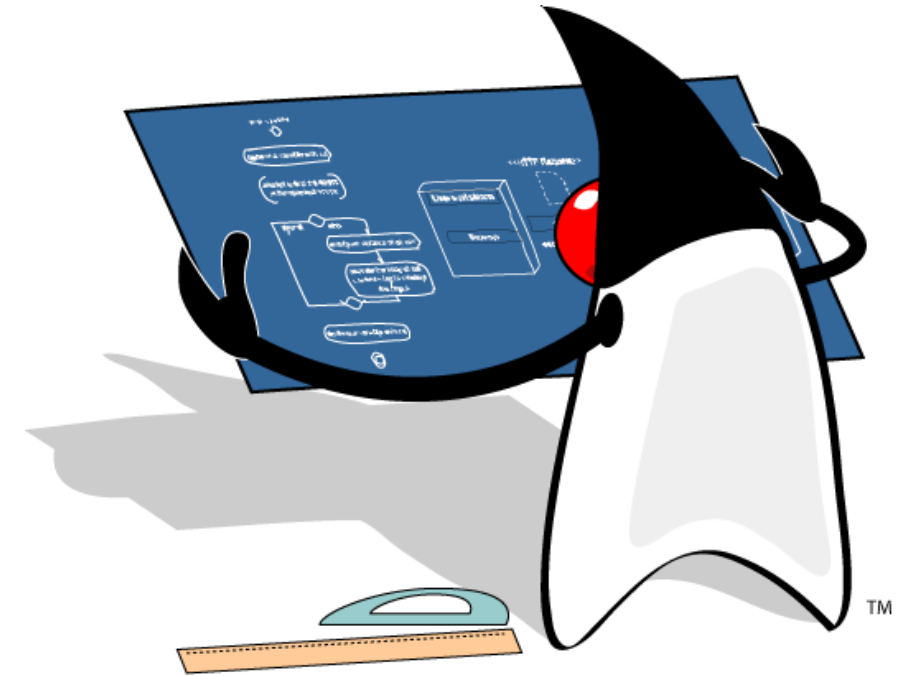# Workshop:
Advanced Java Application Code Review

Philippe Arteau
Security Researcher at GoSecure

44CON

14/09/2016

What is this Training About?

- Agenda (2 hours training)
  - Introduction to SonarQube
  - **Code review** exercises divided in 6 modules
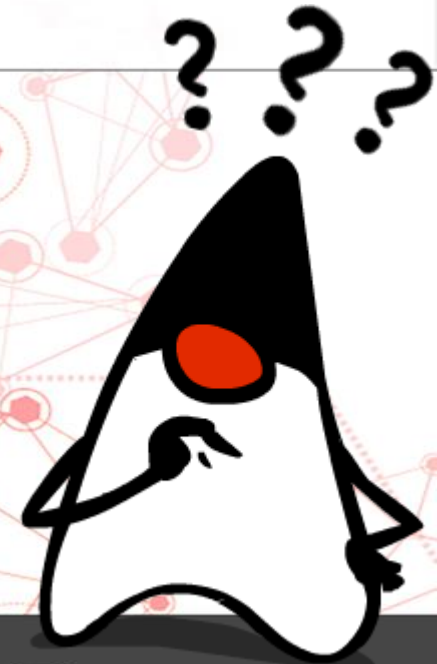 - Some **exploitation**..

