Getting more out of Java Stacktraces

Whoami

- Eric Sesterhenn
  - Chaos: http://www.cccmz.de
  - Work: http://www.lsexperts.de
  - Private: http://www.rusty-ice.de

What is this about?

- Getting more information out of Java Web Application Stacktraces
- Nothing fancy – simple fingerprinting
- But useful when doing black box tests

Java Webapplications

- Often possible to trigger errors
  - Insert 0-Bytes in requests
  - Make the XML Parser fail \00
  - Cause timeouts
  - Input malformed Dates

Stacktraces

at java.net.SocketOutputStream.socketWrite0(Native Method)

at java.net.SocketOutputStream.socketWrite(SocketOutputStream.java:92)

at java.net.SocketOutputStream.write(SocketOutputStream.java:136)

at org.apache.coyote.http11.InternalOutputBuffer.realWriteBytes(InternalOutputBuffer.java:756)

at org.apache.tomcat.util.buf.ByteChunk.flushBuffer(ByteChunk.java:448)

… [SNIP] …

at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:861)

at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:606)

at org.apache.tomcat.util.net.JIoEndpoint$SocketProcessor.run(JIoEndpoint.java:396)

at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:886)

at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:908)

at java.lang.Thread.run(Thread.java:662)

What can we get from that?

- Java JDK
  - 1.6.0_22 1.6.0_23 1.6.0_24 1.6.0_25 1.6.0_26 1.6.0_27 1.6.0_29 1.6.0_31 1.6.0_38
- Tomcat
  - v6.0.36

How?

at java.net.SocketOutputStream.socketWrite0(Native Method)

at java.net.SocketOutputStream.socketWrite(SocketOutputStream.java:92)

at java.net.SocketOutputStream.write(SocketOutputStream.java:136)

We know the start and end of each function

We know on what line functions are called

How?

- How is the database filled?
  - Downloading the libraries
  - Unzipping
  - Using Java BCEL to extract the information
  - Dump into MySQL
  - Retrieve with dumb PHP Script

What is currently in there?

- PsiProbe, Tomcat, Struts, Oracle JDK, Jboss, SpringFramework, WoodStox, Javamelody, Spring Security, JavaX Faces, Turbine, Url Rewrite Filter, UJAC, ACEGI Security, Jaspter Reports, Jetty, Apache Commons, Hibernate, Grizzly, Velocity, OpenSymphony, Xerces, Freemarker, Log4J, Axis2, Axis2 Rampart, Geronimo
- 2649075 different class files in total

Try it!

- No captcha (yet?)
- I am not logging
- If it doesn't work for you → drop me a mail
- If it does work for you → drop me a mail

Questions?

Available at http://www.rusty-ice.de/javafp.php

snakebyte@gmx.de