

SLEEP
WELL



ALL YOUR TESTS
ARE GREEN

“... use the source ...”

How secure your web framework is?

Based on Apache Struts 2

@lukaszlenart
@TheApacheStruts
lukaszlenart@apache.org



Agenda

- About me
- What is the Apache Struts 2
- Hacking the framework
 - S2-006 aka Client side code injection
 - S2-008 aka Remote Command Execution
 - S2-009 aka RCE strikes back
 - S2-011 aka DoS
- What about the others
- Home work
- Q&A



About me

- Apache Struts 2 Lead & Member of ASF
- Creative Software Engineer  SOFTWAREMILL
- Blogger, @lukaszlenart
- IntelliJ IDEA addict ☺
- JetBrains Development Academy Member
- Husband, father ☺

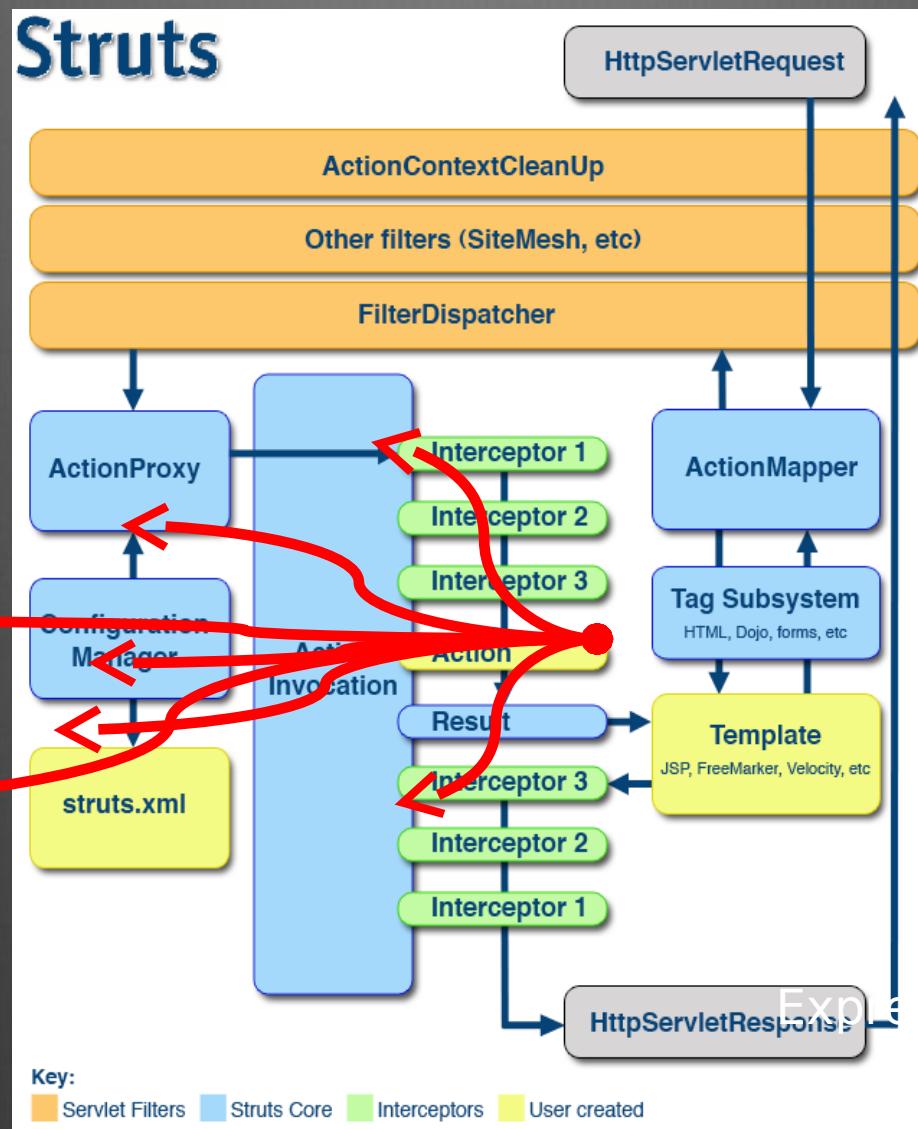
Struts 1 is dead, baby ☐

- Struts 2 is a new kid on the block
 - No single line shared with Struts 1
 - No form beans, no session-scoped actions
 - Pure POJOs, Interface steering
 - Strongly interceptor oriented
 - Highly extendable – lots of plugins
 - Designed to be customizable
 - Powerful OGNL expression language
- Struts 1 reached EOL!

