

Hewlett Packard Enterprise

Capabilities to help expand and mature SWA program

Haleh Nematollahy – Sr. Security Solutions Architect

Fortify Security Assistant



Fortify security assistant

Building in security as you code





Spell check security scanning



Identify issues earlier in the SDLC



Educate developer about security



Accelerate appsec program (increase productivity & efficiency)

Fortify security assistant

É Eclipse File Edit Source Refactor Navi	gate Search Project Run	Fortify Window Help	SD 🖲 🕂 😤	🙀 1642) Fri 9:17 AN	१ 0 🔵 🗉
●●● □• □ □ ■ ≝• \$• 0• %• @ #• § •§ •	workspace - Res	Analyze Project Advanced Analysis	nse.jsp - Eclipse	Quick Access	BCC
Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers	<pre>response.jsp % i= <body> 2 <jsp:usebean id="my 3 <jsp:setProperty nd 4 <hl>Hello, <jsp:get 5 </body></pre></td><td>Show Project Summary
Audit Guide
Project Configuration
Extract Source Code
Generate Legacy Report
Configure Bugtracker</td><td>hello.NameHandler"></jsp:usebean> /h1></body></pre>		- 0		
		W Upload Audit Project			
		Export Audit Project			
		Open Collaborative Audit Open Audit Project Merge Audit Projects Load Saved Audit Project			
		Manage License Options			
	Casks 🔮 Error Log 🔉 Workspace Log	C Upload project(s) to FoD		周创·回篇1	(🗟 🧬 🗢 🖻
	type filter text	Configure Security Assistant			
	Message Message Market of the ima Message Message Market of the ima Message M	Open Security Issue List Inspect the Project(s) Update Security Content Connect to Software Security Center Download Generated Report Generate Report Options command: plug-in-"com.hp.fortify.securityassistant. id	point. 'com.devinspect.securityassistant.commands.build' gins/eclipse/plugins/. joint. 'com.devinspect.securityassistant.commands.build' gins/eclipse/plugins/. 4/16 by an external source. This value will be over point. *com.devinspect.securityassistant.commands.build'	Plug-in org.eclipse.ul org.eclipse.ul org.eclipse.ul org.eclipse.ul org.eclipse.ul org.eclipse.org.nc.p2.m org.eclipse.core.net org.eclipse.ui org.eclipse.ui	Date 2/24/17, 9:13 AM 2/24/17, 9:13 AM 2/21/17, 1:29 PM 2/21/17, 1:28 PM 2/21/17, 1:28 PM 2/17/17, 12:30 PM 2/17/17, 11:39 AM 2/17/17, 11:39 AM

Fortify security assistant Real-time lightweight analysis of the source code



Vulnerable line of code additional information

Type of vulnerability, detailed remediation

Audit Assistant/ Scan Analytics



Machine Learning - scan analytics & audit assistant

Do more with your AppSec DATA

|--|

Streamline appsec program by making the auditing process more efficient



Increase the relevancy and consistency of findings unique to your organization preferences



Identify relevant issues earlier in the SDLC



Scale and accelerate your AppSec program with existing resources



Static analysis workflow

Or: How I scan a singe application



Finding relevant scan results is expensive and hard to scale because it requires:

- Security expertise
- Knowledge of scanned application's context

Challenge: Identifying Issues at scale can be painstaking





Software Security Center (SSC) - Audit assistant

Machine learning assisted identification of relevant scan results





Seamless workflow integration with existing tools

Audit Workbench – Security Auditor's View

🖻 Summary	🛛 🖻 Details 🖻 Recommendation
Issue: Check	summedOutputStream.java:53 (Comn
User:	▼
Analysis:	
x Prediction:	Not an Issue 🔹
x Confide	0.680 👻
x Bucket:	Not an Issue 🔹
Edit	

