Visual analysis of code security

John R. Goodall
Oak Ridge National Lab • goodalljr@ornl.gov • 865 576 5943

Hassan Radwan
Applied Visions, Inc. • hassanr@avi.com • 518 207 3106

Lenny Halseth
Applied Visions, Inc. • lennyh@avi.com • 518 207 3108

VizSec
09.14.2010
Ottawa, Canada

This effort was performed at

Applied Visions, Inc.

Secure Decisions division

for DHS Science & Technology

The Problem

More than **98% of all PCs** have one or more vulnerable programs

http://secunia.com/blog/56/

“**Software Assurance**: poorly written software is at the root of all of our security problems

Doug Maughan, CACM 53(2)
Top 10 Hard Problems in Cyber Security

More than **98% of all PCs** have one or more vulnerable programs

http://secunia.com/blog/56/

Lots of Bad Code

Software Assurance: poorly written software is at the root of all of our security problems

Doug Maughan, CACM 53(2)
Top 10 Hard Problems in Cyber Security

> ...**everybody should be using static analysis tools today**. And if you are not using them, then basically you are **negligent**, and you should prepare to be sued by the army of lawyers that have already hit the beach.
>
> Cigital's CTO Gary McGraw

> **enterprises must adopt SAST** [Static Application Security Testing]
>
> Gartner

“…**everybody should be using static analysis tools today**. And if you are not using them, then basically you are **negligent**, and you should prepare to be sued by the army of lawyers that have already hit the beach.

Cigital's CTO Gary McGraw

Tools Exist Today

“**enterprises must adopt SAST** [Static Application Security Testing]

Gartner

“**No tool** stands out as an **uber-tool**.
Each has its **strengths** and **weaknesses**.

Kris Britton, Technical Director
NSA’s Center for Assured Software

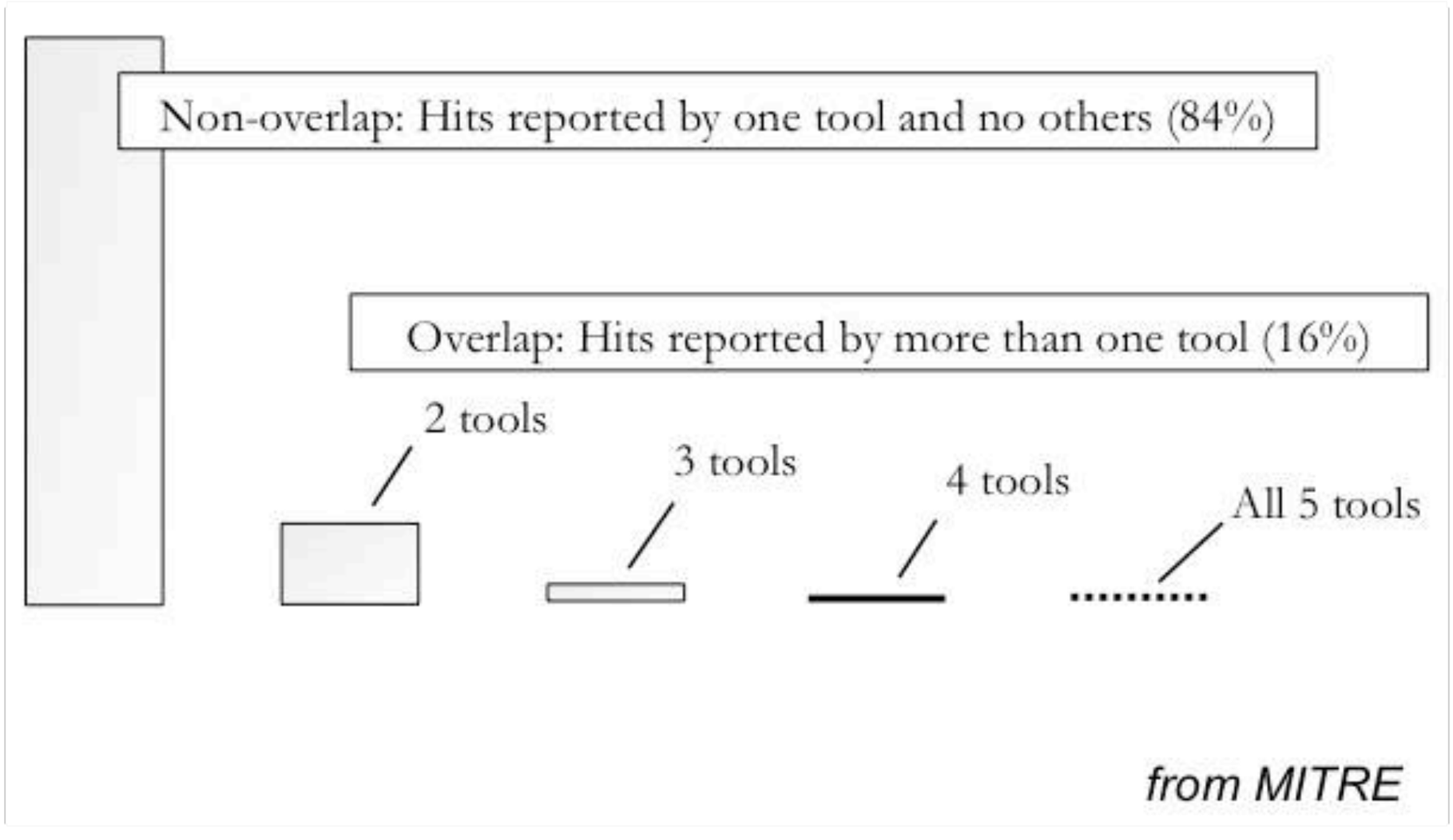
84% of the vulnerabilities were identified by **one tool** and **one tool alone**

> **No tool** stands out as an **uber-tool**.
> Each has its **strengths** and **weaknesses**.
>
> Kris Britton, Technical Director
> NSA's Center for Assured Software

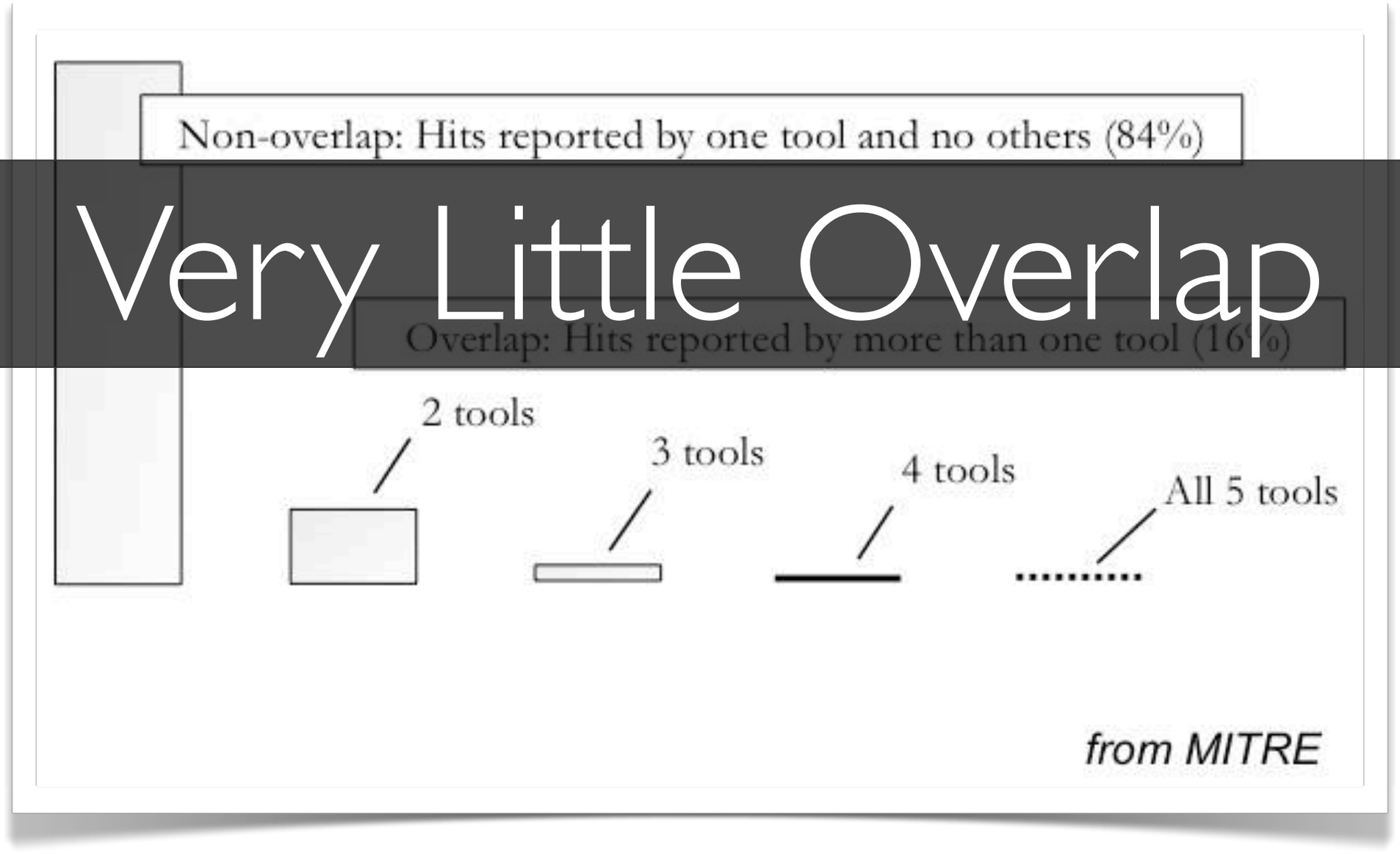
No Tool is Perfect

84% of the vulnerabilities were identified by **one tool** and **one tool alone**

Tools find different vulnerabilities



Tools find different vulnerabilities



Very Little Overlap

... with different semantics

```
 <BugInstance type="NP_NULL_ON_SOME_PATH" priority="1" abbrev="NP"
category="CORRECTNESS">
    <Class
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator">
      <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/
securedecisions/tva/model/linksettransform/LinkSetAggregator.java"/>
    </Class>
    <Method
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
name="createFromExploit" signature="(Lcom/securedecisions/tva/model/xml/ag/
LinkDocument$Link;Lcom/securedecisions/tva/model/xml/pdag/
ProtectionDomainDocument$ProtectionDomain;Z)Lcom/securedecisions/tva/model/
xml/pdag/ExploitDocument$Exploit;" isStatic="false">
      <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="540" end="563" startBytecode="0" endBytecode="479"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java"/>
    </Method>
    <LocalVariable name="machine" register="5" pc="124"
role="LOCAL_VARIABLE_VALUE_OF"/>
    <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="550" end="550" startBytecode="125" endBytecode="125"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_DEREF"/>
    <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="549" end="549" startBytecode="85" endBytecode="85"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_KNOWN_NULL"/>
  </BugInstance>
```

```
<problem>
 <problemID>2</problemID>
 <file>C:\Users\drscott\workspaceB\GMU Graph Viz 2.1.2\src\com\securedecisions\tva
\common\Contract.java</file>
 <method>Require</method>
 <line>57</line>
 <column>5</column>
 <code>EXC.BROADTHROWS</code>
 <message>The &apos;Require&apos; method throws a generic exception
&apos;java.lang.Exception&apos;</message>
 <anchor>-1088321900</anchor>
 <prefix>ed*@sinceVersion1.0,Mar12,2006*/</prefix>
 <postfix>{if(assertion==false)throwexcept</postfix>
 <severity>Style</severity>
 <severitylevel>8</severitylevel>
 <displayAs>Warning</displayAs>
 <category>Java/Poor Error Handling</category>
 <citingStatus>Analyze</citingStatus>
 <lastCommit>0</lastCommit>
 <state>New</state>
 <dateOriginated>1264106407000</dateOriginated>
 <url>http://NPT-0779-WV1:8080/klocwork/insight-
review.html#goto:project=gmu212,pid=2</url>
</problem>
```

... with different semantics


```
 <BugInstance type="NP_NULL_ON_SOME_PATH" priority="1" abbrev="NP"
category="CORRECTNESS">
    <Class
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator">
      <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/
securedecisions/tva/model/linksettransform/LinkSetAggregator.java"/>
    </Class>
    <Method
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
name="createFromExploit" signature="(Lcom/securedecisions/tva/model/xml/ag/
LinkDocument$Link;Lcom/securedecisions/tva/model/xml/pdag/
ProtectionDomainDocument$ProtectionDomain;Z)Lcom/securedecisions/tva/model/
xml/pdag/ExploitDocument$Exploit;" isStatic="false">
      <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="540" end="563" startBytecode="0" endBytecode="479"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java"/>
    </Method>
    <LocalVariable name="machine" register="5" pc="124"
role="LOCAL_VARIABLE_VALUE_OF"/>
    <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="550" end="550" startBytecode="125" endBytecode="125"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_DEREF"/>
    <SourceLine
classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
start="549" end="549" startBytecode="85" endBytecode="85"
sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/
linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_KNOWN_NULL"/>
  </BugInstance>
```



```
<problem>
 <problemID>2</problemID>
 <file>C:\Users\drscott\workspaceB\GMU Graph Viz 2.1.2\src\com\securedecisions\tva
\common\Contract.java</file>
 <method>Require</method>
 <line>57</line>
 <column>5</column>
 <code>EXC.BROADTHROWS</code>
 <message>The &apos;Require&apos; method throws a generic exception
&apos;java.lang.Exception&apos;</message>
 <anchor>-1088321900</anchor>
 <prefix>ed*@sinceVersion1.0,Mar12,2006*/</prefix>
 <postfix>{if(assertion==false)throwexcept</postfix>
 <severity>Style</severity>
 <severitylevel>8</severitylevel>
 <displayAs>Warning</displayAs>
 <category>Java/Poor Error Handling</category>
 <citingStatus>Analyze</citingStatus>
 <lastCommit>0</lastCommit>
 <state>New</state>
 <dateOriginated>1264106407000</dateOriginated>
 <url>http://NPT-0779-WV1:8080/klocwork/insight-
review.html#goto:project=gmu212,pid=2</url>
</problem>
```


working with **different tool vendors is a confusing and challenging and time-consuming process**: the engines work differently, which is good since they catch different types of problems…

Jim Bird, *Building Real Software*
http://swreflections.blogspot.com/2009_04_01_archive.html