Agenda

- Warm up (Path traversal, Cryptography, XSS)

- Xml eXternal Entity (XXE)

- Template injection

- Deserialisation vulnerabilities

- Expression Language (EL) injection

- Hibernate Query Language injection

GoSecure

Module 1
Warm up

SonarQube interface

SonarQube interface

Open the short description

Open the detailed explanation and resolution

Module 2
Xml eXternal Entity (XXE)
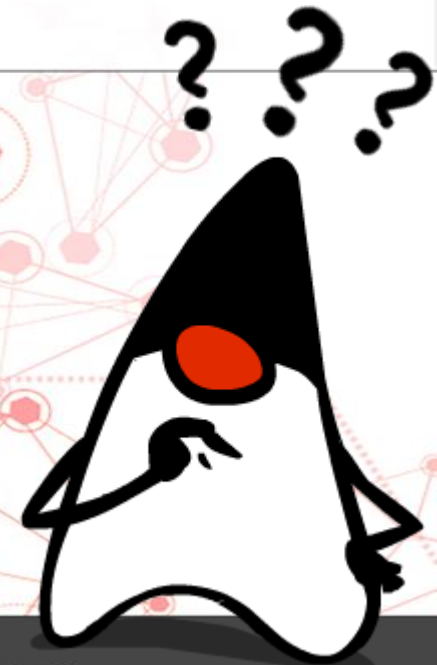
Xml eXternal Entity (XXE)

Example of simple payload and out-of-bound:

- http://blog.h3xstream.com/2014/06/identifying-xml-external-entity.html

Example with jar: protocol trick

- http://www.agarri.fr/kom/archives/2013/11/27/compromising_an_unreachable_solr_server_with_cve-2013-6397/index.html

XML Schema, DTD, and Entity Attacks

- http://vsecurity.com/download/papers/XMLDTDEntityAttacks.pdf

More examples

- http://web-in-security.blogspot.com/2016/03/xxe-cheat-sheet.html

Module 3
Template Injection
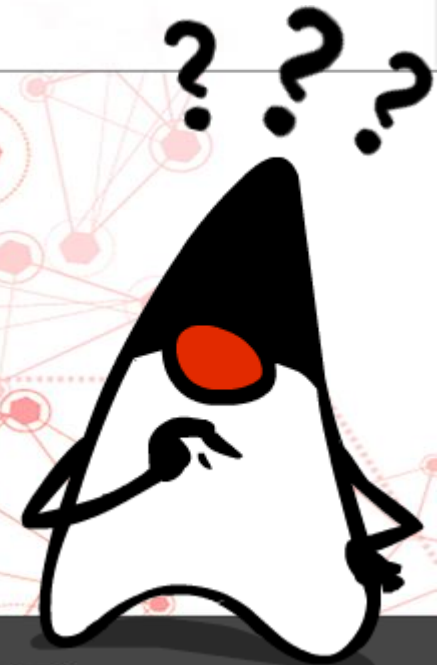
GoSecure

Template Injection

Server-Side Template Injection

- http://blog.portswigger.net/2015/08/server-side-template-injection.html

Server-Side Template Injection (White-paper version)

- https://www.blackhat.com/docs/us-15/materials/us-15-Kettle-Server-Side-Template-Injection-RCE-For-The-Modern-Web-App-wp.pdf

Module 4
Deserialization vulnerabilities

GoSecure

Deserialization Vulnerabilities

Proof of concept for WebLogic, WebSphere, JBoss, ...

- https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/

AppSecCali : first presentation on the subject with a working gadget demo

- http://frohoff.github.io/appseccali-marshalling-pickles/
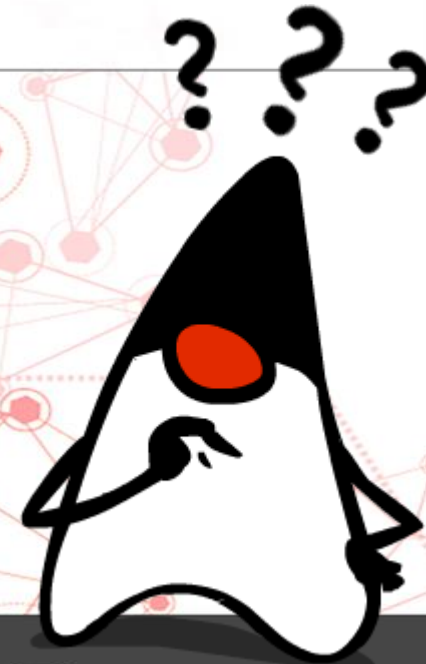
Great article to understand the risk and differentiate safe and unsafe implementations

