Java-Web-Security Anti-Patterns

Entwicklertag | 20.05.2015

Dominik Schadow | bridgingIT

Failed with only the best intentions

Design

Implement

Maintain

Design

Ignoring

… threat modeling

… defense in depth

Threat model prior to implementation

Develop software that is secure by design

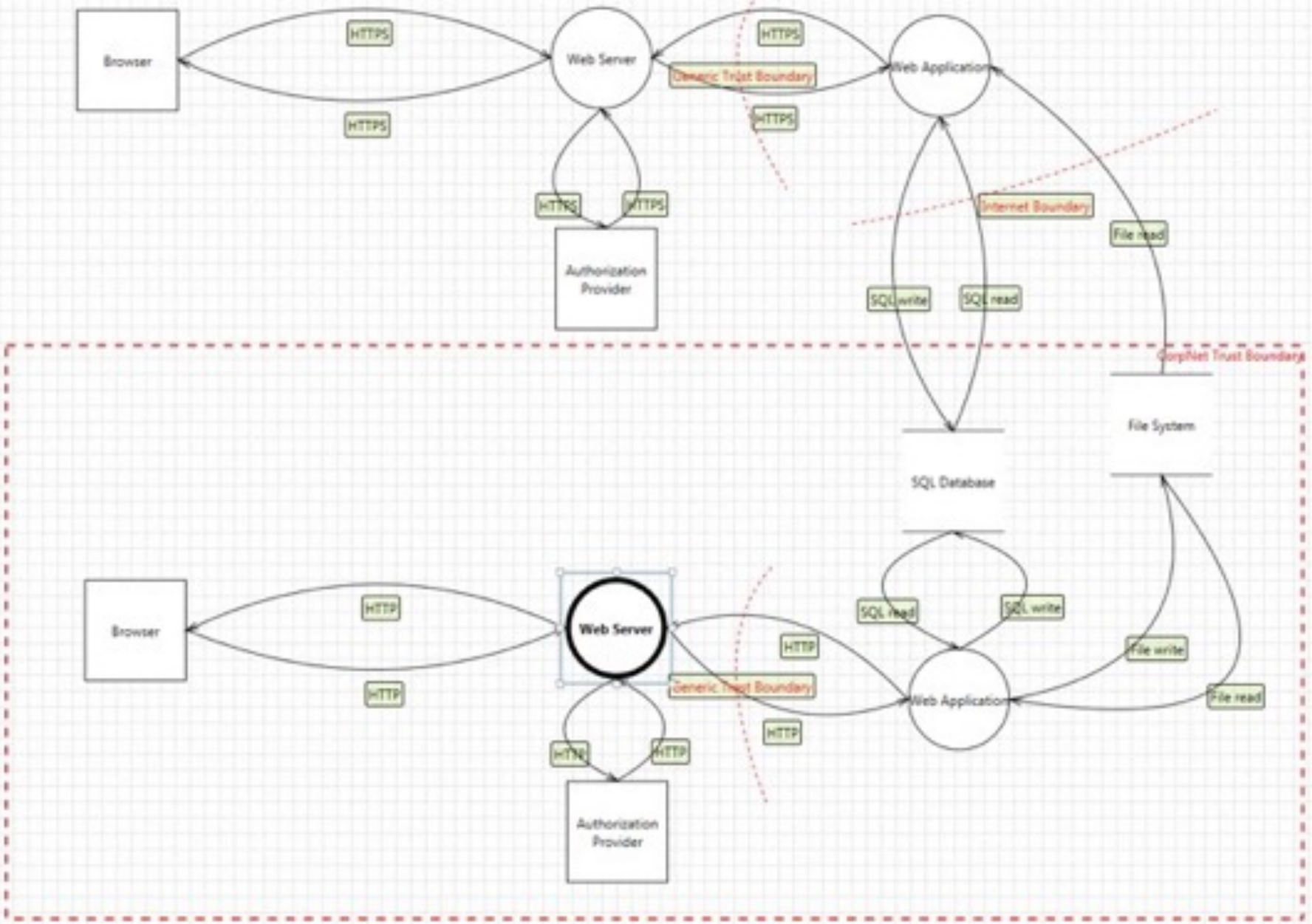
Know the web application

- Environment
- All external entities

Complex Threat Model - Threat Modeling Tool 2024

File Edit View Settings Diagram Reports Help

Portal



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
- Win32 Service
- Web Application

Properties

Web Server

Name	Web Server
Out Of Scope	
Reason For Out Of Scope	

Configurable Attributes

Code Type	Managed
Sanitizes Input	Not Selected
Sanitizes Output	Not Selected

As Generic Process

Running As	Not Selected
Isolation Level	Not Selected
Accepts Input From	Not Selected
Implements or Uses an Authentication Mechanism	No
Implements or Uses an Authorization Mechanism	No
Implements or Uses a Communication Protocol	No

Add New Custom Attribute

Messages - 4 issues found

Description	Severity	Diagram	Ignore
External interactor should communicate over trust boundary.	Warning	Portal	
External interactor should communicate over trust boundary.	Warning	Portal	
External interactor should communicate over trust boundary.	Warning	Portal	
External interactor should communicate over trust boundary.	Warning	Portal	

Messages - 4 issues found | Notes - no entries

Defense in depth

Utilize every software involved

Implement

Passwords stored

… as plaintext (+/- db encryption)

… encrypted

… as a simple hash (+/- salt)

.com

Password Retriever

Forgotten your password? No problem! Just enter your email address and postcode
with your password will be also sent to you, please make sure the email address er

