DA – All I Need

Table of Contents

[TO DO 1](#_Toc226907965)

[Software 1](#_Toc226907966)

[Begriffe 2](#_Toc226907967)

[Übersetzungen 3](#_Toc226907968)

[Papers 3](#_Toc226907969)

[Hilfreiche Links 4](#_Toc226907970)

[SDQ und FZI 4](#_Toc226907971)

[Sonstig 4](#_Toc226907972)

[Sonstige 5](#_Toc226907973)

[Mailinglisten 5](#_Toc226907974)

# TO DO

# Repository

svn://i43pc13.ipd.uka.de/code,

Verzeichnis /stud/ChristinaPildner

Verzeichniss security\DA\_C\_Pildner - nur Stabiler Code

user christina.pildner

Passwort pheT4aj9.

# Software

1. Eclipse und Plugins - weiter machen

|  |  |
| --- | --- |
| Plugin | Status |
| PCM – Palladio Component Model  http://sdqweb.ipd.uka.de/wiki/PCM\_Installation |  |
| Voraussetzungen   * Eclipse Modeling Framework (EMF) Runtime + End-User Tools Europa Discovery Site Models and Model Development * Graphical Modeling Framework (Europa Edition) Europa Discovery Site Models and Model Development * Eclipse Project Equinox bundle feature Europa Discovery Site Enabling Features - läst sich nicht installieren * EMF Model Query Europa Discovery Site Enabling Features * EMF Model Query OCL Integration Europa Discovery Site Enabling Features * EMF Validation Framework Europa Discovery Site Enabling Features * EMF Model Transaction Europa Discovery Site Enabling Features * EMF Model Transaction Workbench Integration Europa Discovery Site Enabling Features * Object Constraint Language (OCL) 2.0 Europa Discovery Site Enabling Features * Object Constraint Language (OCL) 2.0 Compatibility Europa Discovery Site Enabling Features * openArchitectureWare core feature openArchitectureWare (http://www.openarchitectureware.org/updatesite/milestone) Classic * openArchitectureWare core plugins feature openArchitectureWare (http://www.openarchitectureware.org/updatesite/milestone) Classic * openArchitectureWare Library feature openArchitectureWare (http://www.openarchitectureware.org/updatesite/milestone) Classic * openArchitectureWare Stdlib feature openArchitectureWare (http://www.openarchitectureware.org/updatesite/milestone) Classic   Link   * <http://sdqweb.ipd.uka.de/eclipse/PCM/> | Done  Lässt sich nicht installieren |
| FindBugs | Done |
| Update Site: <http://findbugs.cs.umd.edu/eclipse/> |  |
| CheckStyle | Done |
| Update Site: <http://eclipse-cs.sourceforge.net/update> |  |
| Maven | Done |
|  |  |
| Subversion | Done |
|  |  |

