Java-Web-Security Anti-Patterns

Java Forum Stuttgart 2015

Dominik Schadow | bridgingIT

Failed with nothing but
the best intentions

Design

Implement

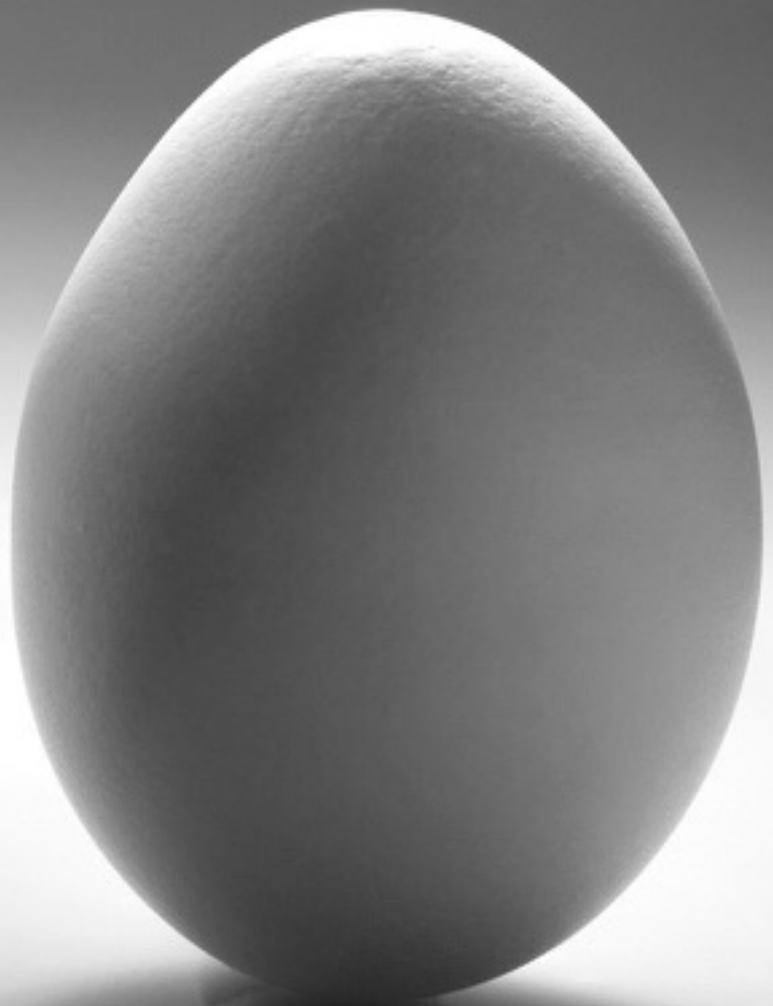
Maintain

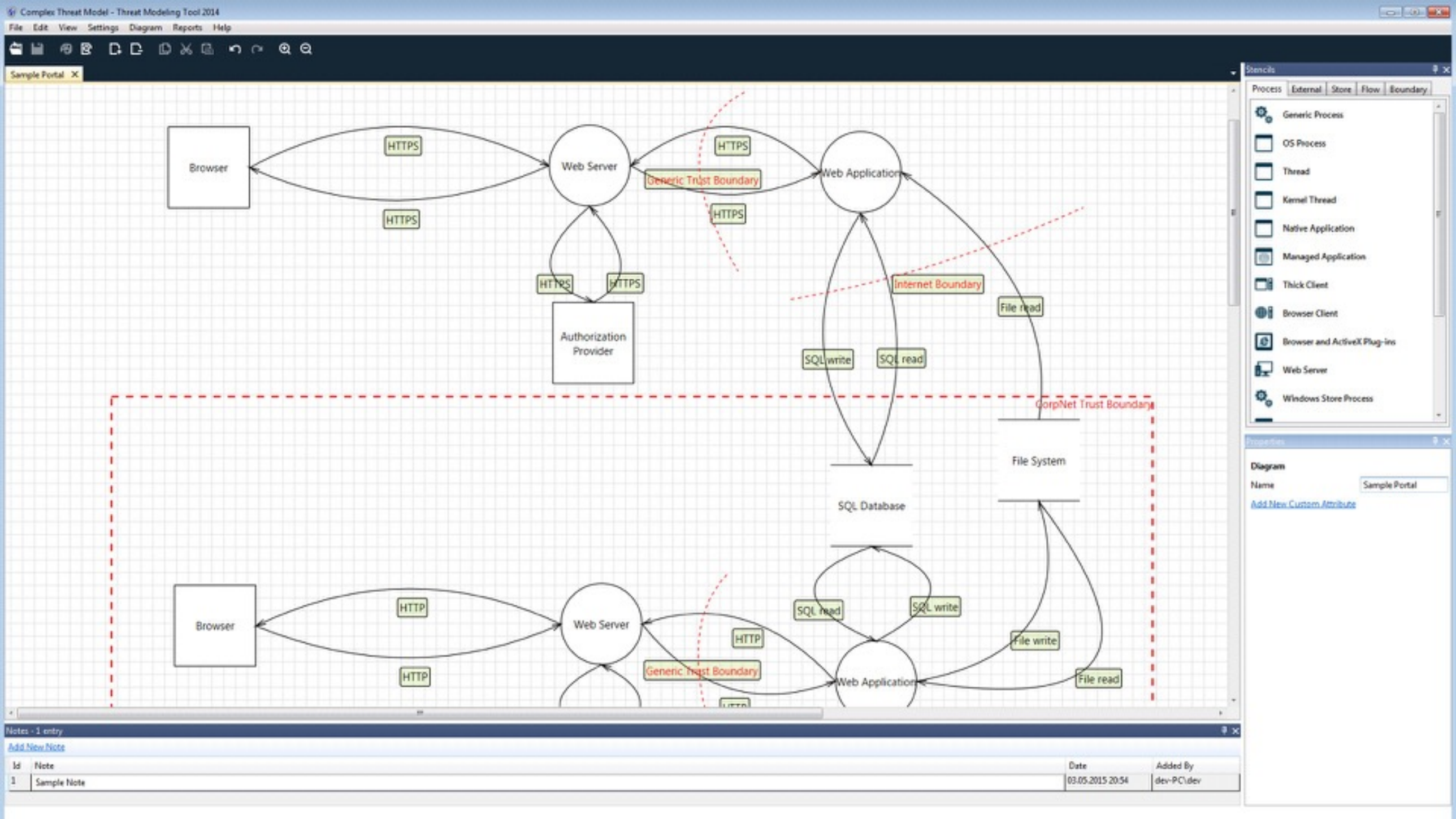
Design

Skipping threat modeling

Develop software that is secure by design

1. Know the web application
2. Know all external entities
3. Threat model




Complex Threat Model - Threat Modeling Tool 2014
File Edit View Settings Diagram Reports Help
Sample Portal
Browser
HTTPS
HTTPS
Web Server
HTTPS
Generic Trust Boundary
HTTPS
Web Application
HTTPS
HTTPS
Authorization Provider
Internet Boundary
File read
SQL write
SQL read
CorpNet Trust Boundary
File System
SQL Database
Browser
HTTP
HTTP
Web Server
HTTP
Generic Trust Boundary
SQL read
SQL write
Web Application
File write
File read
Stencils
Process External Store Flow Boundary
Generic Process
OS Process
Thread
Kernel Thread
Native Application
Managed Application
Thick Client
Browser Client
Browser and ActiveX Plug-ins
Web Server
Windows Store Process
Properties
Diagram
Name
Sample Portal
Add New Custom Attribute
Notes - 1 entry
Add New Note
Id
Note
Date
Added By
1
Sample Note
03.05.2015 20:54
dev-PC\dev

Implement

- **Storing plaintext passwords**
- **Encrypting passwords**
- **Simply hashing passwords**

Password Retriever

Forgotten your password? No problem! Just enter your email address and postcode below and click the "Retrieve" button. Your password will display on the screen. An email with your password will be also sent to you, please make sure the email address entered is the same as you used when you created your account.

