

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
AppliedVisions, 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.

Digital'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.

Tools Exist Today

Cigital's CTO Gary McGraw

“**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

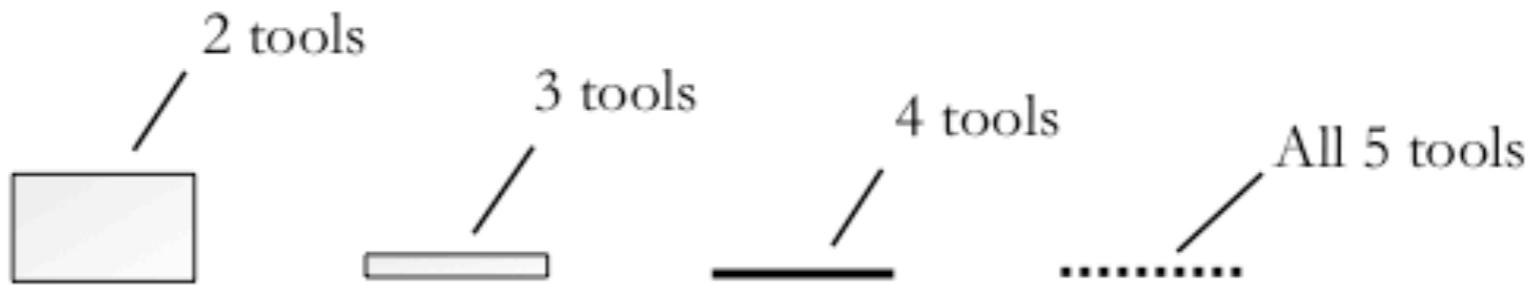
No Tool is Perfect

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

Tools find different vulnerabilities

Non-overlap: Hits reported by one tool and no others (84%)

Overlap: Hits reported by more than one tool (16%)



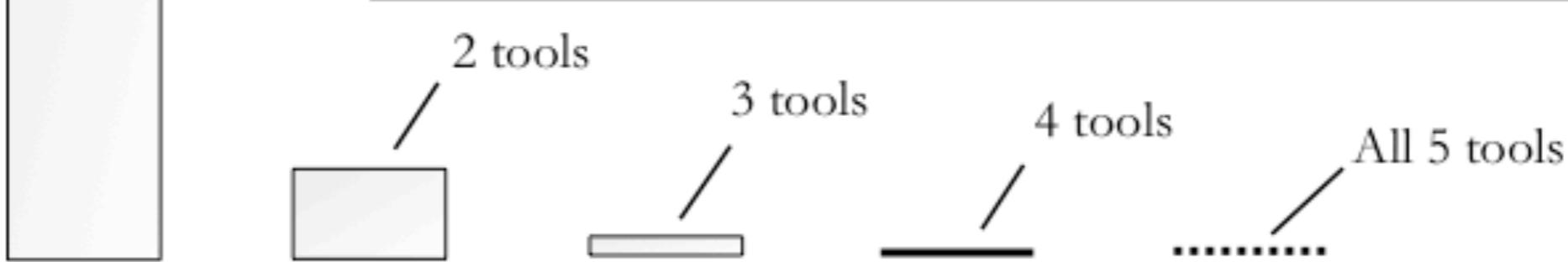
from MITRE

Tools find different vulnerabilities

Non-overlap: Hits reported by one tool and no others (84%)

Very Little Overlap

Overlap: Hits reported by more than one tool (16%)



from MITRE

... with different semantics

```
<BugInstance type="NP_NULL_ON_SOME_PATH" priority="I" 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/secureddecisions/tva/model/xml/ag/
LinkDocument$Link;Lcom/secureddecisions/tva/model/xml/pdag/
ProtectionDomainDocument$ProtectionDomain;Z)Lcom/secureddecisions/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/secureddecisions/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/secureddecisions/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/secureddecisions/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\secureddecisions\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
<apos;java.lang.Exception'</apos;></message>
<anchor>-1088321900</anchor>
<prefix>ed* @sinceVersion 1.0, Mar 12, 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-WVI:8080/klocwork/insight-
review.html#goto:project=gmu212,pid=2</url>
</problem>
```

... with different semantics

```
<BugInstance type="NP_NULL_ON_SOME_PATH" priority="I" 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/secureddecisions/tva/model/xml/ag/
LinkDocument$Link;Lcom/secureddecisions/tva/model/xml/pdag/
ProtectionDomainDocument$ProtectionDomain;Z)Lcom/secureddecisions/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/secureddecisions/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/secureddecisions/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/secureddecisions/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\secureddecisions\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
<apos;java.lang.Exception'</apos;></message>
<anchor>-1088321900</anchor>
<prefix>ed* @since Version 1.0, Mar 12, 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-WVI: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...

... with different semantics

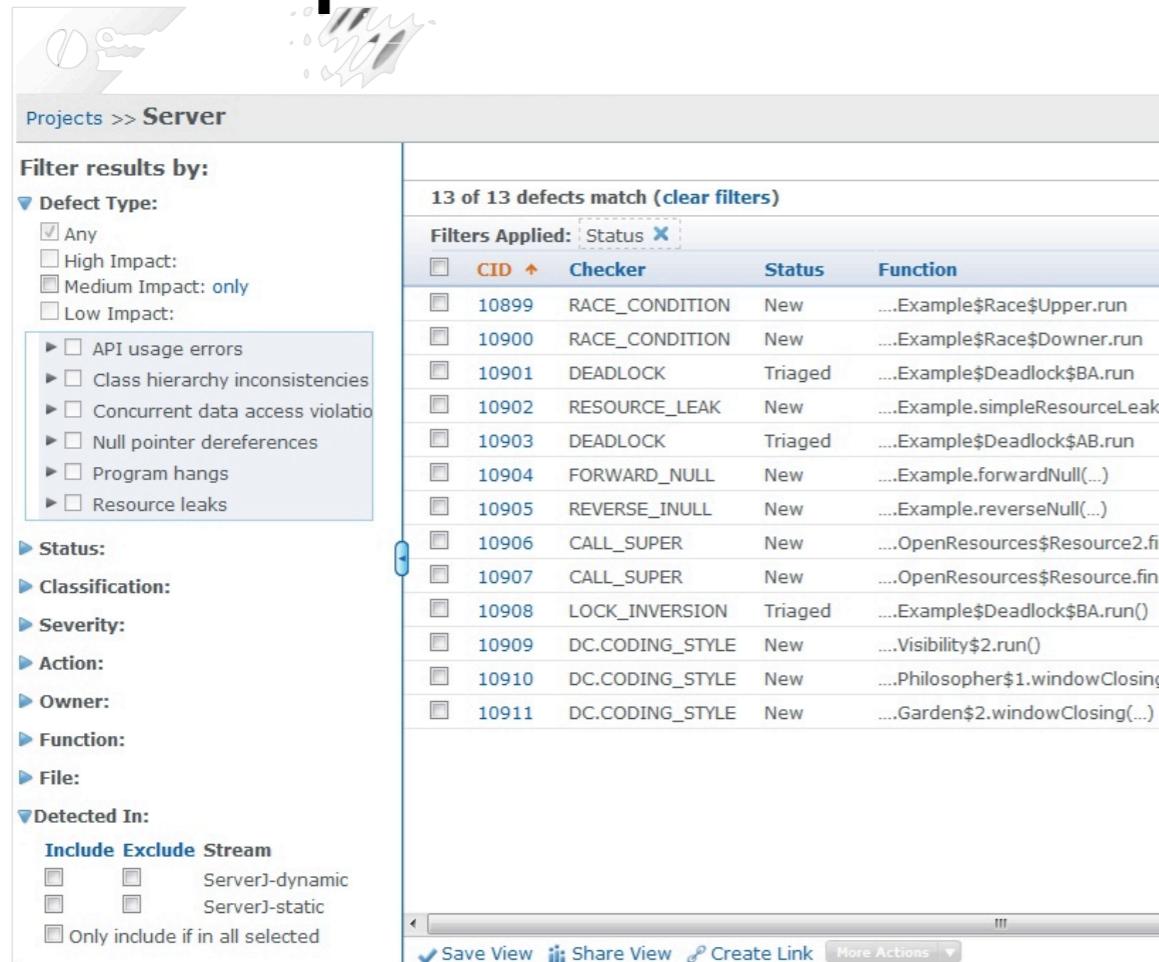
```
<BugInstance type="NP_NULL_ON_SOME_PATH" priority="I" abbrev="NP"
category="CORRECTNESS">
  <Class
  classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator">
    <SourceLine
    classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
    start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/
securedecisions/tva/model/linksettransform/LinkSetAggregator.java"/>
  </Class>
  <Method
  classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
  name="createFromExploit" signature="(Lcom/secureddecisions/tva/model/xml/ag/
LinkDocument$Link;Lcom/secureddecisions/tva/model/xml/pdag/
ProtectionDomainDocument$ProtectionDomain;Z)Lcom/secureddecisions/tva/model/
xml/pdag/Exploitsumer$Exploit;" static="false">
    <SourceLine
    classname="com.securedecisions.tva.model.linksettransform.LinkSetAggregator"
    start="541" end="563" startBytecode="124" endBytecode="125"
    sourcefile="LinkSetAggregator.java" sourcepath="com/secureddecisions/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/secureddecisions/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/secureddecisions/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\secureddecisions\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
<apos;java.lang.Exception'</apos;></message>
<anchor>-1088321900</anchor>
<prefix>ed* @sinceVersion 1.0.Mar12.2006*</prefix>
<postfix>(if(assertion==false)throwexcept</postfix>
<severity>Style</severity>
<severitylevel>8</severitylevel>
<displayAs>Warning</displayAs>
<category>Navigation From Handling</category>
<category>Analysis</category>
<category>Commit</category>
<state>New</state>
<dateOriginated>1264106407000</dateOriginated>
<url>http://NPT-0779-WVI:8080/klocwork/insight-
review.html#goto:project=gmu212,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...

Tools present vulnerabilities



Projects >> Server

Filter results by:

Defect Type:

- Any
- High Impact:
- Medium Impact: **only**
- Low Impact:

- API usage errors
- Class hierarchy inconsistencies
- Concurrent data access violations
- Null pointer dereferences
- Program hangs
- Resource leaks

Status:

Classification:

Severity:

Action:

Owner:

Function:

File:

Detected In:

Include Exclude Stream

- ServerJ-dynamic
- ServerJ-static
- Only include if in all selected

13 of 13 defects match (clear filters)

Filters Applied: Status X

CID	Checker	Status	Function
10899	RACE_CONDITION	New	...Example\$Race\$Upper.run
10900	RACE_CONDITION	New	...Example\$Race\$Downer.run
10901	DEADLOCK	Triaged	...Example\$Deadlock\$BA.run
10902	RESOURCE_LEAK	New	...Example.simpleResourceLeak
10903	DEADLOCK	Triaged	...Example\$Deadlock\$AB.run
10904	FORWARD_NULL	New	...Example.forwardNull(...)
10905	REVERSE_INULL	New	...Example.reverseNull(...)
10906	CALL_SUPER	New	...OpenResources\$Resource2.fir
10907	CALL_SUPER	New	...OpenResources\$Resource.fin
10908	LOCK_INVERSION	Triaged	...Example\$Deadlock\$BA.run()
10909	DC.CODING_STYLE	New	...Visibility\$2.run()
10910	DC.CODING_STYLE	New	...Philosopher\$1.windowClosing
10911	DC.CODING_STYLE	New	...Garden\$2.windowClosing(...)

Save View Share View Create Link More Actions

-  junit.extensions
- ▲  junit.framework
 -  Assert.java
 - ▲  AssertionFailedError.java
 -  AssertionFailedError
 -  serialVersionUID
 -  AssertionFailedError()
 -  AssertionFailedError(String)
 -  ComparisonCompactor.java
 - ▲  ComparisonCompactor
 -  DELTA_END
 -  DELTA_START
 -  ELLIPSIS
 -  fActual
 -  fContextLength
 -  fExpected
 -  fPrefix
 -  fSuffix
 -  ComparisonCompactor(int, String, String)
 -  areStringsEqual() : boolean
 -  compact(String) : String
 -  compactString(String) : String
 -  computeCommonPrefix() : String
 -  computeCommonSuffix() : String
 -  findCommonPrefix() : void
 -  findCommonSuffix() : void

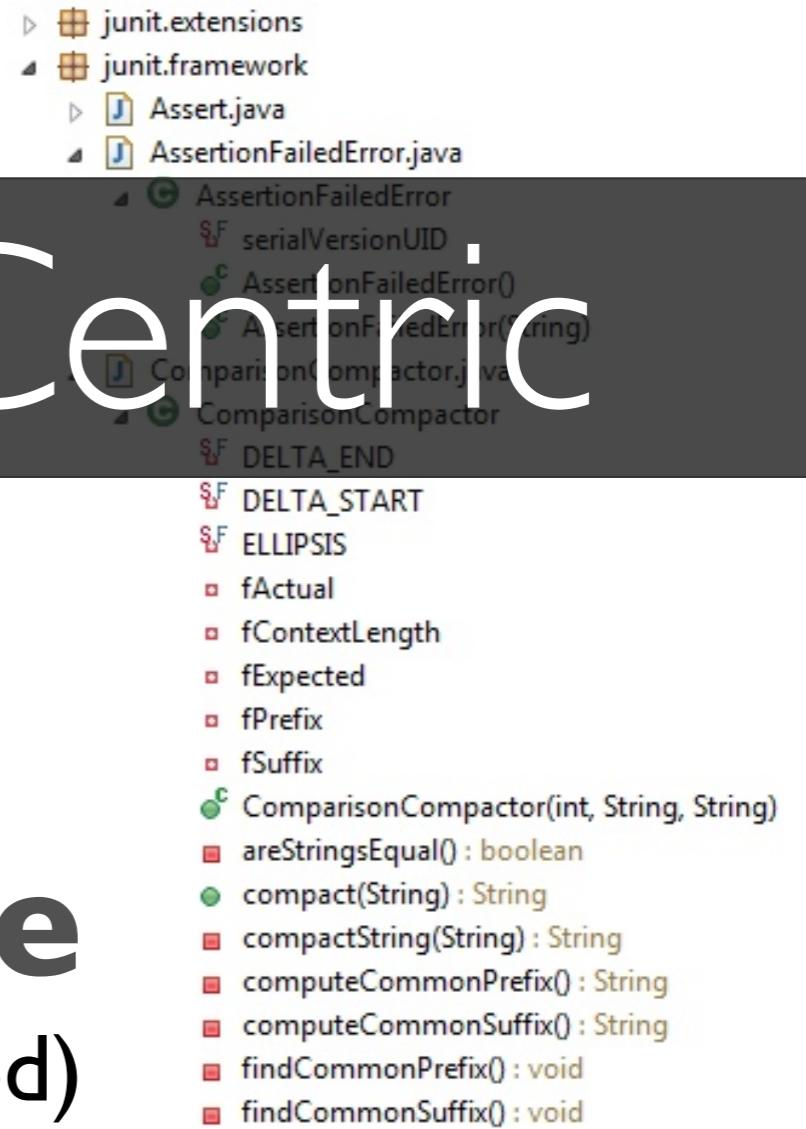
Developers think in **code** (namespace/class/method)