With great power...



How does it work?



Expansion Language

Expressions are everywhere

struts.xml

```
<action name="index" class="org.demo.MyAction" method="index">
    <result name="input">index.jsp</result>
    <result type="redirect">${actionName}</result>
</action>
```

index.jsp

```
<s:form action="submitAddressesInfo" namespace="/conversion">
    <s:iterator value="%{new int[3]}" status="stat">
        <s:textfield label="%{'Address '#stat.index}"
                     name="%{'addresses(\\"id'#{stat.index}+'\\").address'}" />
    </s:iterator>
    <s:submit cssClass="btn btn-primary"/>
</s:form>
```

indexAction.properties

```
HelloWorld.message= Struts is up and running ...
requiredstring = ${getText(fieldName)} is required.
password = Password
username = User Name
Missing.message = This feature is under construction.
```

have one's finger on the pulse

Prior Releases

As a courtesy, we retain archival copies of the website for releases that initially were considered "General Availability" but which has been reclassified as "Not recommended" since they contain security issues

Release	Release Date	Vulnerability	Version Notes
Struts 2.3.7	19 November 2012		Version notes
Struts 2.3.4.1	13 August 2012		Version notes
Struts 2.3.4	12 May 2012	S2-010, S2-011	Version notes
Struts 2.3.3	16 April 2012	likely: S2-010, S2-011	Version notes
Struts 2.3.1.2	22 January 2012	likely: S2-010, S2-011	Version notes
Struts 2.3.1.1	25 December 2011	S2-009 likely: S2-010, S2-011	Version notes
Struts 2.3.1	12 December 2011	S2-008, likely: S2-009, S2-010, S2-011	Version notes
Struts 2.2.3.1	7 September 2011	likely: S2-008, S2-009, S2-010, S2-011	Version notes
Struts 2.2.3	7 September 2011	S2-007, likely: S2-008, S2-009, S2-010, S2-011	Version notes
Struts 2.2.1.1	20 December 2010	S2-006, likely: S2-007, S2-008, S2-009, S2-010, S2-011	Version notes
Struts 2.2.1	16 August 2010	likely: S2-006, S2-007, S2-008, S2-009, S2-010, S2-011	Version notes
Struts 2.1.8.1	16 November 2009	S2-005, likely: S2-006, S2-007, S2-008, S2-009, S2-010, S2-011	Version notes
Struts 2.1.8	30 September 2009	likely: S2-005, S2-006, S2-007, S2-008, S2-009, S2-010, S2-011	Version notes

First question to keep your focus □

Is it Cruiser or Chopper?



Cruiser

Hacking the framework

....

be the bad guy

S2-006 aka Client side code injection

- When Dynamic Method Invocation is enabled action name is generated base on the provided request
- Non-existing action will generate an error page with injected client code
 - Issue is specific to Weblogic server
- <http://struts.apache.org/2.x/docs/s2-006.html>

S2-006 aka Client side code injection - example

- /HelloWorld.action?action%3Alogin!login
%3AcantLogin%3Cscript%3Ealert
%28window.location%29%3C%2Fscript%3E
%3Dsome_value=Submit

S2-006 aka Client side code injection - solution

- Disable DMI
- <constant name="struts.enable.DynamicMethodInvocation" value="false" />
- Upgrade to Struts 2.2.3
- Don't use Weblogic ;-)

S2-008 aka Remote Command Execution

- Conversion error is evaluated as an expression
- Cookie name is evaluated as an expression
- With “!” (bang) you can access any public method of action
 - Only when Dynamic Method Invocation is set to true, is set to true by default
- <http://struts.apache.org/2.x/docs/s2-008.html>

