# ZeroDay

Alast Quick-start Guide Advanced Interactive Application Security Testing





This guide takes the Java language web application and Tomcat as an example. This guide aims to allow users to quickly get started with the AIAST SaaS platform and gain hands-on experience by completing the easiest and most complete usage process.



Deploy Container - Download Agent - Configure Agent - Deploy Range (Web Application) -Test Range - View Results - Export Report

Unlike ordinary Java programs that are started through the main method, the Agent is not a program that can be started independently but must be attached to a Java application (JVM), run in the same process as it, and interact with the virtual machine through the Instrumentation API.

# 🥪 Deploy Container

The Tomcat version of this document example is 8.5.83. On the official download address <u>https://tomcat.apache.org/download-80.cgi</u>, please choose the download link as the figure below. For the installation , please refer to the official Tomcat instructions <u>https://dlcdn.apache.org/tomcat/tomcat-8/v8.5.83/README.html</u>.

Tomcat Connectors	a na inita n
Tomcat Native 2 Tomcat Native 1.2	8.5.83
Wiki Migration Guide Presentations	Please see the <u>README</u> file for packaging information. It explains what every distribution contains.
Specifications	Binary Distributions
Problems?	• Core:
Security Reports Find help FAQ Mailing Lists Bug Database IRC	<ul> <li>2<u>I</u>p (<u>reg. sha512</u>)</li> <li><u>tar.gr</u> (<u>reg. sha512</u>)</li> <li><u>32-bit Windows zip</u> (<u>reg. sha512</u>)</li> <li><u>64-bit Windows zip</u> (<u>reg. sha512</u>)</li> <li><u>32-bit/64-bit Windows zervice Installer</u> (<u>reg. sha512</u>)</li> <li>Full documentation:</li> </ul>
Get Involved	<ul> <li>(ar,g2 (pg), sha12)</li> <li>Deployer:</li> </ul>
Overview Source code Buildbot Translations Tools	<ul> <li><u>zip</u> (pgp, sha512)</li> <li><u>tar.gz</u> (pgp, sha512)</li> <li>Extras:</li> <li><u>Web services jar (pgp, sha512)</u></li> <li>Embedded:</li> </ul>
<b>Media</b> Twitter	<ul> <li>○ tar.gz (pgp, sha512)</li> <li>○ zip (pgp, sha512)</li> </ul>
YouTube Blog	Source Code Distributions
Misc Who We Are	• <u>tar.gz (pgp, sha512)</u> • <u>zip (pgp, sha512</u> )





After the user account has been created, you could log in to the system with the group admin account and password. There are 3 ways to download the Agent:

1) On the Homepage, click [Quick Start]/[Add Application] on the top sidebar;

2) When using AIAST for the first time, click [Add Application] in the middle of the Homepage;

3) In the [Applications] page, click [Add Application] in the upper right corner of this page;



Figure 2 Download Agent on the Homepage (method #1 & #2)

AIAST		A Quick Start
	Home / Applications     Easter to Search     Q     Last Detection Time V     Shart date ~ End date P     C	Export Report     + Add Application
Tyler Wang ∨ Group Admin	App Status:         Apps         Tagged Apps           Please choose         V         Please choose         V	3
🖷 Home	All Apps Favourite Apps	<ul> <li>∞</li> <li>∞</li> </ul>
Projects	Applications 💠 Number of Tested Requests 💠 URL Last Detection Time 💠 First Reported Time 💠 Severity 💠	Number of Vulnerabilities 💠 Tags Options
Applications		
📰 Resources 🛛 👻		
賽 Vulnerabilities	No Data	
My Files		
Recycle Bin	Total: 0	
Œ		

Figure 3 Download Agent on the Applications page (method #3)

After you click on the [Add Application] button, the content of the page will display as below in default (take Java as our example):

AIAST	Aulik San 🖉 💿
	Image: Step 1         Image: Step 2         Image: Step 3
Tyler Wang ∨ Group Admin	Step 1: Download AIAST Agent
	Select a Programming Language
🖶 Home	V evel
Projects	JDK6 - JDK11
	Select a Type of Tracking Template
Applications	Full tracking $\lor$
Resources *	Select a Project to Assign
🕸 Vulnerabilities	Please select an L.Y
My Files	Suppose the project was not selected when the Agent was downloading. In that case, the user can choose a project by assigning the Agent startup parameter [ProjectName = XXX] in the command line after downloading the Agent.
🖻 Recycle Bin	Default Application Name
	Enable HTTP/HTTPS Proxy
	When the network of the tested application cannot communicate with the AIAST server (ie, this current site) directly, AIAST allows uses to use a proxy to communicate with the server through HITP/HITPS. Currently, we support BASIC, NTDM, and DIGEST authentication methods for proxy. Of course, users can also not use
	L Download Agent Go to the next step

