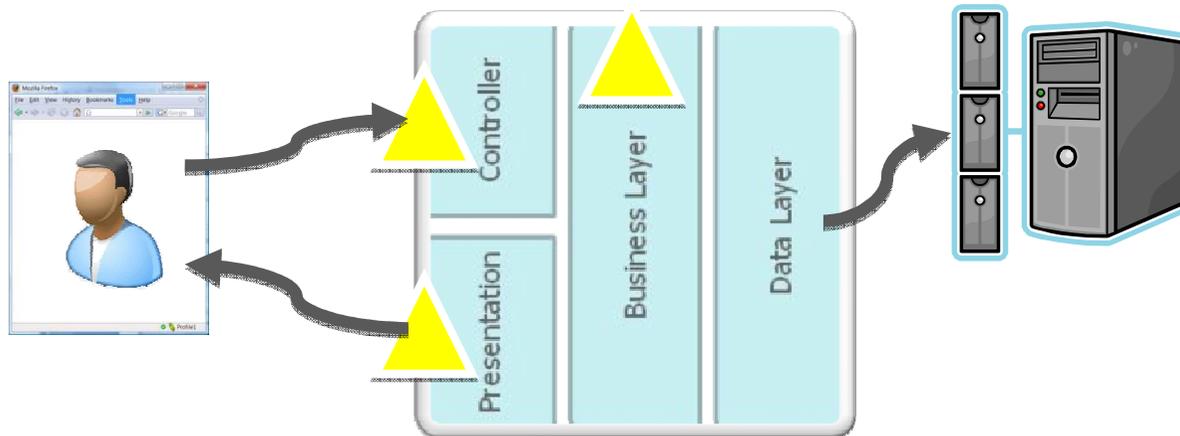
# ESAPI Web App Firewall (WAF)