1. Malicious Software 'Malicious Bundles':  
   svn checkout svn://scm.gforge.inria.fr/svn/maliciousosgi

# Begriffe

|  |  |
| --- | --- |
| Begriff | Beschreibung |
|  |  |
| BSIMM | Building Security in Maturity Model |
| CBSE | Component-based Software Engineering |
| COTS |  |
| HIPAA |  |
| IDS | Intrusion Detection System |
| JSR | Java Specification Request |
| OSGi | Open Services Gateway initiative |
| OTS | on-the-shelf |
| PCI | Payment Card Industry |
| PCI DSS | Payment Card Industry Data Security Standard |
| PII | Personally identifiable information |
| SDL | Security Development Lifecycle |
| SLA | Service Level Agreement |
| SOP | Service Oriented Programming |
| SSDL | Software Security Development Lifecycle |
| SSF | Software Security Framework |
| SSG | Software Security Group |
| STRIDE |  |
| VCA | Vurnerable Component Analysis |
| WCA | Weak Component Analysis |
| Decompression bomb / zip bomb | Malicious archive file designed to crash or render useless the program or system reading it. It is often employed to disable antivirus software, so that a more traditional virus sent afterwards could get through undetected.  Rather than hijacking the normal operation of the program, a zip bomb allows the program to work as intended, but the archive is carefully crafted so that unpacking it (e.g. by a virus scanner in order to scan for viruses) requires inordinate amounts of time, disk space or memory.  A zip bomb is usually a small file (up to a few hundred kilobytes) for ease of transport and to avoid suspicion. However, when the file is unpacked its contents are more than the system can handle.  The term was apparently first coined in July 2001, but the same technique has been used on dialup bulletin board systems at least as long as compressing data archive programs have been around.  Today, most antivirus programs can detect whether a file is a zip bomb and so avoid unpacking it. One example of a Zip bomb was the file "42.zip" which was 42 kilobytes of compressed data, containing six layers of nested zip files in sets of 16, each bottom layer archive containing a 4.0 gigabyte file for a total of 4.0 petabytes of uncompressed data. This file is still available for download on various websites across the internet. |
| Stack Smashing | Causes a stack in an application or OS to overflow. This makes it possible to subvert the program or system or cause it to crash. |
| SSISy | **S**tructural **I**nvestigation of **S**oftware **Sy**stems – platform that allows you to run automated analyses in order to assess the maintainability of an oriented system using static analysis techniques |
| Zyklomatische Komplexität | Software Metrik, mit der die Komplexität eines Software-Moduls gemessen werden kann.  <http://de.wikipedia.org/wiki/McCabe-Metrik> |
| SPIP | Spiral Process for Intrusion Prevention |
| CBAC | Component based Access Control |
| INRIA | Institut National de Recherche en Informatique et Automatique |

# Übersetzungen

|  |  |
| --- | --- |
| Englisch | Deutsch |
| Vulnerability | Schwachstelle |

# Papers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Autor | Name | D | L | Sonstig |
|  | R.F. Crew | ASTLOG: A Language for Examining Abstrakt Syntax Tree | ja |  |  |
|  | P. Parrent, S. Frenot | Enhancing Automated Detection of Vulnerabilities in Java Components | ja | noch | BNF Definition der Schwächen |
|  | M. Martin, B. Livshits, M.S. Sam | Finding Application Errors and Security Flaws Using PQL: a Program Query Language | ja |  |  |
|  | K. De Volder | Jquery: A Generic Code Browser with a Declarative Configuration Language | ja |  |  |
|  | K. De Volder, L. Markle | JQueryScapes: Customisable Java Code Perspectives | ja |  |  |
|  | D. Janzen, K. De Volder | Navigating and Querying Code Without getting Lost | ja |  |  |
|  | K. De Volder, R. Rajagopalan | QJBrowser: A Query-Based Browser Model | ja |  |  |
|  |  | Secure Coding Guidelines for the Java Programming Language, version 2.0 |  |  |  |
|  | P. Parrent, S. Frenot | Secure Component Deployment in the OSGi Release 4 Platform | ja |  |  |
| issre04 | N. Rutar, C.B. Almazan, J.S. Foster | A Comparison of Bug Finding Tools for Java | ja |  |  |
| RR6231 | P. Parrent, S. Frenot | Java Components Vulnerabilities - An Experimental Classification Targeted at the OSGi Platform | ja | ja |  |
| BA586F80d01 | Reimer, Schonberg, Srinivas | Validating Structural Properties of Nested Objects (about FindBugs) |  |  |  |
| QBench-V04 |  | QBench – Systemmetamodell |  |  | SSISy |
|  | A. Trifu, M. Trifu | SISSy: Catalog of Detected Problem Patterns |  |  | SSISy |

# Hilfreiche Links

## PQL

* <http://pql.sourceforge.net/>
* <http://cs.nyu.edu/~lharris/content/programquerylangs.html>

## SISSY

* SSISy - **S**tructural **I**nvestigation of **S**oftware **Sy**stems
  + <http://ssisy.fzi.de>
  + Ansprechpartner: Mircea Trifu
* Code link: <http://sourceforge.net/projects/sissy>

## Java Schwachstellen

* Technische Reports
  + [www.sei.cmu.edu/pu b/documents/05.reports/pdf/05tn044.pdf](http://www.sei.cmu.edu/pu%09b/documents/05.reports/pdf/05tn044.pdf) (JOhn Long 2005)
  + <http://java.sun.com/security/seccodeguide.html> (Sun Java Security Guidelines)
  + [www.cs.umd.edu/~jfoster/papers/issre04.pdf](http://www.cs.umd.edu/~jfoster/papers/issre04.pdf) (a comparison of bug finding tools).