Figure 4 Steps of downloading Agent

Click on the [Download Agent] button as above(take Chrome Version 106.0.5249.119(Official Build)(64-bit) as an example), if the browser asks you to prevent the AIAST.jar, please just keep it, the AIAST.jar in the folder is shown as below:

$\downarrow$ Downloads					- 0	×
🕀 New 🗸 👗	(Û 🗋 🗳 🖄 🕅 ↑↓ Sort	~ 🗮 View ~ 🛛 🚥				
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\land$	> This PC > Downloads			~ C		م
> 🧥 Home	Name > A long time ago	Date modified	Туре	Size		
> lesson OneDrive	> Earlier this year					
🔉 💻 This PC	> Last month > Last week					
> 湟 Network	✓ Today					
	🕌 AIAST.jar	10/17/2022 11:13 AM	Executable Jar File	1,4	16 KB	
78 items 27 items select	ted					

Figure 5 AIAST.jar is displayed in the folder



Place the downloaded AIAST.jar file in the root directory of the container (take Tomcat as an example, for other containers, please refer to the AIAST detailed interface guidance section), as shown in the following figure:



Figure 6 Place AIAST.jar in the apache-tomcat folder

The Tomcat installation directory used in the example is: C:\apache-tomcat In the Tomcat root directory, enter the bin subdirectory:

bin				-	
🕀 New ~ 🛛 👗		$\land$ Sort $\checkmark$ $\equiv$ View $\checkmark$ $\cdots$			
$\leftrightarrow \rightarrow \checkmark \uparrow$	This PC > Windows (C:) > apache	e-tomcat > bin		~ C	م
> 🏫 Home	Name ugustan	Date modified	Туре	Size	
> 🌰 OneDrive	🐁 setclasspath.bat	4/1/2022 12:05 AM	Windows Batch File	4 KB	
	setclasspath.sh	4/1/2022 12:05 AM	SH File	4 KB	
This PC	🖏 shutdown.bat	4/1/2022 12:05 AM	Windows Batch File	2 KB	
> 🗽 Network	shutdown.sh	4/1/2022 12:05 AM	SH File	2 KB	
	😼 startup.bat	9/21/2022 3:01 PM	Windows Batch File	3 KB	
	startup.sh	4/1/2022 12:05 AM	SH File	2 KB	
	💩 tomcat-juli.jar	4/1/2022 12:05 AM	Executable Jar File	51 KB	
	s tool-wrapper.bat	4/1/2022 12:05 AM	Windows Batch File	5 KB	
	tool-wrapper.sh	4/1/2022 12:05 AM	SH File	6 KB	
	🗞 version.bat	4/1/2022 12:05 AM	Windows Batch File	2 KB	
	version.sh	4/1/2022 12:05 AM	SH File	2 KB	
27 items					

Figure 7 startup script of Tomcat in the bin subdirectory

Configure the startup script: startup.bat

Add the statement associated with the Agent as below:

set "JAVA\_OPTS=%JAVA\_OPTS% -javaagent:C:\apache-tomcat\AIAST.jar"

Where C:\apache-tomcat\AIAST.jar is the absolute path where the file is located.





The instructions for preparing the environment are as follows:

- •Hardware environment: personal computer with more than 4G memory, Windows 7/8/10/11.
- ●JDK version: JDK8

JDK download address: https://www.oracle.com/java/technologies/downloads/#java8-

#### windows

• Application name: WebGoat

Cyber range download address: (both jar package and war package can be downloaded) https://github.com/WebGoat/WebGoat-Legacy/releases/download/v6.0.1/WebGoat-6.0.1.war https://github.com/WebGoat/WebGoat-Legacy/releases/download/v6.0.1/WebGoat-6.0.1-warexec.jar

If the JDK environment is not installed, please install the JDK first. Please refer to the official installation guide, and set the environmental variables.

Put WebGoat-6.0.1.war in the tomcat application directory C:\apache-tomcat\webapps:

🚞 webapps						- 0 ×	
🕀 New - 🐰		↑ Sort $\sim$ $≡$ View $\sim$ $ $ …					
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	> This PC > Windows (C:) > apache-tom	cat → webapps			~ C		
> 🟫 Home	Name	Date modified	Туре	Size			
	🗀 docs	4/22/2022 6:02 PM	File folder				
> CneDrive	🚞 examples	4/22/2022 6:02 PM	File folder				
🔉 💻 This PC	host-manager	4/22/2022 6:02 PM	File folder				
> 🗽 Network	🚞 manager	4/22/2022 6:02 PM	File folder				
	ROOT	4/22/2022 6:02 PM	File folder				
	🚞 spring-demo	4/22/2022 6:31 PM	File folder				
	🖿 WebGoat-6.0.1	7/18/2022 5:53 PM	File folder				
	spring-demo.war	4/22/2022 6:27 PM	WAR File	66,005 KB			
	WebGoat-6.0.1.war	12/7/2021 12:22 PM	WAR File	48,456 KB			
9 items							]
							1