# AuthN and AuthZ

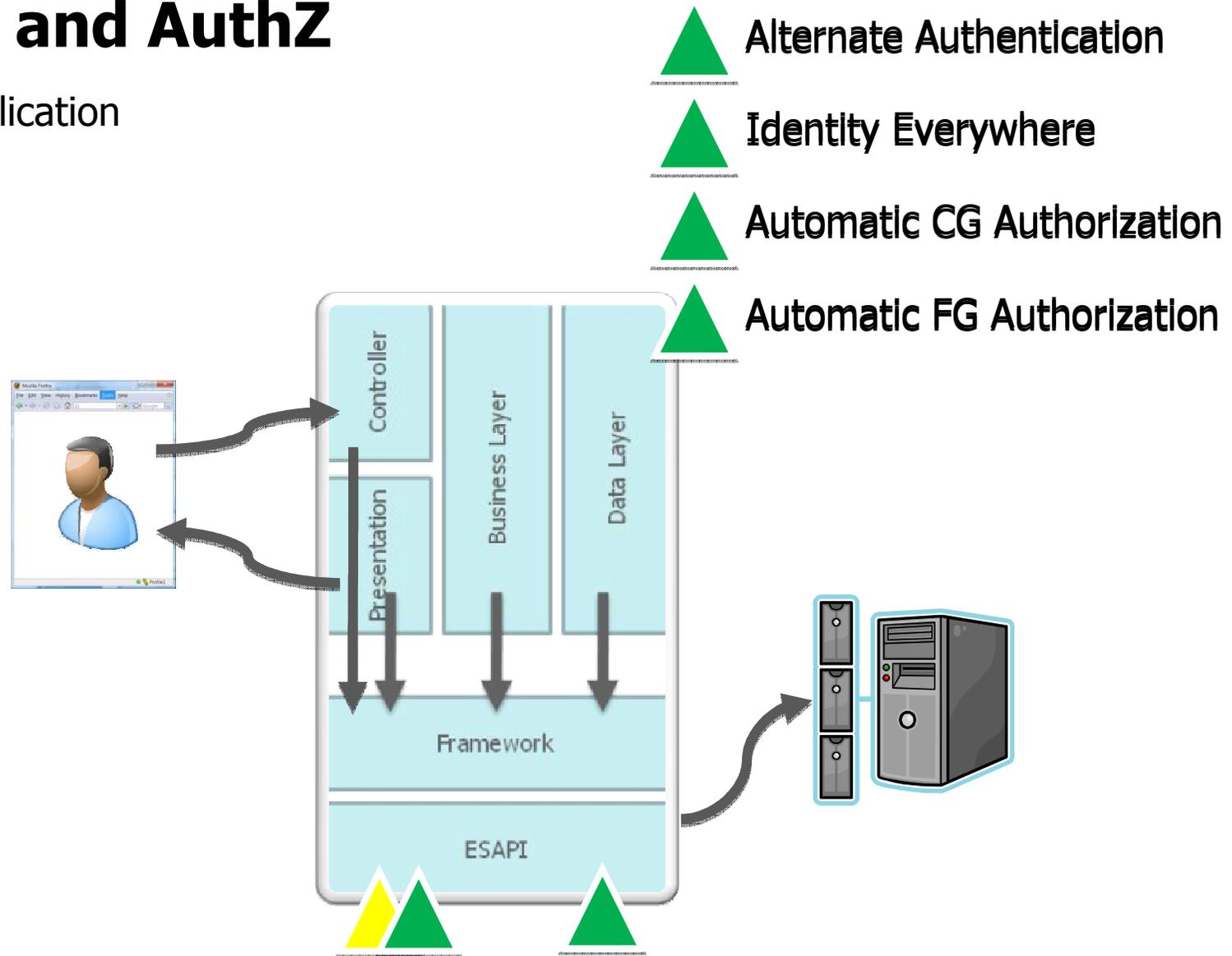
Quick and Dirty

- ▲ User In Session
- ▲ Simple Authentication Model
- ▲ Ad Hoc Authorization



# AuthN and AuthZ

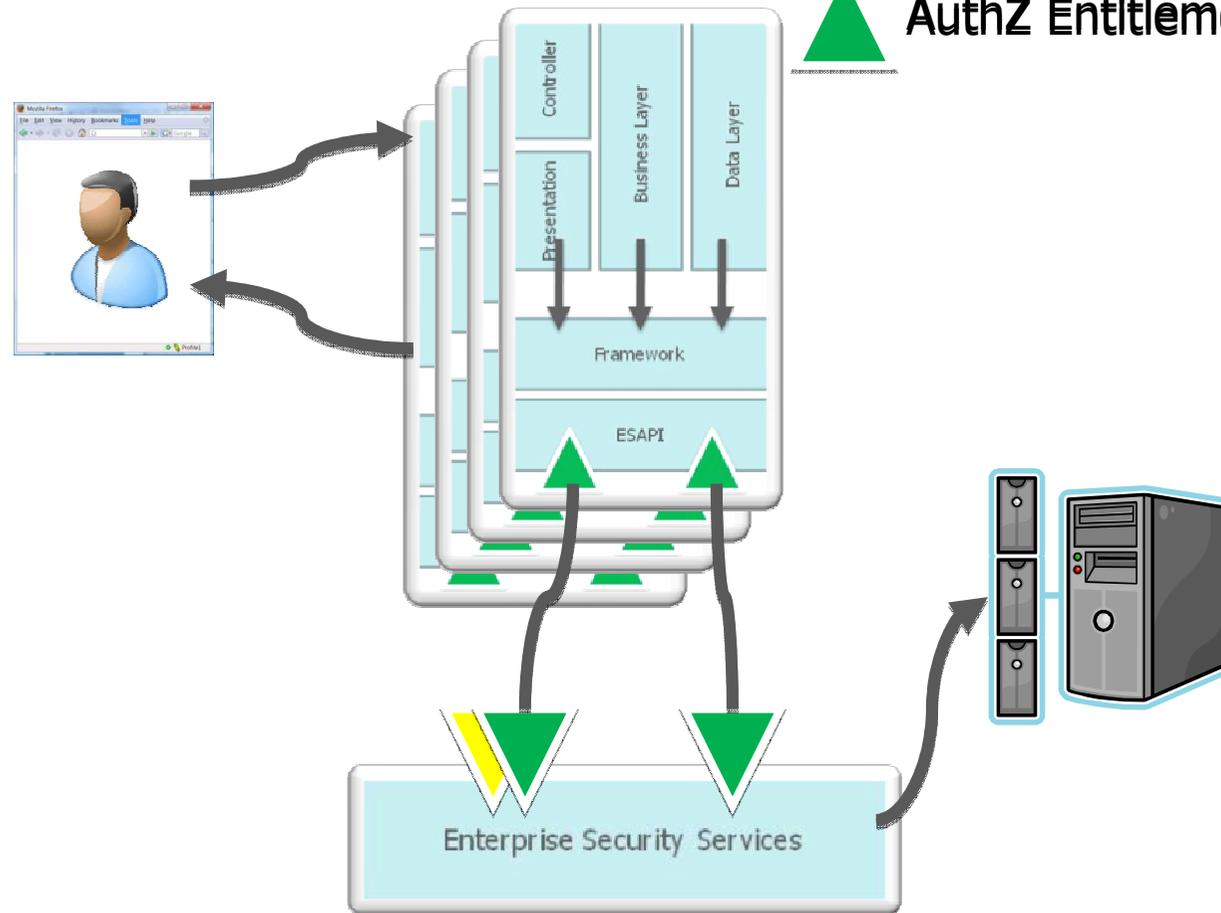
Strong Application



# AuthN and AuthZ

Enterprise

- ▲ Identity Management
- ▲ AuthZ Policy Management
- ▲ AuthZ Entitlement Mgmt



# Applications Enjoy Attacks

## Live Search

YouTube

Blogger

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-b3m72LNowtIK\_Z37nv288gq  
qWXJ-y2Fb3iM98dp1j1\_Z27QvTiK4  
iFmlT0WYJUuXmJbKdLZUeyQoAFUZXW  
L3Ky6vHb51\_U4F-DZLJVm386x8K2u0  
BoFdz\_yL8On9FRPYAgDdyNHc3eC7xgBS\_17RyeyXpB2FvG8QTPi4XQ0eL5N  
3bDh6BN2aNdLNcaDIw1VvqQ76TNOFLiQmhwf98tFJmRe5Qqfayuxh87oQ4i  
bMY59pDNW6HzibDbb2JUimdVTT1xN65YmoHa\_FJlmlv3F6yIt8e\_EUrzA7XZ  
RTIjwQ-Cw1xYok7qtnpps02BXDpJ1GBFoNTmB2e0P\_YjeFXnFz-7mah4KHcU  
