

2012 DHS S&T/ASD(R&E) CYBER SECURITY SBIR WORKSHOP



Code Dx Software Assurance Analysis and Visual Analytics

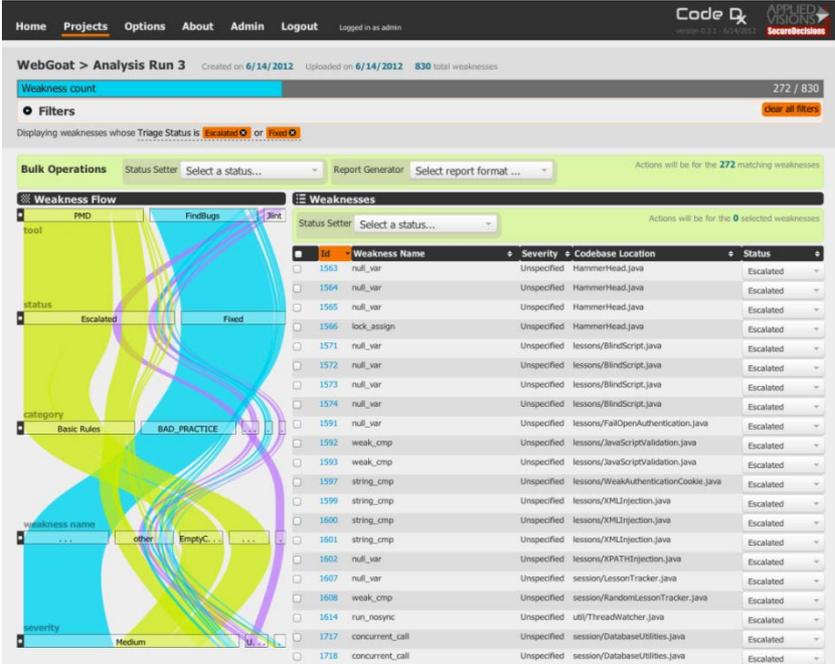
Ken Prole

Ken.Prole@securedecisions.com

631-759-3907

DHS SBIR Topic H-SB09.2-004

Contract # N10PC20014



WebGoat > Analysis Run 3 Created on 6/14/2012 Updated on 6/14/2012 830 total weaknesses

Weakness count 272 / 830

Filters Clear all filters

Displaying weaknesses whose Triage Status is Escalated or Fixed

Bulk Operations Status Setter Select a status... Report Generator Select report format ... Actions will be for the 272 matching weaknesses

Weakness Flow

Weaknesses

id	Weakness Name	Severity	Codebase Location	Status
1563	null_var	Unspecified	HammerHead.java	Escalated
1564	null_var	Unspecified	HammerHead.java	Escalated
1565	null_var	Unspecified	HammerHead.java	Escalated
1566	lock_assign	Unspecified	HammerHead.java	Escalated
1571	null_var	Unspecified	lessons/BlindScript.java	Escalated
1572	null_var	Unspecified	lessons/BlindScript.java	Escalated
1573	null_var	Unspecified	lessons/BlindScript.java	Escalated
1574	null_var	Unspecified	lessons/BlindScript.java	Escalated
1591	null_var	Unspecified	lessons/FallOpenAuthentication.java	Escalated
1592	weak_cmp	Unspecified	lessons/JavaScriptValidation.java	Escalated
1593	weak_cmp	Unspecified	lessons/JavaScriptValidation.java	Escalated
1597	string_cmp	Unspecified	lessons/WeakAuthenticationCookie.java	Escalated
1599	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1600	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1601	string_cmp	Unspecified	lessons/XMLInjection.java	Escalated
1602	null_var	Unspecified	lessons/XPATHInjection.java	Escalated
1607	null_var	Unspecified	session/LessonTracker.java	Escalated
1608	weak_cmp	Unspecified	session/RandomLessonTracker.java	Escalated
1614	run_reopen	Unspecified	util/ThreadWatcher.java	Escalated
1717	concurrent_call	Unspecified	session/DatabaseUtilities.java	Escalated
1718	concurrent_call	Unspecified	session/DatabaseUtilities.java	Escalated

There's lots of bad software out there

Our industry still hasn't learned how to deploy secure software...