# Ausarbeitungshinweise:

* <http://sdqweb.ipd.uka.de/wiki/Ausarbeitungshinweise>
* Wie schreibe ich ein Gute Diplomarbeit <http://www.informatik.uni-oldenburg.de/studium/azwa/wie.html>
* Ablauf Diplomarbeit: <http://sdqweb.ipd.uka.de/wiki/Ablauf_Diplomarbeit>
* Proposal Beispiele:
  + <http://sdqweb.ipd.uka.de/mediawiki/images/4/42/Proposal_Rico.pdf>
  + <http://sdqweb.ipd.uka.de/mediawiki/images/9/91/Proposal_Klaus.pdf>
  + <http://sdqweb.ipd.uka.de/mediawiki/images/e/e7/Proposal_Heiko.pdf>
* Proposal Folien:
  + <http://sdqweb.ipd.uka.de/mediawiki/images/d/d3/Proposal_Folien_Henning.pdf>
  + <http://sdqweb.ipd.uka.de/mediawiki/images/f/fc/Proposal_Folien_Thomas.pdf>

## Sonstig

· Useful Web pages:

<https://buildsecurityin.us-cert.gov/>

<http://www.securecoding.org/>

· Reference Documents

The Software Security Assurance State of the Art Report,

<http://iac.dtic.mil/iatac/download/security.pdf>

· Associations:

OWASP, Open Web Application Security Project: <http://www.owasp.org>

ISSECO, International Secure Software Engineering Council:

<http://www.isseco.org/>

· Research Teams

Distrinet, <http://distrinet.cs.kuleuven.be/>

· Researchers

Brian Chess, <http://www.vantuyl.com/chess/>

Jan Jürjens, <http://mcs.open.ac.uk/jj2924/>

Michael Howard, <http://blogs.msdn.com/michael_howard/>

Fabio Martinelli, <http://www.iit.cnr.it/staff/fabio.martinelli/>

Fabio Masacci, <http://www.disi.unitn.it/~massacci/index.html>

<<http://www.disi.unitn.it/%7Emassacci/index.html>>

Gary Mc Graw, <http://www.citigal.com/gem/>

Markus Schumacher, <http://www.securitypatterns.org/markus/>

Jean-Marc Seigneur, <http://www.cui.unige.ch/~seigneur/>

<<http://www.cui.unige.ch/%7Eseigneur/>>

Mein Diss (u.a. für die Definitionen) findest Du hier:

<http://www.rzo.free.fr/parrend08phd.php>

Die links zu meinem tech reports sind:

<http://www.rzo.free.fr/parrend07OSGivulnerabilities.php> (Grundlagen)

<http://www.rzo.free.fr/parrend08rr6649.php> (Liste of Komponenten

Schwachstellen)

# Sonstige

## Mailinglisten

Hier sind Passwörter und Mailinglisten für [c.pildner@web.de](mailto:c.pildner@web.de):

Liste Passwort // URL

---- --------

[lesegruppe@ira.uka.de](mailto:lesegruppe@ira.uka.de) otgeicgu

<https://lists.ira.uni-karlsruhe.de/mailman/options/lesegruppe/c.pildner%40web.de>

[sdq-dev@ira.uka.de](mailto:sdq-dev@ira.uka.de) enminisa

<https://lists.ira.uni-karlsruhe.de/mailman/options/sdq-dev/c.pildner%40web.de>

<http://www.securecoding.org/list/> wie sonst…