Tools present vulnerabilities

The screenshot shows a software interface for managing code quality. At the top, there's a logo of a key and a gear, followed by the text "Projects >> Server". Below this is a sidebar titled "Filter results by:" which includes sections for "Defect Type", "Status", "Classification", "Severity", "Action", "Owner", and "Function". Under "Defect Type", "Medium Impact: only" is selected. The main area displays a table with 13 rows of defect details:

CID	Checker	Status	Function
10899	RACE_CONDITION	New	...Example\$Race\$Upper.run
10900	RACE_CONDITION	New	...Example\$Race\$Downer.run
10901	DEADLOCK	Triaged	...Example\$Deadlock\$BA.run
10902	RESOURCE_LEAK	New	...Example.simpleResourceLeak
10903	DEADLOCK	Triaged	...Example\$Deadlock\$AB.run
10904	FORWARD_NULL	New	...Example.forwardNull(...)
10905	REVERSE_INULL	New	...Example.reverseNull(...)
10906	CALL_SUPER	New	...OpenResources\$Resource\$2.fin...
10907	CALL_SUPER	New	...OpenResources\$Resource\$Final...
10908	LOCK_INVERSION	Triaged	...Example\$Deadlocks\$A.run()
10909	DC_CODING_STYLE	New	...Visibility\$2.run()
10910	DC_CODING_STYLE	New	...Garden\$2.windowClosing(...)
10911	DC_CODING_STYLE	New	...Garden\$2.windowClosing(...)

At the bottom of the interface are buttons for "Save View", "Share View", "Create Link", and "More Actions".



Vulnerability-Centric

Developers think in **code** (namespace/class/method)

Coverity® Integrity Manager

Admin User | Sign out | Preferences | Help | About | Jump to CID:

Dashboard Projects Configuration Administration

Projects >> Covtel Kernel Code >> New View*

Defects Source Metrics Trends Dashboard

Filter results by:

Defect Type:

- Any
- High Impact: only
- Medium Impact: only
- Low Impact: only

- Memory - corruptions
- Memory - illegal accesses
- Resource leaks
 - Resource leak
 - RESOURCE_LEAK
- Uninitialized variables
 - Uninitialized scalar variable
 - UNINIT
- API usage errors
- Control flow issues
- Error handling issues
- Incorrect Expression
- Insecure data handling
- Integer handling issues
- Null pointer dereferences
- Program hangs
 - Infinite loop
 - INFINITE_LOOP
- Build system issues
- Code maintainability issues
- Performance inefficiencies
- Security best practice violations
- Warnings

Severity:

- Any
- Unspecified: only
- Major: only
- Moderate: only
- Minor: only
- Various: only

Status:

- Any
- Outstanding
- Resolved
- Inspected

New: only

59 of 4700 defects match (clear filters)

Filters Applied: Checker Status Detected In

CID	Checker	Severity	Status	Owner	Classification	Action	Function
10001	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	acpi_ex_store()
10002	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	acpi_ex_opcode_1A_0T_1R()
10005	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	skb_copy_datagram()
10006	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	rt_fill_info()
10007	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	rt6_fill_node()
10008	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	tcp_sendpage()
10009	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Undclassified	Undecided	tcpdiag_bc_run()
10012	BAD_FREE	Unspecified	New	Unassigned	Undclassified	Undecided	sctp_endpoint_destroy()
10013	BAD_FREE	Unspecified	New	Unassigned	Undclassified	Undecided	sctp_transport_destroy()
10014	BAD_FREE	Unspecified	New	Unassigned	Undclassified	Undecided	sctp_association_free()
10022	BUFFER_SIZE	Unspecified	New	Unassigned	Undclassified	Undecided	fat_new_dir()
10028	BUFFER_SIZE	Unspecified	New	Unassigned	Undclassified	Undecided	msdos_add_entry()
10031	BUFFER_SIZE	Unspecified	New	Unassigned	Undclassified	Undecided	vfat_fill_slots()
10039	BUFFER_SIZE	Unspecified	New	Unassigned	Undclassified	Undecided	packet_getname_split()
10328	NEGATIVE RETURNS	Unspecified	New	Unassigned	Undclassified	Undecided	handle_inirtd()
10556	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	DAC960_V2_ReadControllerConfiguration()
10560	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	scsi_cmd_free()
10565	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	do_cqis_request()
10567	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	do_ida_request()
10615	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	64_bit_prefix()
10618	OVERRUN_STATIC	Unspecified	New	Unassigned	Undclassified	Undecided	inet_to_dname()
10727	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	PCI0_Process_implied_command()
10770	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	cciss_update_non_disk_devices()
10771	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	register_new_disk()
10772	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	register_new_disk()
10773	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	compaq_nvram_load()
10774	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	compaq_nvram_load()
10775	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	compaq_nvram_load()
10776	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	compaq_nvram_load()
10801	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	i2c_parport_attach()
10802	RESOURCE LEAK	Unspecified	New	Unassigned	Undclassified	Undecided	rd_load_image()
							irimp_open_isap()
							ax25_connect()

Save View Share View Create Link More Actions

Load Your View Load Shared View

X

Filter results by:

Defect Type:

- Any
- High Impact: only
- Medium Impact: only
- Low Impact: only

Memory - corruptions

- Memory - illegal accesses

Resource leaks

- Resource leak
- RESOURCE LEAK

Uninitialized variables

- Uninitialized scalar variable
- UNINIT

API usage errors

Control flow issues

Error handling issues

Incorrect Expression

Insecure data handling

Integer handling issues

Null pointer dereferences

Program hangs

- Infinite loop
- INFINITE_LOOP

Build system issues

Code maintainability issues

Performance inefficiencies

Security best practice violations

Warnings

Severity:

- Any
- Unspecified: only
- Major: only
- Moderate: only
- Minor: only
- Various: only

Status:

- Any
- Outstanding
- Resolved
- Inspected

 New: only59 of 4700 defects match ([clear filters](#))Filters Applied: Checker Status Detected In

CID	Checker	Severity	Status	Owner	Classification	Action	Function
10001	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	acpi_ex_store()
10002	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	acpi_ex_opcode_1A_0T_1R()
10005	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	skb_copy_datagram()
10006	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	rt_fill_info()
10007	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	rt6_fill_node()
10008	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	tcp_sendpage()
10009	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	tcpdiag_bc_run()
10012	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sctp_endpoint_destroy()
10013	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sctp_transport_destroy()
10014	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sctp_association_free()
10022	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	fat_new_dir()
10028	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	msdos_add_entry()
10031	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	vfat_fill_slots()
10039	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	packet_getname_spkt()
10328	NEGATIVE_RETURNS	Unspecified	New	Unassigned	Unclassified	Undecided	handle_intrd()
10550	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	DAC900_V2_ReadControllerConfiguration()
10560	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cmd_free()
10565	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	do_csiis_request()
10567	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	do_ida_request()
10615	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	i686_prefetch()
10618	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	inet_dtr_to_dname()
10727	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	PCI0_Process_implied_command()
10770	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	cciss_update_non_disk_devices()
10771	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	register_new_disk()
10772	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	register_new_disk()
10773	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	compaq_nvram_load()
10774	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	compaq_nvram_load()
10775	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	compaq_nvram_load()
10776	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	compaq_nvram_load()
10800	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	i2c_parport_attach()
10801	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	rd_load_image()
10802	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	irimp_open_isap()
							ax25_connect()

No Big Picture

50,000 vulnerabilities...

Now what?

 Save View Share View Create Link More Actions Load Your View Load Shared View

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 \neq 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

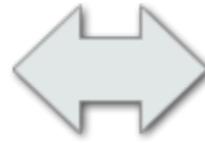
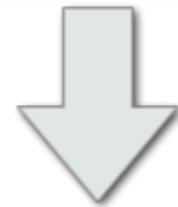
Better analysis tools are only a part
of improving code security

Technical Approach

Technical Approach

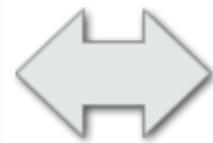
SoftWare Assurance ViSual Analysis

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



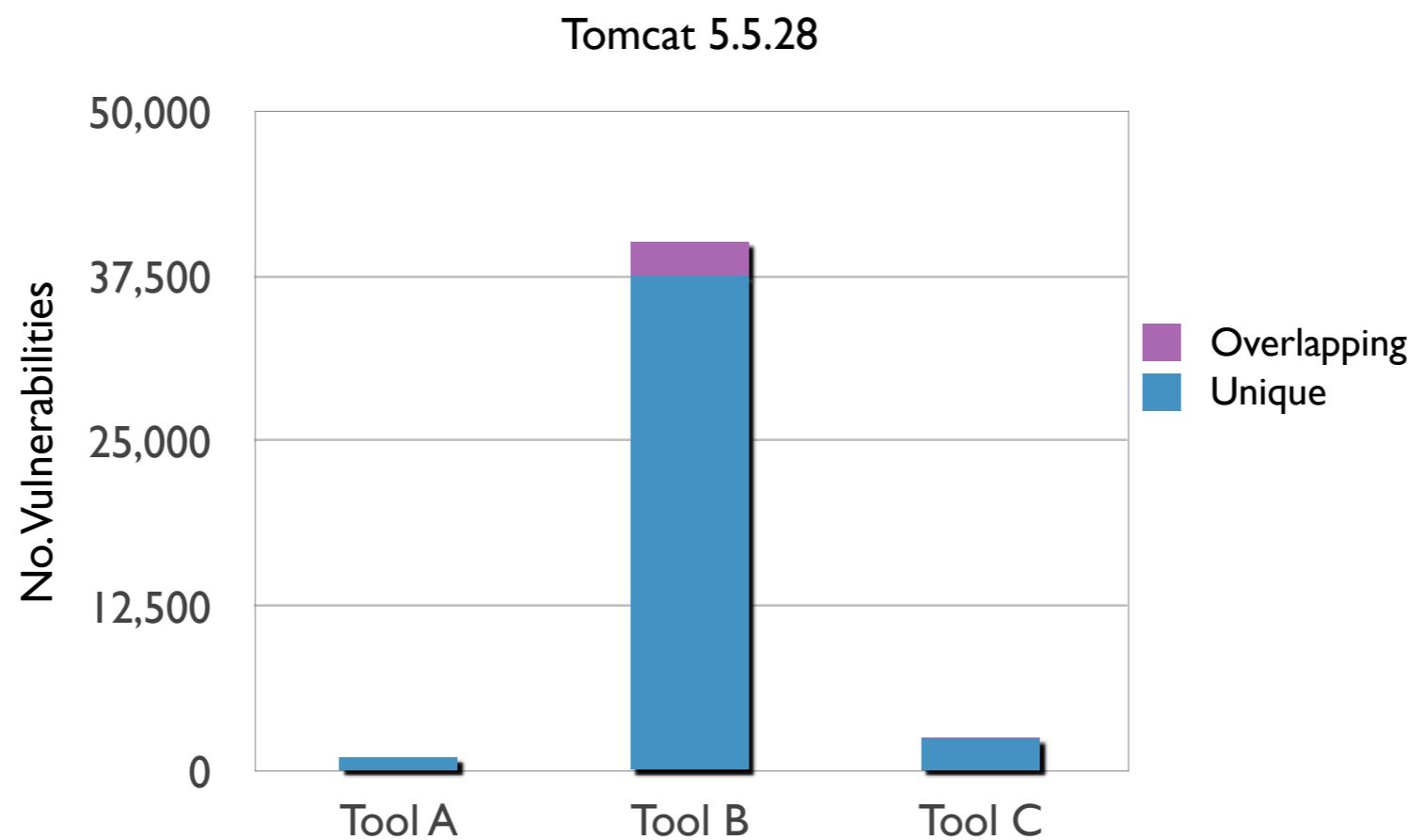


integrate / correlate / normalize



Test Data

- Three software analysis tools
- Two test data sets



SwA Tool Output

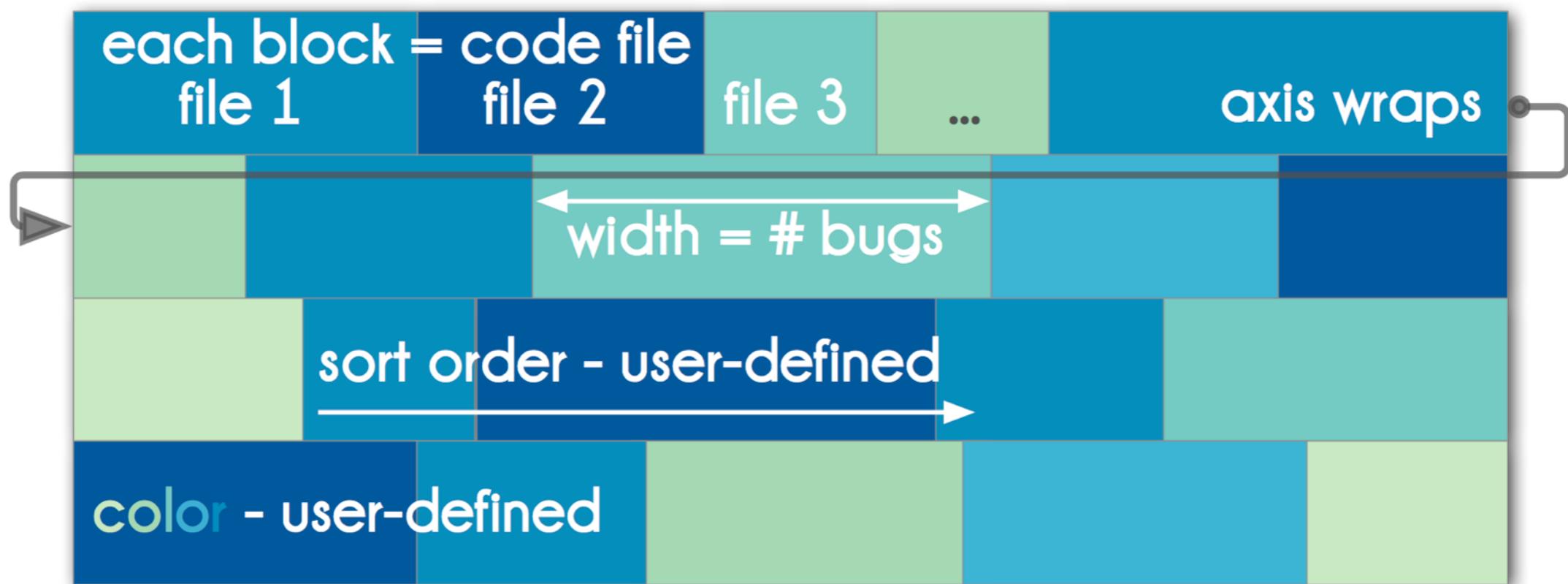
- Tool output is in varying XML schemas
- Results are parsed and correlated
- Severity and category are normalized