- http://www.ibm.com/developerworks/library/se-lookahead/

YSoSerial (tool needed for the exercise)

- https://github.com/frohoff/ysoserial
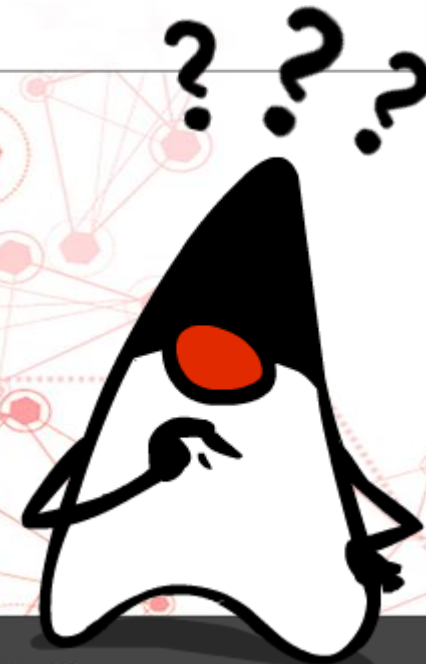
GoSecure

Deserialization Vulnerabilities

YSoSerial

- List the gadgets available
  - java -jar ysoserial-0.0.5-all.jar

- Generate a payload
  - java -jar ysoserial-0.0.5-all.jar **[GADGET_NAME]** "YOUR_COMMAND" > payload.bin

Module 5
Expression Language (EL) injection

Expression Language Injection

Spring Expression Language (SpEL) and ScriptEngine/Rhino examples

- http://blog.h3xstream.com/2014/11/remote-code-execution-by-design.html

Java EL Injection (Mostly used in JSP)

- http://sectooladdict.blogspot.com/2014/12/el-30-injection-java-is-getting-hacker.html

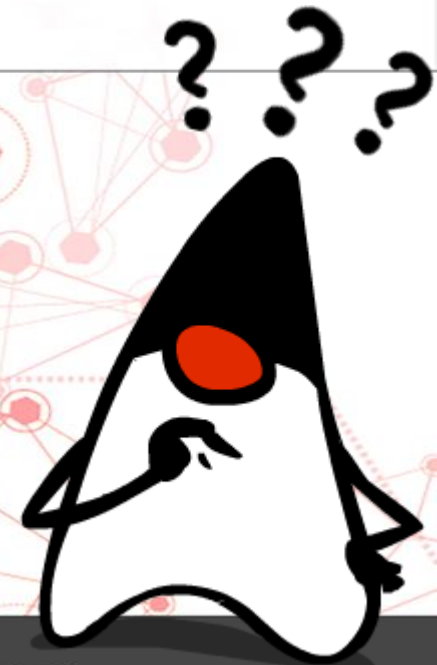Java EL Injection (Mostly used in JSP)

- http://blog.mindedsecurity.com/2015/11/reliable-os-shell-with-el-expression.html

Spring Expression Language (SpEL)

- http://danamodio.com/appsec/research/spring-remote-code-with-expression-language-injection/

Module 6
Hibernate Query Language (HQL)

Hibernate Query Language

Introduction to HQL

- http://blog.h3xstream.com/2014/02/hql-for-pentesters.html

Reference for "advanced" exploitation (Zeronights 2015)

- http://www.slideshare.net/0ang3el/orm2pwn-exploiting-injections-in-hibernate-orm

HQLmap: tool for automation

- https://github.com/PaulSec/HQLmap

GoSecure

Questions?

Contact
✉ parteau@gosecure.ca
🌐 blog.gosecure.ca
🐦 @h3xstream

GOSECURE