... with different semantics

<BugInstance type="NP_NULL_ON_SOME_PATH" priority="1" abbrev="NP" category="CORRECTNESS">
<Class classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator">
<SourceLine classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator" start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/linksettransform/LinkSetAggregator.java"/>
</Class>
<Method classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator" name="createFromExploit" signature="(Lcom/securedecisions/tva/model/xml/ag/LinkDocument$Link;Lcom/securedecisions/tva/model/xml/pdag/ProtectionDomainDocument$ProtectionDomain;Z)Lcom/securedecisions/tva/model/xml/pdag/ExploitDocument$Exploit;" static="false">
<SourceLine classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator" start="540" end="563" startBytecode="0" endBytecode="0" sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/linksettransform/LinkSetAggregator.java"/>
</Method>
<LocalVariable name="machine" register="5" pc="124" role="LOCAL_VARIABLE_VALUE_OF"/>
<SourceLine classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator" start="550" end="550" startBytecode="125" endBytecode="125" sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_DEREF"/>
<SourceLine classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator" start="549" end="549" startBytecode="85" endBytecode="85" sourcefile="LinkSetAggregator.java" sourcepath="com/securedecisions/tva/model/linksettransform/LinkSetAggregator.java" role="SOURCE_LINE_KNOWN_NULL"/>
</BugInstance>

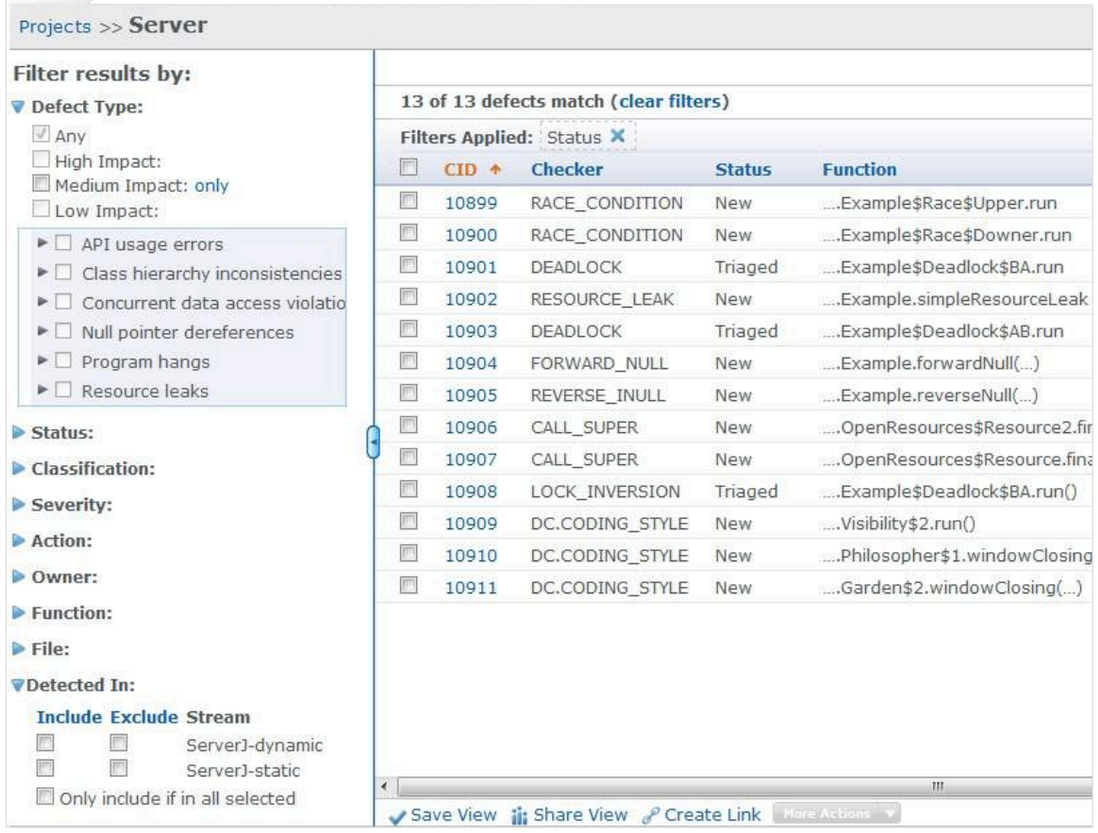
<problem>
<problemID>2</problemID>
<file>C:\Users\drscott\workspaceB\GMU Graph Viz 2.1.2\src\com\securedecisions\tva\common\Contract.java</file>
<method>Require</method>
<line>57</line>
<column>5</column>
<code>EXC.BROADTHROWS</code>
<message>The 'Require' method throws a generic exception 'java.lang.Exception'</message>
<anchor>-1088321900</anchor>
<prefix>ed*@sinceVersion1.0.Mar12,2006*/</prefix>
<postfix>{if(assertion==false)throwexcept</postfix>
<severity>Style</severity>
<severitylevel>8</severitylevel>
<displayAs>Warning</displayAs>
<category>Java Code Problem/Declaring</category>
<citingStatus>analyze</citingStatus>
<lastCommit>0</lastCommit>
<dateOriginated>1264106407000</dateOriginated>
<url>http://NPT-0779-WV1:8080/klocwork/insight-review.html#goto:project=gmu12,pid=2</url>
</problem>

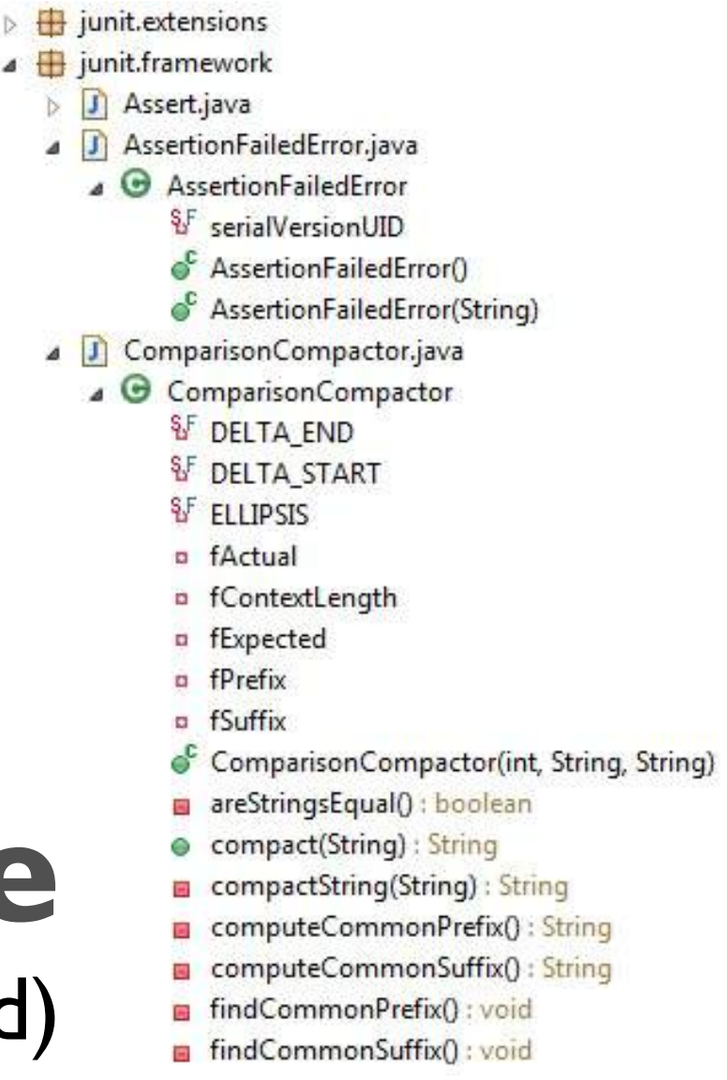
Different Semantics

working with **different tool vendors is a confusing and challenging and time-consuming process**: the engines work differently, which is good since they catch different types of problems…

Jim Bird, *Building Real Software*
http://swreflections.blogspot.com/2009_04_01_archive.html

Tools present **vulnerabilities**

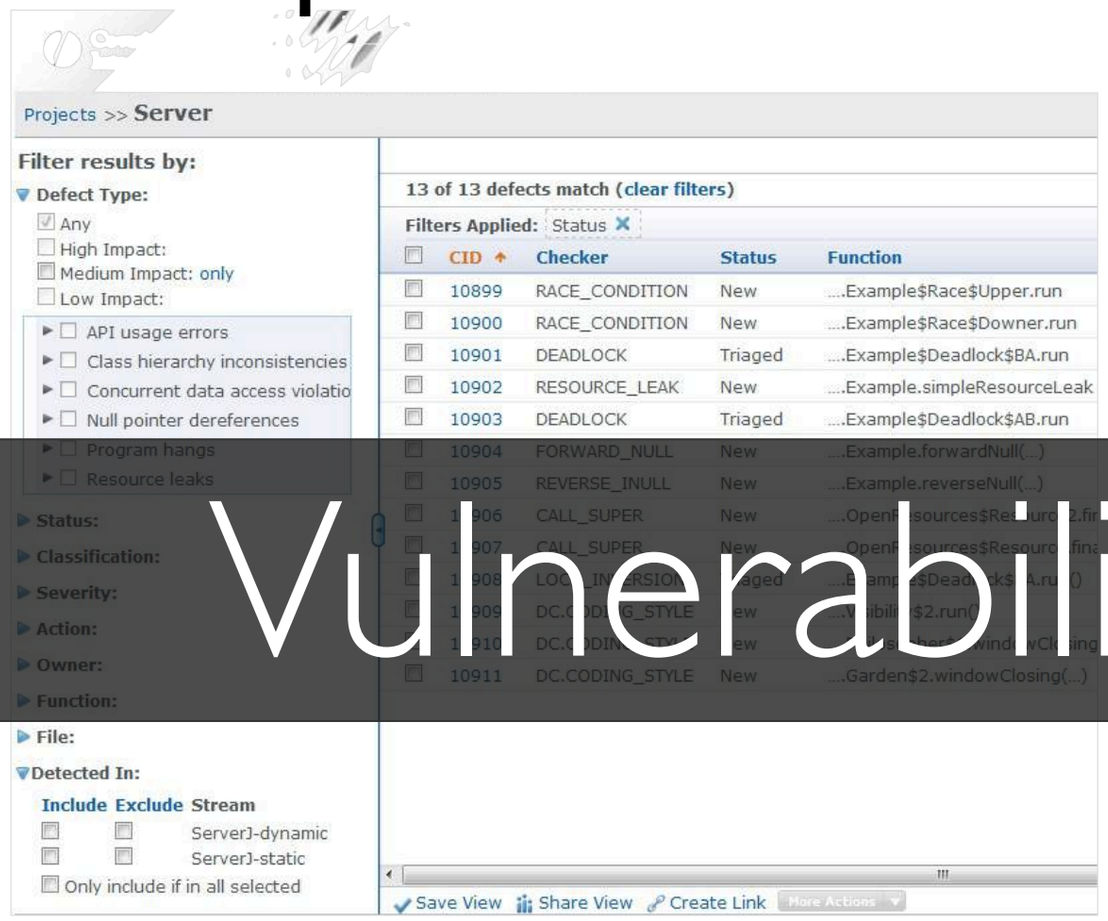


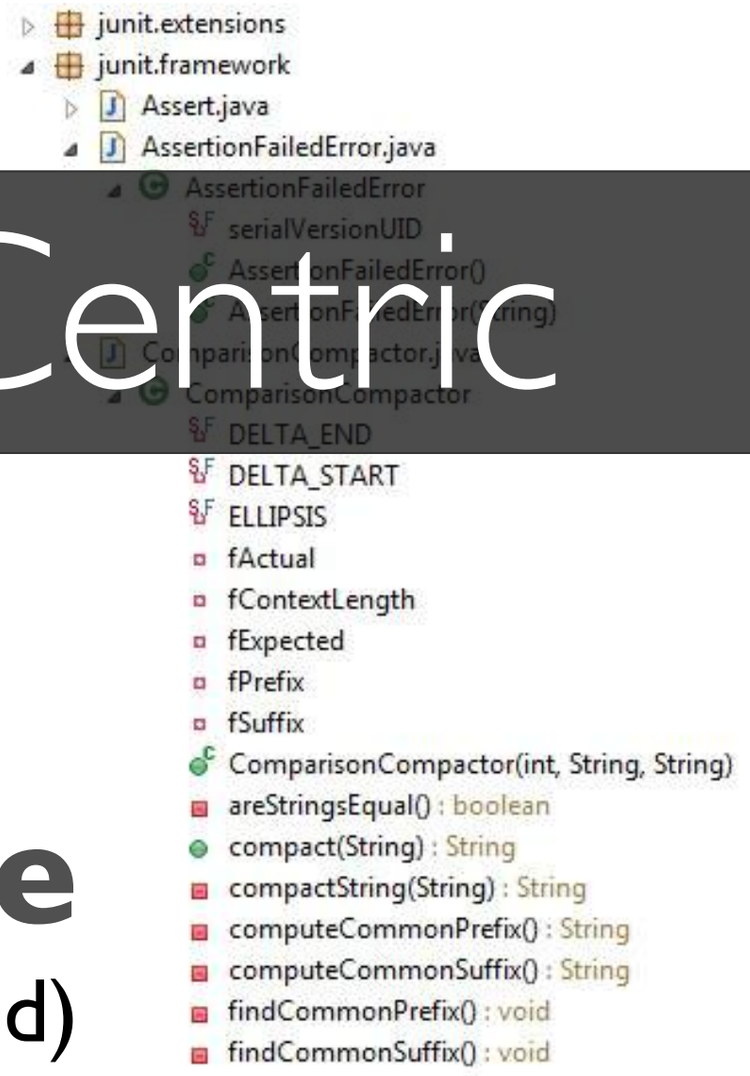


Developers think in **code**

(namespace/class/method)

