

Java ist doch schon sicher?!



Entwicklertag - 21.05.2014
Dominik Schadow - bridgingIT



Ungefähr 56.800.000 Ergebnisse (0,31 Sekunden)

Java | heise Security - Heise Online

www.heise.de › [Security](#) › [Erste Hilfe](#) › [Browsercheck](#) ▾

Wegen einer aktuellen Sicherheitslücke sollten Sie **Java** derzeit nicht einsetzen. Falls **Java** oben als "aktiv" angezeigt wird, deaktivieren Sie die Erweiterung im ...

Java security - Wikipedia, the free encyclopedia

en.wikipedia.org/wiki/Java_security ▾ [Diese Seite übersetzen](#)

The **Java** platform provides a number of features designed to improve the **security** of **Java** applications. This includes enforcing runtime constraints through the ...

Was muss ich tun, wenn ich einen Sicherheitshinweis ... - Java

<https://www.java.com/de/download/help/appsecuritydialogs.xml> ▾

Das Update 21 für **Java** 7 hat Veränderungen im Verhalten des **Java**-Browser-Plug-ins eingeführt, durch die Sie besser informierte Entscheidungen treffen ...

java.com Java Security Resources

www.java.com/en/security/ ▾ [Diese Seite übersetzen](#)

This page is a reference on **security** for **Java**. It also provides additional resources to related sites.

What Developers Need to Know About Java Security

www.java.com/en/security/developer-info.jsp ▾ [Diese Seite übersetzen](#)

What Developers Need to Know About **Java Security**. Duke and security shield. Java is the most powerful tool you can use as a developer to deliver full featured ...

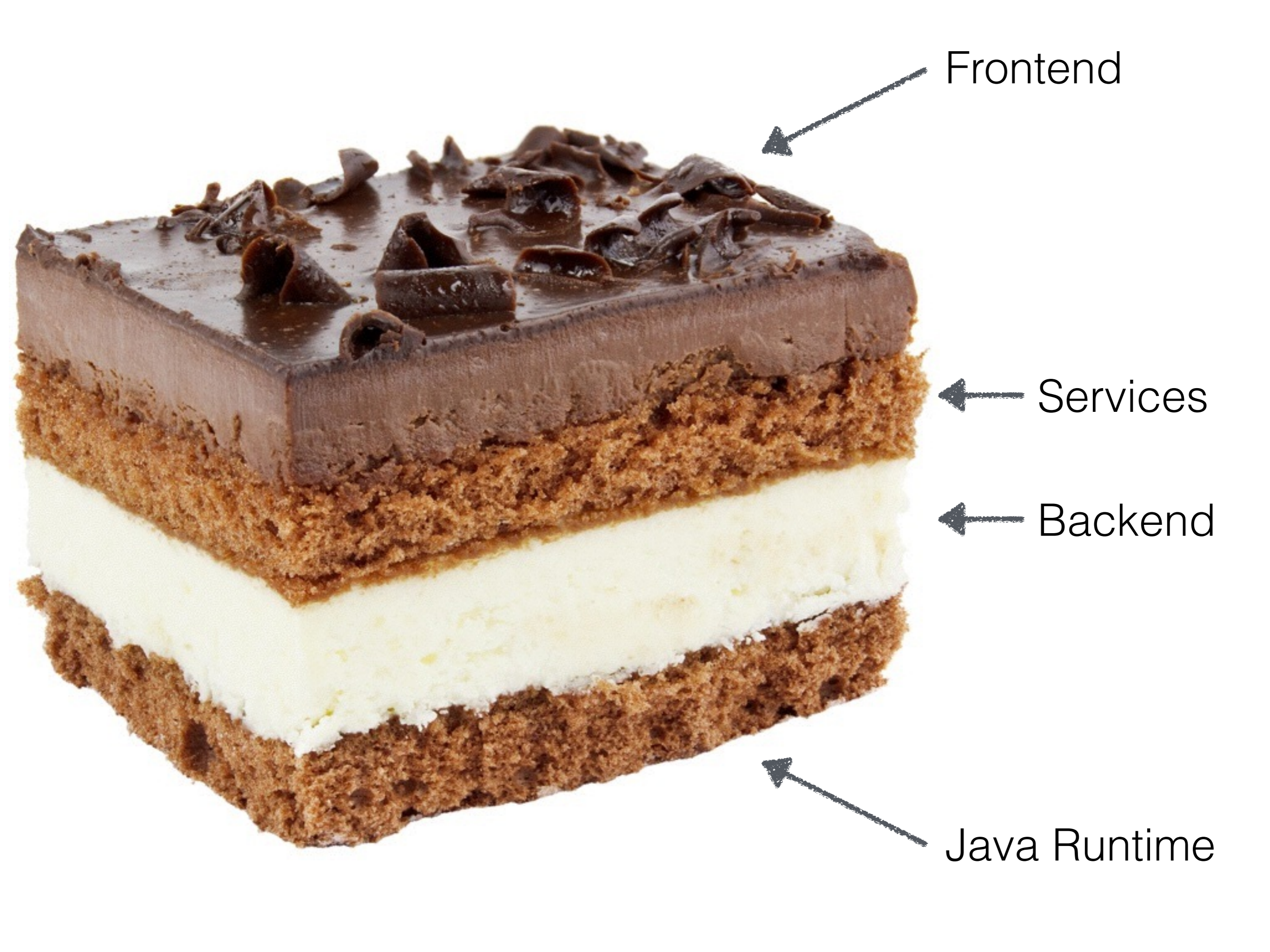
How to Control Concurrent Active User session in Java Web ...