Email *

Display password on screen directly

Retrieve

Important: for your security, please change your password after you get the old one back. To change your password, please Go Here

passw0rd$

6kWK1d4A3ov7YFsuj/2zAA==

U2iuONg98D+CEHkz5n5vUg==

MsBLPOvD/Au05dUmYj/KHA==

Password hash algorithms

1. **PBKDF2**
   - Integrated in plain Java
   - *Iterations* against brute force attacks
2. **bcrypt**
   - Integrated in Spring Security
   - *Iterations* against brute force attacks
3. **scrypt**
   - DoS possibility on servers
   - *Memory* against brute force attacks

Demo

Change # iterations with new hardware

Set a transition period

- Define period of time to update all passwords

Update hashed user password during log-in

- Calculate new random salt
- Calculate new hash with new # iterations

Deactivate not updated user accounts

- Set password to null
- Requires password reset process afterwards

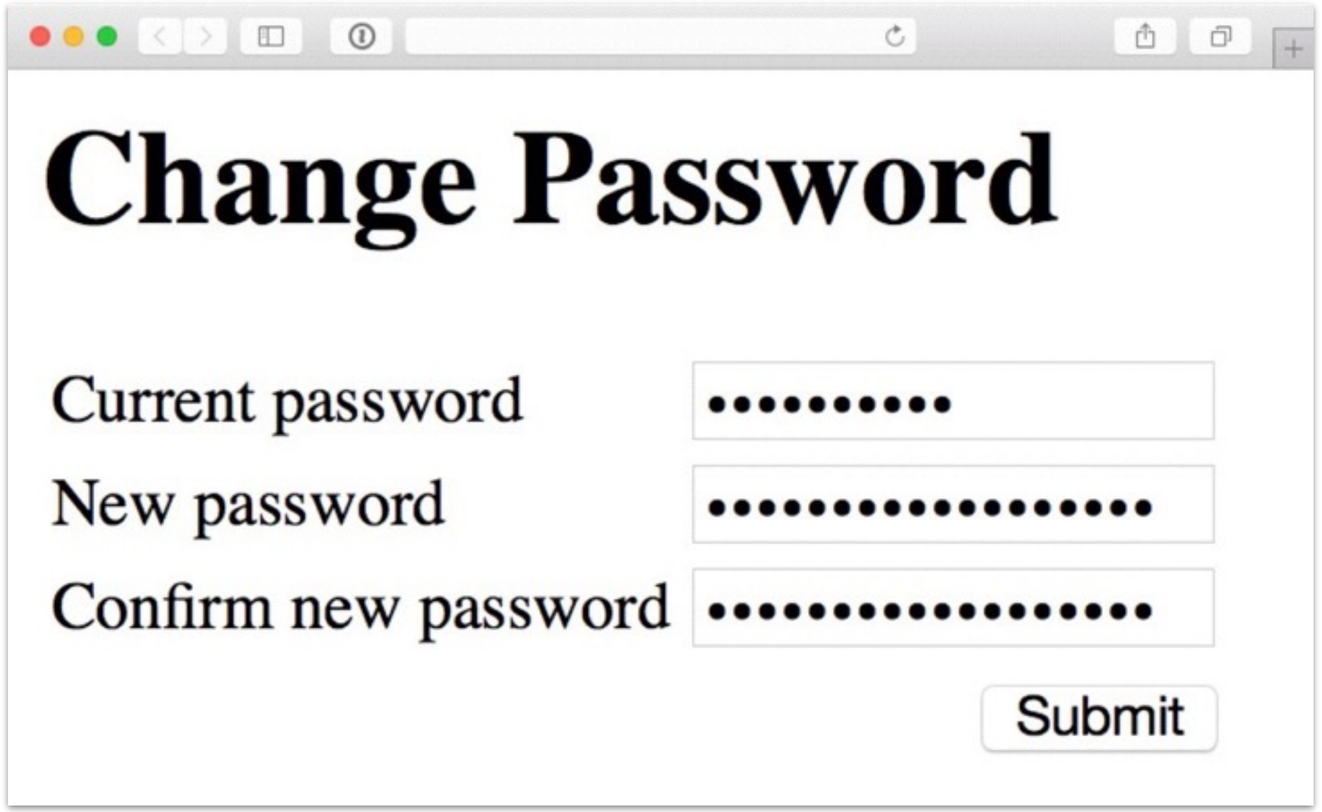
Enforce length limit on password fields

```
<h:inputSecret id="password" maxlength="1024">
 <f:validateLength minimum="10" maximum="1024"/>
</h:inputSecret>
```