Tools present **vulnerabilities**

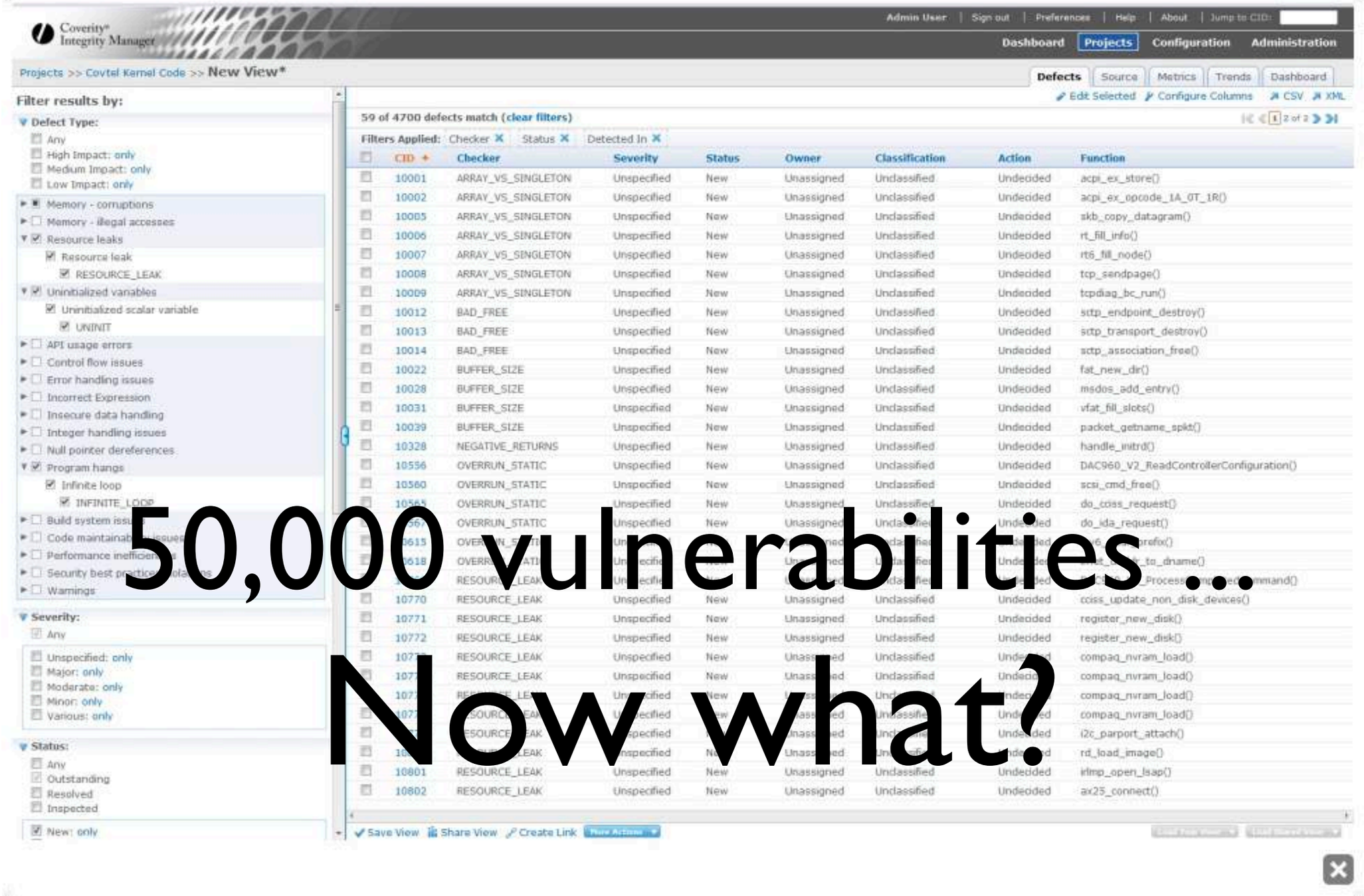




Vulnerability-Centric

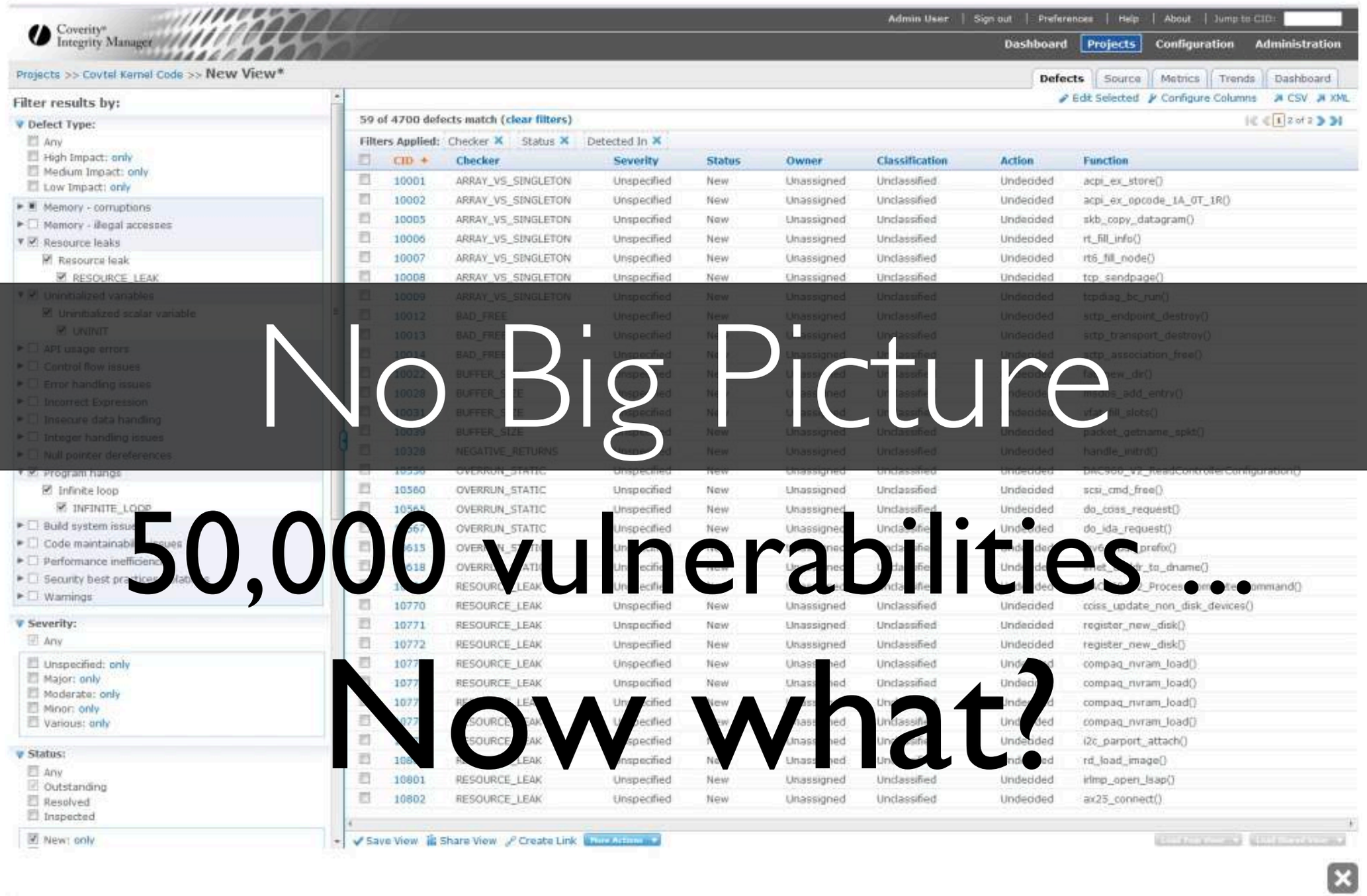
Developers think in **code**

(namespace/class/method)



50,000 vulnerabilities…

Now what?



No Big Picture

50,000 vulnerabilities…

Now what?

Better Tools ≠ Total Security

- Tool results have very little overlap
- Tools use different semantics for results
- Tools present a vulnerability-centric view
- Tools offer no big picture overviews

Better Tools ≠ Total Security

- Tool results have very little overlap
- Tools use different semantics for results
- Tools present a vulnerability-centric view
- Tools offer no big picture overviews

Better analysis tools are only a part of improving code security

Technical Approach

Technical Approach

SoftWare Assurance ViSual Analysis

Provide a **workflow** for developers to

bring together **disparate** security analysis results

visually **analyze** and **prioritize** those results

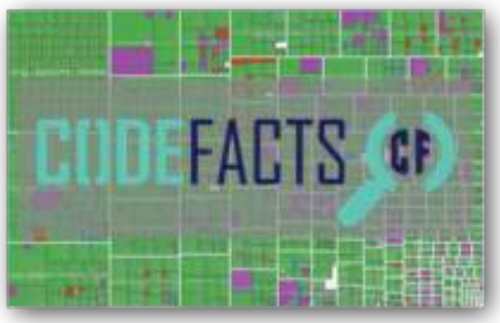
explore those results to uncover hidden trends

use code **context** to assess the impact of those results

see **who is responsible** for vulnerabilities

assign vulnerabilities to developers responsible


Pmd
DON'T SHOOT THE MESSENGER
FindBugs
coverity
a higher code
FORTIFY
SOFTWARE
PARASOFT
We make software work.
Klocwork


CODEFACTS
CF


SwA Vis

SDLC Tools

integrate / correlate / normalize

context

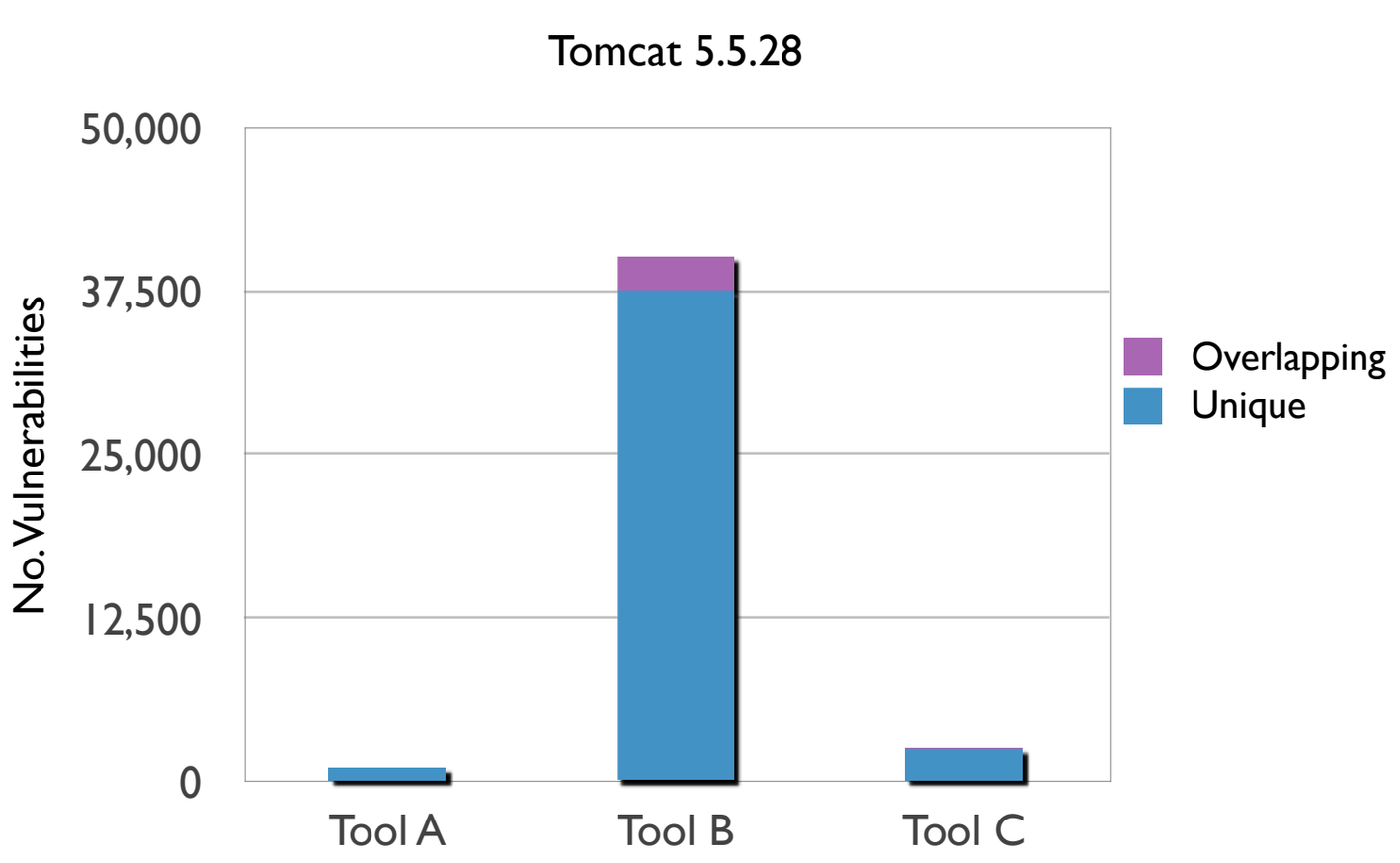
visual analysis

workflow

SDLC Tools

Test Data

- Three software analysis tools
- Two test data sets



SwA Tool Output

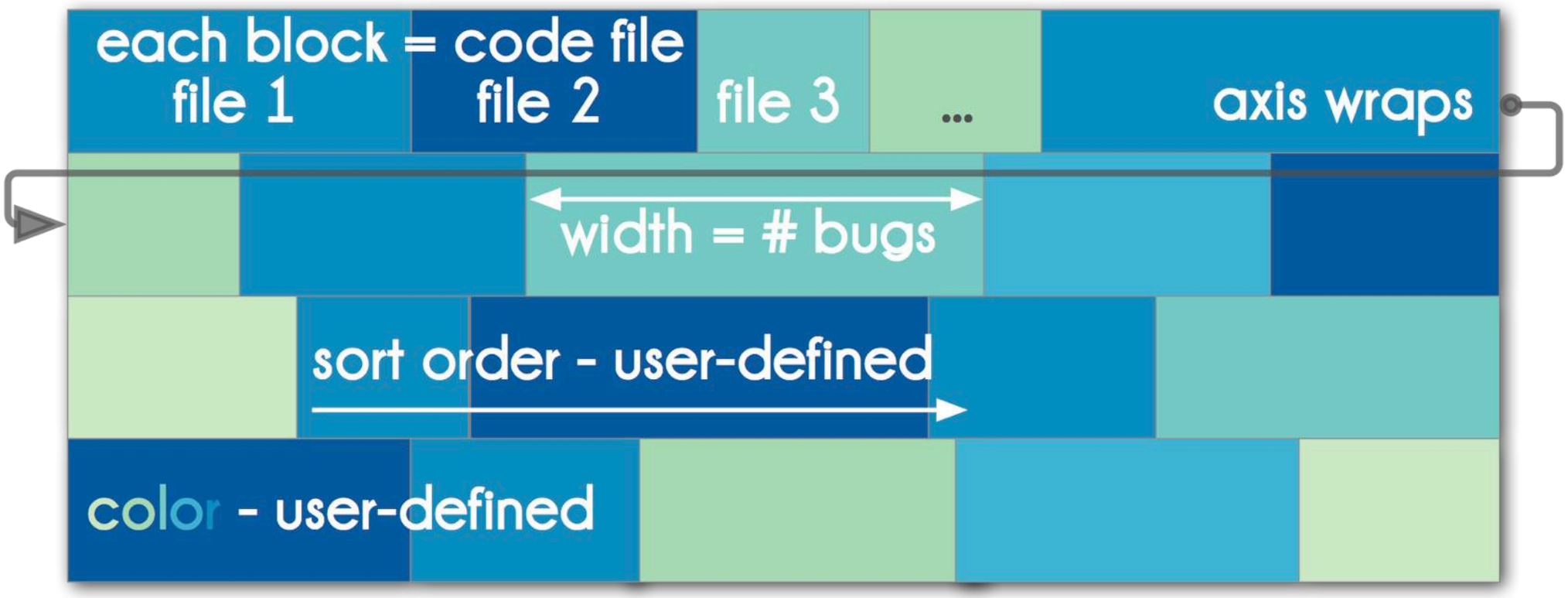
- Tool output is in varying XML schemas
- Results are parsed and correlated
- Severity and category are normalized