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



Load



By Severity



By Count



By Date



By User



By Severity



By User



Hide/Show



CodeFacts



File Bug

Application Files

Severity Score Distribution

Detection Intersection

Analysis Tools

Categories

Overview first, zoom & filter, details on demand...
– Ben Schneiderman



Load



By Severity



By Count



By Date



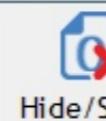
By User



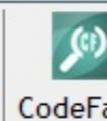
By Severity



By User



Hide/Show



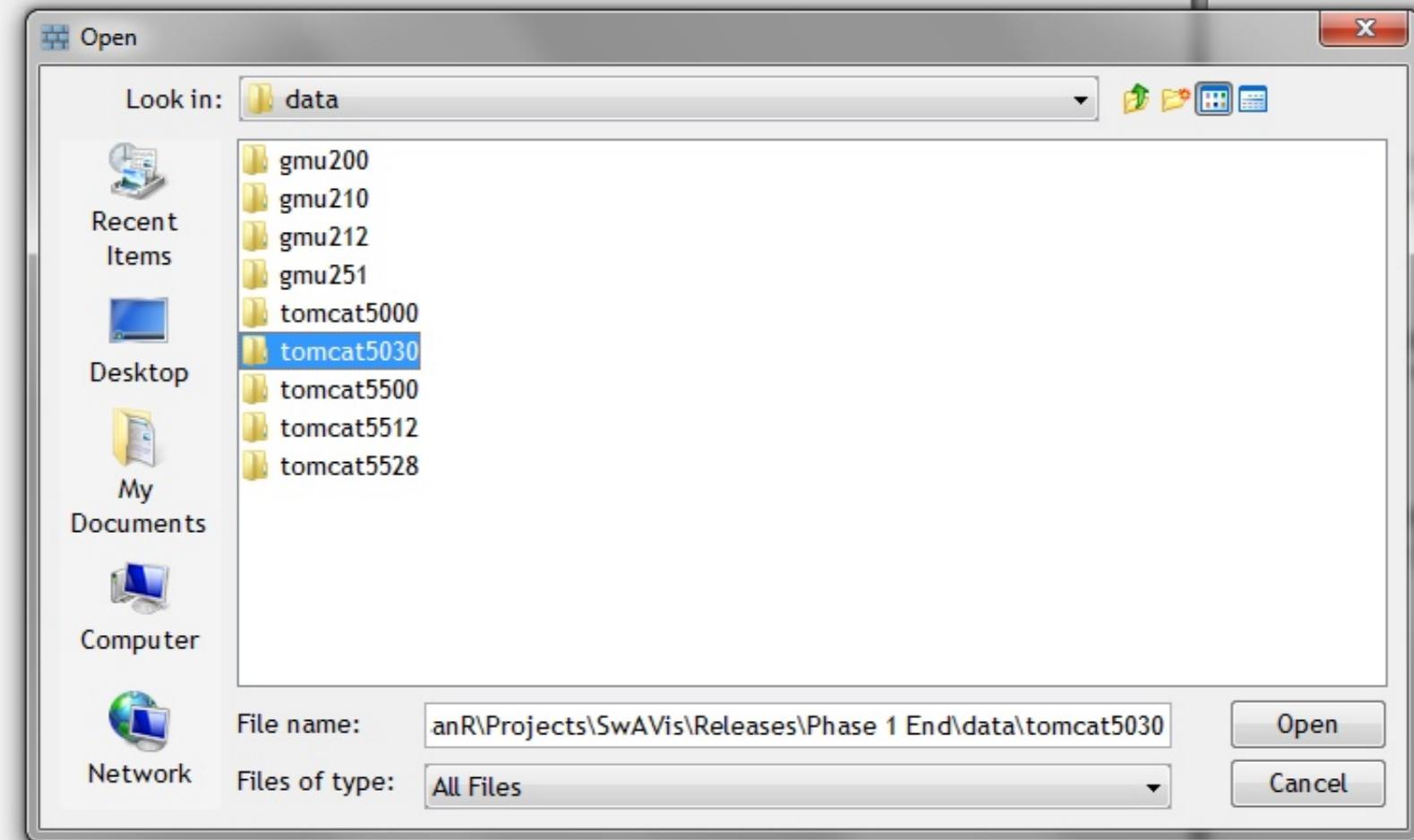
CodeFacts

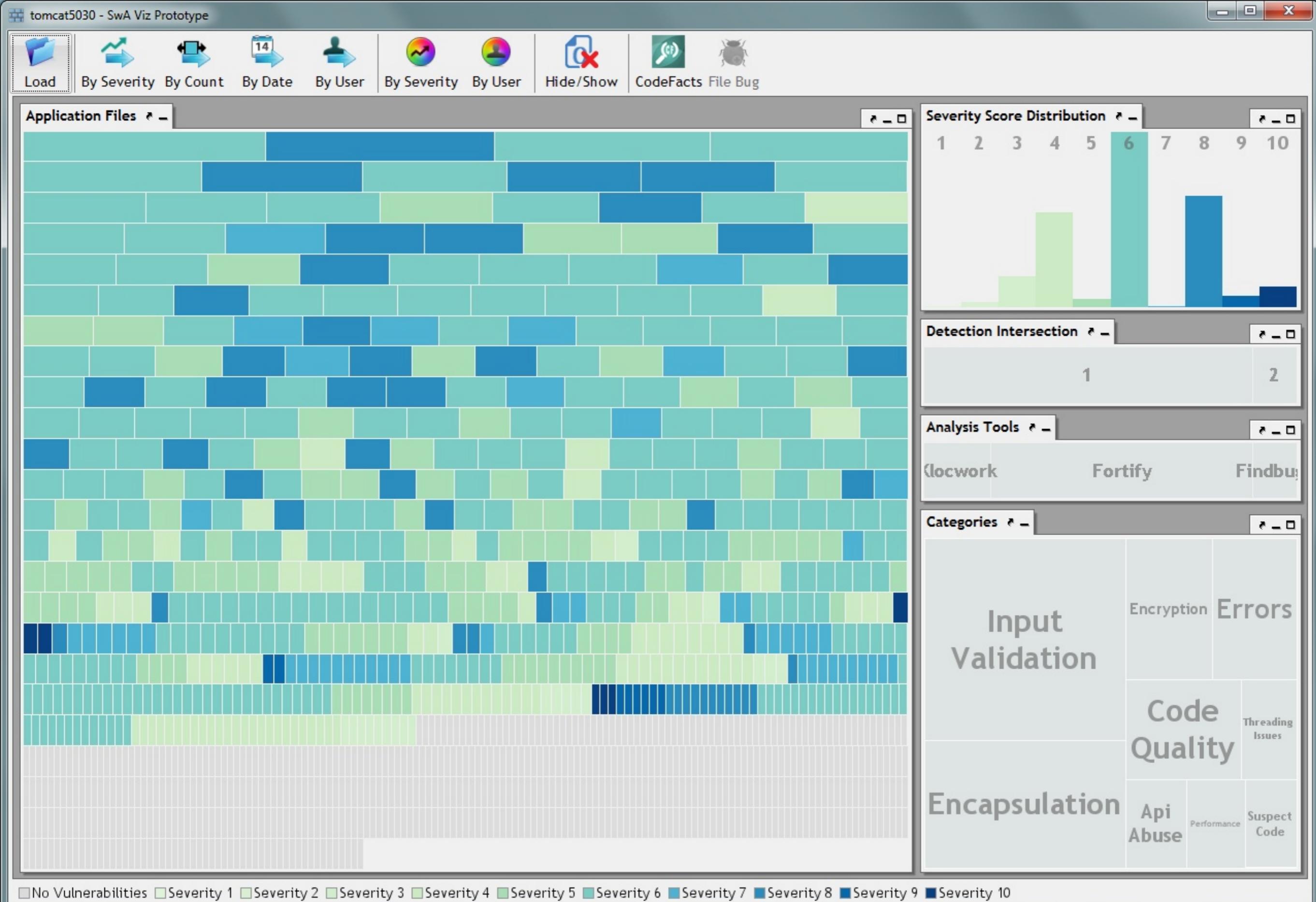


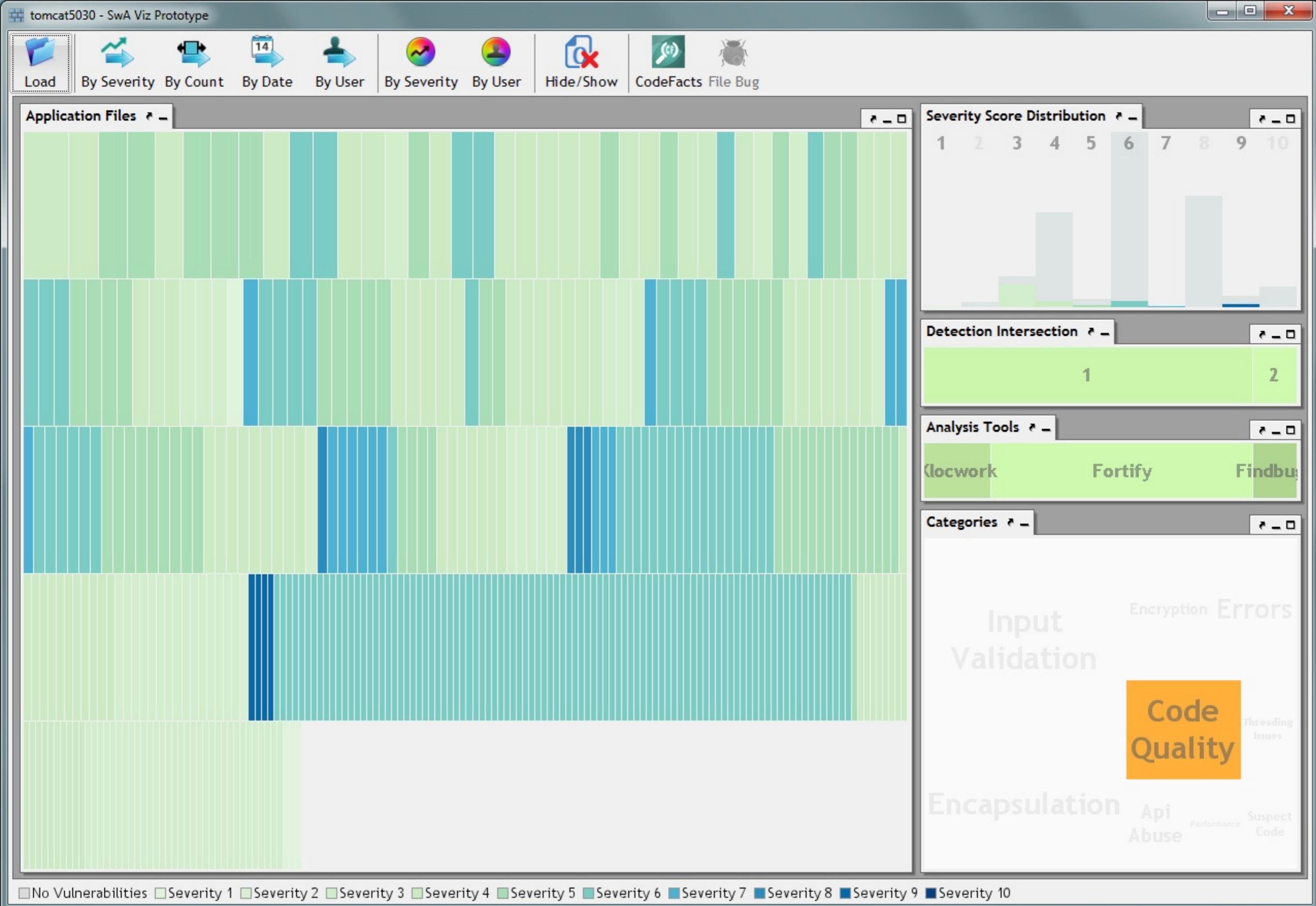
File Bug

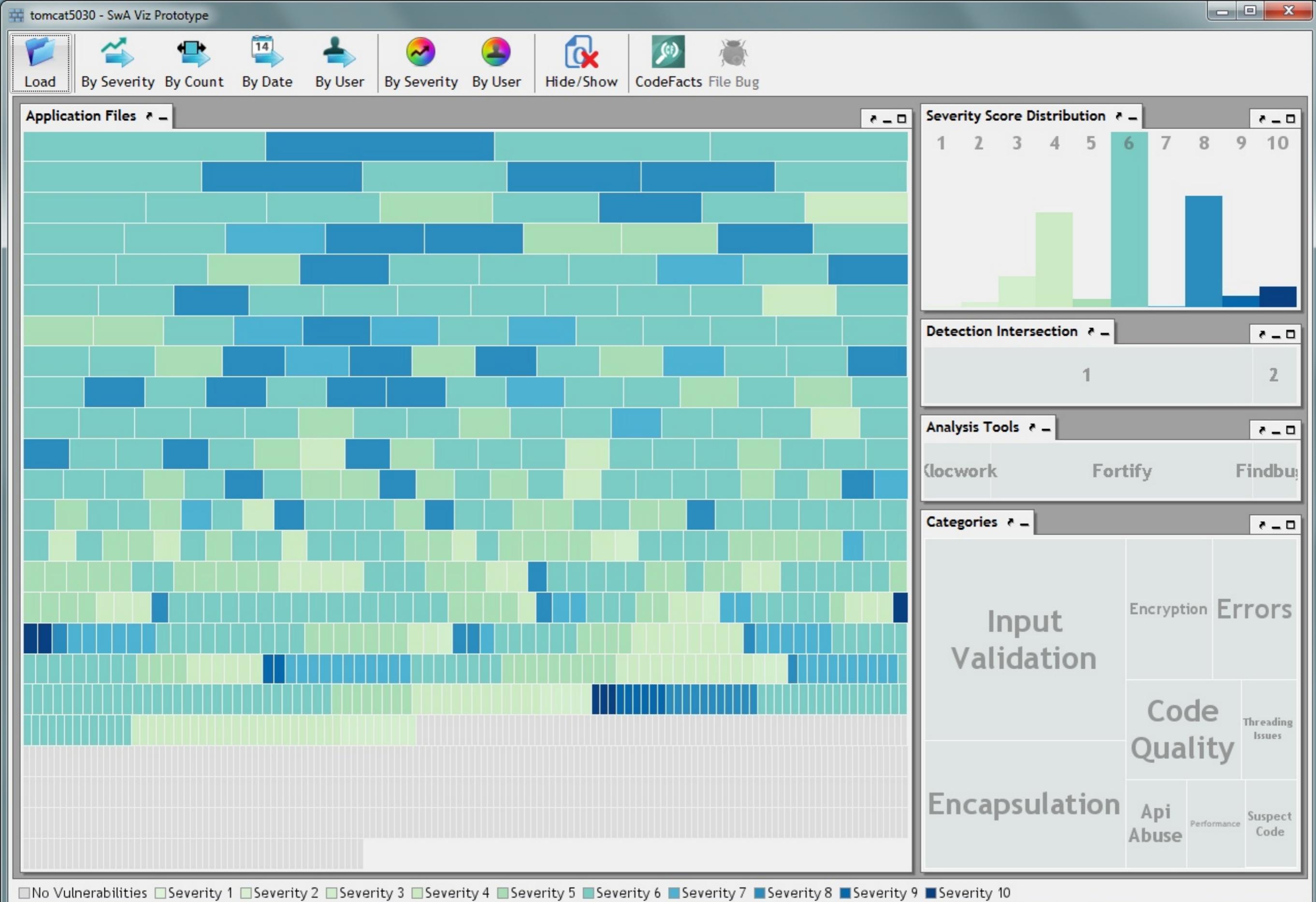
