



Development of Security Framework based on  
OWASP ESAPI for JSF2.0



**OWASP**

The Open Web Application Security Project



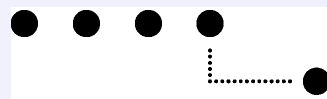
- About Us

- Rakesh Kachhadiya

- Master work, Univeristy of Freiburg (Germany)

- Emmanuel Benoist

- Professor, Bern University of Applied Sciences (Swizerland)



**Bern University of Applied Sciences**

Engineering and Information Technology



- Enterprise Security API
  - OWASP Project
  - Support for : Java, Dot NET, Classic ASP, PHP, ColdFusion, Python, Objective C, Ruby, 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

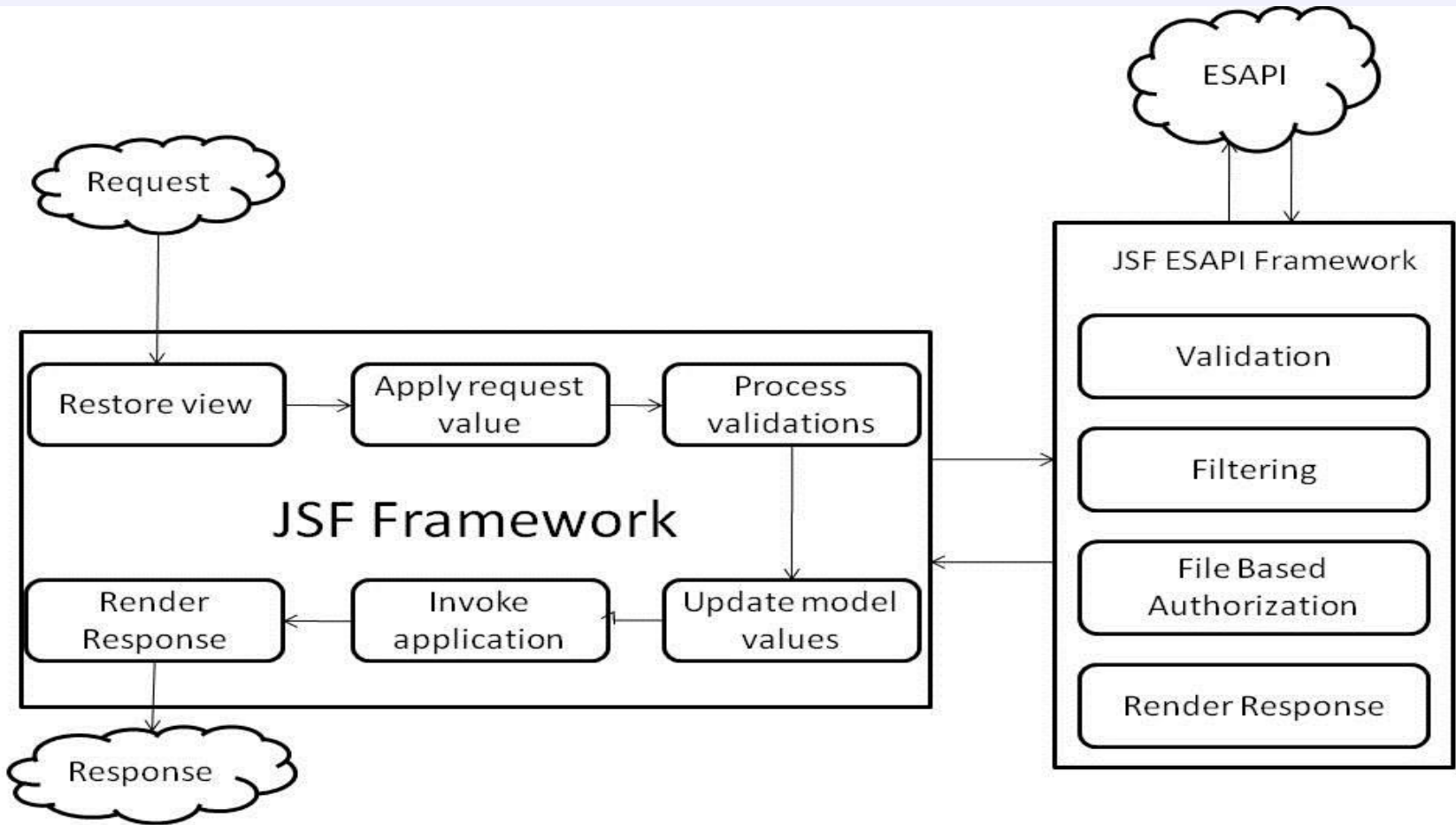


- At different levels
  - In the Model
    - Authorization, Access control, logging, SQL/LDAP/XML/-encoding, ...
  - In the View
    - Create Validators
  - In the Controller (in the Faces Servlet)
    - Enhancing HTTP
    - HTML Encoding

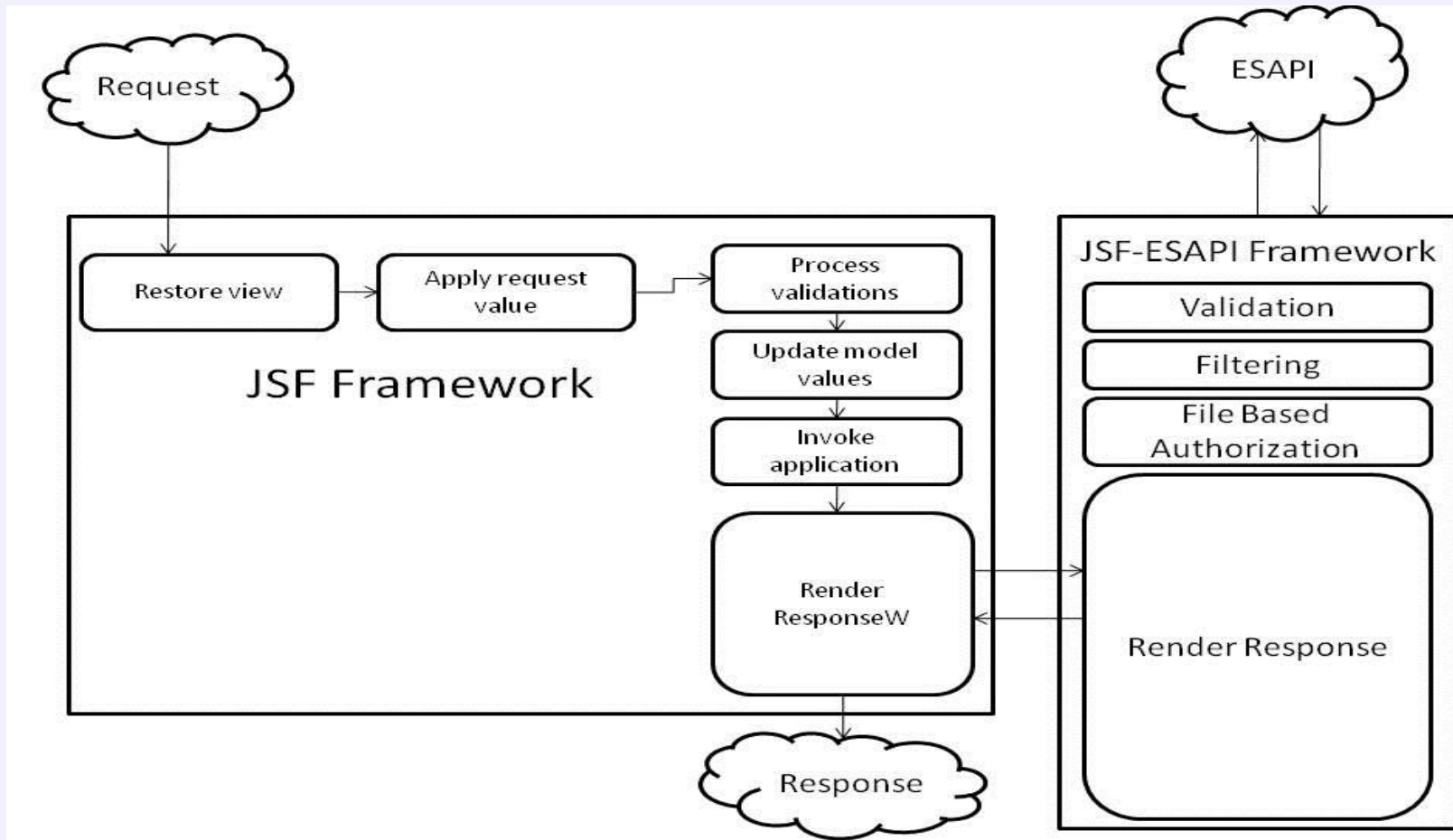


- Provide a library for integrating ESAPI in JSF
  - Reduces the work for the developers
  - Secure implementation
- Adapt ESAPI to JSF "culture"
  - Provide out of the box tools
  - Easy to integrate in a project
  - Can be used by simple developers