<https://plus.google.com/.../dkn7Nw9r1YN> ▾ [Diese Seite übersetzen](#)

Javarevisited

04.04.2014 - How to Control Concurrent Active User session in **Java** Web Application using Spring **Security** Spring **security** offer many Out Of Box feature required in a Secure ...



Frontend

Services

Backend

Java Runtime

Java Runtime takes care of the security baseline



Cross-Site Request Forgery

Authorization
SQL Injection

3rd Party Libraries

Web Application Firewall Authentication
Cross-Site Scripting

Access Control Redirects

Transport Layer Security
Clickjacking

Security

Session Management

Output Escaping

Input Validation

Security Misconfiguration

Presentation Layer Access Control

Session Fixation

Direct Object References

Cookie Theft

Cryptography

Privacy

XPath Injection

Vulnerabilities Man in the Middle Attacks

Sensitive Data Exposure



**3rd party
library usage**

**Cross-Site
Request Forgery**

**Cross-Site
Scripting**

Cross-Site Scripting (XSS)

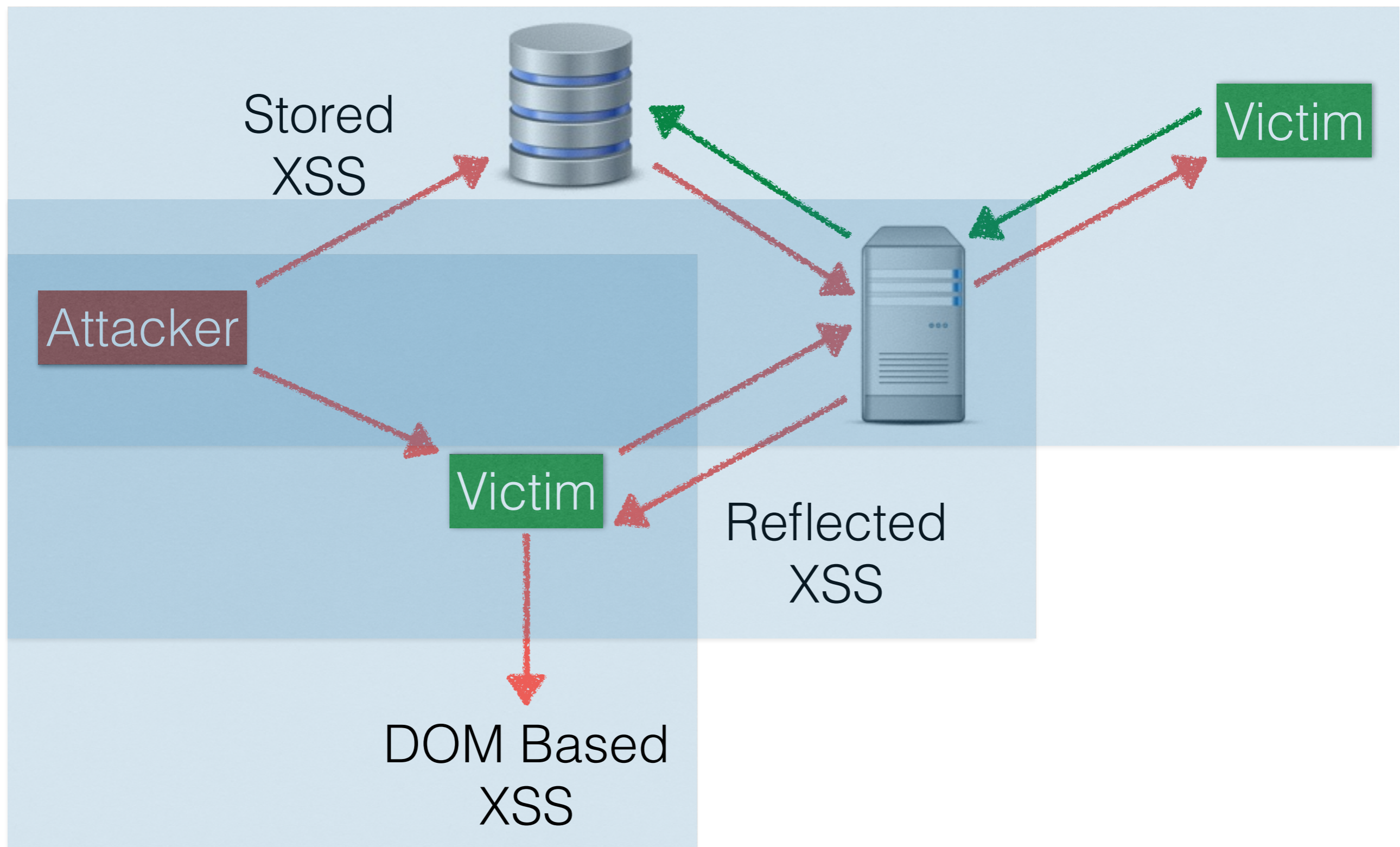


Access victims' session credentials

- ▣ Site defacement
- ▣ Undermine CSRF defense
- ▣ Redirects (phishing)
- ▣ Load scripts
- ▣ Data theft



Attacker injected code executed in web application



Always validate all input and escape all output



Libraries for Cross-Site Scripting countermeasures

Output escaping

Coverity Security Library

github.com/coverity/coverity-security-library

OWASP Java Encoder

www.owasp.org/index.php/OWASP_Java_Encoder_Project

Allow selected HTML tags/ attributes

OWASP HTML Sanitizer

www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project

Content Security Policy is framework independent

~~<script>alert(document.cookie)</script>~~

Send

**Blocks ALL
inline scripts**

Whitelist valid resource URLs

```
response.setHeader("Content-Security-Policy",  
"default-src 'self'; img-src *; object-src  
applets.sample.de; script-src  
scripts.sample.com; style-src *.sample.com");
```

Report only as test mode

```
response.setHeader("Content-Security-Policy-  
Report-Only", "default-src 'self'; report-uri  
CSPReporting");
```