	and a subsection of the section of t	as a de a de la			
iummary [Certification Runtime Analysis	Build Information Analysis Informat	Silven		
Build II Scan De Warnie	n Sel 701 his 16550-4244-adds etaz: Jan 10, 2014 ga: 3661 isrranned duarny ana	eri sirta kurta:	Scannul: Total Issues: Certification	11,404 (Aux, 206 ₀ 56 103 Results Centificatio	BLOC (Eventetable) er Valid
		All Issue	s by Folder		
	Unsure (31)	Hot an	65au (217)		Real Valuerabilities (567)
Summery	S E Details E Recomme	ndations 🖻 History 🗗 Diagram	E Screenshots E Filters		
Summery	1 Si E Details E Recomme commet/OxfputStream (era 53	ndations 🗲 History 🗲 Diagram	E Screenshots E Ritters		so Commont Dynchon (Joput Vakiation and
Summery Line Chick	1 Si E Details E Recomme commedColputStream jara 557	indetions) 📂 History 📂 Diagram (Command byscicae)	E Screenshots E Ritters	4.4	Commont Dipotion (Deput Validation and Representation, Data Films)
Summery lie: Check at: utype:	1 33 📂 Details 🗲 Recomme continuedOutputStream jaca 233	Indetions E History E Diagram	E Screenshots E Ritters		Semmand Dijectori (Joput Validation and Representation, Data Firm) The mathod work(in Checksurence(Chepatineer) and concerned
Summery are Check are universe freedection	1 33 E Details E Recomme summedOutputStream java 53 Not an Inve	Indetions E History E Diagram	E Screenshots E Ritters	**	Commont Expection Deput Validation and Representation, Data Terre) The method work() in ChecknownicD/op/offmem.pairs cells with() with commond built from retricted data. They cell cen- culars the program to restude multimet command counts.
Summery ine: Check act [ine:] ine:	1 33 C Details C Recomme nummedOutputStream jaca 53 Net an Inne Salat	Indetions F History Diagram	E Screenshots E Filters		Command legistion deput Validation and Representation, Data Film) The method work() in Checknewschifting of free my are cells with () with command half frem introduced data. Thes cell can cause the program to conclude methoms commands on behalf of an attacker.
Summery sam Check antypes Presiction Confide_ Burlett Man	1 33 C Details C Pecomme nummer/OutputStream jaca 53 Net an Innee 0.680 Not an Innee	Indetions F History F Diagram	E Screenshuts E Filters	* *	Commont Report Validation and Report Validation and Report Validation (State Film) The method write() in Checknowed(Support Filmer, para cality write() with command hash from retruined data. This call are cause the program to exclude mathematicity adminester to behalf of an attacker.
5 Summary Ine Check Ine Ch	1 22 E Details E Recomme commentCorputStream java 53 Not an Innee 5000 Not an Innee	Indetions: E History E Diagram (Command Injection)	E Screenshots E Filters		The method write() in Command Representation, Data Timo) The method write() in Checksurement/District(Teem part calls write() with command built from perturbed data. Das call any cause the program to constraint methods commands on behalf of an attacker.

All product views are illustrations and might not represent actual product screens



Return value-added time to auditors and developers

Without sacrificing scan integrity



Results obtained are based on real world applications and scenarios.

Results vary based on training and customization. They are not guarantees of future performance.

Scan analytics

Machine learning to make AppSec more efficient

- Identify true vulnerabilities and prioritize them for remediation faster
- Focus on triaging and investigating high priority vulnerabilities.
- <u>Return value-added time to your developers and auditors</u>





New and Improved .Net scanning



Scanning with our new .NET front end

Before 16.20	After 16.20
Pre-compilation required	No pre-compilation
Compilation required	No compilation necessary
DLL only translation	Source code translation
Visual Studio required - Compilation	Visual Studio required BUT for completely different reasons - Command-line generation



.NET translation options

.NET Command-Line Options

vsversion option is obsolete

The following table describes the .NET command-line options.

Note: These options are not required if you translate the code with the Visual Studio Command Prompt and you have HPE Security Fortify Package for Visual Studio Installed.

NET Option	Description
-dotnet-version <version></version>	Specifies the .NET framework version. See the HPE Security Fortify Software System Requirements for a list of supported versions. This adds the location of .NET framework libraries (DLLs) for the specified .NET framework version to the list of directories/paths specified by the – libdirs option, unless the –libdirs-only option is specified.
-libdirs <dirs> <paths></paths></dirs>	Specifies a semicolon-separated list of directories where referenced system or third-party DLLs are located. You can also specify paths to specific DLLs with this option.
-libdirs-only	Sets the list of directories or paths to only those specified by the -libdirs option. Otherwise, Fortify Static Code Analyzer Indudes the location of the .NET framework libraries (DLLs) that correspond to the .NET framework version specified with the -dotnet-version option.
-dotnet-preproc- symbols < <i>symbols</i> >	Specifies a semicolon-separated list of preprocessor symbols used in the source code. For example:
	-dotnet-preproc-symbols "DEBUG;TRACE"
-dotnet-assembly- name <assembly_ name></assembly_ 	Specifies the name of the target .NET assembly as specified in Visual Studio project settings.
-dotnetwebroot <root_dir></root_dir>	.NET Web projects only. Specifies the home directory of an ASP.NET project.
-cs-extern-alias <aliases_path_ pairs></aliases_path_ 	C# projects only. Specifies a list of external aliases for a specified DLL file In the following format: alias1, alias2,= <path_to_dll>. If multiple DLLs are assigned external aliases, specify multiple -cs-extern-alias options on the command line.</path_to_dll>
-vb-root <namespace></namespace>	.VB.NET projects only. Specifies the root namespace for the project as specified in Visual Studio project settings.
<pre>-vb-imports <namespaces></namespaces></pre>	VB.NET projects only. Specifies a semicolon-separated list of namespaces imported for all source files in the project.