Arbitrary length

```
private byte[] hash(PBEKeySpec keySpec) {
   return secretKeyFactory.generateSecret
        (keySpec).getEncoded();
}
```

Fixed length



Prevent unintended password change via

- Cross-Site Request Forgery vulnerability
- Session id knowledge

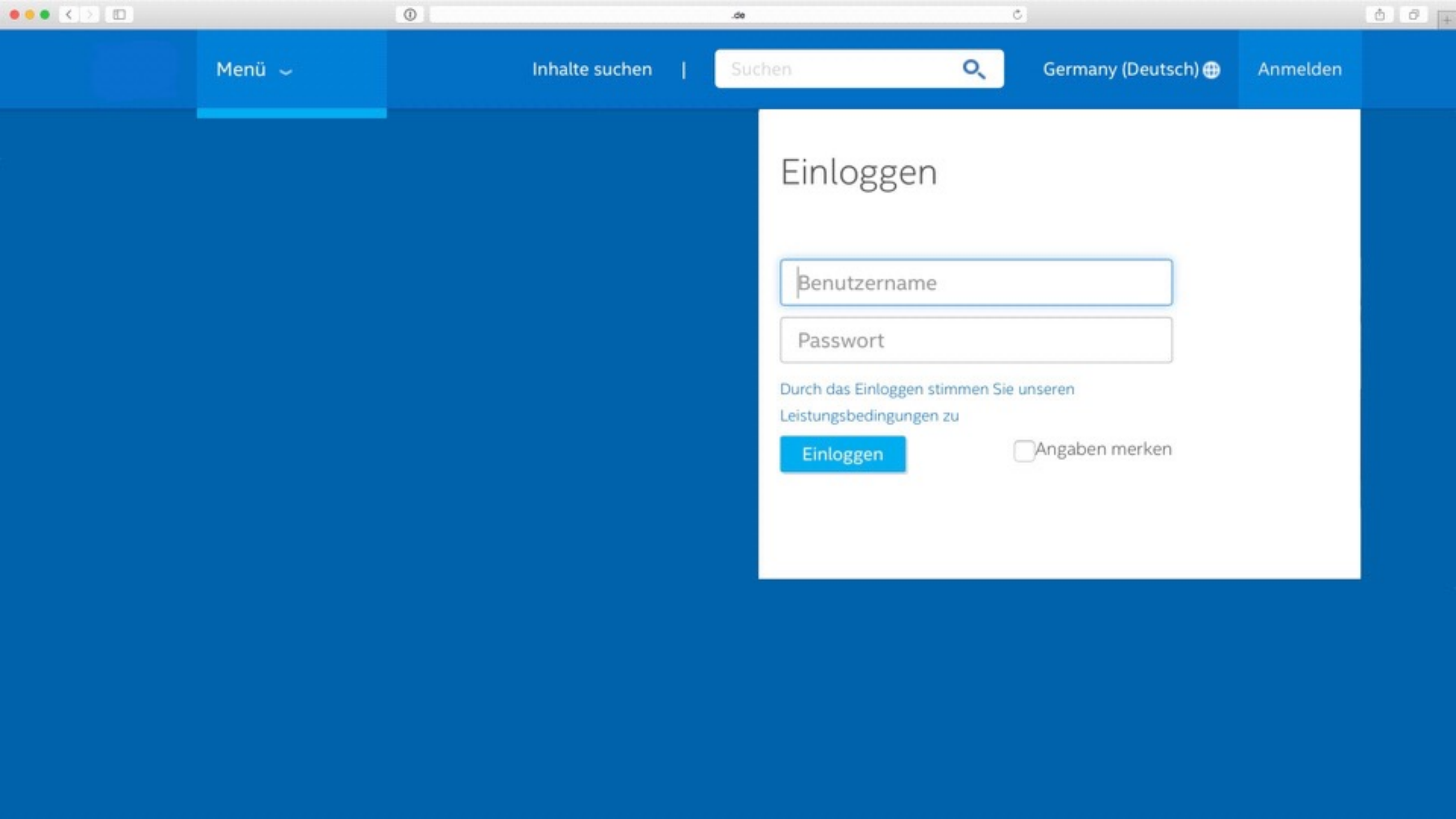
Require password to change account email address