Use case : Triage

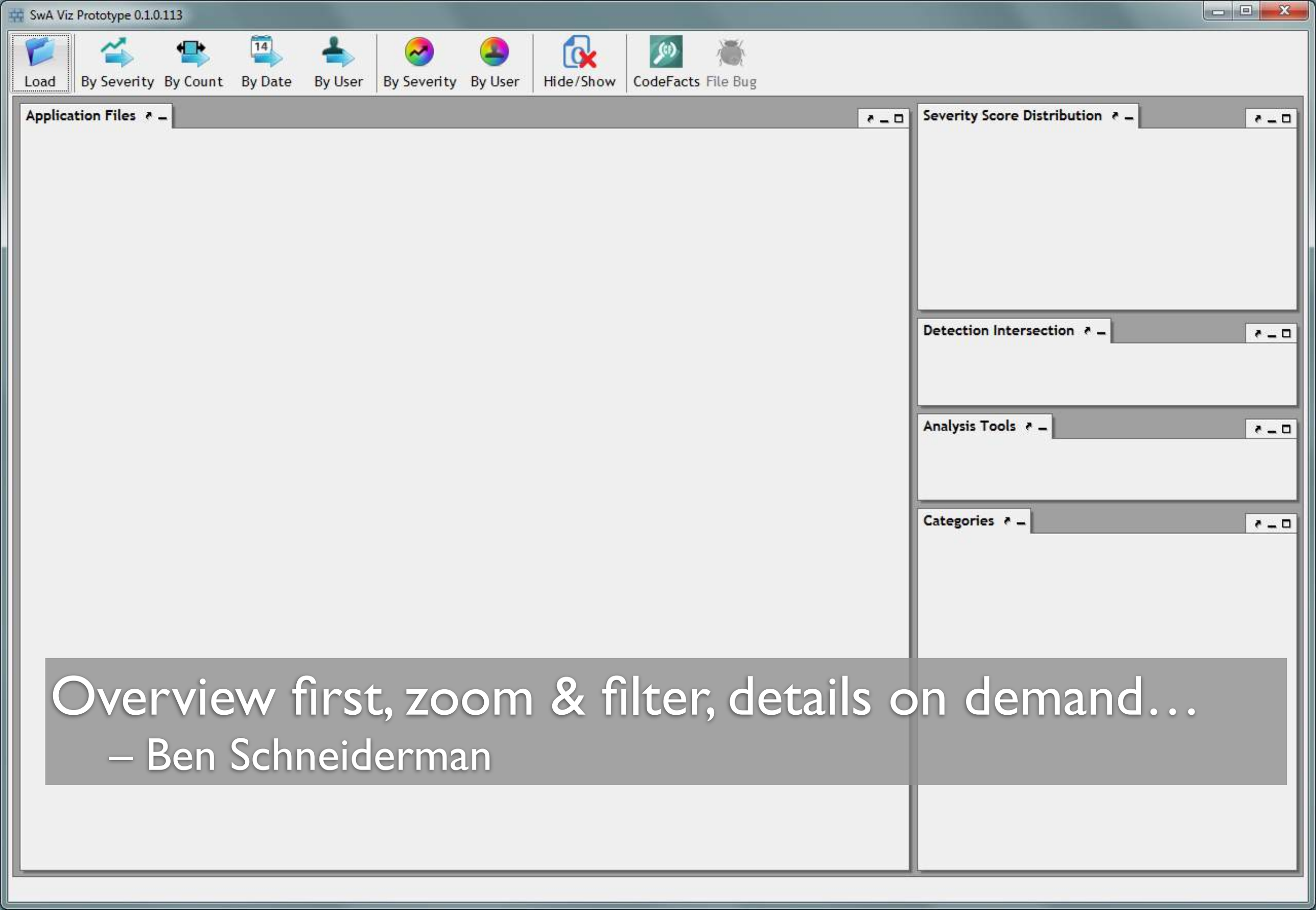
- Which vulnerabilities are noise / most important
- What vulnerability categories are most common
- What vulnerabilities are found by multiple tools
- Where in the code are the vulnerabilities
- Who do confirmed vulnerabilities get assigned to

Visualization

- Each source code file is represented as a block
- Each block aggregates the vulnerabilities found
- Very compact, space filling method
- Flexible (color/sort) data > visual mappings



Demonstration



Overview first, zoom & filter, details on demand…

– Ben Schneiderman

SwA Viz Prototype 0.1.0.113

Load | By Severity | By Count | By Date | By User | By Severity | By User | Hide/Show | CodeFacts | File Bug

Application Files

Severity Score Distribution

Open

Look in: data

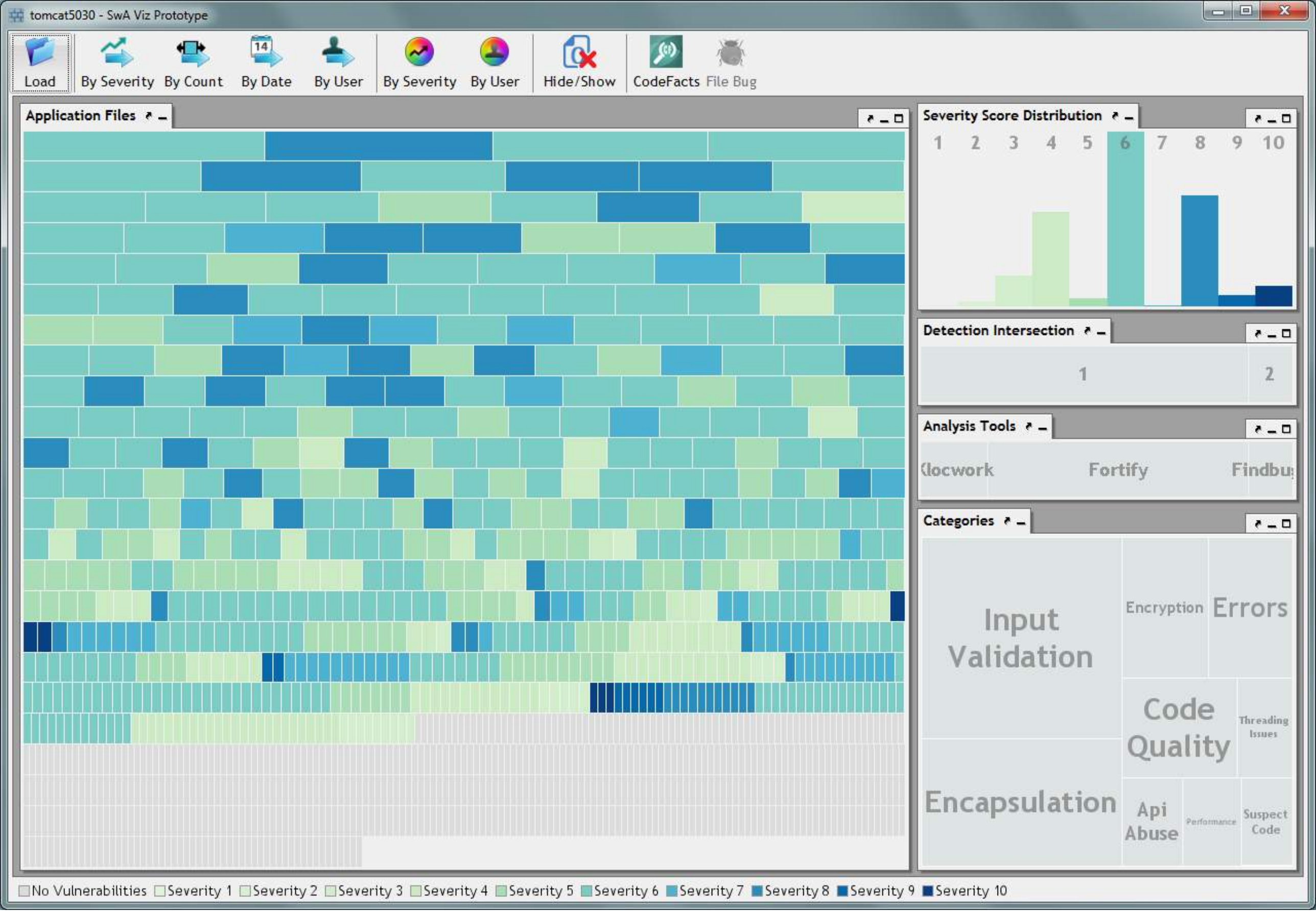
Recent Items
Desktop
My Documents
Computer
Network

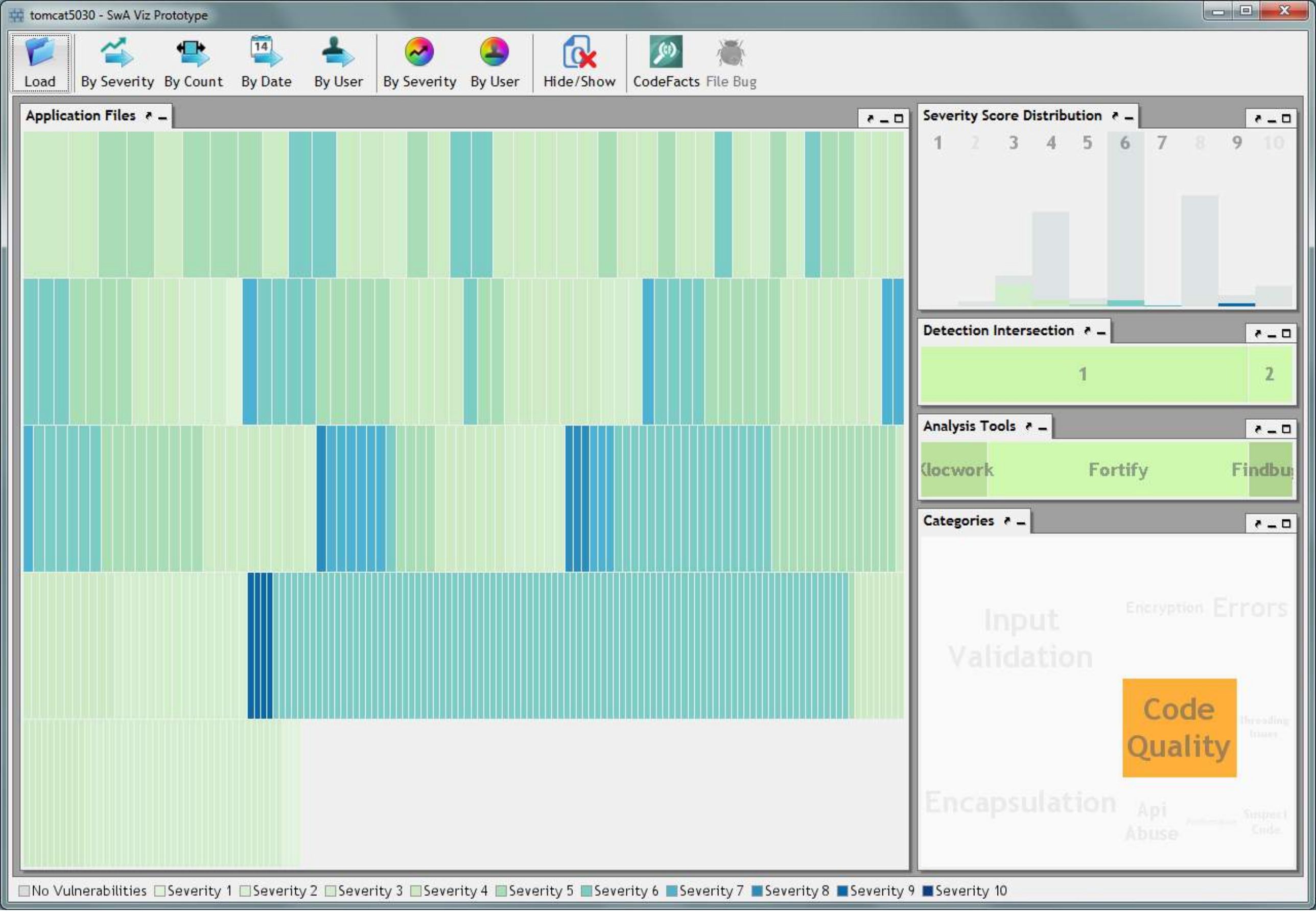
gmu200
gmu210
gmu212
gmu251
tomcat5000
tomcat5030
tomcat5500
tomcat5512
tomcat5528

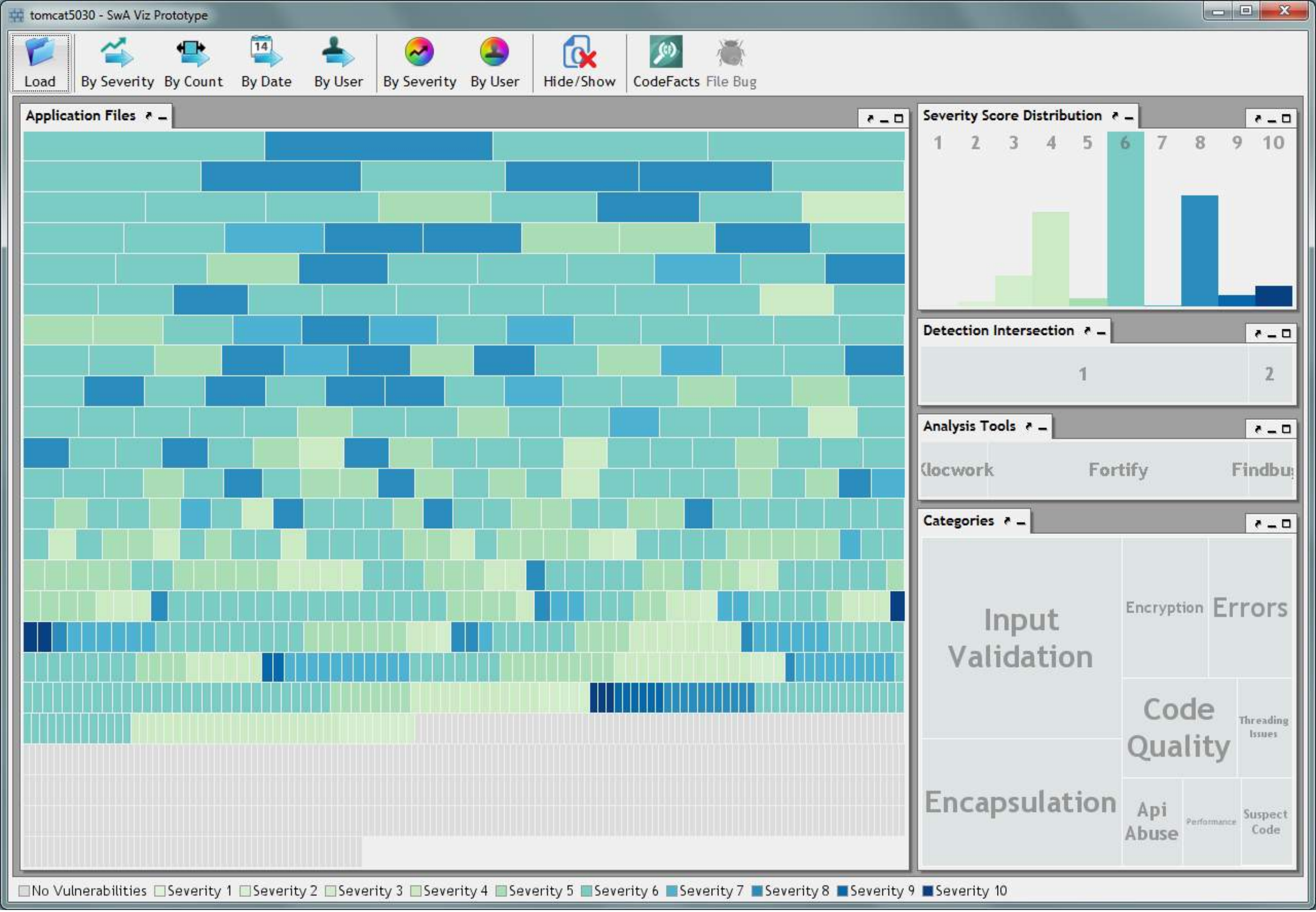
File name: anR\Projects\SwAVis\Releases\Phase 1 End\data\tomcat5030

