Development of Security Framework based on OWASP ESAPI for JSF2.0
• About Us
  – Rakesh Kachhadiya
    • Master work, University of Freiburg (Germany)
  – Emmanuel Benoist
    • Professor, Bern University of Applied Sciences (Switzerland)
• Enterprise Security API
  – OWASP Project
  – Support for: Java, Dot NET, Classic ASP, PHP, ColdFusion, Python, Objective C, Tuby, C, Perl, ...

• Groups all security features into one library:
  – Authentication, Authorization
  – Access control, logging and intrusion detection
  – Validation, decoding, encoding (for HTML, XML, SQL, Ldap, ...)
  – Crypto functionalities
• JSF: Advantages
  – Model View Controller
    • Controller: Faces Servlet
    • View: xhtml files
      – Component tree
    • Model: Java files using notations
  – Separation of layers
    • Front End: xhtml and components
    • Back End: Java
  – Libraries with reusable components
    • Apache, RichFaces, Oracle, etc...
  – Concepts like: Validators and Converters
At different levels

- In the Model
  - Authorization, Access control, logging, SQL/LDAP/XML/encoding, ...

- In the View
  - Create Validators

- In the Controller (in the Faces Servlet)
  - Enhancing HTTP
  - HTML Encoding
Project goals

• Provide a library for integrating ESAPI in JSF
  – Reduces the work for the developers
  – Secure implementation

• Adapt ESAPI to JSF "culture"
  – Provide out of the box tools
  – Easy to integrate in a project
  – Can be used by simple developers
OWASP
The Open Web Application Security Project

Demo1: Render Response

Request

Restore view
Apply request value

Process validations
Update model values
Invoke application

Render ResponseW
Response

JSF Framework

ESAPI

JSF-ESAPI Framework
Validation
Filtering
File Based Authorization
Render Response
Demo2: Validation

[Diagram of the JSF-ESAPI Framework showing the flow from Request to Response through Restore View, Apply Request Value, Invoke Application, Update Model Values, and Validation, Filtering, File Based Authorization, and Render Response compartments.]
Demo3: Filtering

OWASP
The Open Web Application Security Project

Response

Request

JSF Framework
- Render Response
- Invoke application
- Update model values
- Process validations

JSF-ESAPI Framework
- Validation
- Filtering
- File Based Authorization
- Render Response

ESAPI
• Integrate ESAPI into JSF
  – It will help programmers
  – Makes security “invisible”

• Known issues
  – Access Control: prevent updating of the model
  – CSRF: make it transparent for the programmer

• Need feedback from security experts
  – What are the common vulnerabilities for JSF
• Feedback for OWASP

QUESTIONS?