Implement

- Disabling pasting passwords
- Delivering log-in form via HTTP

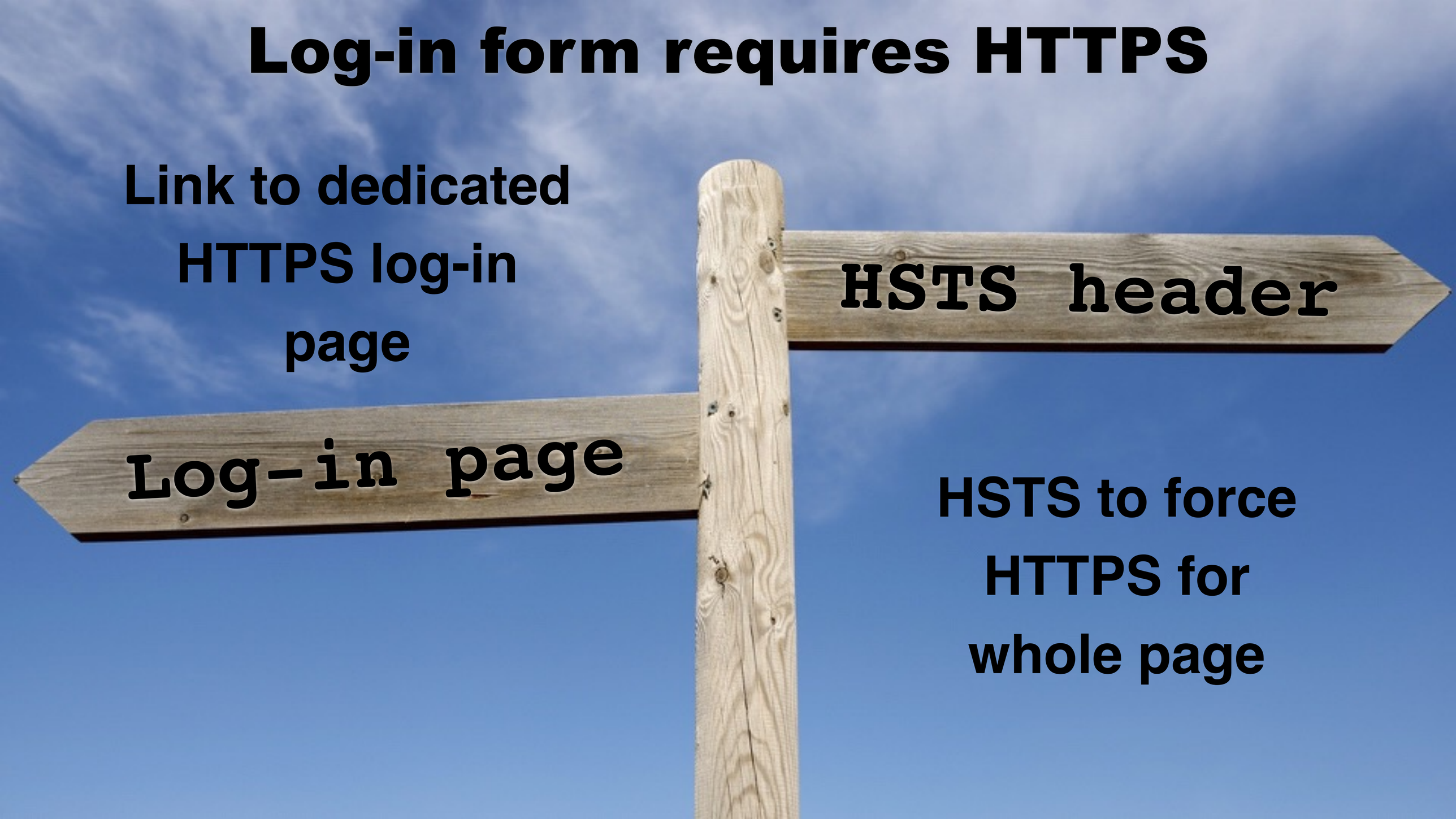
Disabling pasting into password fields

- **Does not** stop any attack
- **Does not** provide any more security
- **Does** frustrate users


.de
Menü
Inhalte suchen
Suchen
Germany (Deutsch)
Anmelden
Einloggen
Benutzername
Passwort
Durch das Einloggen stimmen Sie unseren
Leistungsbedingungen zu
Einloggen
Angaben merken

HTTP log-in page puts security in jeopardy

Log-in form requires HTTPS



Link to dedicated HTTPS log-in page

HSTS to force HTTPS for whole page

```
@WebFilter(urlPatterns = {"/*"})
public class HSTS implements Filter {
  public void doFilter(…) {
    HttpServletResponse response =
     (HttpServletResponse) res;
    response.addHeader(
      "Strict-Transport-Security",
      "max-age=31556926");
    chain.doFilter(req, response);
  }
  // …
}
```

Implement

- Skipping session configuration
- Keeping session id after log-in

```
<plugin>
 <groupId>org.apache.maven.plugins</groupId>
 <artifactId>maven-war-plugin</artifactId>
 <version>2.6</version>
 <configuration>
  <failOnMissingWebXml>
     false
   </failOnMissingWebXml>
 </configuration>
</plugin>
```

```
<web-app ... version="3.1">
 <session-config>
  <!-- idle timeout after session expires -->
  <session-timeout>30</session-timeout>
  <cookie-config>
   <!-- prevent session id script access -->
   <http-only>true</http-only>
   <!-- transfer cookie via https only -->
   <secure>true</secure>
  </cookie-config>
  <!-- session id in cookie, not URL -->
  <tracking-mode>COOKIE</tracking-mode>
 </session-config>
</web-app>
```

User usually receives a session id when visiting web application

Session fixation & session hijacking

Session fixation

- Physical access, URL manipulation, XSS, …
- Victim uses session id provided by attacker