S2-008 aka Remote Command Execution - example

- /hello.action?id='%2b(new Object())%2b'
- Cookie:
@java.lang.Runtime@getRuntime().exec()=1
- /mywebapp/recover!getPassword.action

S2-008 aka Remote Command Execution - solution

- Disable DMI
 - <constant name="struts.enable.DynamicMethodInvocation" value="false" />
- Review your action public methods
- Use Strict DMI – list of allowed methods
- DMI disabled by default as from Struts 2.3.1
- Upgrade to Struts 2.3.1!

Does Poland has access to sea?

As defined by EU

No □

S2-009 aka RCE strikes back

- An arbitrary code can be executed on server
 - Encoded value of parameter is parsed as an OGNL expression
- <http://struts.apache.org/2.x/docs/s2-009.html>

S2-009 aka RCE strikes back - example

```
•/action?foo=%28%23context[%22xwork.MethodAccessor.denyMethodExecution%22]%3D+new+java.lang.Boolean%28false%29,%20%23_memberAccess[%22allowStaticMethodAccess%22]%3d+new+java.lang.Boolean%28true%29,%20@java.lang.Runtime@getRuntime%28%29.exec%28%27mkdir%20/tmp/PWNAGE%27%29%29%28meh%29&z[%28foo%29%28%27meh%27%29]=true
```

S2-009 aka RCE strikes back - solution

- Stronger pattern for parameter names
- OGNL only sets value, does not evaluate it
- Workaround
 - add a filter to filter out all the suspicious looking parameters/headers
- Upgrade to Struts 2.3.1.2

S2-011 aka DoS

- Denial of Service
 - Long request parameter name is evaluated by OGNL and consumes significant CPU cycle
- <http://struts.apache.org/2.x/docs/s2-011.html>

S2-011 aka DoS - example

- POST /home
veryveryveryevenveryveryveryveryveryveryveryve
ryevenevenveryveryveryverylong
parametername=1
- 300 request
- parameter name length = 1000000

S2-011 aka DoS - solution

- Add parameter name length limit
 - By default 100 characters
 - User can change the limit
- Workaround
 - add a filter to filter out all the parameters longer than xxx
- Upgrade to Struts 2.3.4.1

Sx-xxx aka more to come

....

You never know what future will bring for us ☺

What about the others

www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-6117/Apache-Struts.html

CVE Details

The ultimate security vulnerability datasource

Log In Register Reset Password Activate Account

Log In Register Reset Password Activate Account

Home

Browse :

- Vendors
- Products
- By Date
- 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

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback

Apache » Struts : 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

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2012-4387	264		DoS	2012-09-05	2012-09-13	5.0
2	CVE-2012-4386	352		CSRF	2012-09-05	2012-09-06	6.8
3	CVE-2012-1007	79		XSS	2012-02-06	2012-02-13	4.3
4	CVE-2012-1006	79		XSS	2012-02-06	2012-02-13	4.3
5	CVE-2012-0838	20		Exec Code	2012-03-02	2012-03-05	7.5
6	CVE-2012-0394	94	1	Exec Code	2012-01-08	2012-01-09	6.8

** DISPUTED ** The DebuggingInterceptor component in Apache Struts before 2.3.1.1, when developer mode is enabled, evaluates a string as an OGNL expression during the handling of a conversion of an arbitrary code, via invalid input to a field.

NOTE: the vendor characterizes this behavior as not "a security vulnerability itself."

Home work

- Check how vulnerable your current web framework is
- Find a security vulnerability, try to inject JavaScript, etc.
- Report back to the project team

Q&A

This is the end,
questions?

<https://github.com/lukaszlenart/how-secure-your-framework-is>

@lukaszlenart
@TheApacheStruts
lukaszlenart@apache.org

Are these questions are related
to presentation?

Yes

I own Yamaha DragStar and I'm from Poland!

T-Shirts sponsored by

.ill. SOFTWAREMILL

Thank you!