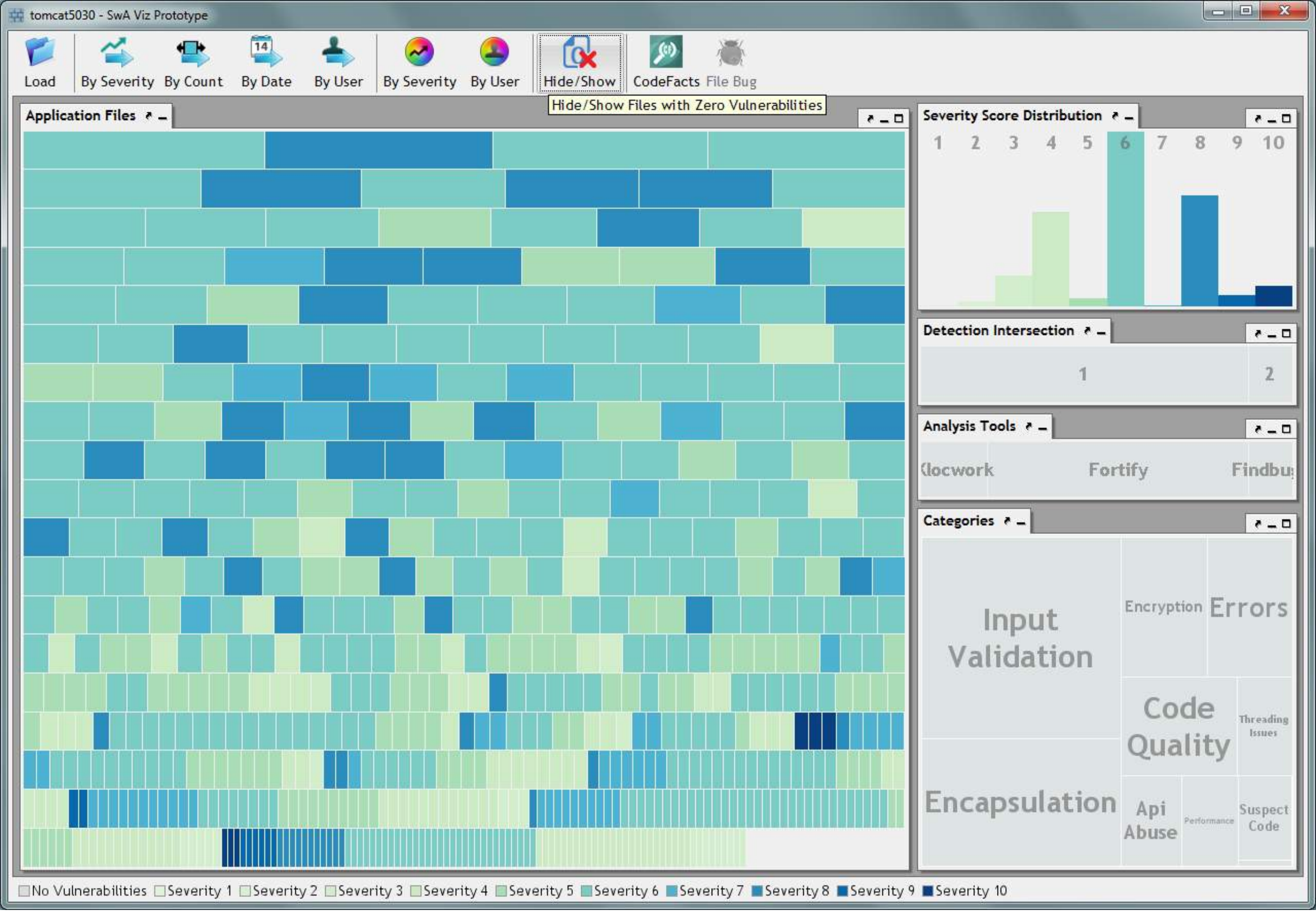
Files of type: All Files

Open
Cancel









tomcat5030 - SwA Viz Prototype

Load | By Severity | By Count | By Date | By User | By Severity | By User | Hide/Show | CodeFacts | File Bug