Session hijacking

- Attacker gains access to unprotected session id

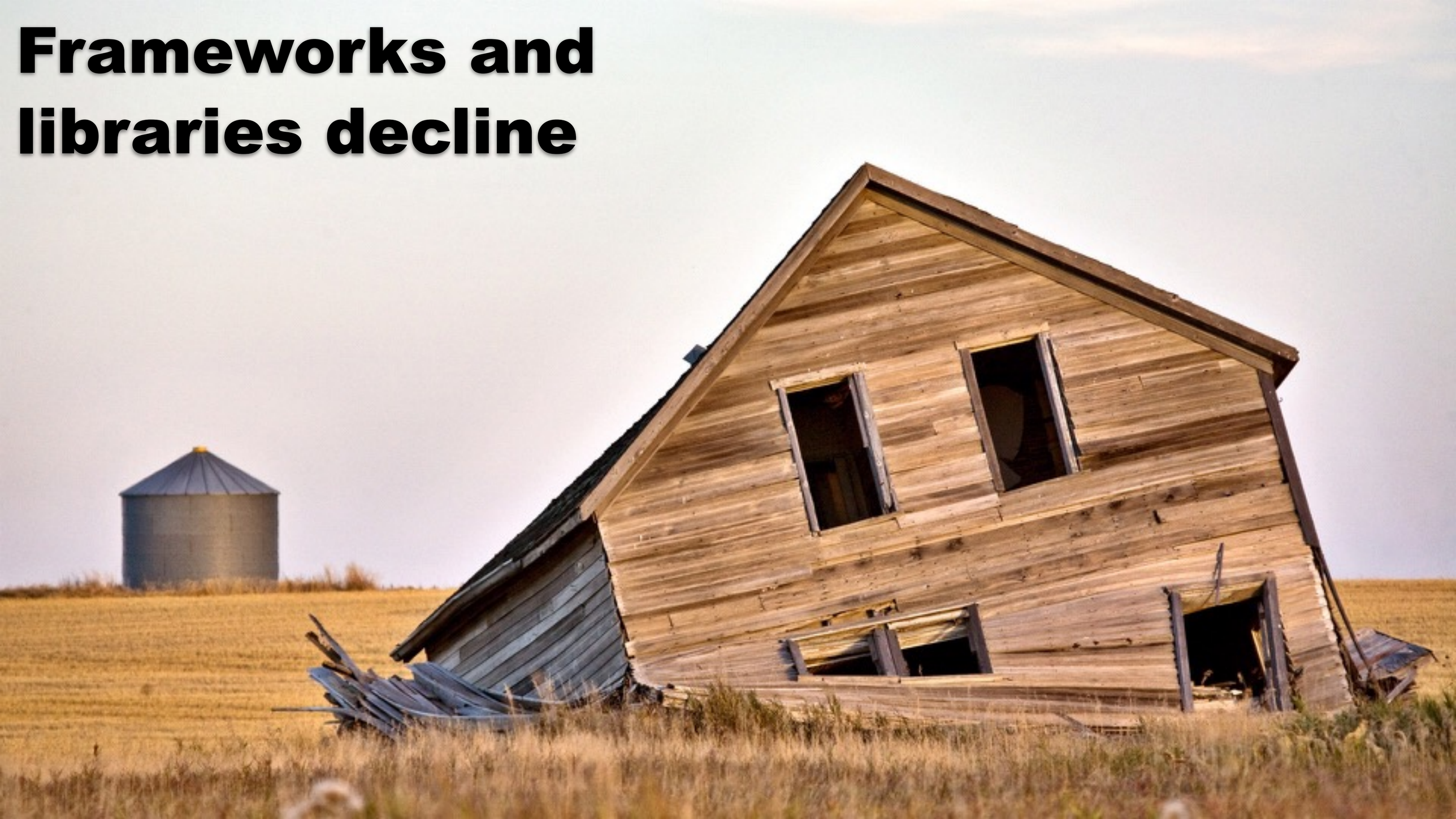
- Limit session duration
- **Force HTTPS**
- **Invalidate session after log-out**
- **Change session id after log-in**

Demo

Maintain

Using outdated libraries

Frameworks and libraries decline



```
Marvin:xss dos$ dependency-check.sh -a XSS -s target/dependency/
Mai 05, 2015 8:42:54 PM org.owasp.dependencycheck.Engine doUpdates
INFORMATION: Checking for updates
Mai 05, 2015 8:44:25 PM org.owasp.dependencycheck.Engine doUpdates
INFORMATION: Check for updates complete
Mai 05, 2015 8:44:25 PM org.owasp.dependencycheck.Engine analyzeDependencies
INFORMATION: Analysis Starting
Mai 05, 2015 8:44:30 PM org.owasp.dependencycheck.Engine analyzeDependencies
INFORMATION: Analysis Complete
Marvin:xss dos$
```

```
<reporting>
 <plugins><plugin>
  <groupId>org.owasp</groupId>
  <artifactId>dependency-check-maven</artifactId>
  <version>1.2.11</version>
  <reportSets>
   <reportSet>
    <reports>
     <report>aggregate</report>
    </reports>
    </reportSet>
   </reportSets>
  </plugin></plugins>
</reporting>
```

Post-build Actions

Publish OWASP Dependency-Check analysis results

Dependency-Check results

Fileset includes setting that specifies the generated raw Dependency-Check XML report files, such as **/dependency-check-report.xml. Basedir of the fileset is the workspace root. If no value is set, then the default **/dependency-check-report.xml is used. Be sure not to include any non-report files into this pattern.