.NET Option	Description
-vb-mytype <symbol></symbol>	VB.NET projects only. Specifies the value for the _MYTYPE preprocessor symbol that is specified in the <mytype> tag in the project settings. This is required if the source code to be translated uses My namespace.</mytype>
-vb-webproject	VB.NET projects only. Indicates that the project is a pure Web project (no code-behind the source files).
<pre>vb-compile- options <compile_ options=""></compile_></pre>	VB.NET projects only. Specifies any special compilation options required for the correct translation of the source code, such as OptionStrict, OptionInfer, and OptionExplicit.
	The format for <compile_options> Is a comma-separated list of: <option>=On Off. For example:</option></compile_options>
	<pre>-vb-compile-options "OptionStrict=On,OptionExplicit=Off"</pre>
-vsversion <version></version>	(Deprecated - Replaced by -dotnet-version option) Specifies the version number that corresponds to your Visual Studio version. Visual Studio 2012: 11.0
	 Visual Studio 2013: 12.0 Visual Studio 2015: 14.0



Sample Translation File (Generated by 17.10 VS plugin)

"-b" "WebGoat.NET"

"-machine-output"

"-dotnet-assembly-name" "DotNetGoat"

"-cs-extern-alias "global="- <.Net framework DLLs, User lib DLLs>"

-dotnet-preproc-symbols" "DEBUG"

"-dotnetwebroot" "C:\Users\nematoll\Documents\nematollVS2017\OWASP-WebGoat.NETe9603b9\WebGoat\\"

"-libdirs-only"

"-libdirs" "<.Net framework DLLs, User lib DLLs>"

"-dotnet-applibs" "<User bin DLLs>""

"C:\VS2017\OWASP-WebGoat.NET-e9603b9\WebGoat\AddNewUser.aspx"

"C:\VS2017\OWASP-WebGoat.NET-e9603b9\WebGoat\AddNewUser.aspx.cs"

"C:\VS2017\OWASP-WebGoat.NET-e9603b9\WebGoat\AddNewUser.aspx.designer.cs"

<... All source files – C#, VB.NET, ASPX, ASCX, XML, CONFIG etc.>



Key Points

Scanning: Ease of use	Scanning is a lot more simple. No need for pre-compilation is a game changer from ease of use perspective
Scanner Architecture: Build vs Folder	You may do folder scans now but leverage Visual Studio to build the translate command until you feel confident
Results: WebForms Application (ASPX)	Significantly improved since 16.2



Extended .NET Frontend supports async/await

□ Async/await support

□ SCA can now find vulnerabilities in aync/await constructs

□ New file extension support

□ SCA can now scan .winmd files

□ SCA can now scan Silverlight apps

□ SCA supports latest versions of:

□ C# 6

□ VB.Net 14

MSbuild support improvements



Parallel Processing/ Multithreaded scanning



Parallel scanning – The old way

- Introduced in version 4.0
- SCA used to spawn multiple processes in parallel
- Process was resource heavy and required mathematical computation
 - For example, if the machine had 32 GB of RAM and 8 cores, the recommended configuration would be: sourceanalyzer ... -j 2 –Xmx14G –Dcom.fortify.sca.RmiWorkerMaxHeap=7G

... And this may still lead to memory errors depending on complexity of code.

Deprecated as of 17.10



Multithreaded parallel mode

Solution

- Redesigned and reimplemented
 - Uses native Java multithreading instead of creating master process and spawning separate processes
 - Removed need for communications and monitoring between master and child processes added burden
- Simple to enable (no complex mathematics)

Results

- Scans complete in 50% of the time compared to single-threaded on average
- Process is optimized and scales to available resources automatically

Risks

 Running the SCA security analyzers in multithreaded mode may introduce non-determinism into issue results. If this occurs, switch back to single-threaded scan.