# Architecture

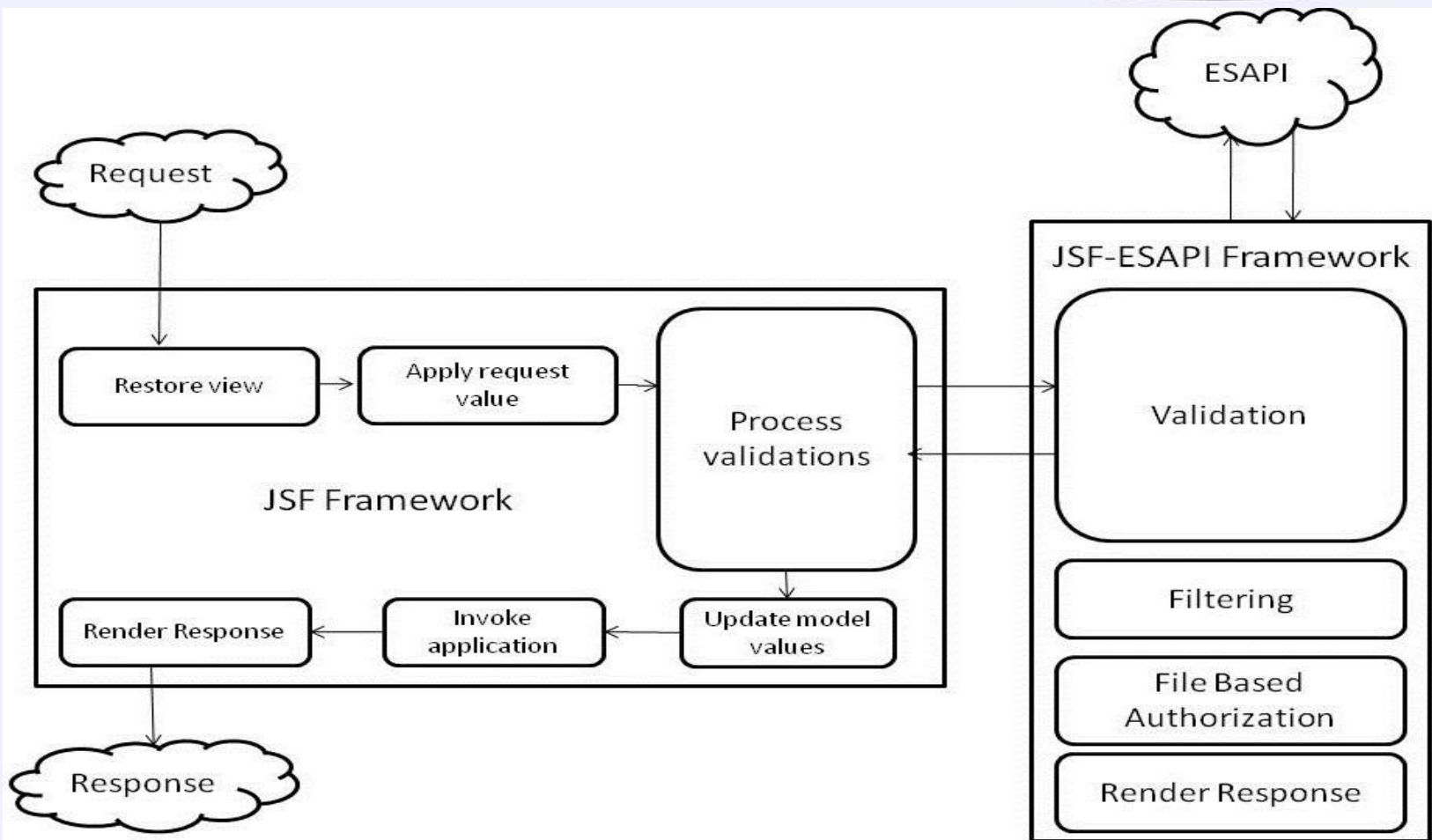


# Demo1 : Render Response

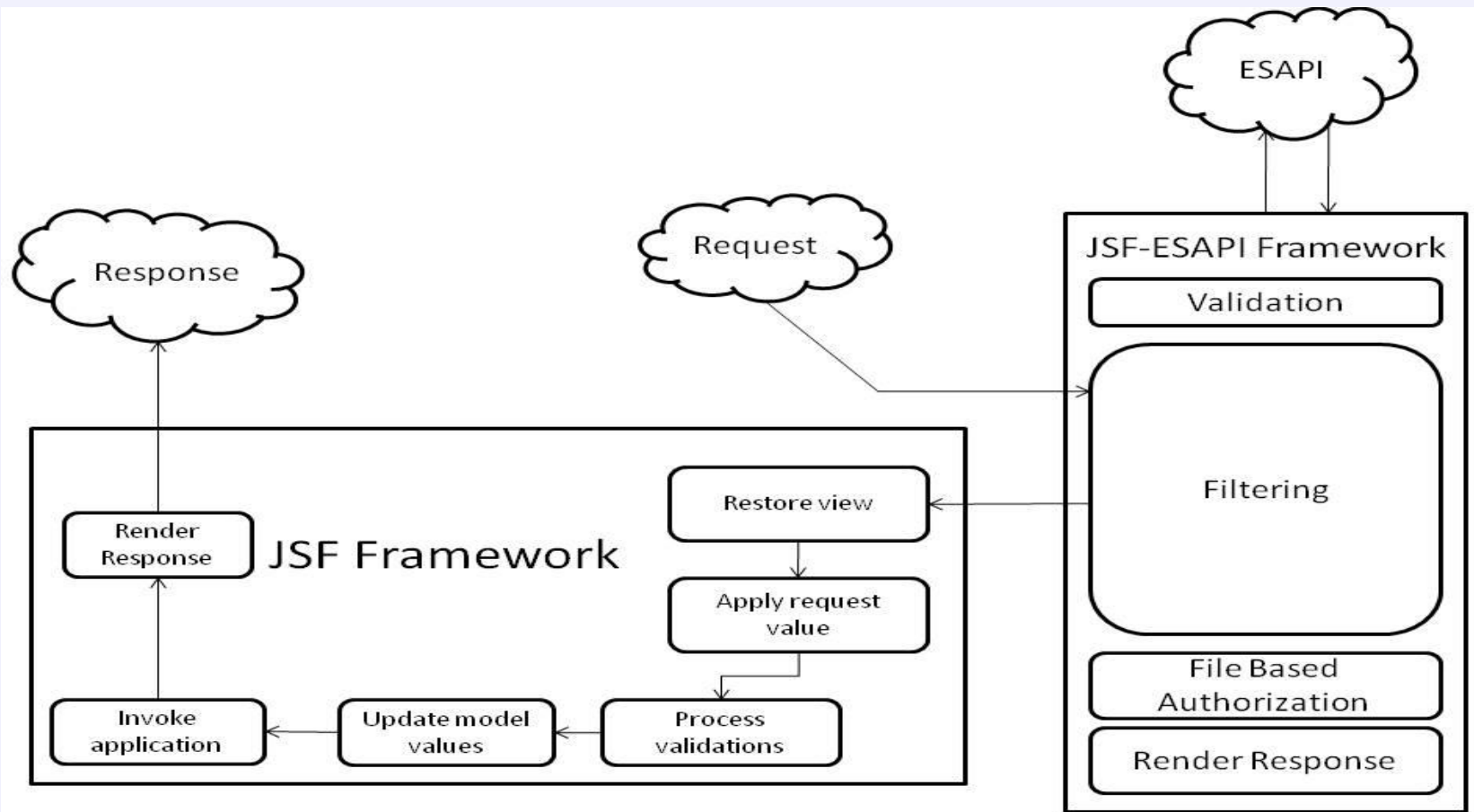




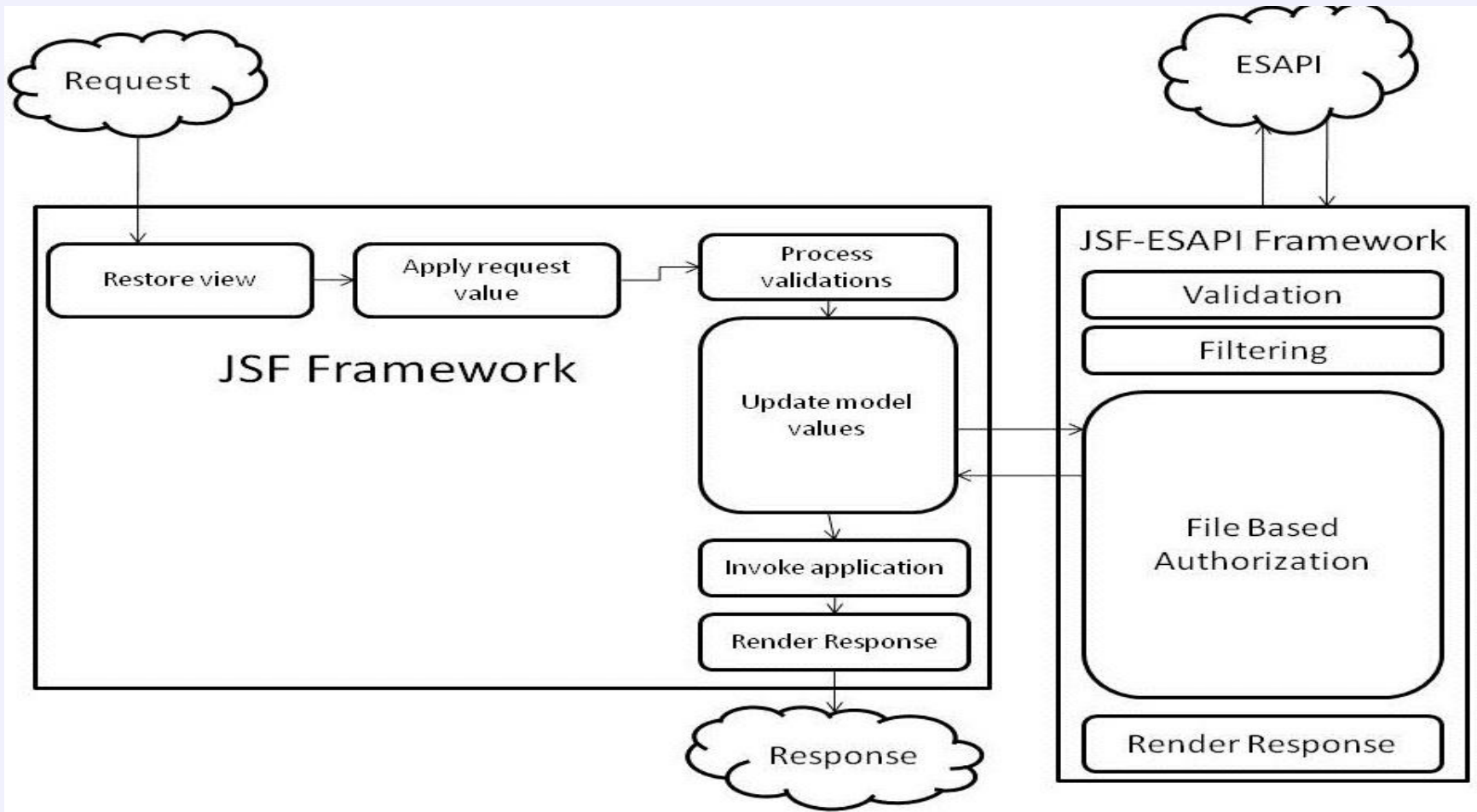
# Demo2: Validation



# Demo3 : Filtering



# Demo4: File based Authorization





- 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



## OWASP

The Open Web Application Security Project

- Feedback for OWASP



- Contacts us:
  - Emmanuel.Benoist (AT) bfh.ch
  - RakeshKachhadiya (AT) gmail.com

# QUESTIONS ?