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

Storing passwords

… as plaintext

… encrypted

… simply hashed

Password hash algorithms

1. **PBKDF2**
   - Supported on many platforms
   - Brute force attacks: iteration count
2. **bcrypt**
   - Password length up to 56 bytes
   - Brute force attacks: iteration count
3. **scrypt**
   - Problematic on limited devices/ busy servers
   - Brute force attacks: required memory (RAM)

Demo

Plan for the future

 # iterations must change with new hardware

- Make it configurable
- Define period of time to update all passwords

Update hashed user passwords during log-in

- Change the salt
- Calculate new hash with new # iterations

Deactivate not updated user accounts

- Set password to null
- Setup password reset process to change

Passwords

Change salt during password change

- Never reuse same salt

Add length limit to password fields

- 1024 or 2048 characters are reasonable
- Hashing always reduces it to the same size

Require old password for password change

- Cross-Site Request Forgery vulnerability
- Session id exposed to attacker

Ask for the password when changing the email address

Log-in form

… prevents pasting passwords

… delivered via HTTP

Don’t disable pasting into password fields

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

.com

Email address

Password

Forgot password?

Remember me on this computer

Sign in

"Remember me" uses a cookie. View our Cookie Policy.

Sign in with Twitter

HTTP log-in page puts security in jeopardy

Attacker might change the log-in form action

Load the log-in form over HTTPS

Link to a 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);
  }
  // …
}
```

Sessions

… without configuration

… without changing session id

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

web.xml

session-timeout: 30 (or 60 or 90)

- Idle time in minutes after session expires

http-only: true

- Prevent script access to session cookie

secure: true

- Transfer session cookie only via HTTPS

tracking-mode: cookie

- Prevent session rewriting by storing session id in cookie, not in URL

```
<web-app ... version="3.1">
 <!-- ... -->
 <session-config>
  <!-- idle timeout -->
  <session-timeout>30</session-timeout>
  <cookie-config>
   <!-- prevent script access -->
   <http-only>true</http-only>
   <!-- HTTPS only -->
   <secure>true</secure>
  </cookie-config>
  <!-- no session rewriting -->
  <tracking-mode>COOKIE</tracking-mode>
 </session-config>
</web-app>
```


4E01EF46D8446D1C1
0CB5C08EDA69DD1
User usually receives a session id when visiting web application

Attacker dictates user's session id

- Attacker uses physical access, URL manipulation or Cross-Site Scripting to create known session id
- Victim logs in, keeps using session id

Mitigate session fixation

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

Demo

Maintain

Deployment

… with outdated 3rd party libs

Frameworks and libraries decline

```
Last login: Fri Apr 17 12:14:00 on ttys000
Marvin:sql-injection dos$ dependency-check.sh -a SQL-Injection -s target/dependency/
Apr 17, 2015 12:15:22 PM org.owasp.dependencycheck.Engine doUpdates
INFORMATION: Checking for updates
Apr 17, 2015 12:16:08 PM org.owasp.dependencycheck.data.update.task.DownloadTask call
INFORMATION: Download Started for NVD CVE - Modified
Apr 17, 2015 12:16:32 PM org.owasp.dependencycheck.data.update.task.DownloadTask call
INFORMATION: Download Complete for NVD CVE - Modified
Apr 17, 2015 12:16:32 PM org.owasp.dependencycheck.data.update.task.ProcessTask processFi
les
INFORMATION: Processing Started for NVD CVE - Modified
Apr 17, 2015 12:16:37 PM org.owasp.dependencycheck.data.update.task.ProcessTask processFi
les
INFORMATION: Processing Complete for NVD CVE - Modified
Apr 17, 2015 12:16:37 PM org.owasp.dependencycheck.data.update.StandardUpdate update
INFORMATION: Begin database maintenance.
Apr 17, 2015 12:16:44 PM org.owasp.dependencycheck.data.update.StandardUpdate update
INFORMATION: End database maintenance.
Apr 17, 2015 12:16:45 PM org.owasp.dependencycheck.Engine doUpdates
INFORMATION: Check for updates complete
Apr 17, 2015 12:16:45 PM org.owasp.dependencycheck.Engine analyzeDependencies
INFORMATION: Analysis Starting
Apr 17, 2015 12:17:13 PM org.owasp.dependencycheck.analyzer.CentralAnalyzer analyzeFileTy
pe
WARNUNG: Unable to download pom.xml for hibernate-jpa-2.1-api-1.0.0.Final.jar from Centra
l; this could result in undetected CPE/CVEs.
Apr 17, 2015 12:17:25 PM org.owasp.dependencycheck.Engine analyzeDependencies
INFORMATION: Analysis Complete
Marvin:sql-injection dos$
```

```
<reporting>
 <plugins><plugin>
   <groupId>org.owasp</groupId>
   <artifactId>
    dependency-check-maven
   </artifactId>
   <version>1.2.10</version>
   <reportSets><reportSet>
     <reports>
      <report>aggregate</report>
     </reports>
   </reportSet></reportSets>
  </plugin></plugins>
</reporting>
```

DEPENDENCY-CHECK

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.

File Path: /Users/dos/.m2/repository/commons-fileupload/commons-fileupload/1.2/commons-fileupload-1.2.jar
MD5: c9021a6ed3d7d399ca96a7d9d9c84bb1
SHA1: a10c06183fe21f3bb3dda3b5946b93db6e2ad5cc
Referenced In Projects:

- Direct Object References
- SQL-Injection

Evidence

Integrate Dependency Check into your Jenkins toolchain

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

BridgingIT GmbH

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

Recx Security Analyser
www.recx.co.uk/products/chromeplugin.php

Spring Security
projects.spring.io/spring-security

Pictures
www.dreamstime.com