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

Doug Maughan, DHS

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

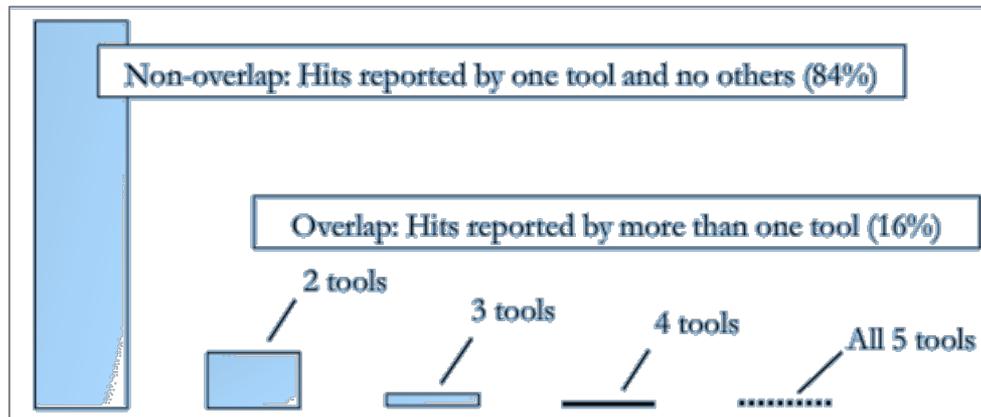
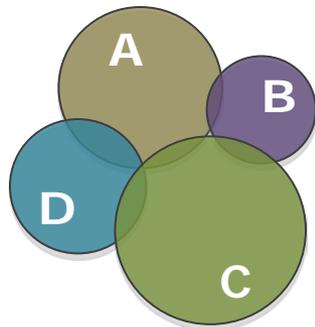


A screenshot of a PCWorld Business Center article. The article is titled "Patch Tuesday Updates Fix Critical Flaws in IE and DirectShow" and is dated June 08, 2010, 12:42 PM. The author is Tony Bradley, PC World. The article discusses Microsoft's Patch Tuesday for June 2010, which released 10 new security bulletins addressing 34 vulnerabilities, including critical flaws in DirectShow and Internet Explorer. The article also mentions that seven of the security bulletins are rated as important, while three are critical. The critical bulletins include MS10-033 for DirectShow and MS10-035. The article includes social media sharing options for Print, Digg, Twitter, Facebook, and More. There is also a "Tech Audit" sidebar and a "Perfect Pr" sidebar.

The **tools exist** to help us deploy safer software...

...but there's no single solution

Different tools identify different problems...



Source: MITRE

... and present their results with different semantics:

```
<BugInstance type="NP_NULL_ON_SOME_PATH" priority="1" abbrev="NP" category="CORRECTNESS">
```

Tool A

```
<Class classname="com.securedesisions.tva.m...>
<SourceLine classname="com.securedesisions.tva.m...>
sourcepath="com/securedesisions/tva/model/linkse...
</Class>
<Method classname="com.securedesisions.tva.m...
signature="(Lcom/securedesisions/tva/model/xml/a...
odel/xml/pdag/ExploitDocument$Exploit;" isStatic=...
<SourceLine classname="com.securedesisions.tva.m...
sourcefile="LinkSetAggregator.java" sourcepath="...
</Method>
<LocalVariable name="machine" register="5" pc...
<SourceLine classname="com.securedesisions.tva.m...
sourcefile="LinkSetAggregator.java" sourcepath="...
<SourceLine classname="com.securedesisions.tva.m...
sourcefile="LinkSetAggregator.java" sourcepath="...
</BugInstance>
```

Tool B

```
<BugInstance type="NP_NULL_ON_SOME_PATH" priority="1" abbrev="NP" category="CORRECTNESS">
<Class classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator">
<SourceLine classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator" start="58" end="670" sourcefile="LinkSetAggregator.java"/>
</Class>
<Method classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator" name="createFromExploit"
signature="(Lcom/securedesisions/tva/model/xml/ag/LinkDocument$Link;Lcom/securedesisions/tva/model/xml/pdag/ProtectionDomainDocum...
odel/xml/pdag/ExploitDocument$Exploit;" isStatic="false">
<SourceLine classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator" start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/securedesisions/tva/model/linksettransform/LinkSetAggregator.java"/>
</Method>
<LocalVariable name="machine" register="5" pc...
<SourceLine classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator" start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/securedesisions/tva/model/linksettransform/LinkSetAggregator.java" role="SOURCE_L...
<SourceLine classname="com.securedesisions.tva.model.linksettransform.LinkSetAggregator" start="58" end="670" sourcefile="LinkSetAggregator.java" sourcepath="com/securedesisions/tva/model/linksettransform/LinkSetAggregator.java" role="SOURCE_L...
</BugInstance>
```

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

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

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 practices 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 X Status X Detected In X

CTD	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_fil_info()
10007	ARRAY_VS_SINGLETON	Unspecified	New	Unassigned	Unclassified	Undecided	rt6_fil_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	sdtp_endpoint_destroy()
10013	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sdtp_transport_destroy()
10014	BAD_FREE	Unspecified	New	Unassigned	Unclassified	Undecided	sdtp_association_free()
10028	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	fat_new_dir()
10031	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	msdos_add_entry()
10039	BUFFER_SIZE	Unspecified	New	Unassigned	Unclassified	Undecided	vfat_fill_slots()
10328	NEGATIVE_RETURNS	Unspecified	New	Unassigned	Unclassified	Undecided	packet_getname_spkt()
10556	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	handle_inbrd()
10560	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	DAC960_V2_ReadControllerConfiguration()
10565	OVERRUN_STATIC	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cmd_free()
10769	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10770	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10771	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10772	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10773	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10774	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10775	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10776	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10777	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10800	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10801	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()
10802	RESOURCE_LEAK	Unspecified	New	Unassigned	Unclassified	Undecided	scsi_cois_request()

50,000 weaknesses...
Where do I start?