Session-Cookie protection via web.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app ... version="3.1">
  <!-- ... -->
  <session-config>
    <session-timeout>30</session-timeout>
    <cookie-config>
      <http-only>true</http-only>
    </cookie-config>
    <tracking-mode>COOKIE</tracking-mode>
  </session-config>
</web-app>
```



Tomcat 7

Intercept requests/ responses with OWASP ZAP

The screenshot displays the OWASP ZAP interface. The left pane shows a tree view of sites, with the selected site being `http://localhost:8080`. The right pane shows the details of a intercepted POST request to `http://localhost:8080/XSS/index.xhtml`. The request headers include `Host: localhost:8080`, `User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:28.0) Gecko/20100101 Firefox/28.0`, and a `Cookie: JSESSIONID=EF831D89B7CE4F4E4233C66DB1757C8E`. The request body is a form with several parameters, including `standardForm%3Astandard` which contains the payload `<script>alert(document.cookie)</script>`.

Type	Parameter Name	Value	Functions
form	javax.faces.ViewState	8533353928494726999%3A-8205946838961632672	Addins
form	standardForm	standardForm	Addins
form	standardForm%3Aj_idt7	Send	Addins
form	standardForm%3Astandard	<script>alert(document.cookie)</script>	Addins
form			Addins

The bottom pane shows the request history with the following entries:

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	20/04/14 12:29:17	GET	http://localhost:8080/XSS/	200 OK		24 ms	1.61 KiB	Low		Form, Hidden, AntiCSRF
3	20/04/14 12:29:17	GET	http://localhost:8080/XSS/styles.css	404 Not Found		8 ms	979 bytes	Low		Comment
5	20/04/14 12:29:17	GET	http://localhost:8080/XSS/javax.faces.resource/styl...	200 OK		7 ms	123 bytes	Low		

Demo

Content Security Policy as second layer of defense



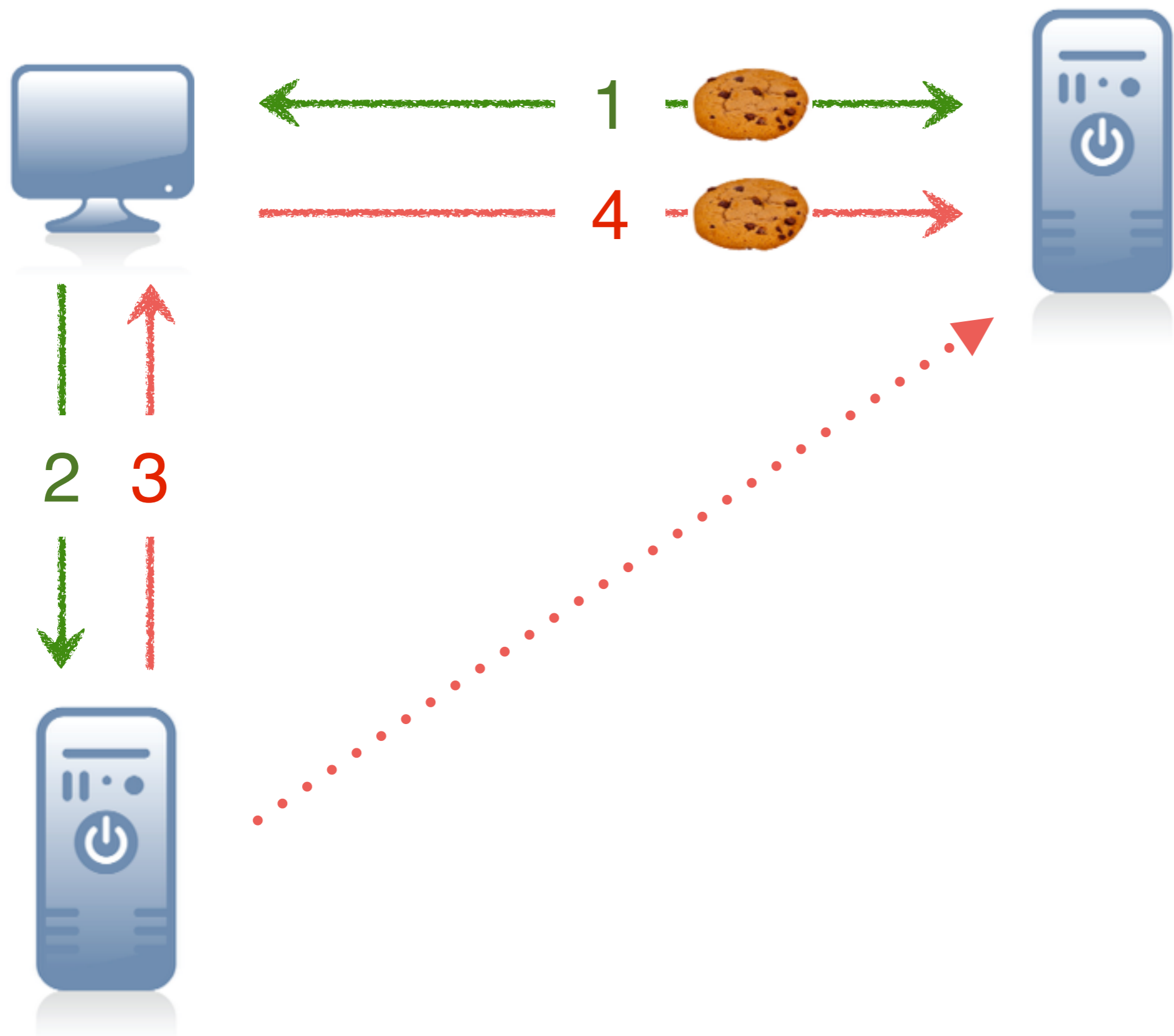
Cross-Site Request Forgery (CSRF)



Using victims' credentials to gain access



CSRF utilizes fire and forget requests



Stop fake requests with random anti CSRF tokens



CSRF protection in libraries and frameworks

Built-in protection

JavaServer Faces (improved in 2.2)

jcp.org/en/jsr/detail?id=344

CSRF extension

Spring Security 3.2

projects.spring.io/spring-security

Enterprise Security API

www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API

Test your CSRF protection with faked tokens

Untitled Session - OWASP ZAP

Schnellstart Request Response Break Skripting-Konsole

Method: POST Header: Text Body: Table