Application Files

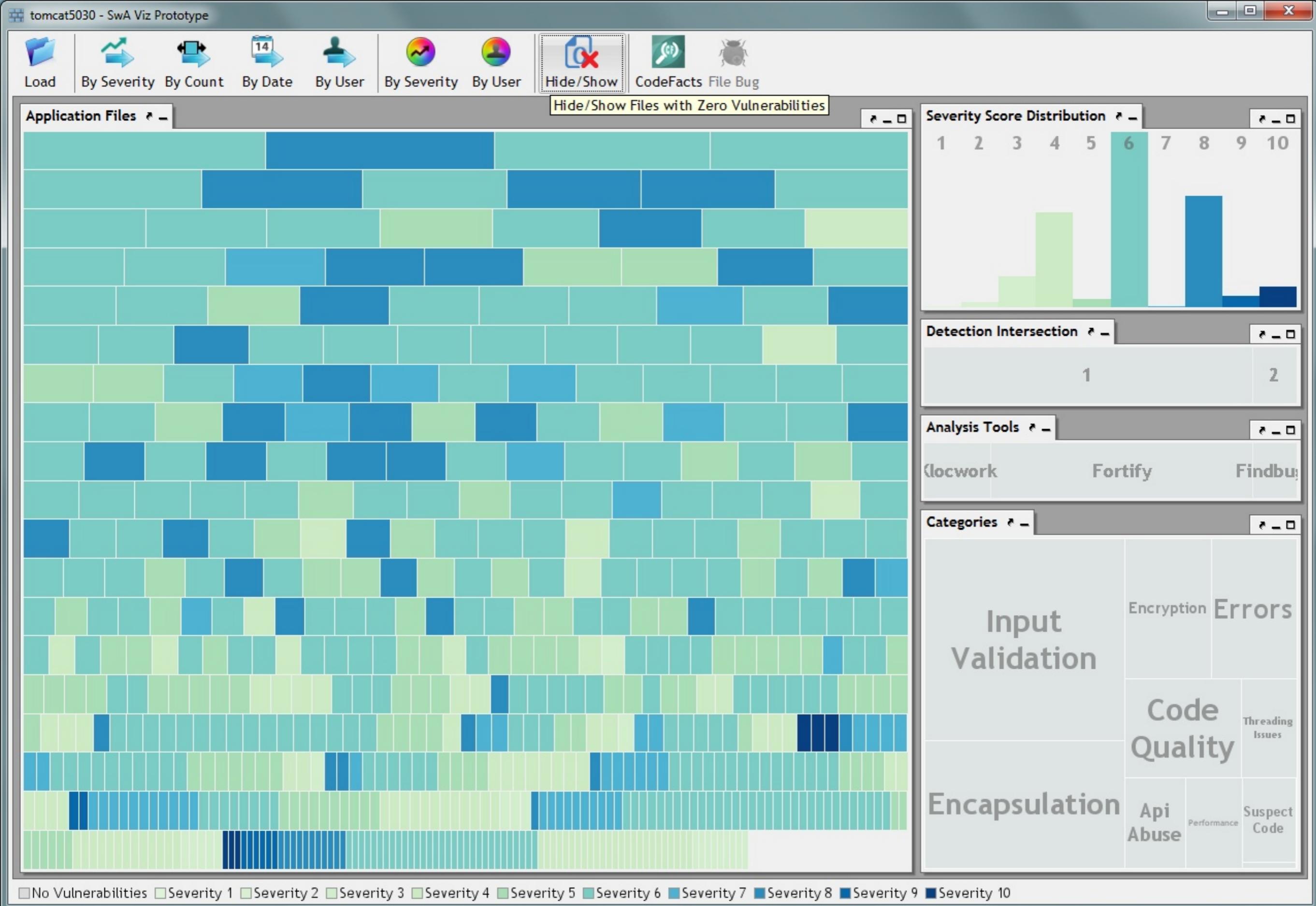
Severity Score Distribution

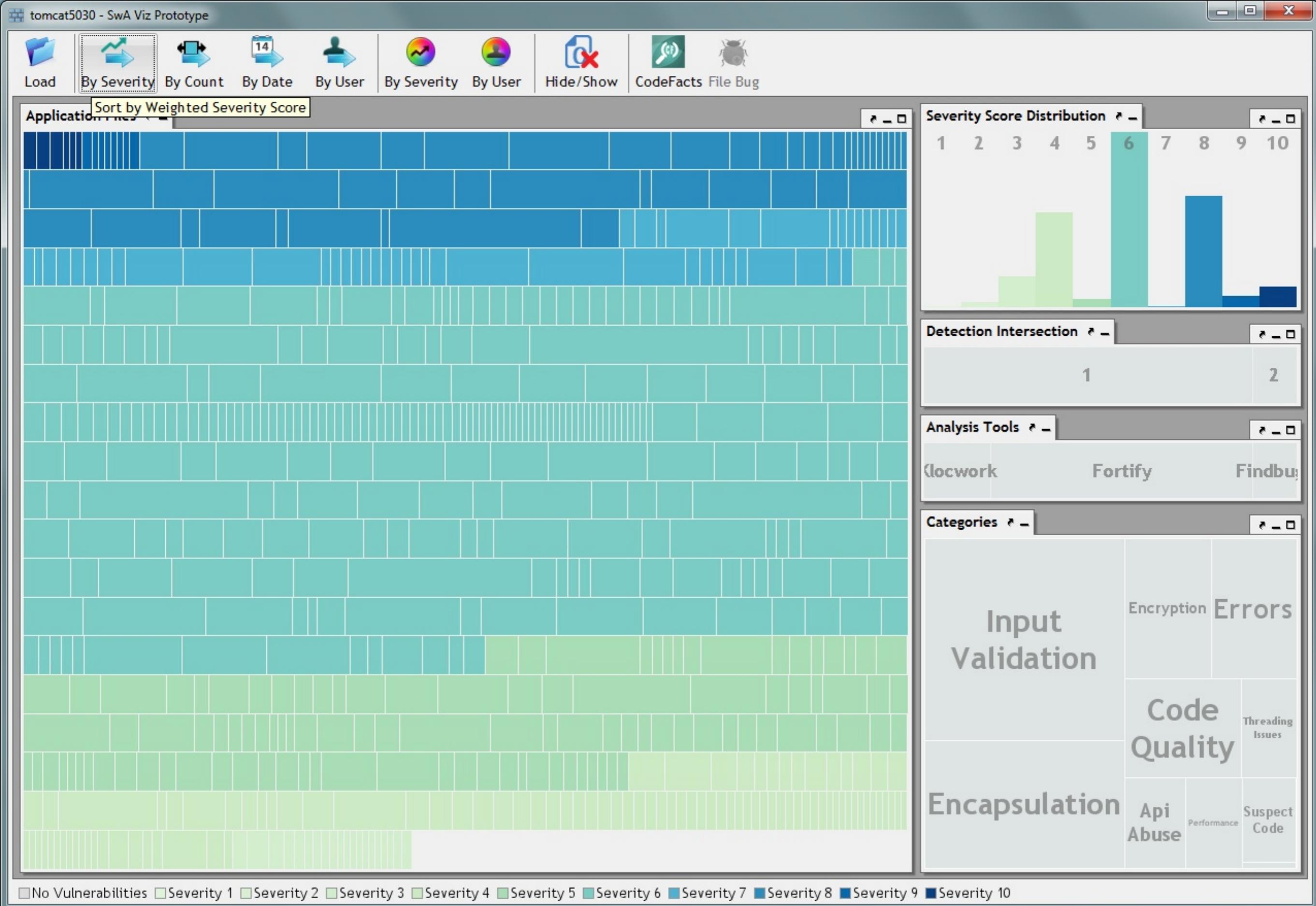


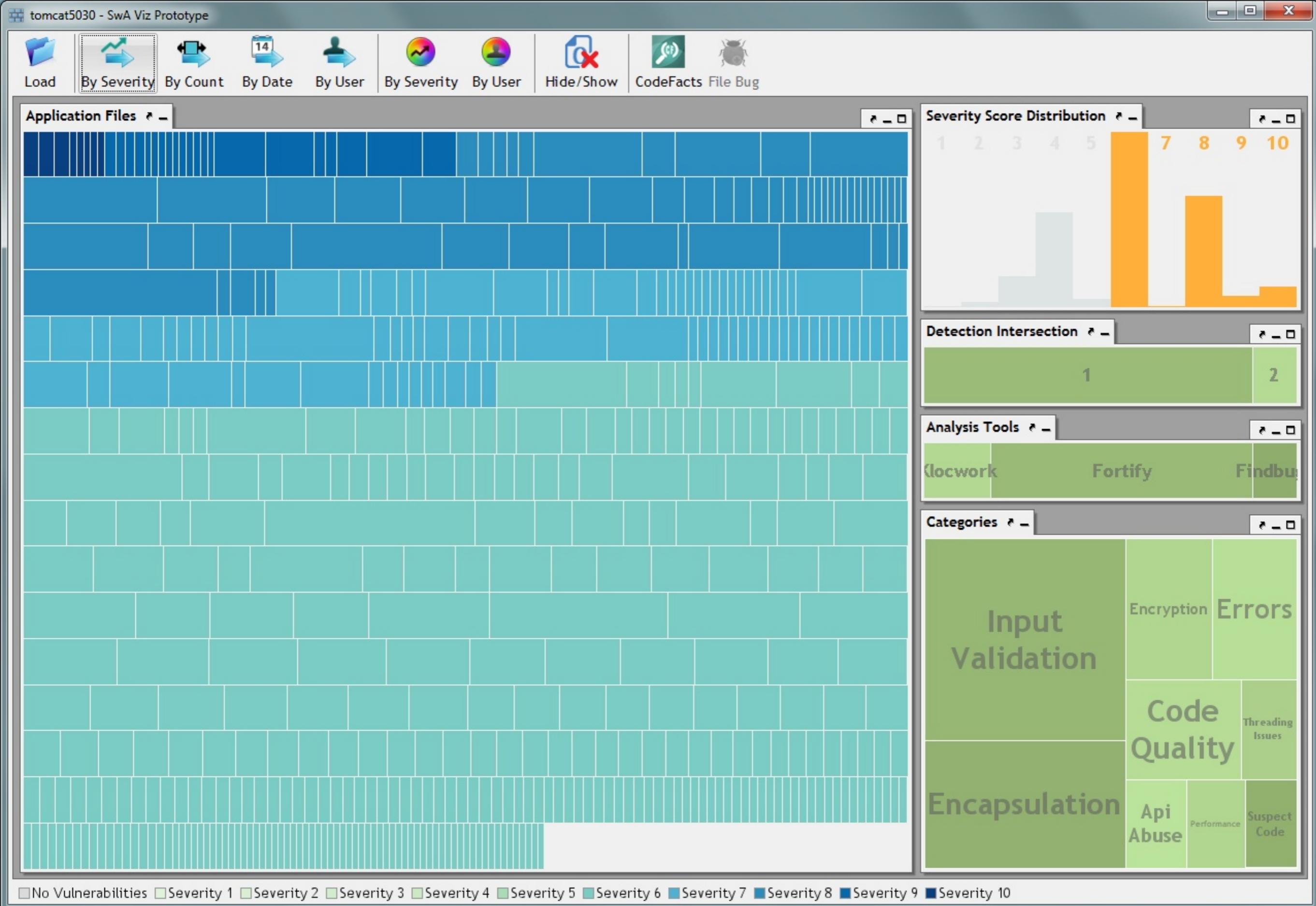


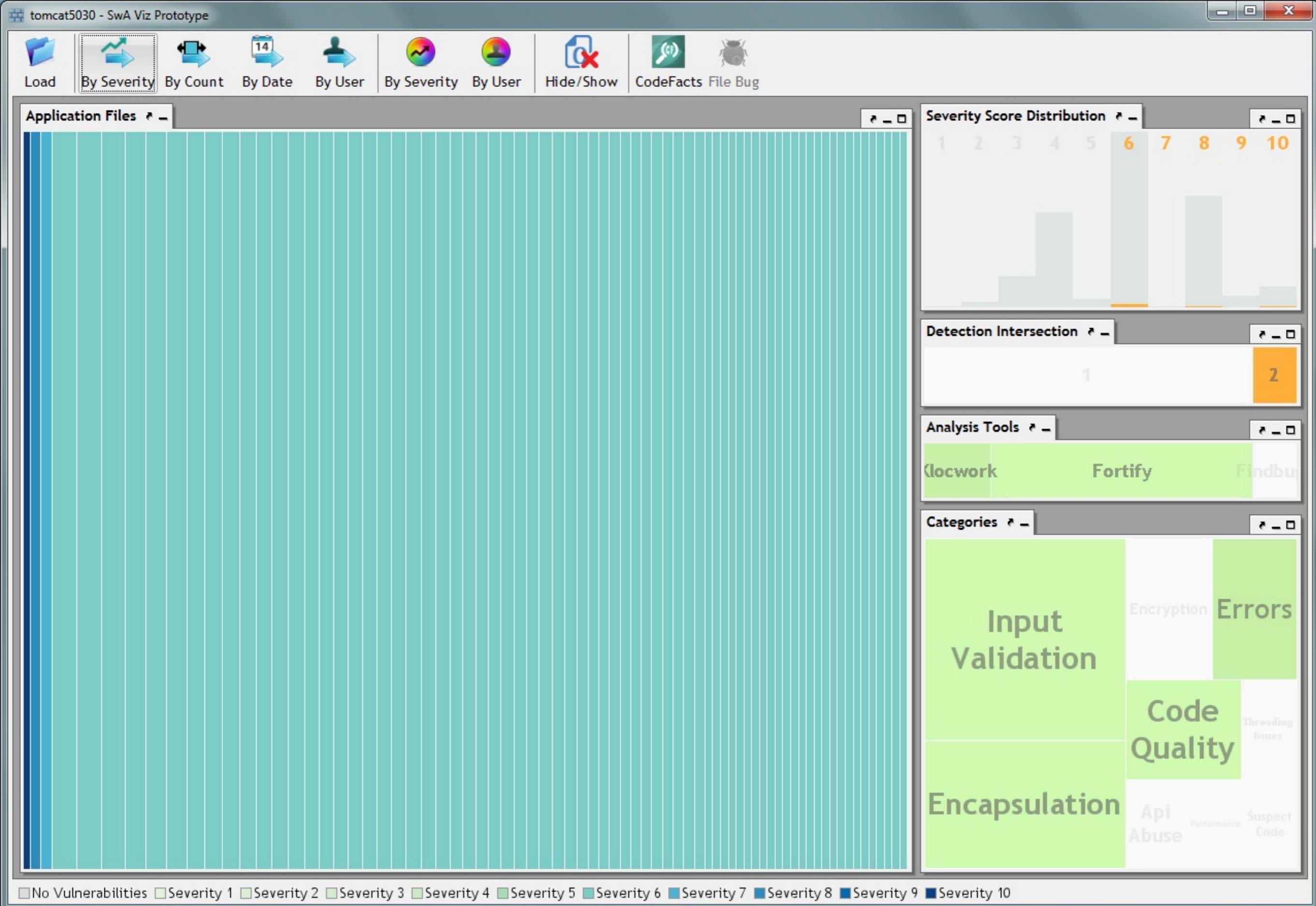


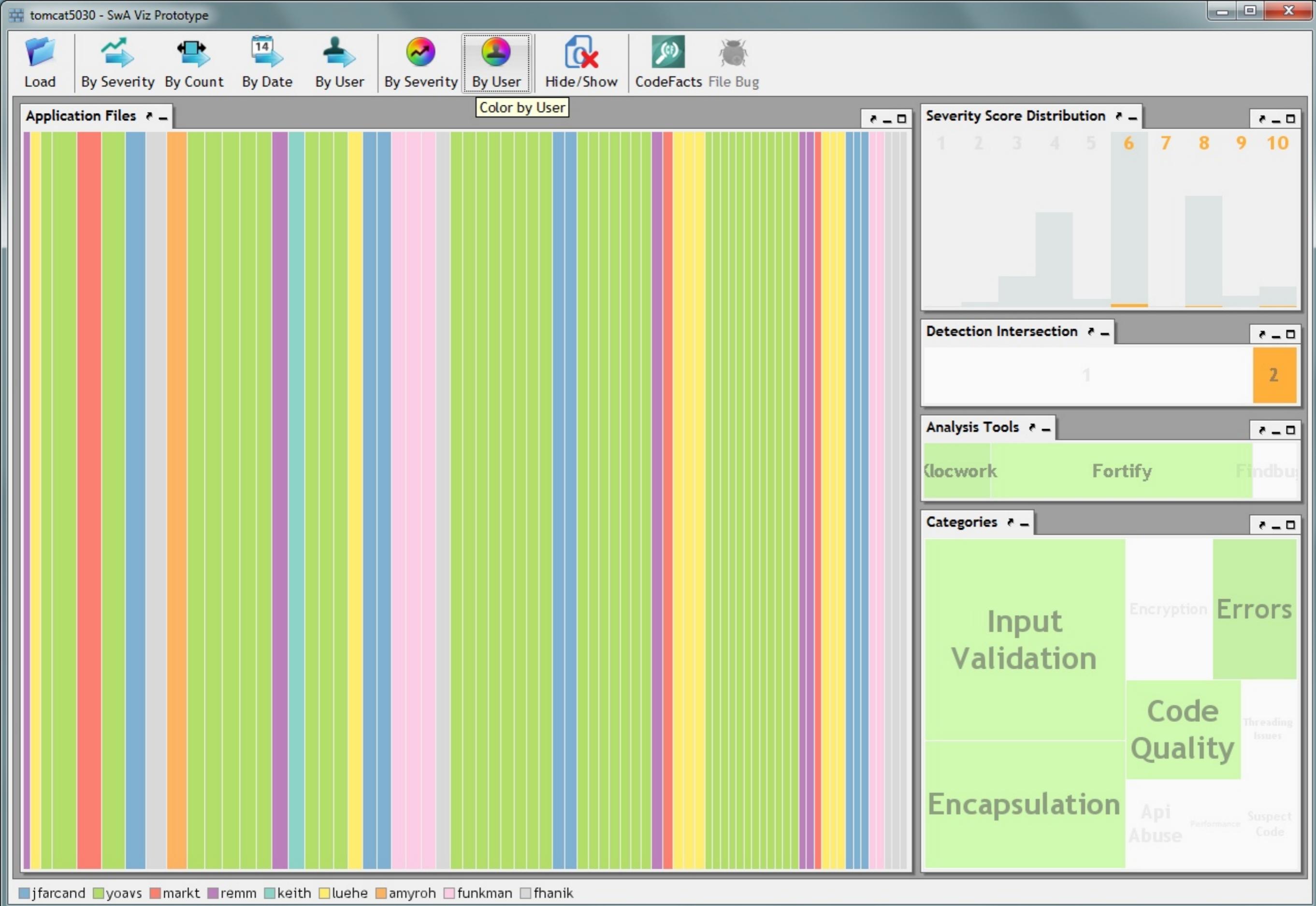


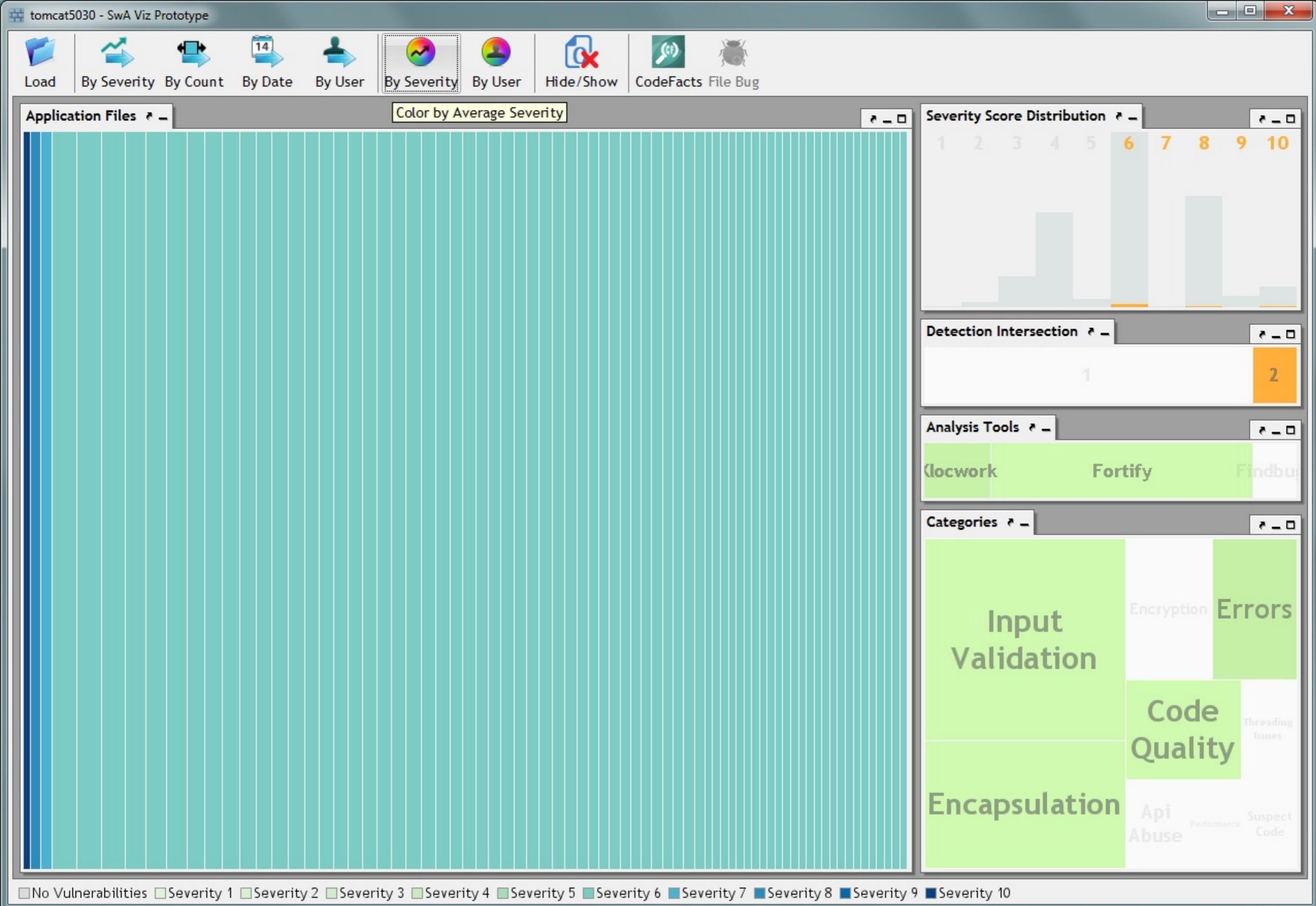


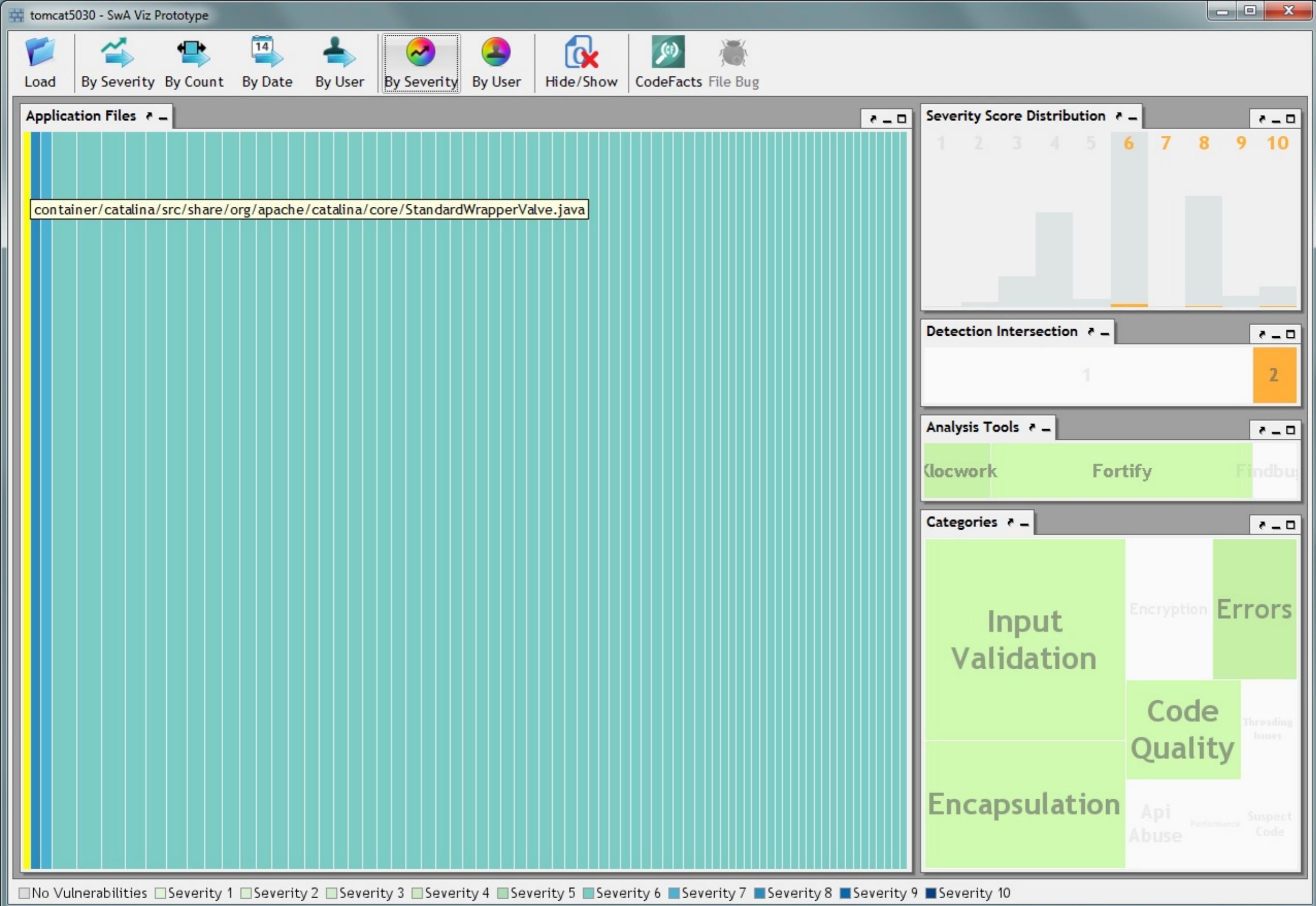