Sort by Weighted Severity Score

Application Files

Severity Score Distribution

1 2 3 4 5 6 7 8 9 10

Detection Intersection

1 2

Analysis Tools

Clocwork Fortify Findbu

Categories

Input Validation

Encryption

Errors

Code Quality

Threading Issues

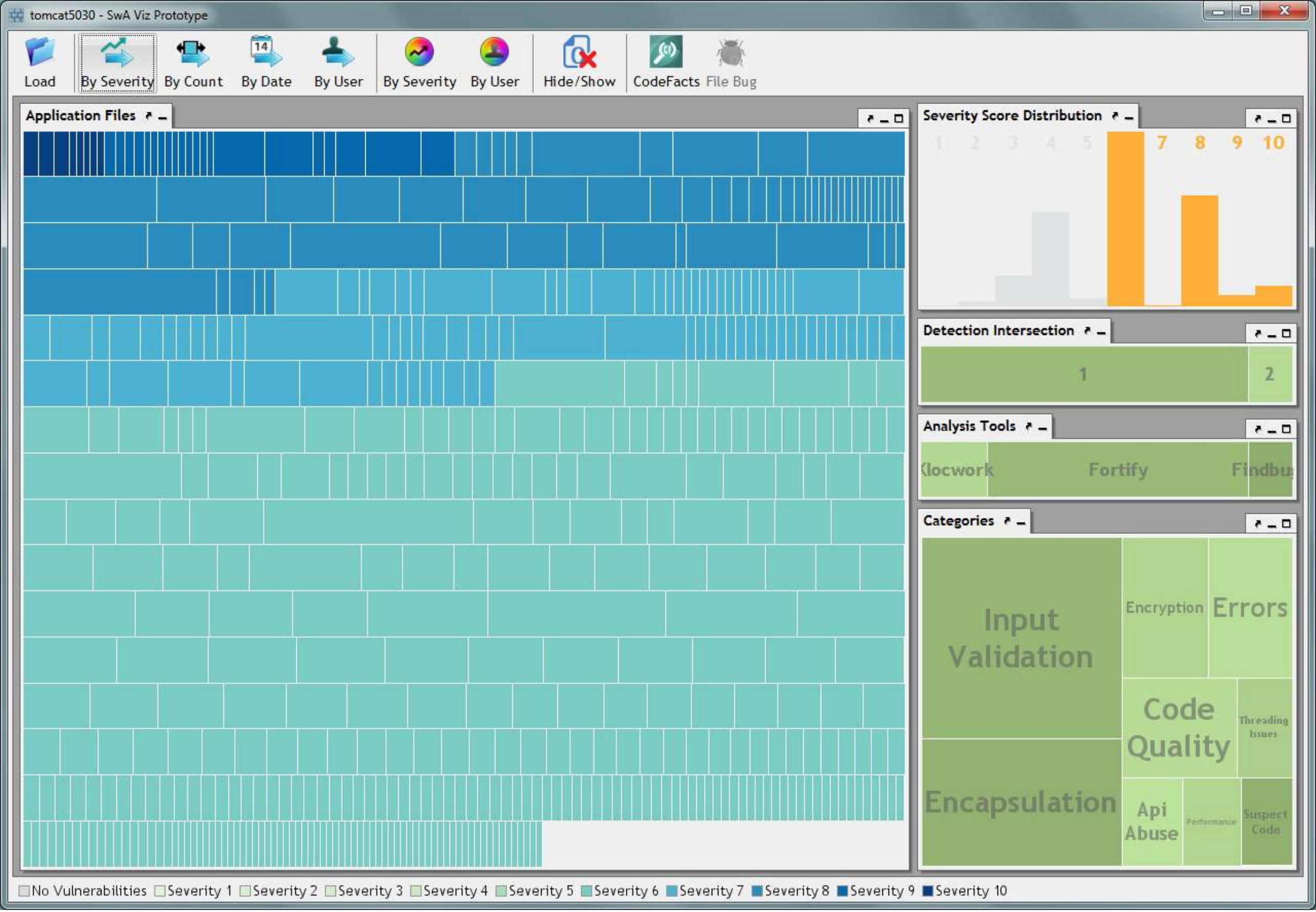
Encapsulation

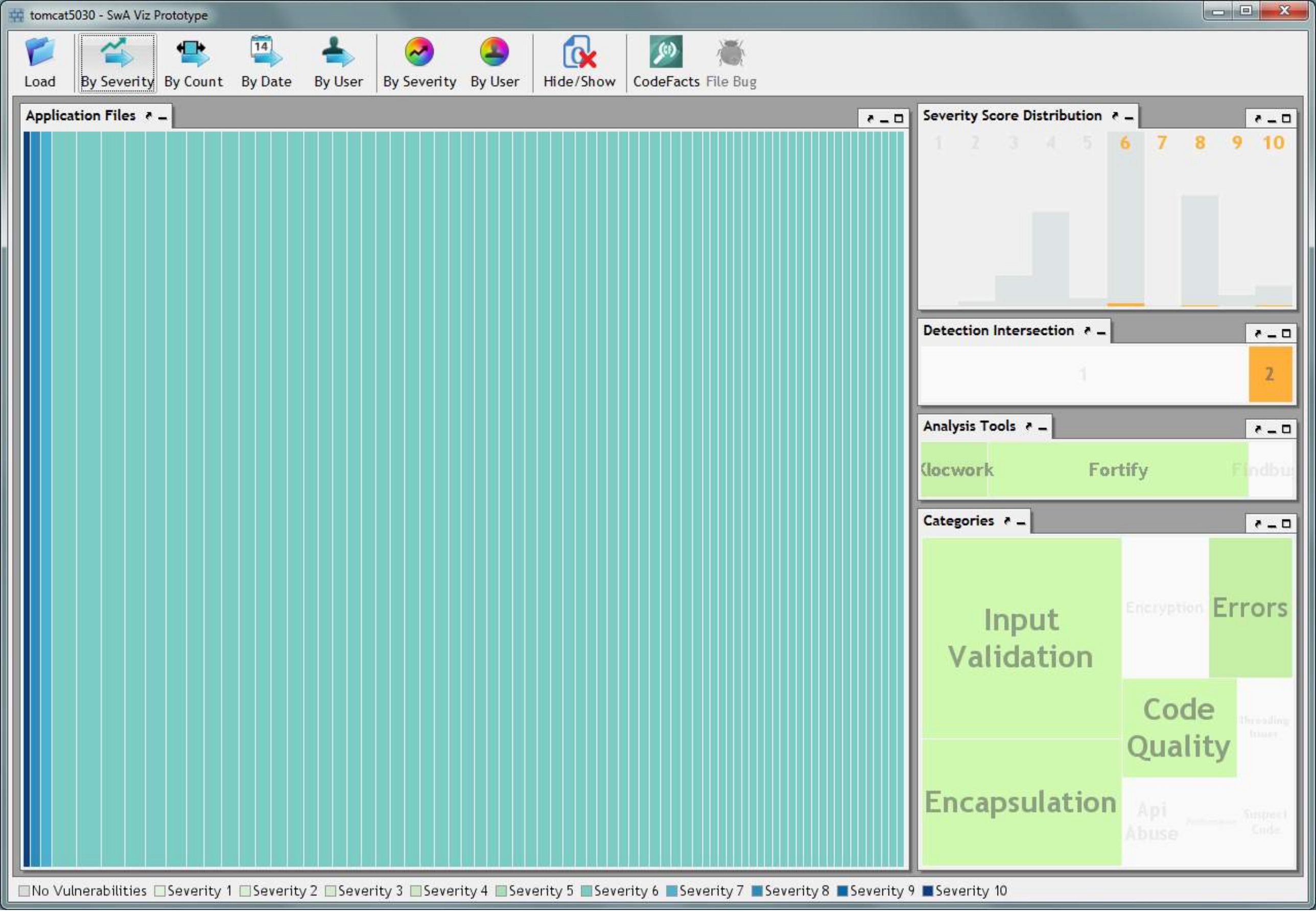
Api Abuse

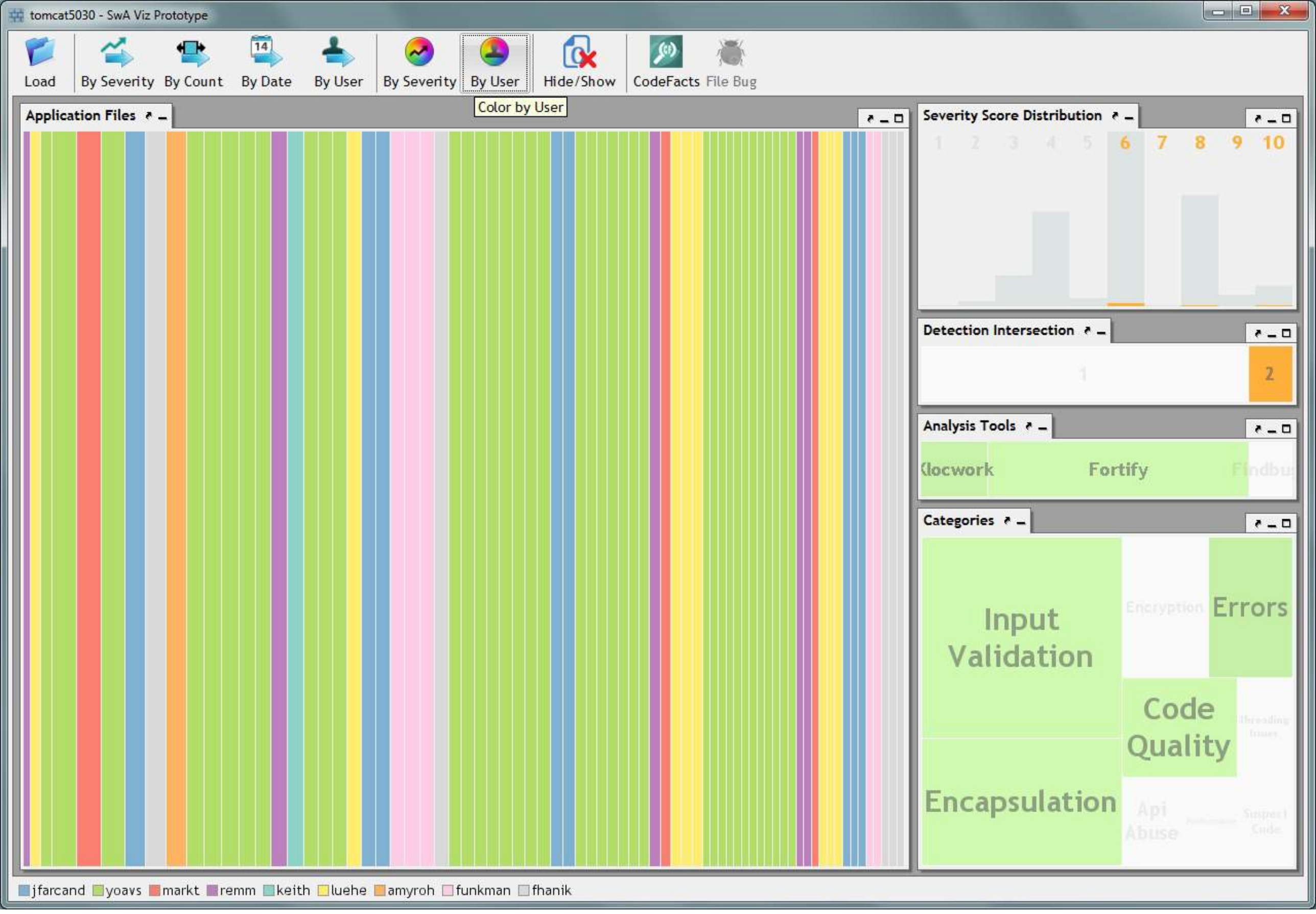
Performance

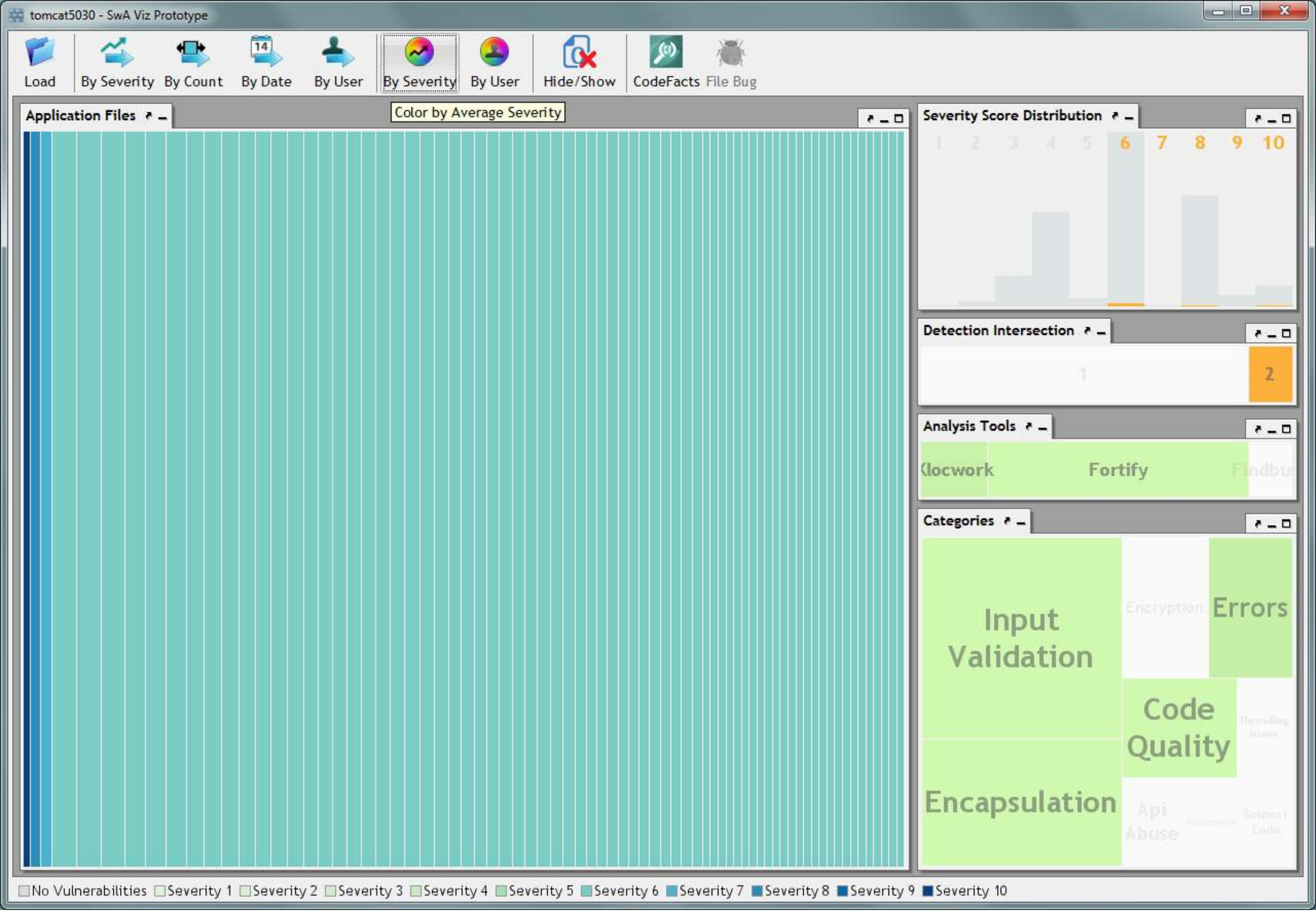
Suspect Code

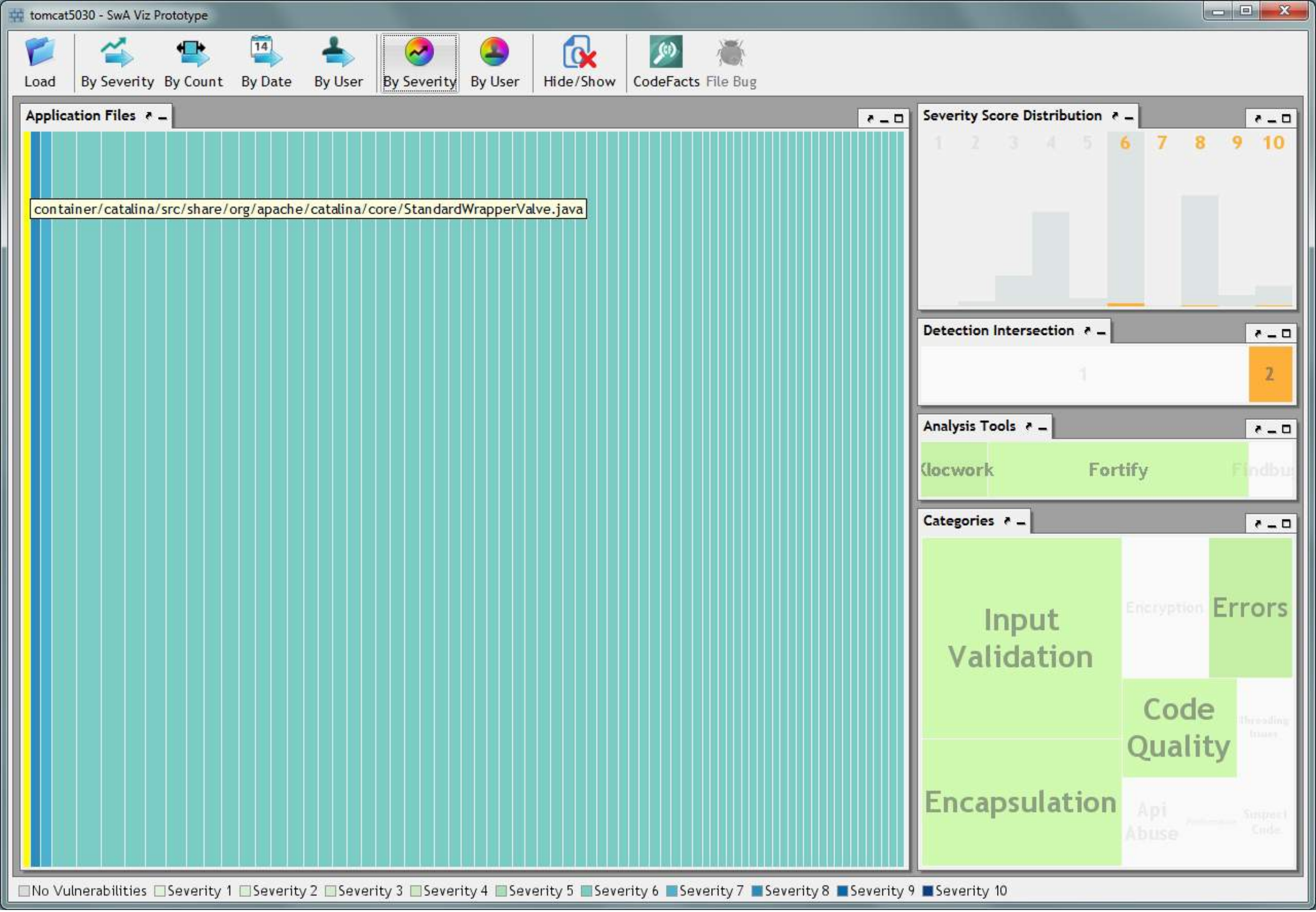
No Vulnerabilities | Severity 1 | Severity 2 | Severity 3 | Severity 4 | Severity 5 | Severity 6 | Severity 7 | Severity 8 | Severity 9 | Severity 10







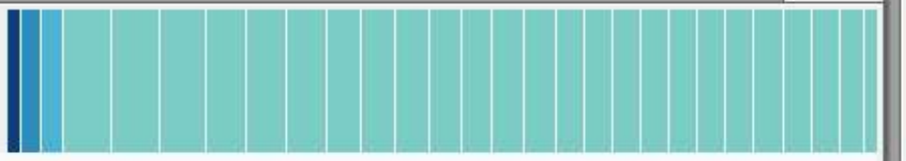




tomcat5030 - SwA Viz Prototype

Load | By Severity | By Count | By Date | By User | By Severity | By User | Hide/Show | CodeFacts | File Bug

Application Files



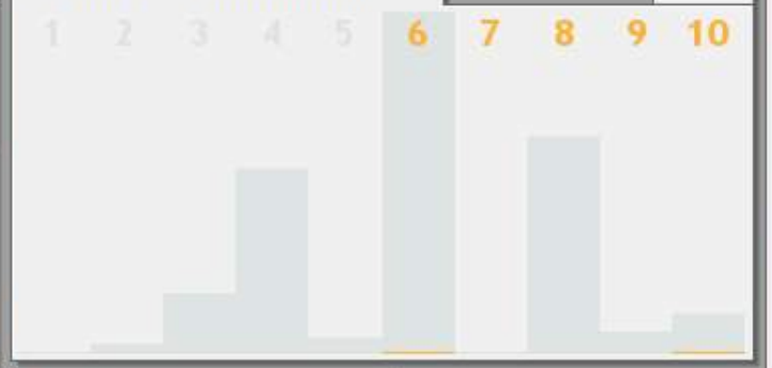
StandardWrapperValve.java

container\catalina\src\share\org\apache\catalina\core

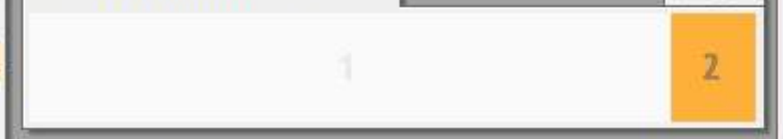
Severity Score: 8.25 Minimum Severity: 6
Vulnerabilities: 2 Maximum Severity: 10

Vulnerabilities	Severity Score	Distribution	Objects
2	**8.25**		- **StandardWrapperValve**
2	8.25		- public invoke(Request request, Response response, ValveContext val
1	10.00		Line 192 - Errors::NPE.COND (Klocwork)
1	6.00		Line 192 - Errors::Null Dereference (Fortify)

Severity Score Distribution

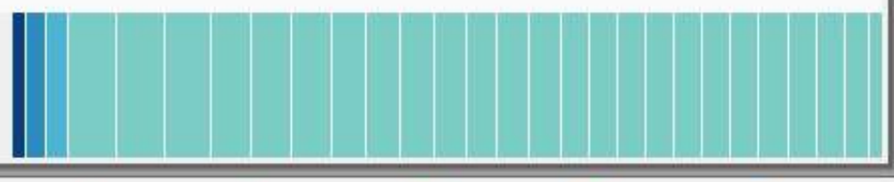


Detection Intersection



Analysis Tools

Categories



No Vulnerabilities | Severity 1 | Severity 2 | Severity 3 | Severity 4 | Severity 5 | Severity 6 | Severity 7 | Severity 8 | Severity 9 | Severity 10