Run always

By default, this plug-in runs only for stable or unstable builds, but not for failed builds. If this plug-in should run even for failed builds then activate this check box.

Detect modules

Determines if Ant or Maven modules should be detected for all files that contain warnings. Activating this option may increase your build time since the detector scans the whole workspace for 'build.xml' or 'pom.xml' files in order to assign the correct module names.

Health thresholds

100% 0%

Configure the thresholds for the build health. If left empty then no health report is created. If the actual number of warnings is between the provided thresholds then the build health is interpolated.

Health priorities

Only priority high Priorities high and normal All priorities

Determines which warning priorities should be considered when evaluating the build health.

Status thresholds (Totals)

	All priorities	Priority high	Priority normal	Priority low
	5	2	3	5

If the number of total warnings is greater than one of these thresholds then a build is considered as unstable or failed, respectively. I.e., a value of 0 means that the build status is changed if there is at least one warning found. Leave this field empty if the state of the build should not depend on the number of warnings.

Compute new warnings (based on the last successful build unless another reference build is chosen below)

Default Encoding

DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

Project: JavaSecurity

Scan Information (show all):

- *dependency-check version*: 1.2.10
- *Report Generated On*: Apr 26, 2015 at 10:21:25 CEST
- *Dependencies Scanned*: 149
- *Vulnerable Dependencies*: 4
- *Vulnerabilities Found*: 23
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
commons-fileupload-1.2.jar	cpe:/a:apache:commons_fileupload:1.2	commons-fileupload:commons-fileupload:1.2	Medium	2	HIGHEST	14
commons-httpclient-3.1.jar	cpe:/a:apache:commons-httpclient:3.1 cpe:/a:apache:httpclient:3.1	commons-httpclient:commons-httpclient:3.1	Medium	2	LOW	15
batik-css-1.7.jar	cpe:/a:apache:batik:1.7	org.apache.xmlgraphics:batik-css:1.7	Medium	1	HIGHEST	14
gson-2.3.1.jar	cpe:/a:google:v8:2.3.1	com.google.code.gson:gson:2.3.1	High	18	LOW	23

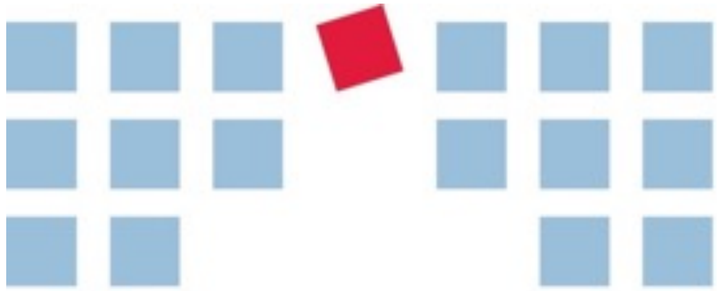
Dependencies

commons-fileupload-1.2.jar

Description: The FileUpload component provides a simple yet flexible means of adding support for multipart file upload functionality to servlets and web applications.

What you do now

- Prepare implementation with threat modeling
- Think when implementing security functionality
- Keep 3rd party libraries up-to-date



bridging IT

Königstraße 42
70173 Stuttgart

dominik.schadow@bridging-it.de
www.bridging-it.de

Blog blog.dominikschadow.de
Twitter @dschadow

Demo Projects
github.com/dschadow/JavaSecurity

HTTP Strict Transport Security RFC
tools.ietf.org/html/rfc6797

Microsoft Threat Modeling Tool
www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

Mozilla SeaSponge
air.mozilla.org/mozilla-winter-of-security-seasponge-a-tool-for-easy-threat-modeling

OWASP Dependency Check
www.owasp.org/index.php/OWASP_Dependency_Check

Spring Security
projects.spring.io/spring-security

Pictures
www.dreamstime.com

Jobs@bridgingIT
www.bridging-it.de/java