Wh7qo2DhPQ-f3bgXR99HnzREq0B\_Y75gpWJ--1Te0KRRj58OM7Snu1IK5eRe  
DNWdas9qxWmv3qSAEKLIJzaRG3E3C\_J1CLT1qcHqmDe96y1qgMW1gVhtM7M6  
7vV1PQJevLHddngV54mza2JcuaVw60V619CFUjWD0mX1gK3et1wLn70DVUoP  
AEqkAe8ab81kcFN2zaNfwa435aZV0j\_R3eQ88F0uXaOupKqapob913Vjo0-Qc  
Y\_bmEiCq1V8ULOZS1mHkvfj8xRfIo0sDvXxvmsPJK49bvk1msw3271g79aQs  
TfevuHptE\_xexYplLeQhpM8aBLf0cN0kELVry-Uc61sqf00kteI\_HKeelySo  
Xum2taN7Y62pU8366pgOgseRbjolIX3DpuwQQdwZrzRh\_#TyuwaT5hw41N3-  
pF1IyQ4KRADCN3UYon7I7pDNBx\_4T0pDuE2WJCFYa4Iw81Q44dn-qyNLEq-4e  
c6hcHQAR16GgoER831AS1MQEMTJhtokL4Vh-HAR2Q6qOoveRR0k1awXEOf  
dHX6nh\_1p12CIvVbQ89Ltw1G5ck66FL5ag\_-qrIFVYxqxm800n\_10Ged9  
QeShdQqrTurPfhmdYoSuarzaQZn\_apbe8ePDFm5c9KVLz03wx  
tJbt\_sbN9FU4b7w2Sutmsvpl1ysDeaMeMgwYqWVinp210\_gw\_Y  
Hduo8jase8tzHivWv0kzc10GDUH1164m05Szl1t17qoGCHGXT  
Ojqui8tYpJL1MN8eR\_d17-p02rw62zdreQSaDFWk99ArMYI  
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**.