```
POST http://localhost:8080/Ch08_CSRF/ProtectedServlet HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:28.0) Gecko/20100101 Firefox/28.0
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
Referer: http://localhost:8080/Ch08_CSRF/requests-protected.jsp
Cookie: JSESSIONID=0F6FDEBCF93BB19AB412C840DCC8ECD2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
```

Type	Parameter Name	Value	Functions
form	CSRF_TOKEN	2952260897245276622	AddIns
form	name	Test	AddIns

Ch08_CSRF

Groundspeed

Reload Forms

Forms

- greetingProtected (FORM)
 - CSRF_TOKEN (HIDDEN)
 - name (TEXT)
 - <unknown> (SUBMIT)

Attributes

- type = hidden
- value = 2952260897245276622
- name = CSRF_TOKEN

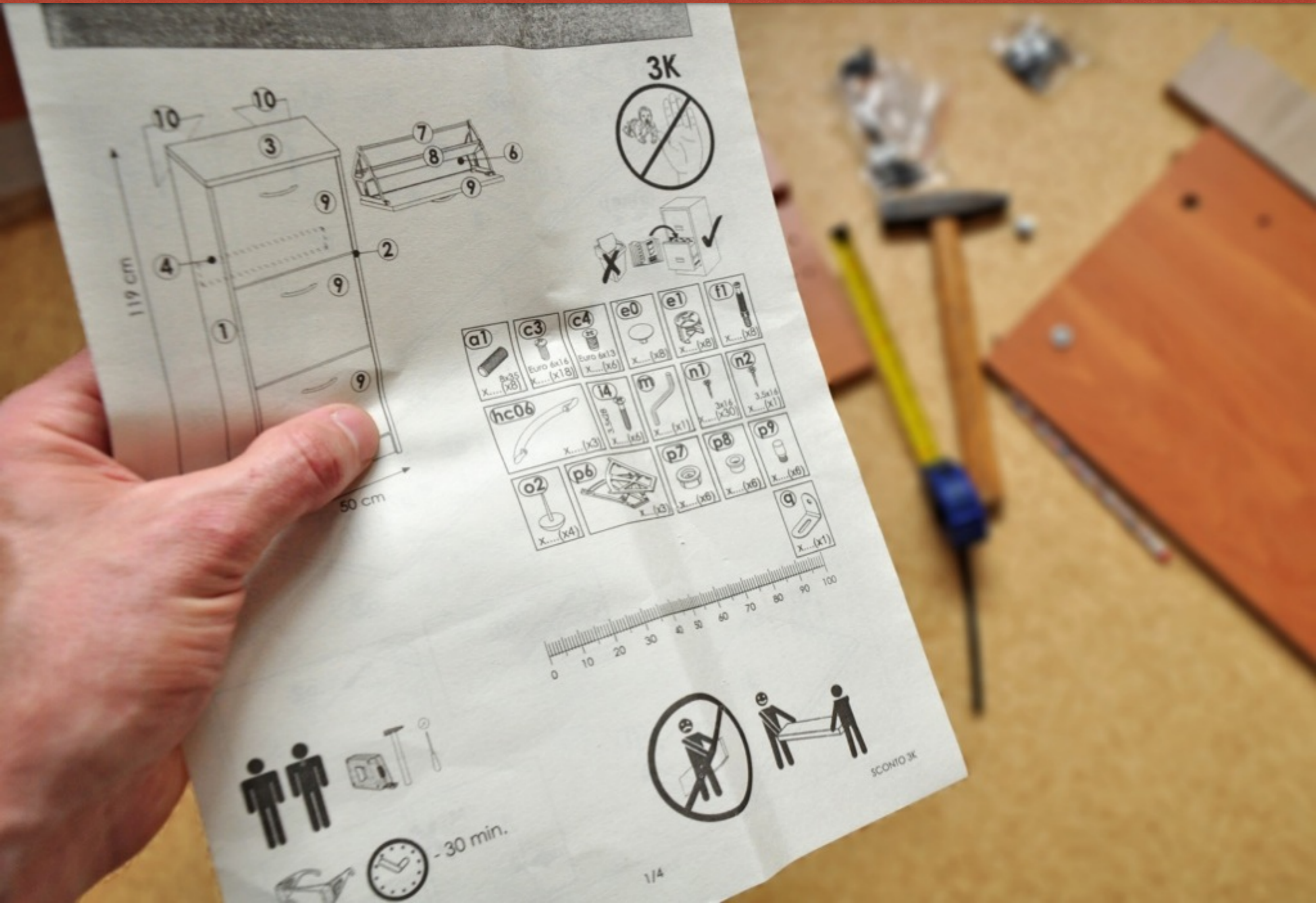
CSRF_TOKEN (HIDDEN)
CSRF_TOKEN = 2952260897245276622

Name

www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
addons.mozilla.org/en-US/firefox/addon/groundspeed

Demo

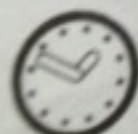
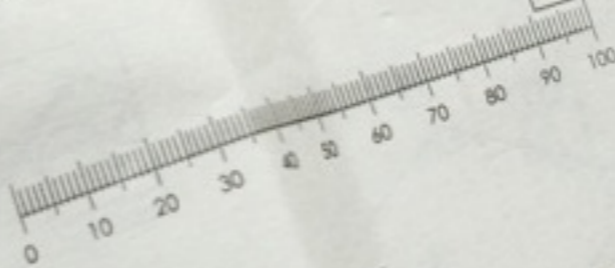
3rd party library usage



3K



a1 x... (x8)	c3 Euro 6x16 x... (x18)	c4 Euro 6x13 x... (x6)	e0 x... (x8)	e1 x... (x8)	f1 x... (x8)
hc06 x... (x3)	l4 x... (x6)	m x... (x1)	n1 3x16 x... (x30)	n2 3.5x16 x... (x1)	
o2 x... (x4)	p6 x... (x3)	p7 x... (x6)	p8 x... (x6)	p9 x... (x6)	g x... (x1)



- 30 min.



SCONTO 3K

Code, libraries and configuration belong together



Test the functionality you rely on



Outdated libraries imply a false sense of security



Find insecure libs with OWASP Dependency Check