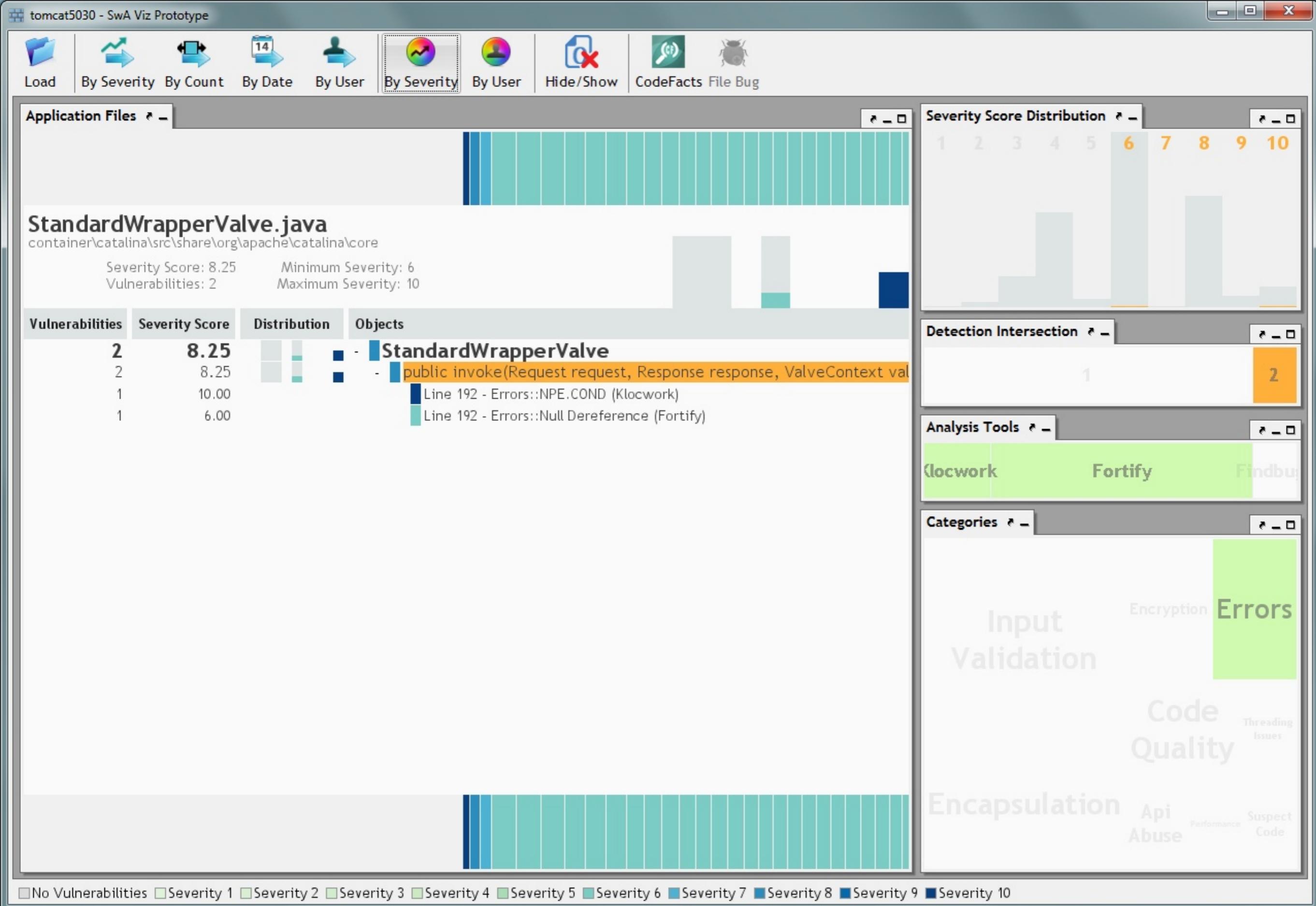




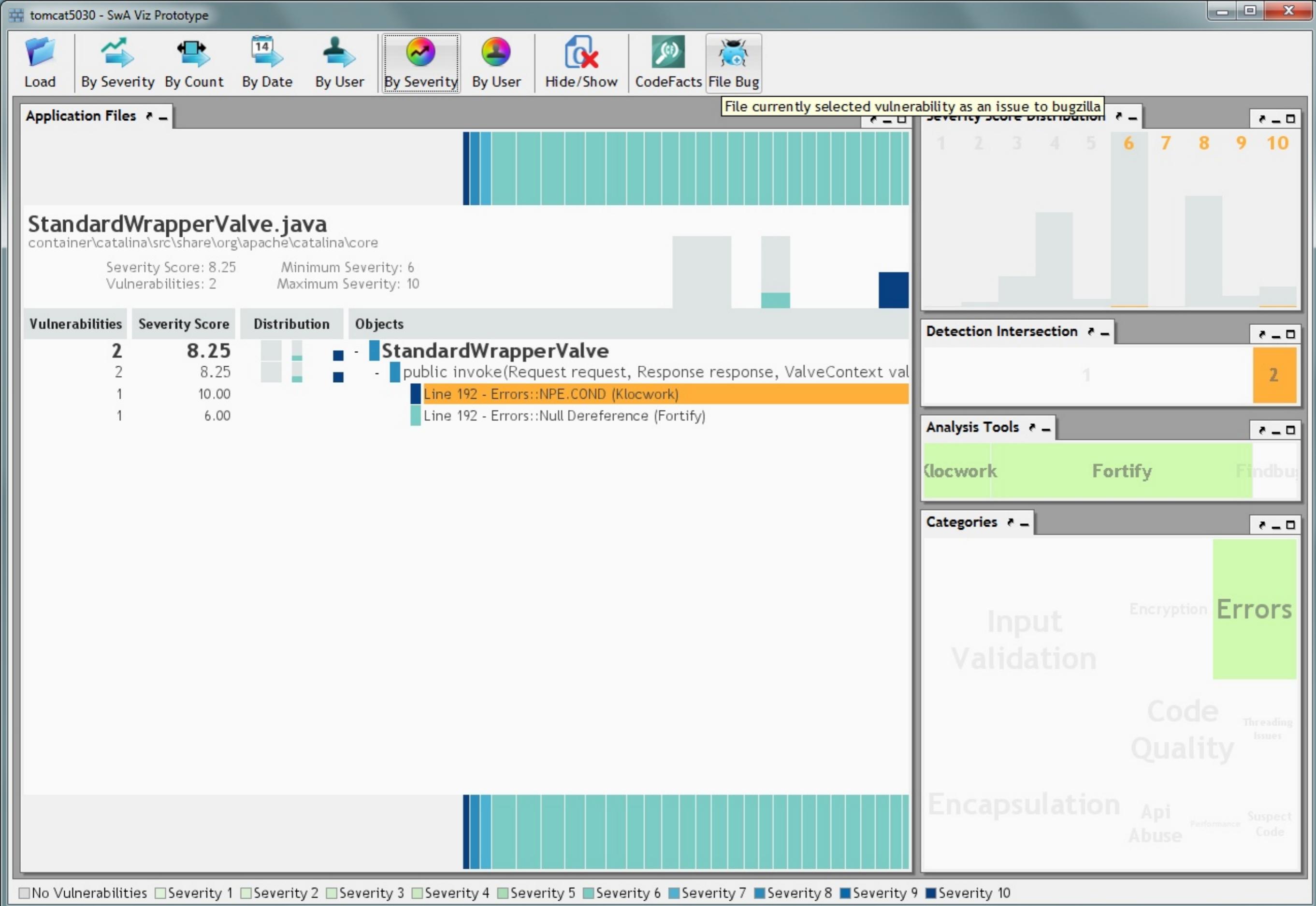


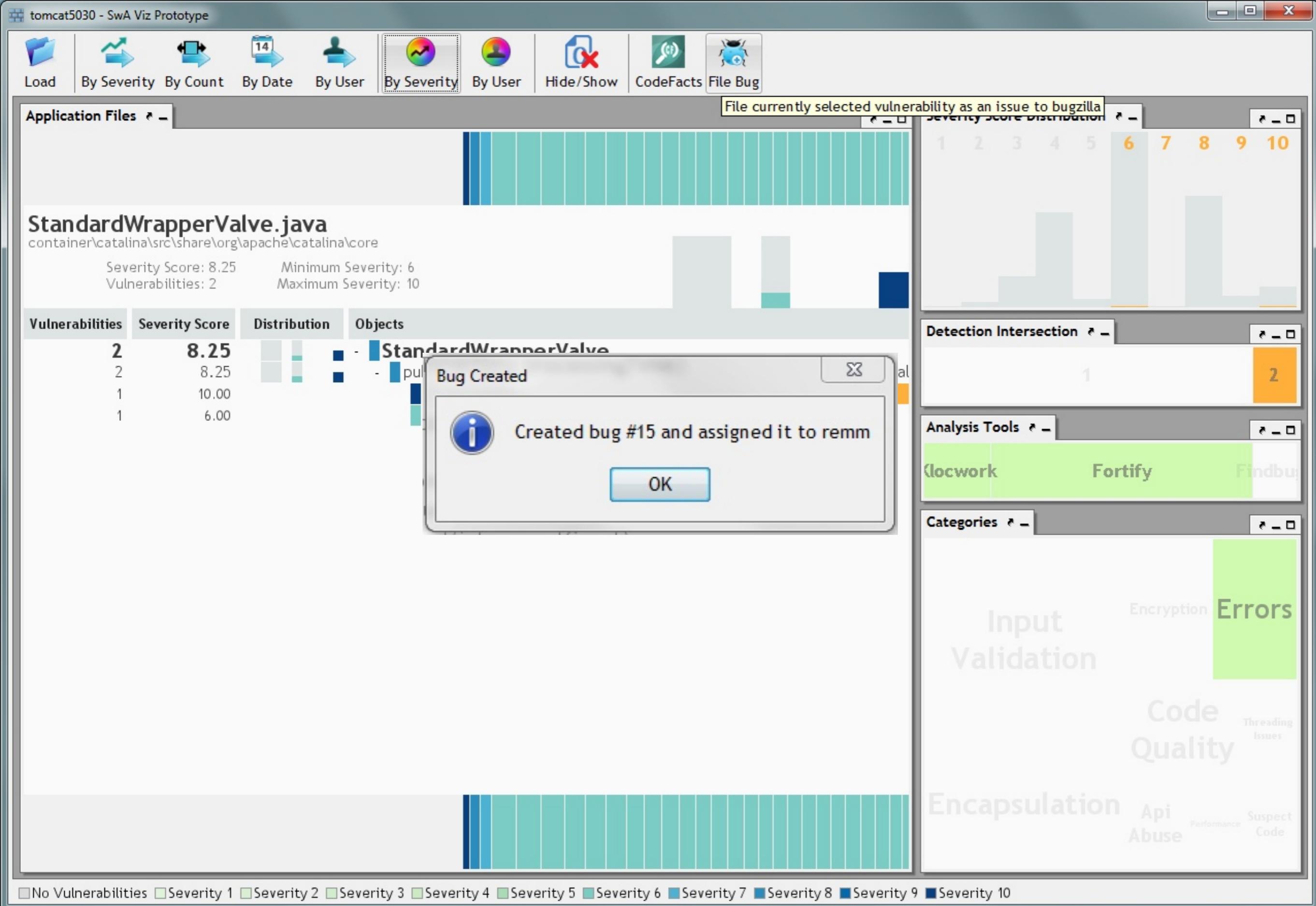


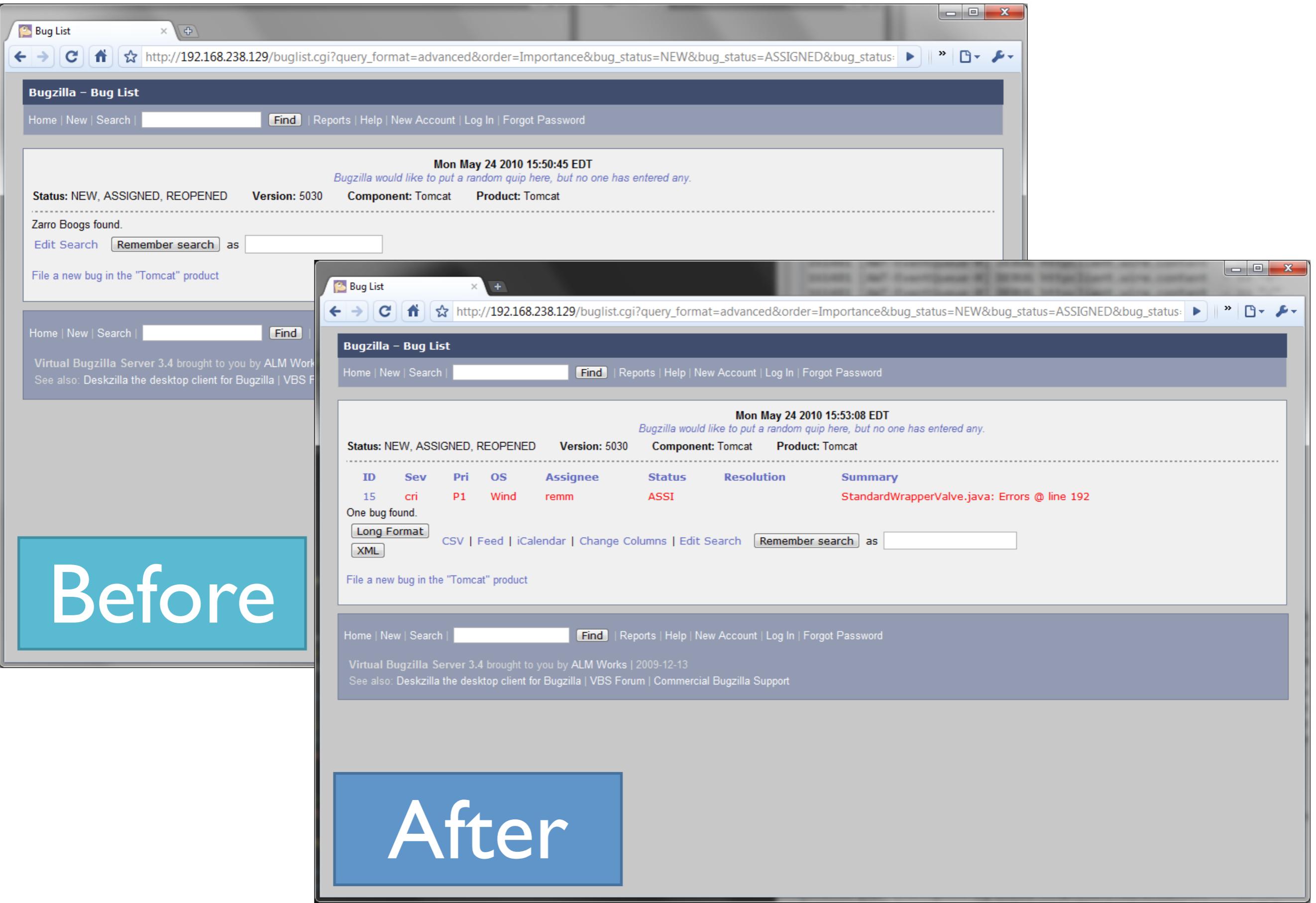


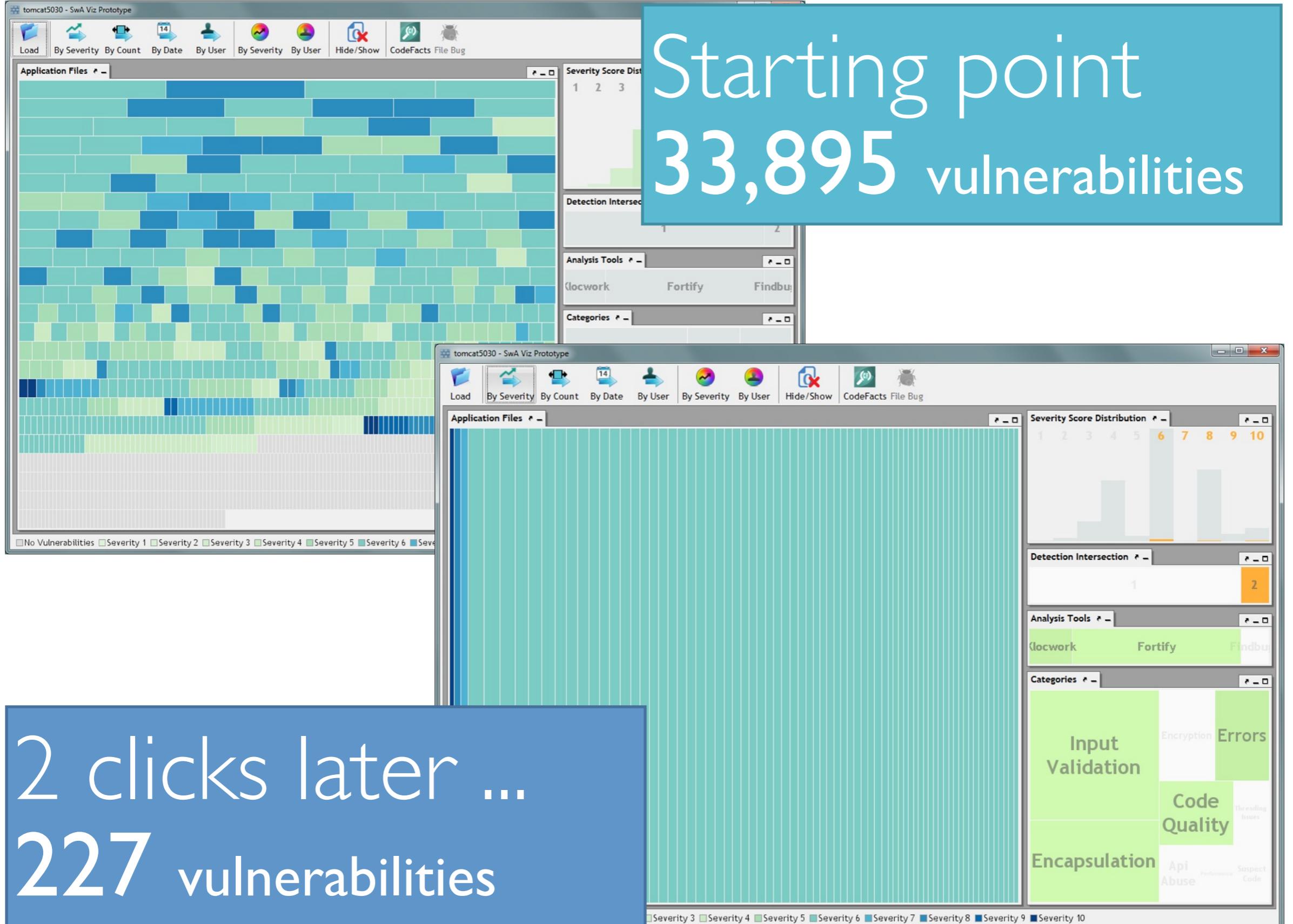


No Vulnerabilities Severity 1 Severity 2 Severity 3 Severity 4 Severity 5 Severity 6 Severity 7 Severity 8 Severity 9 Severity 10