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**

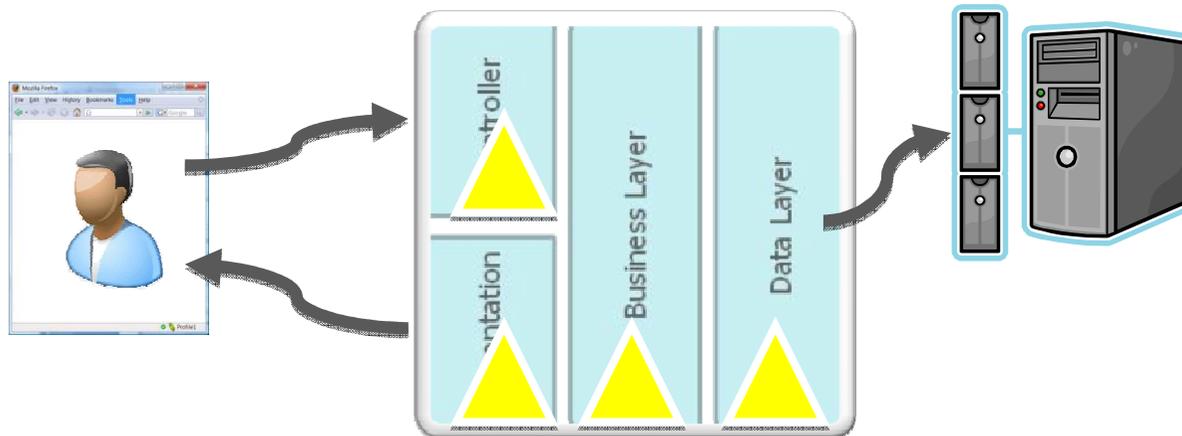
```
javax.servlet.ServletException: Servlet execution threw an exception
    at org.apache.catalina.core.ApplicationFilterChain.internal
    at org.apache.catalina.core.ApplicationFilterChain.doFilter
    at org.apache.catalina.core.StandardWrapperValve.invoke(Sta
    at org.apache.catalina.core.StandardPipeline$StandardPipeli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



# Accountability and Detection

Quick and Dirty

- ▲ Ad Hoc Security Logging
