

Secure Mail – Filtering HTML Mails

Application Security



Inhalt

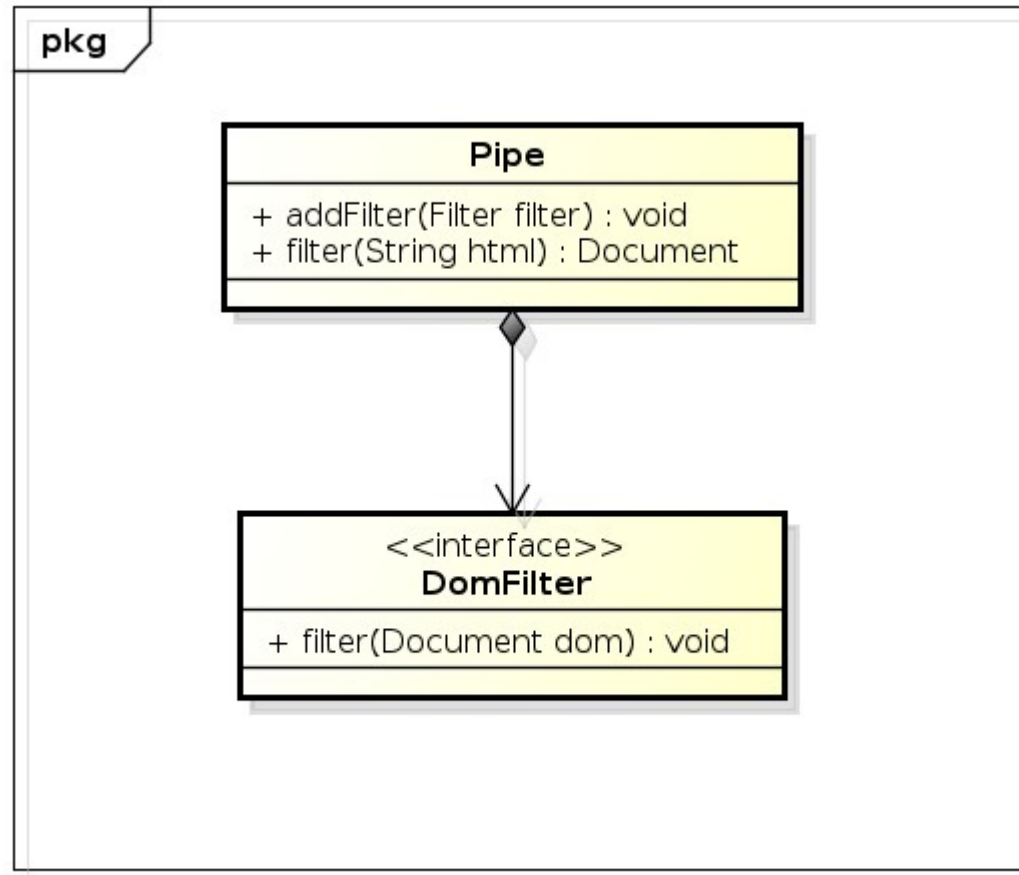
- Architektur
- Authentifizierung
- Filter
- Demonstration