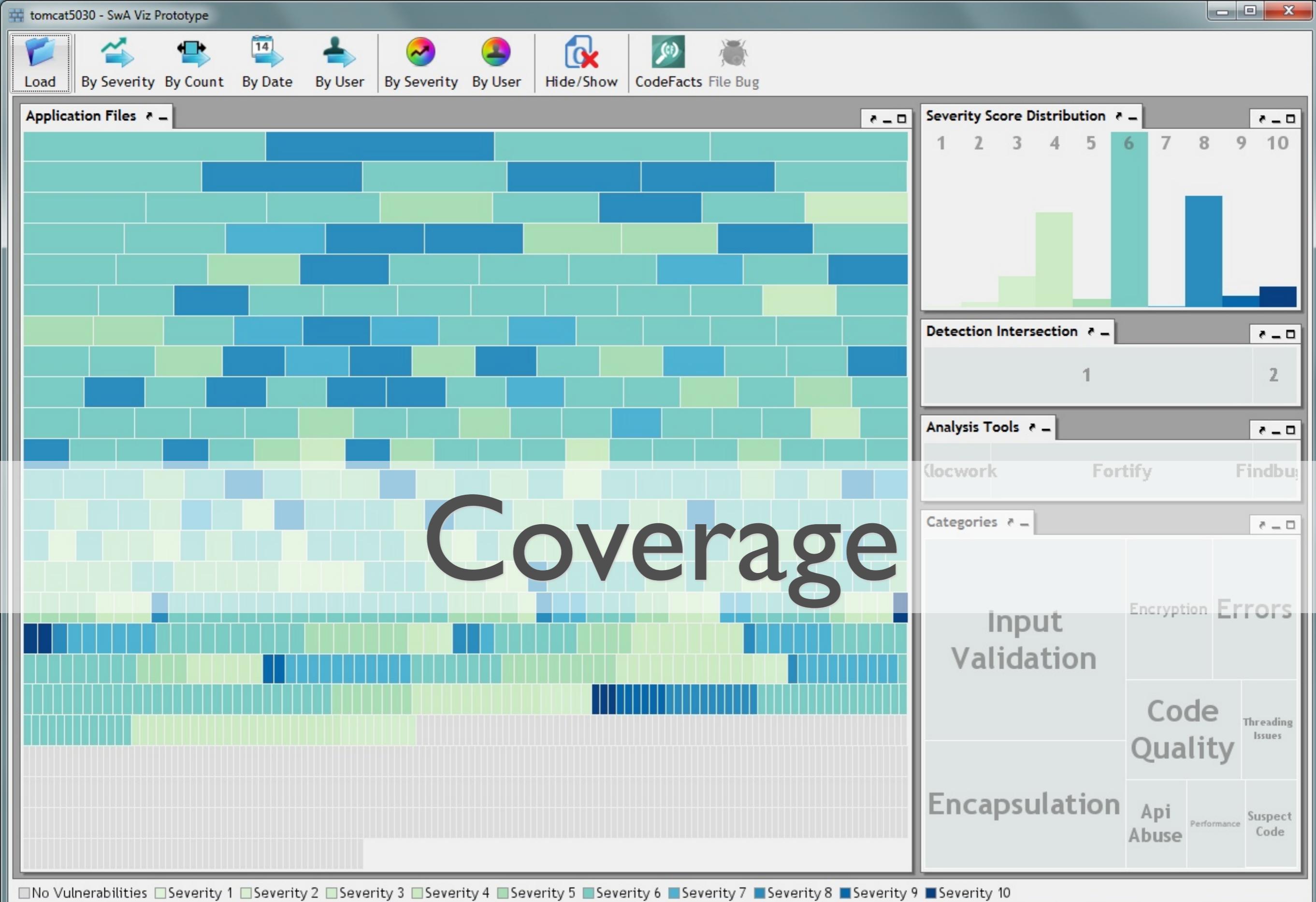
Benefits

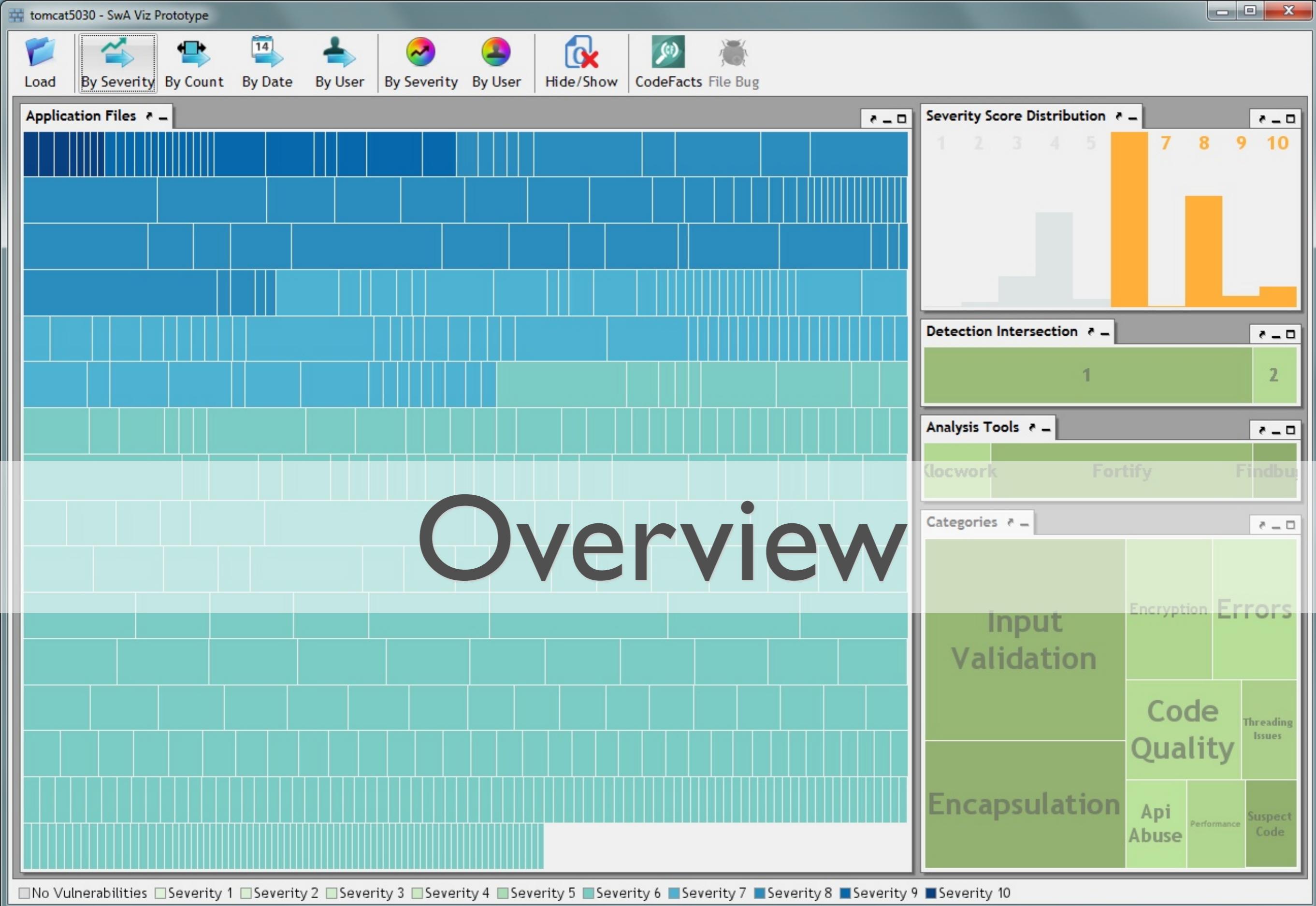
- Increased vulnerability coverage through the integration of multiple tools
- Overview of large number of vulnerabilities
- Visual prioritization of vulnerabilities
- Traceability of developer responsibility
- Remediation via integration with SDLC