- ▲ Security Exceptions (2 msgs)
- ▲ Ad Hoc Authorization

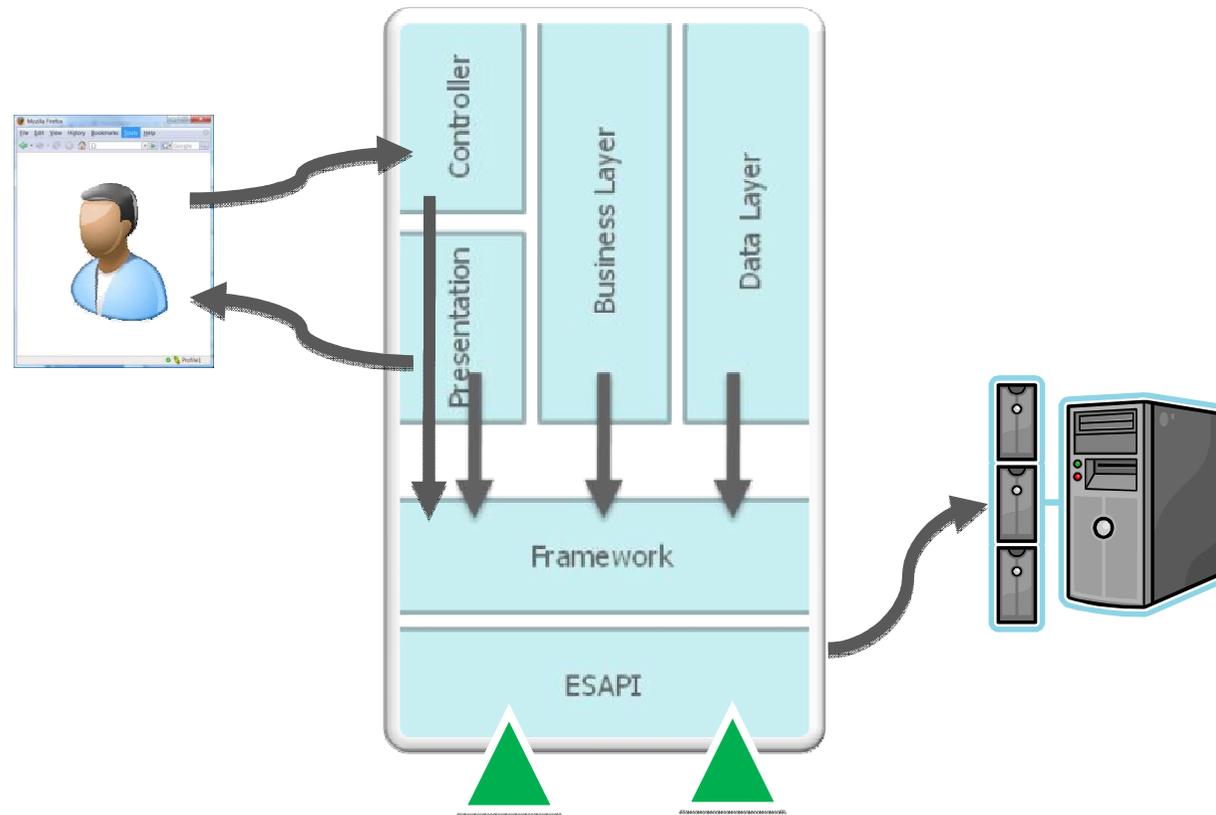


# Accountability and Detection

Strong Application

Automatic Security Logging

Intrusion Detection



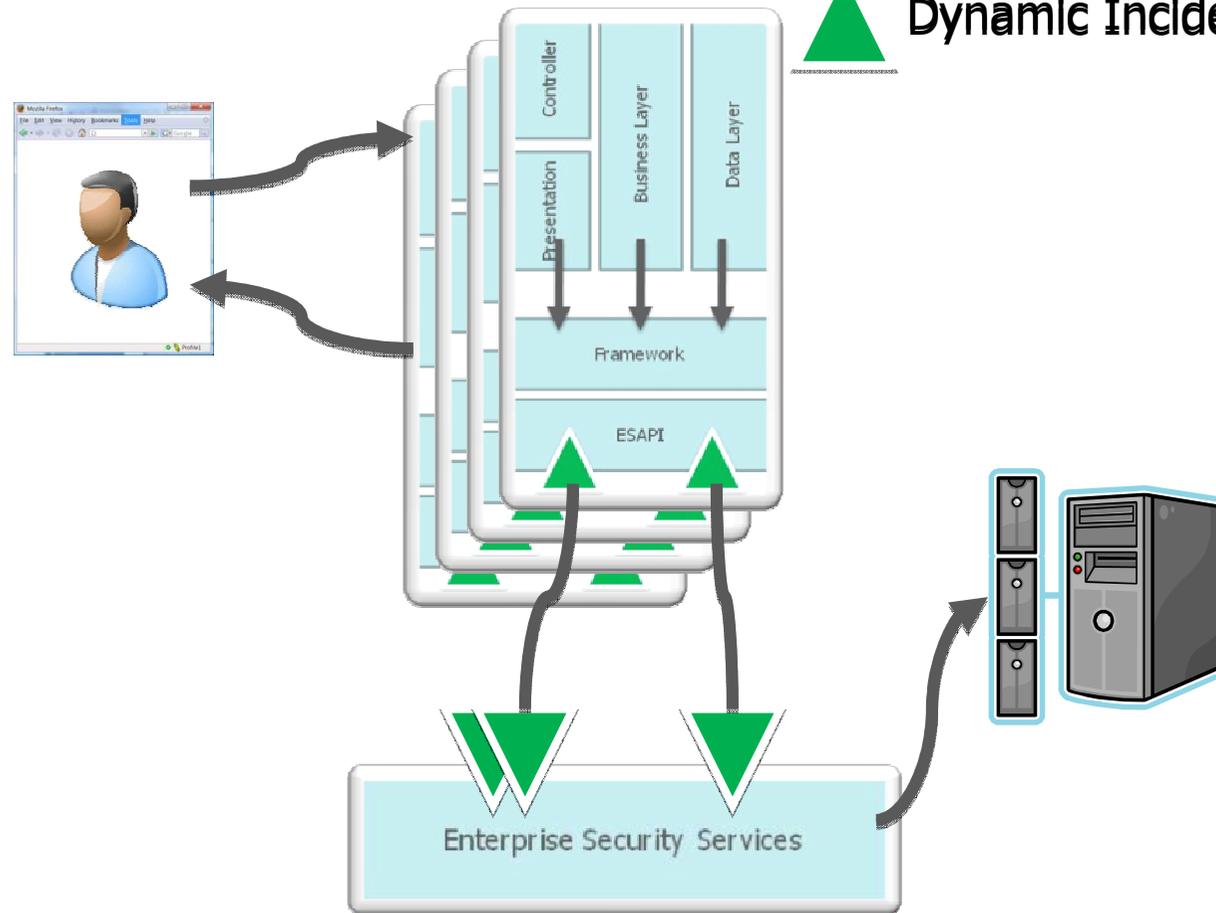
# Accountability and Detection

Enterprise

Centralized Logging

Log Policy Management

Dynamic Incident Response



# ESAPI Swingset



ESAPI SwingSet Demonstration Application beta - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:8080/swingset/main

OWASP

## 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**

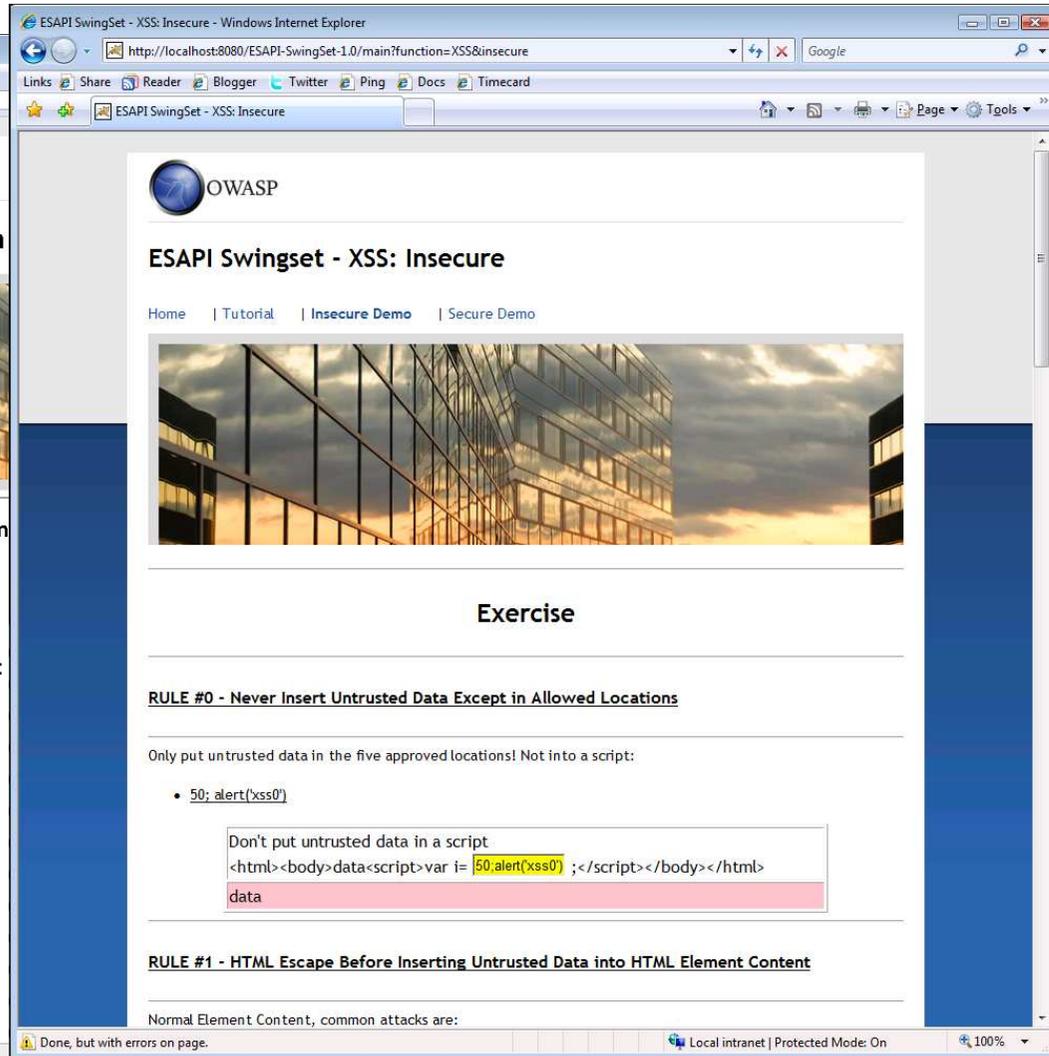
- [Reference a Server-Side Object](#)
- [Access Control](#)

**Encryption, Randomness, and Integrity**

- [Encryption](#)
- [Randomizer](#)
- [Integrity Seals](#)
- [Globally Unique IDs](#)

**Caching**

Done



ESAPI SwingSet - XSS: Insecure - Windows Internet Explorer

http://localhost:8080/ESAPI-SwingSet-1.0/main?function=XSS&insecure

Links Share Reader Blogger Twitter Ping Docs Timecard

ESAPI SwingSet - XSS: Insecure

OWASP

## 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:

Local intranet | Protected Mode: On | 100%