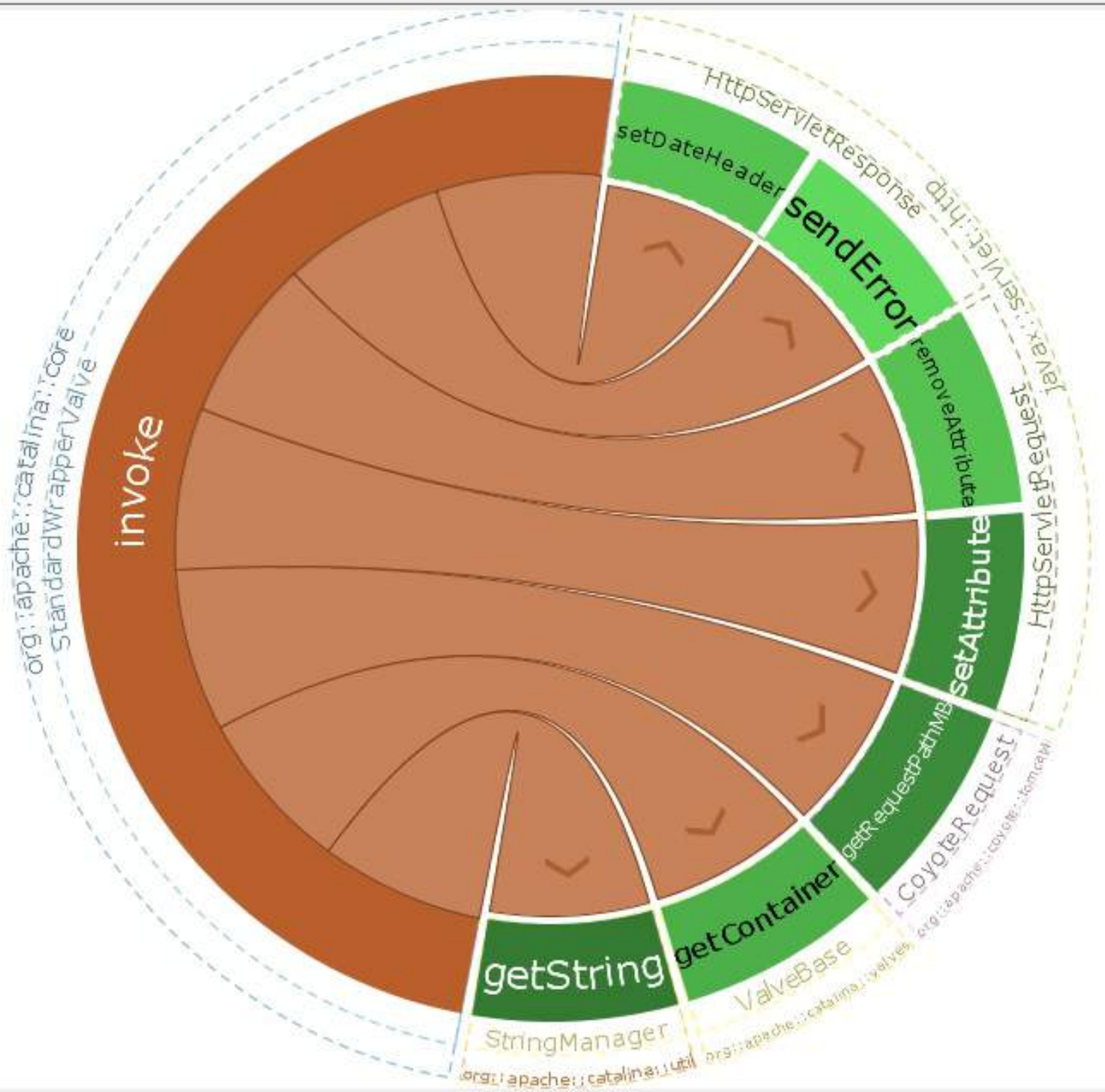
tomcat5030 - SwA Viz Prototype

Load

Tomcat5030 - iTVO 0.1.0.113

File TreeMap Options SAW Options

Treemap SAW



Colors Struct Constructor Destructor Method Static Method Virtual Method

search >>

Ready

tomcat5030 - SwA Viz Prototype

Load | By Severity | By Count | By Date | By User | By Severity | By User | Hide/Show | CodeFacts | File Bug

File currently selected vulnerability as an issue to bugzilla

Application Files

StandardWrapperValve.java

container\catalina\src\share\org\apache\catalina\core

Severity Score: 8.25 Minimum Severity: 6
Vulnerabilities: 2 Maximum Severity: 10

Vulnerabilities	Severity Score	Distribution	Objects
2	**8.25**		- **StandardWrapperValve**
2	8.25		- public invoke(Request request, Response response, ValveContext val
1	10.00		Line 192 - Errors::NPE.COND (Klocwork)
1	6.00		Line 192 - Errors::Null Dereference (Fortify)

Severity Score Distribution

1 2 3 4 5 6 7 8 9 10

Detection Intersection

1 2

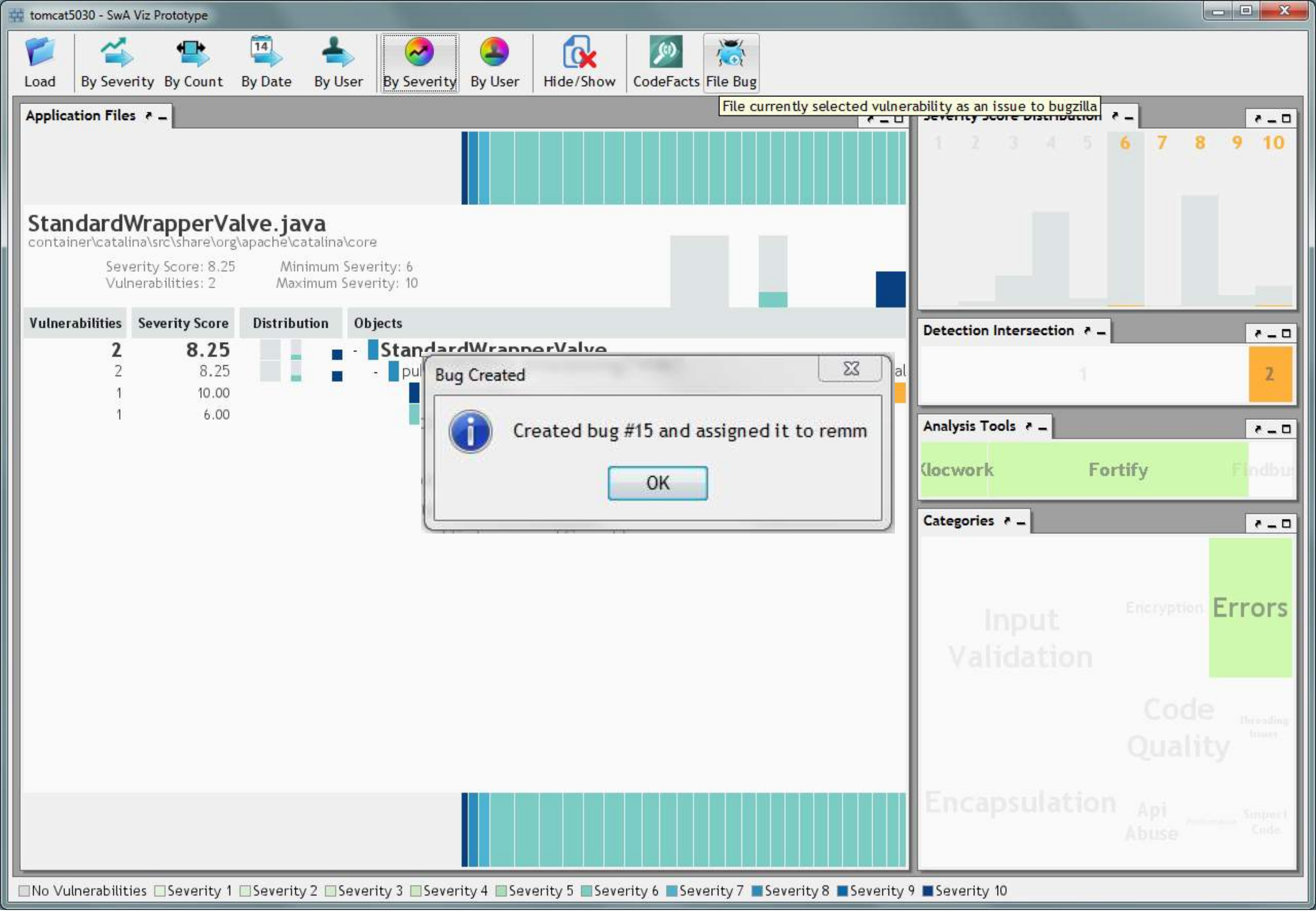
Analysis Tools

Klocwork Fortify Findbu

Categories

Input Validation | Encryption | Errors | Code Quality | Threading Issues | Encapsulation | Api Abuse | Suspect Code

No Vulnerabilities | Severity 1 | Severity 2 | Severity 3 | Severity 4 | Severity 5 | Severity 6 | Severity 7 | Severity 8 | Severity 9 | Severity 10



Bug List

http://192.168.238.129/buglist.cgi?query_format=advanced&order=Importance&bug_status=NEW&bug_status=ASSIGNED&bug_status

Bugzilla – Bug List

Home | New | Search | Find | Reports | Help | New Account | Log In | Forgot Password

Mon May 24 2010 15:50:45 EDT

Bugzilla would like to put a random quip here, but no one has entered any.

Status: NEW, ASSIGNED, REOPENED **Version:** 5030 **Component:** Tomcat **Product:** Tomcat

Zarro Boogs found.

Edit Search Remember search as

File a new bug in the "Tomcat" product

Home | New | Search | Find |

Virtual Bugzilla Server 3.4 brought to you by ALM Work

See also: Deskzilla the desktop client for Bugzilla | VBS F

Before

Bug List

http://192.168.238.129/buglist.cgi?query_format=advanced&order=Importance&bug_status=NEW&bug_status=ASSIGNED&bug_status

Bugzilla – Bug List

Home | New | Search | Find | Reports | Help | New Account | Log In | Forgot Password

Mon May 24 2010 15:53:08 EDT

Bugzilla would like to put a random quip here, but no one has entered any.

Status: NEW, ASSIGNED, REOPENED **Version:** 5030 **Component:** Tomcat **Product:** Tomcat

ID	Sev	Pri	OS	Assignee	Status	Resolution	Summary
15	cri	P1	Wind	remm	ASSI		StandardWrapperValve.java: Errors @ line 192

One bug found.

Long Format XML CSV | Feed | iCalendar | Change Columns | Edit Search Remember search as

File a new bug in the "Tomcat" product

Home | New | Search | Find | Reports | Help | New Account | Log In | Forgot Password

Virtual Bugzilla Server 3.4 brought to you by ALM Works | 2009-12-13

See also: Deskzilla the desktop client for Bugzilla | VBS Forum | Commercial Bugzilla Support

After

Starting point

33,895 vulnerabilities

2 clicks later ...

227 vulnerabilities

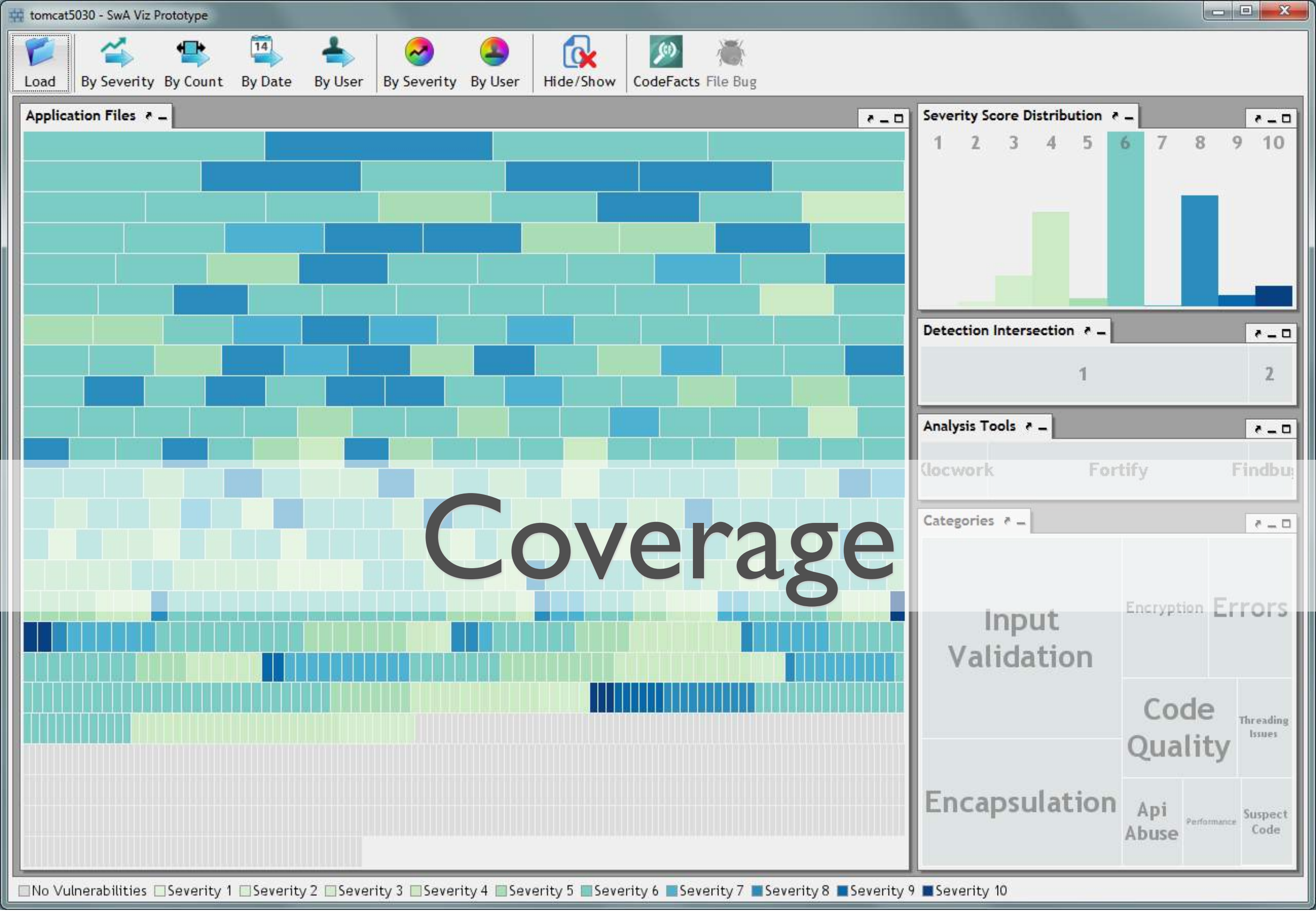
Benefits

- Increased vulnerability coverage through the integration of multiple tools
- Overview of large number of vulnerabilities
- Visual prioritization of vulnerabilities
- Traceability of developer responsibility
- Remediation via integration with SDLC