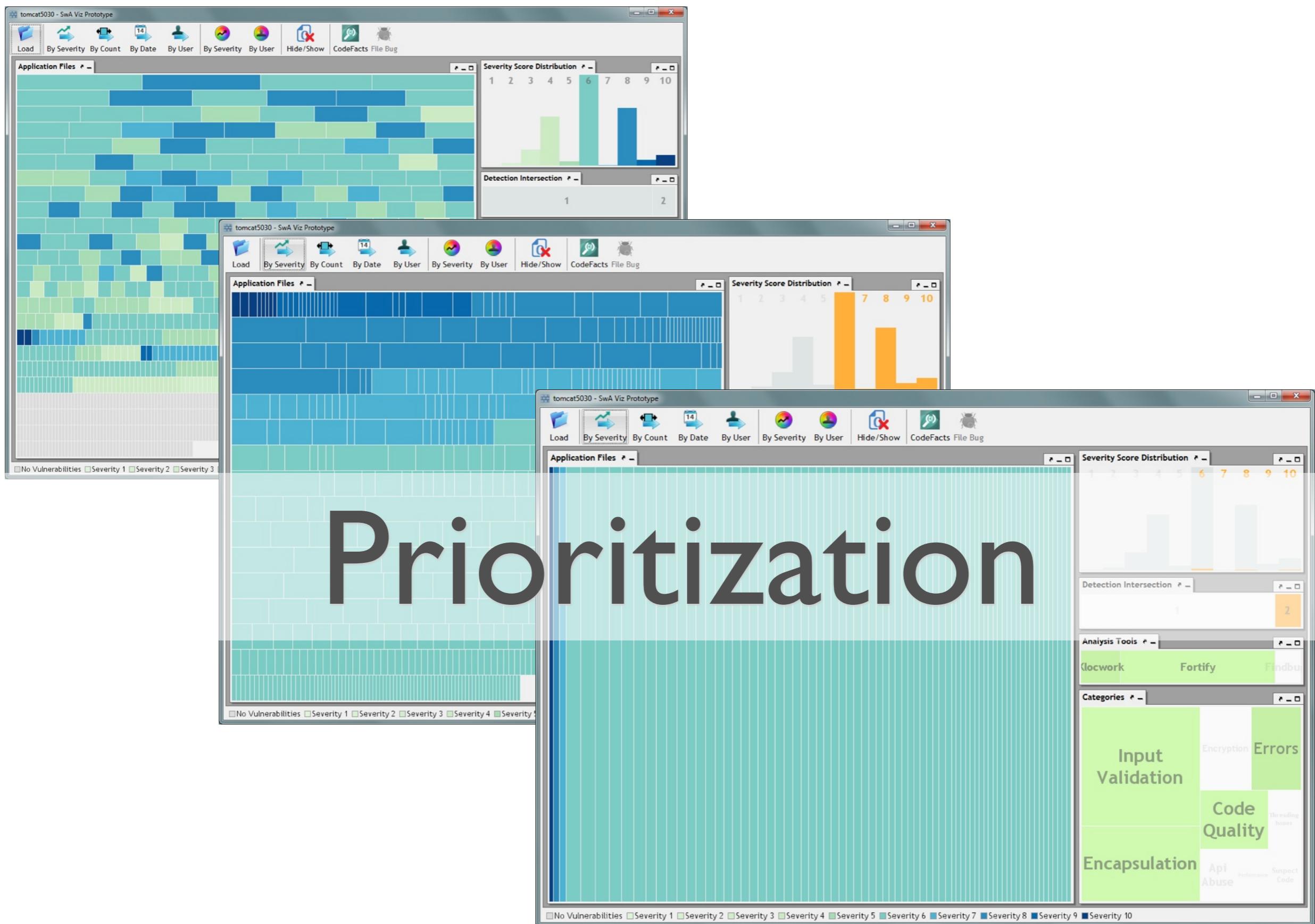
Benefits

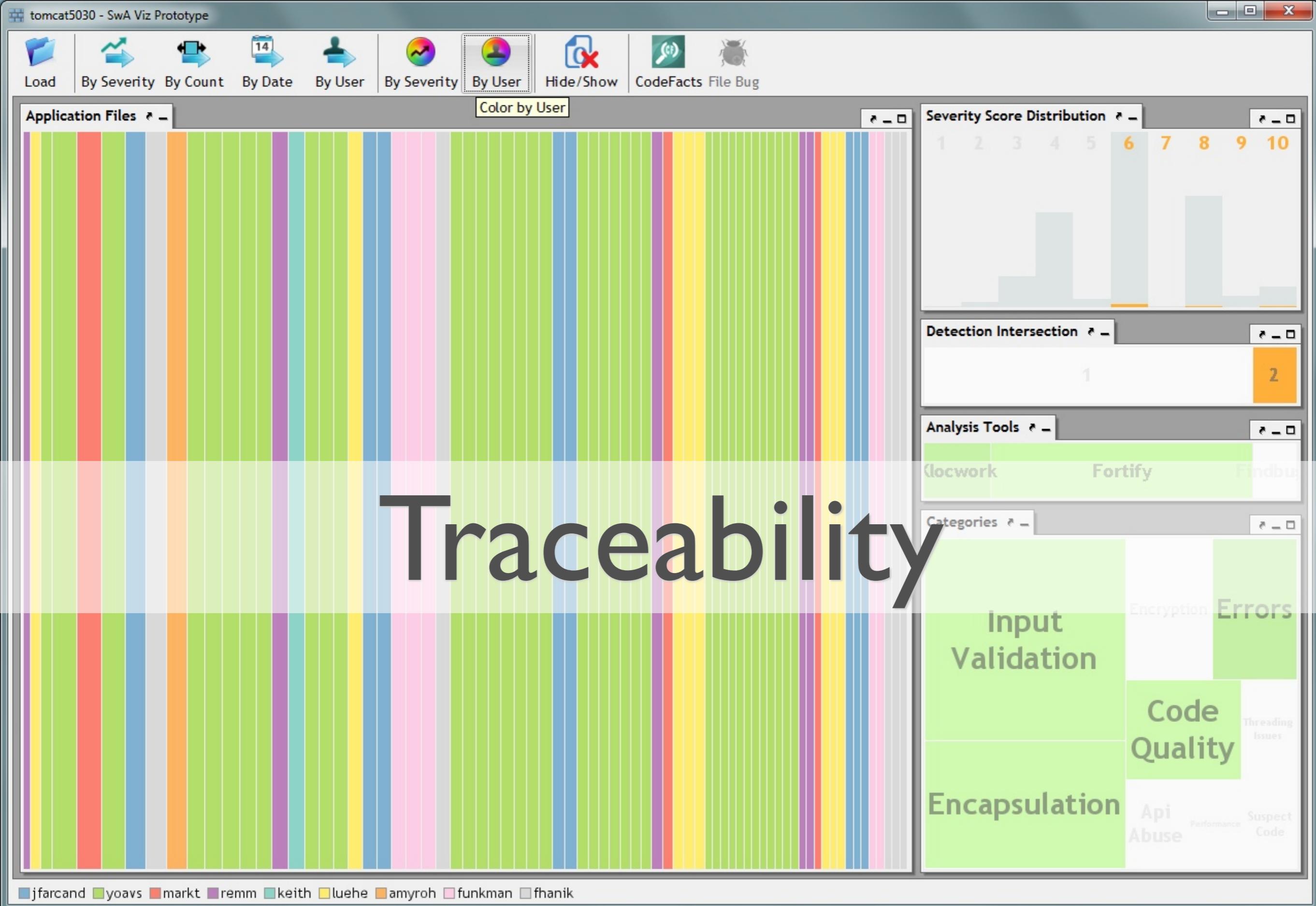
- Increased vulnerability coverage through the integration of multiple tools
- Overview of large number of vulnerabilities
- Visual prioritization of vulnerabilities
- Traceability of developer responsibility
- Remediation via integration with SDLC

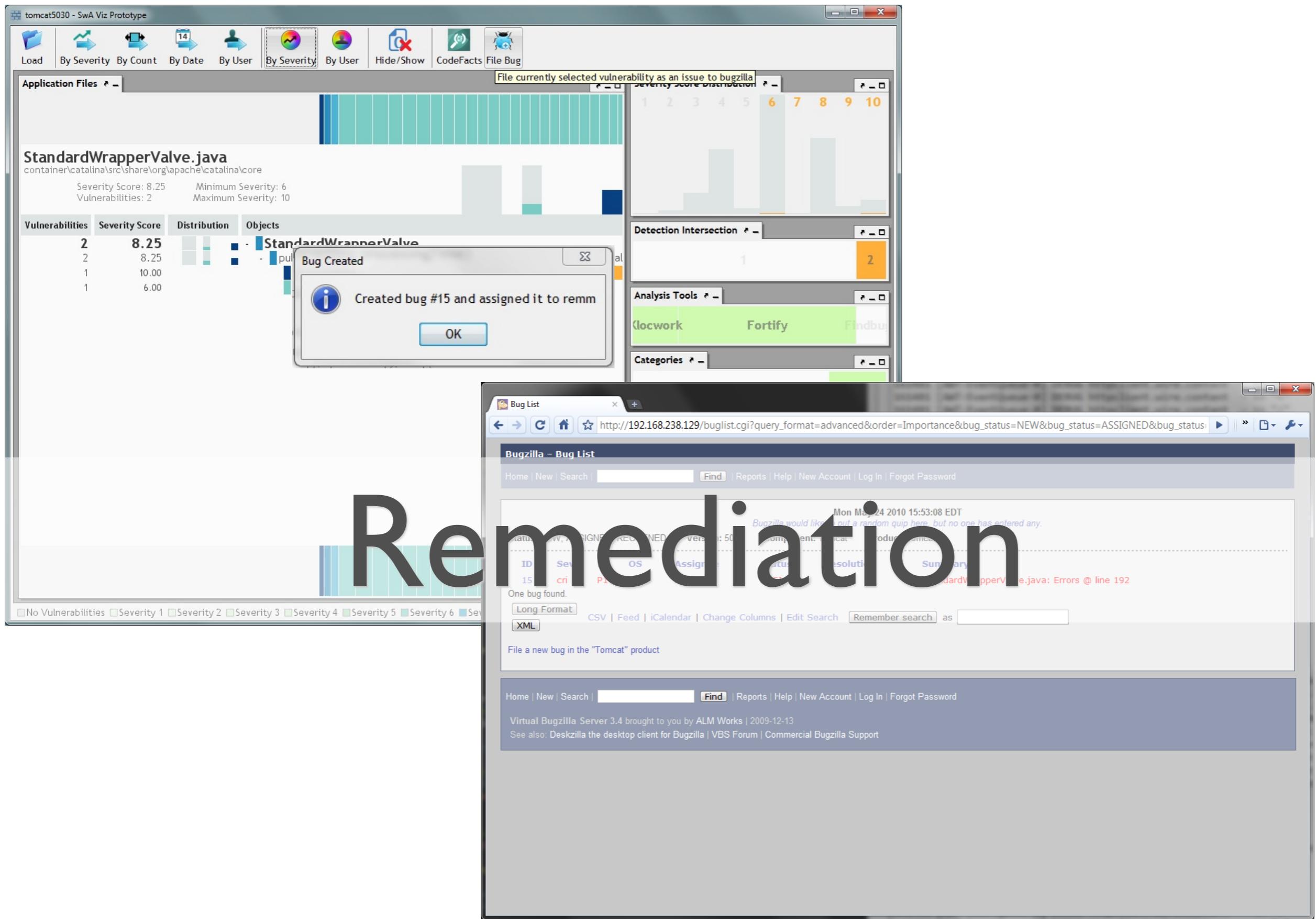
Enhances the coverage & speed for detection & remediation of vulnerabilities



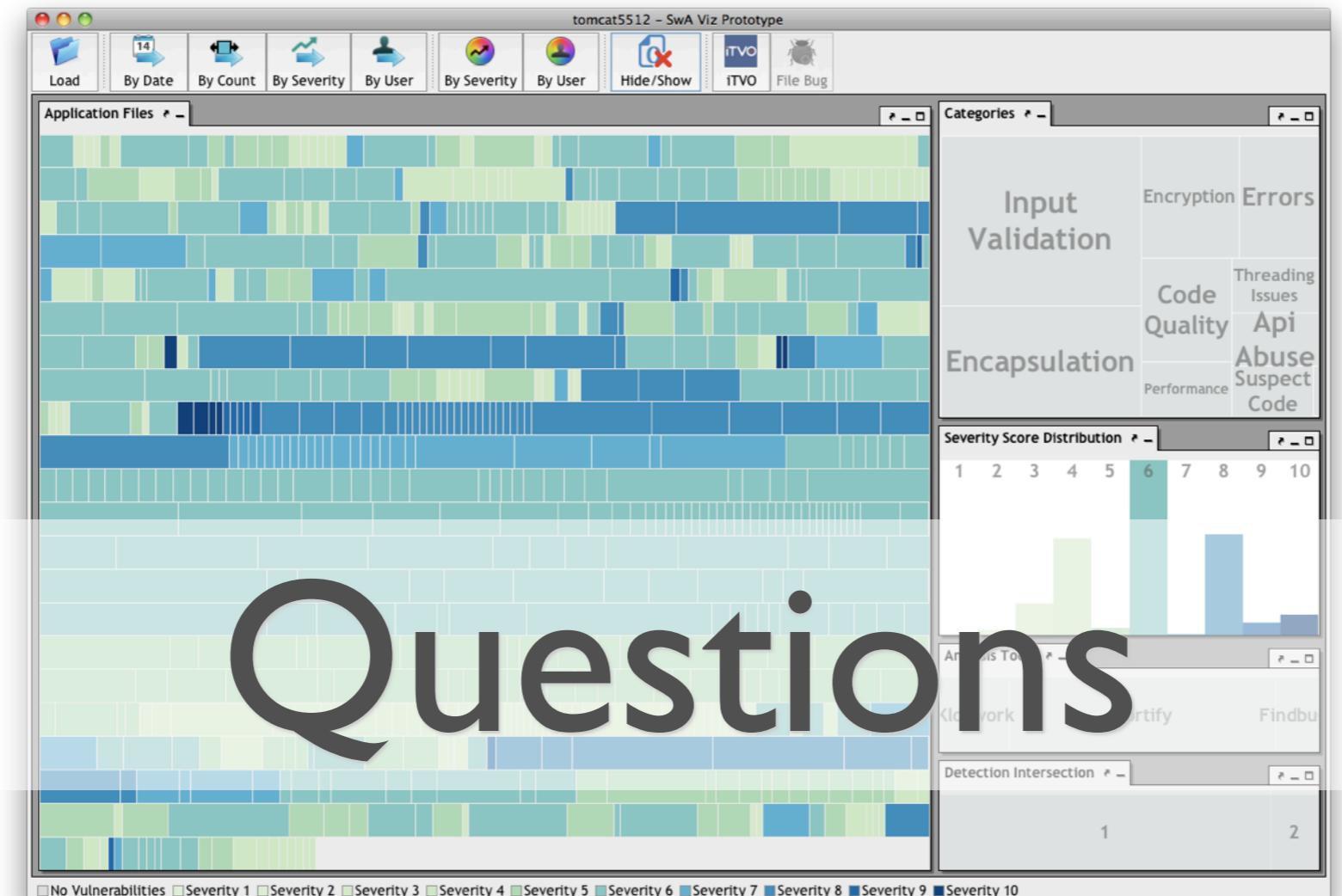








Visual analysis of code security



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