```
Ch07_XSS — bash — 60x5
Last login: Sun Apr 20 13:53:02 on ttys001
marvin:Ch07_XSS dos$ mvn dependency:copy-dependencies
```

```
Ch07_XSS — bash — 63x5
Last login: Sun Apr 20 13:58:32 on ttys001
marvin:Ch07_XSS dos$ dependency-check.sh --app Ch07_XSS --out .
--scan target/dependency
```

Not every vulnerability may affect your application



Dependency-Check Report

Suche oder Adresse eingeben

Dependency-Check Report

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: Ch06

Scan Information ([show all](#)):

- *dependency-check version*: 1.2.1
- *Report Generated On*: Mai 11, 2014 at 15:15:47 MESZ
- *Dependencies Scanned*: 37
- *Vulnerable Dependencies*: 2
- *Vulnerabilities Found*: 3
- *Vulnerabilities Suppressed*: 0
- ...

Dependency Display: [show all](#)

- [commons-fileupload-1.2.jar](#)
- [javassist-3.18.1-GA.jar](#)

Dependencies

commons-fileupload-1.2.jar

Widespread outdated libs impose a greater risk



- ❑ Java is as (in)secure as most other languages
- ❑ Java can't prevent every development bug
- ❑ (Web) application security is always the developers' job

Developers make
the difference





Dominik Schadow

dominik.schadow@bridging-it.de

www.bridging-it.de

BridgingIT GmbH

Königstraße 42

70173 Stuttgart

Blog blog.dominikschadow.de

Twitter/ADN @dschadow

Demo Projects

github.com/dschadow/JavaSecurity

OWASP

www.owasp.org

Pictures

www.dreamstime.com