Benefits

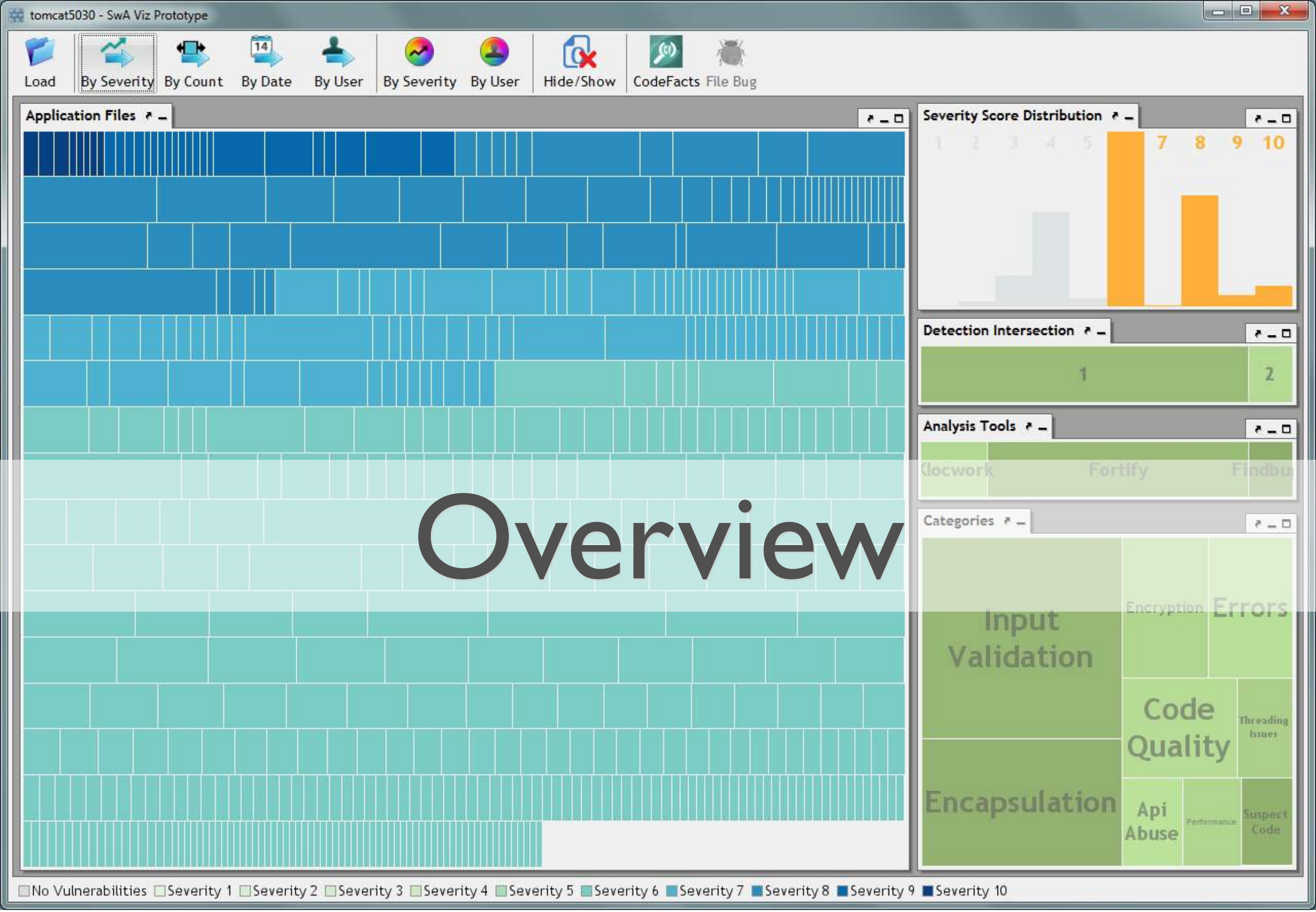
- Increased vulnerability coverage through the integration of multiple tools
- Overview of large number of vulnerabilities
- Visual prioritization of vulnerabilities
- Traceability of developer responsibility
- Remediation via integration with SDLC

Enhances the coverage & speed for detection & remediation of vulnerabilities

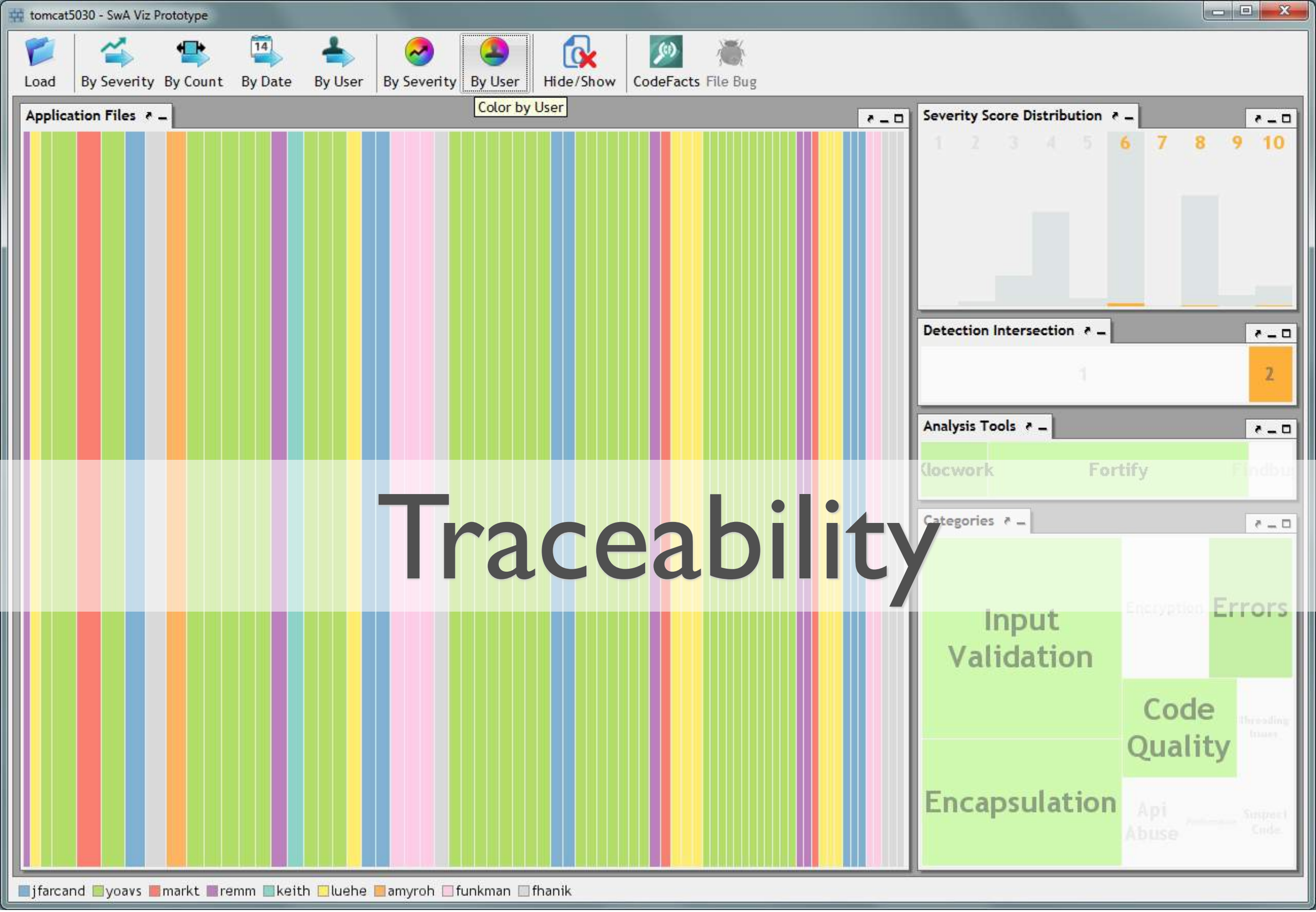


Coverage

Overview

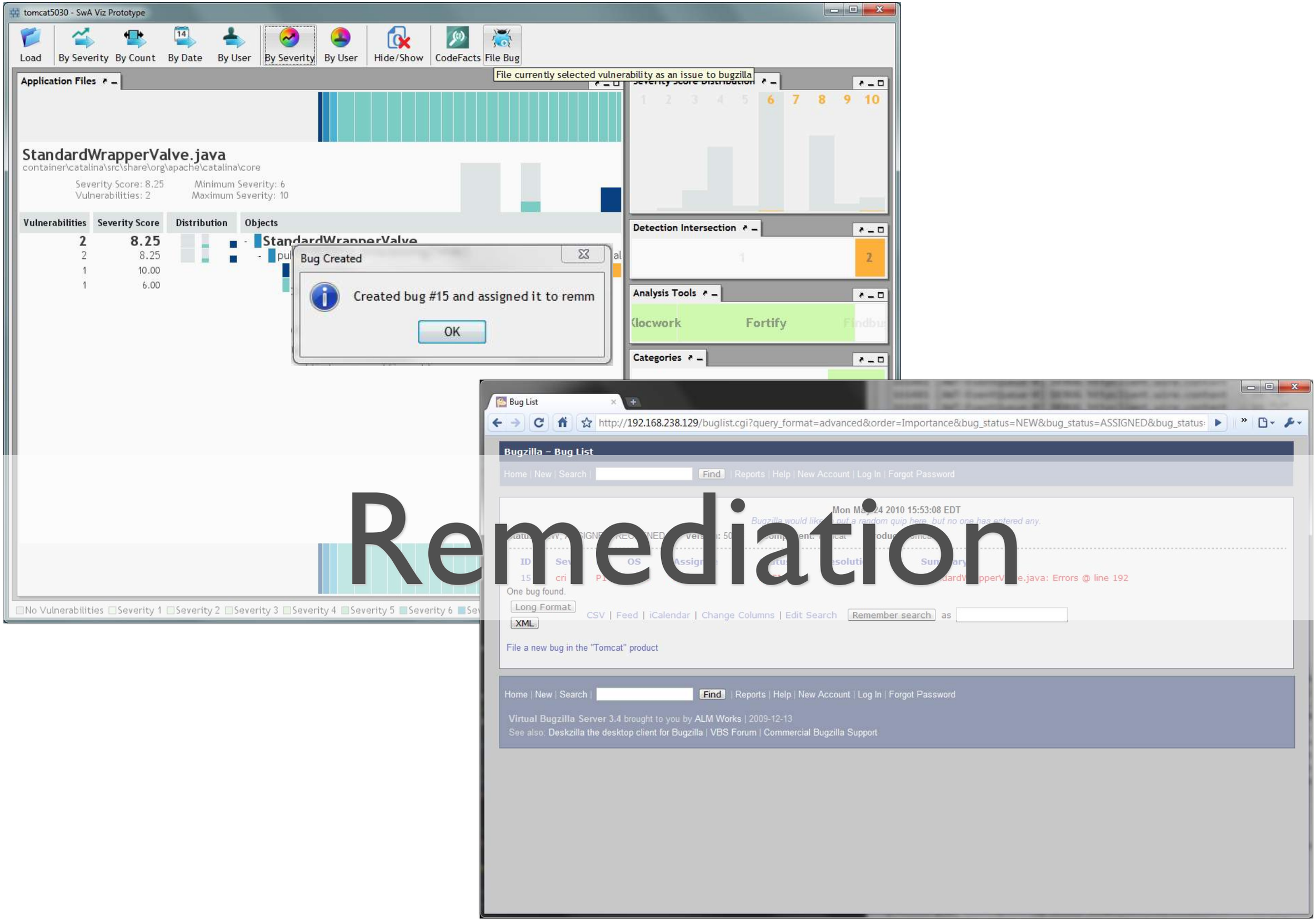


Prioritization

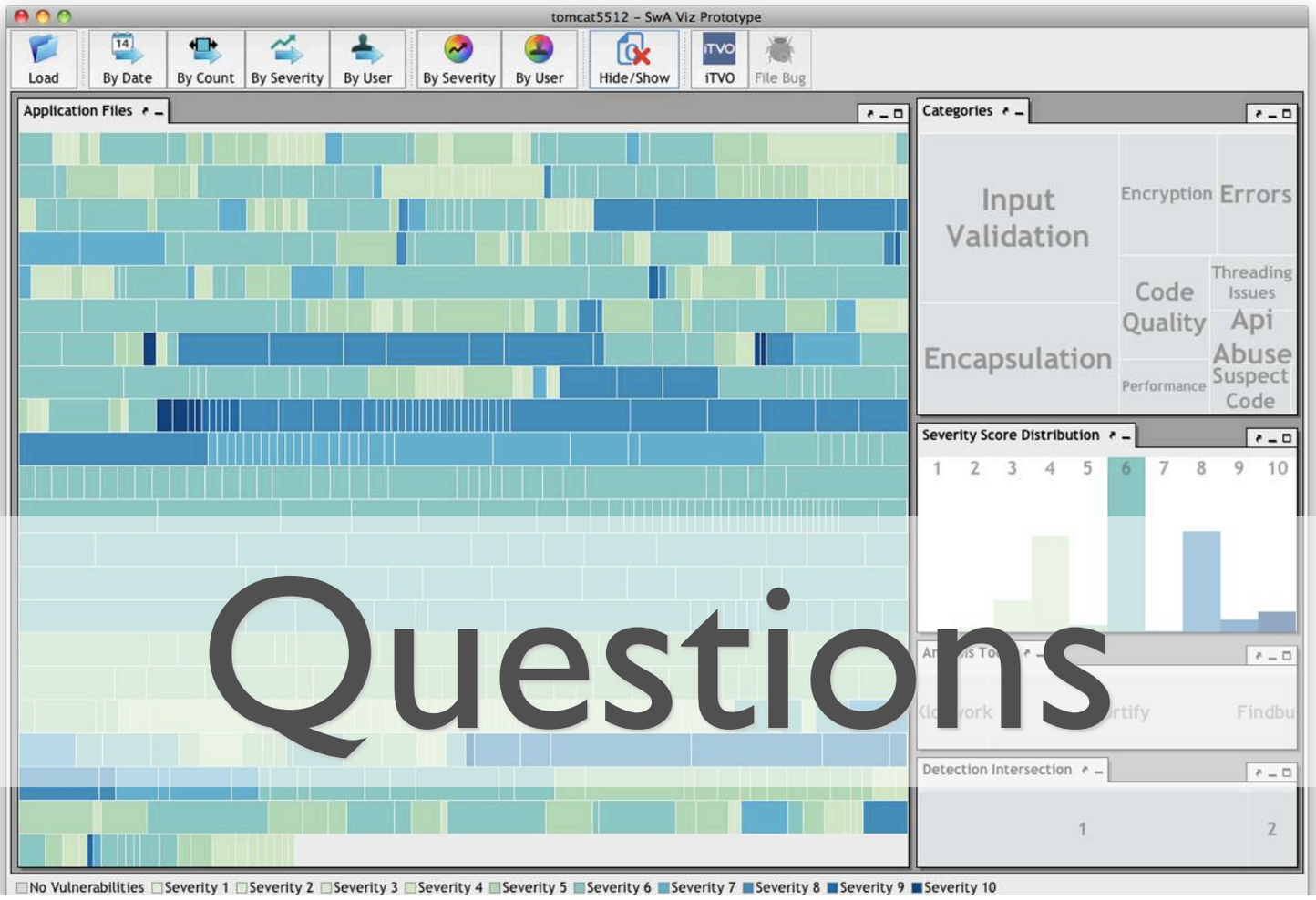


Traceability

Remediation



Visual analysis of code security



Questions

John R. Goodall
Oak Ridge National Laboratory • goodalljr@ornl.gov • 865 576 5943

Hassan Radwan
Applied Visions, Inc. • hassanr@avi.com • 518 207 3106

Lenny Halseth
Applied Visions, Inc. • lennyh@avi.com • 518 207 3108