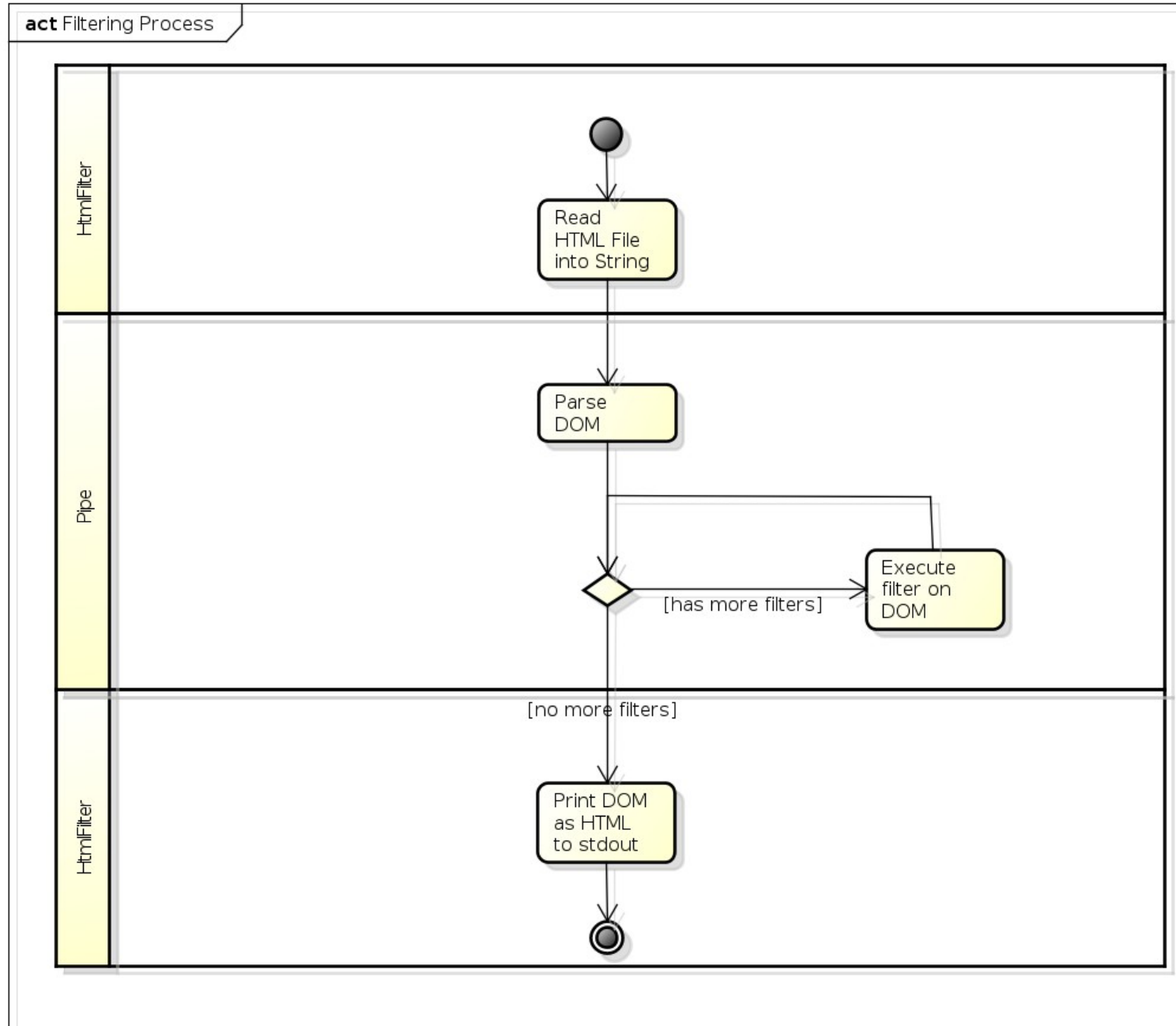
Architektur

- Pipe and Filter Pattern
 - Wart- und erweiterbar
- Filter operieren auf DOM
- DOM mittels Jsoup generiert



Architektur





Authentifizierung

- JAAS verwendet
- Überprüfung von „Well-known-groups“
 - Group ID 0 auf Unix
 - Group SID "S-1-5-32-544" auf Windows

```
Unix {  
    com.sun.security.auth.module.UnixLoginModule required debug=false;  
};  
  
Windows {  
    com.sun.security.auth.module.NTLoginModule required debug=false;  
};
```

Filter - Allgemeines

- Whitelist Filtering
 - Tags
 - Attributen
- Regex für bösesartiges CSS zu entdecken

Filter – Konkrete Implementierungen

- Tag Whitelist Filter
 - Attribute Whitelist Filter
 - Protocol Filter (HTTP, HTTPS)
 - Source URL Filter (Remove Query Parameters)
 - CSS Cleaner (Helper Class)
 - CSS Style Attribute Filter
 - CSS Inline Filter
 - CSS Link Filter
-

Secure Mail – Demonstration

Application Security