Software Assurance Visual Analysis

An application that brings together **disparate** SwA analysis runs and ...

... normalizes the results in a standard format

... removes overlapping results

... visualizes and prioritizes key trouble spots by severity and frequency

... uses code context to assess the impact of those results

... filters and highlights based on weakness type and software class

... shows who is responsible for weaknesses

... helps assign repair of weaknesses

... uncovers trends

KDM Analytics[™]

Tool Output Integration Framework

Coverage Priority Traceability Remediation

Enhances the speed and coverage for detection and remediation of software weaknesses

Code Dx Workflow

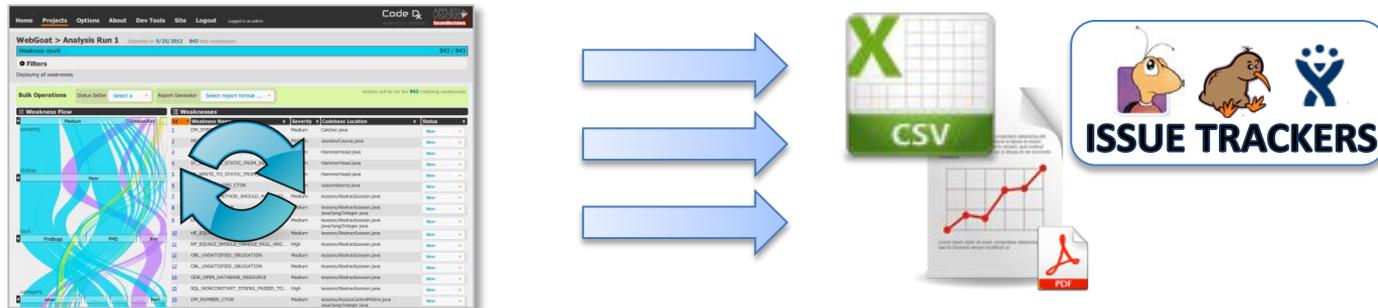
Step 1 – Generate and upload data



Step 2 – Automatic correlation and normalization of the tool results



Step 3 – Visual analytics, weakness triage, and results dissemination



WebGoat > Analysis Run 1 > Weakness 504 MS_SHOULD_BE_FINAL detected by FindBugs

First seen on 6/22/2012 8 weaknesses in this file 3 similar weaknesses in this analysis run

Status
New

Triage status

Description
A mutable static field could be changed by malicious code or by accident from another package. The field could be made final to avoid this vulnerability.

Remediation guidance

Detailed Information

Source Code

The weakness goes from line 61 to 61 in file lessons/XMLInjection.java
show more: (1 weaknesses currently hidden from view)

```
51 *
52 * @author Sherif Koussa <a href="http://www.softwaresecured.co
53 */
54 public class XMLInjection extends LessonAdapter
55 {
56
57     private final static Integer DEFAULT_RANKING = new Integer(
58
59     private final static String ACCOUNTID = "accountID";
60
61     public static HashMap<Integer, Reward> rewardsMap = new Has
62
63     public final static A MAC_LOGO = new A().setHref("http://ww
64
65     protected static HashMap<Integer, Reward> init()
66     {
67         Reward r = new Reward();
68
69         r.setName("WebGoat t-shirt");
70         r.setPoints(50);
71         rewardsMap.put(1001, r);
```

Source code details

show more: (5 weaknesses currently hidden from view)

Activity Stream

Activity Stream input field with a back arrow button

You can write your comments using markdown

admin changed status to New

3 days ago

admin changed status to Assigned to jane

3 days ago

admin changed status to Escalated

3 days ago

admin changed status to Assigned to jane

3 days ago

admin changed status to Escalated

3 days ago

admin changed status to New

21 days ago

Real-time collaboration

Technology Transition

- 5 months left on Phase II contract
- Alpha prototype available now; we are eager to get feedback
- Currently at TRL 4, looking to audience to:
 - Incorporate into larger programs
 - Provide test & evaluation environments
 - Recommend users and transition partners
 - Recommend capabilities to enhance transition

Questions?

Ken Prole

Ken.Prole@securedecisions.com

631-759-3907