Figure 9 WebGoat in the webapps directory

Return to C:\apache-tomcat\bin, and execute the startup.bat:

🚞 bin				-	οx
🕀 New - 👗		N Sort ~ ≣ View ~ ····			
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	> This PC > Windows (C:) > apache-tomcat	: ≻ bin		~ C	م
> 🥎 Home	Name ugcatan	Date modified	Туре	Size	
> 🥌 OneDrive	🐁 setclasspath.bat	4/1/2022 12:05 AM	Windows Batch File	4 KB	
	setclasspath.sh	4/1/2022 12:05 AM	SH File	4 KB	
🔉 💻 This PC	% shutdown.bat	4/1/2022 12:05 AM	Windows Batch File	2 KB	
> 일 Network	shutdown.sh	4/1/2022 12:05 AM	SH File	2 KB	
	😼 startup.bat	9/21/2022 3:01 PM	Windows Batch File	3 KB	
	📄 startup.sh	4/1/2022 12:05 AM	SH File	2 KB	_
	💩 tomcat-juli.jar	4/1/2022 12:05 AM	Executable Jar File	51 KB	
	🐁 tool-wrapper.bat	4/1/2022 12:05 AM	Windows Batch File	5 KB	
	tool-wrapper.sh	4/1/2022 12:05 AM	SH File	6 KB	
	😒 version.bat	4/1/2022 12:05 AM	Windows Batch File	2 KB	
	version.sh	4/1/2022 12:05 AM	SH File	2 KB	
27 items					

#### Figure 10 Execute the startup.bat

#### Double click on the startup.bat to start the Web container as following figure:

🛃 Tomrat	- 0 X
18-Oct-2022       10:49:50.09 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Server version name:       Apache 1         18-Oct-2022       10:49:50.106 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Server version number:       Nar 31         18-Oct-2022       10:49:50.106 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Server version number:       Ns. 5. 78.0         18-Oct-2022       10:49:50.106 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Swame:       Windows         18-Oct-2022       10:49:50.106 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Swame:       Windows         18-Oct-2022       10:49:50.106 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Sverion:       10.0         18-Oct-2022       10:49:50.107 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Architecture:       amd64         18-Oct-2022       10:49:50.107 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log Java Home:       C: Progr         18-Oct-2022       10:49:50.107 INPO       [main]       org. apache. catalina. startup. VersionLoggerListener. log JW Version:       1.8.0         18-Oct-2022       10:49:50.107 INPO       [main]       org. apache. catalina. star	omcat/8.5.78 022 16:05:28 UTC 10 ram Files\Java\jdk1.8.0_181\jre 81-b13 Corporation
18-Oct-2022 10:49:50.107 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE: C:\apact 18-Oct-2022 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -Djava.u omcat\contYlogging.properties 18-Oct-2022 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -Djava.u felotteres 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -Djava.u classLoaderLogManager 18-Oct-2022 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -Djava.u classLoaderLogManager 18-Oct-2022 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.108 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 18-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Tine argument: -java.agu 19-Oct-2022 10:49:50.109 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command Ine argument: -Java.agu	e-tomcat e-tomcat stil.logging.config.file=C:\apache-t itil.logging.manager=org.apache.juli ent:C:\apache-tomcat\AIAST.jar is.ephemeralDHKeySize=2048
18-Oct-2022 10:49:50.110 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.p alina.webresources 18-Oct-2022 10:49:50.111 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dignorc 18-Oct-2022 10:49:50.112 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatali 18-Oct-2022 10:49:50.113 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatali 18-Oct-2022 10:49:50.113 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatali 18-Oct-2022 10:49:50.113 INFO [main] org.apache.catalina.startup.VersionLoggerListener.lifecycleEvent The Apache Tomcat Native 18-Oct-2022 10:49:50.113 INFO [main] org.apache.catalina.core.AprLifecycleIstener.lifecycleEvent The Apache Tomcat Native yas.not found on the iava.library.nath: [C:VPTORDME]les\laya\u00edkl.8.0 18\u00edkl.8.0 Usl\u00edkl.8.0 18\u00edkl.8.0 18\u00edk	rotocol.handler.pkgs=org.apache.cat .endorsed.dirs= .na.base=C:\apache-tomcat .n.home=C:\apache-tomcat .o.tmpdir=C:\apache-tomcat\temp b library which allows using OpenSSL B2:C:\WNONS:C:\Program Files (x86
<pre>\Common Files\Oracle\Java\javapath;C:\Wware\bin\;C:\Program Files\Java\jdkl.8.0_181\bin;C:\Program Files\Java\jdkl.8.0_ rogram Files (x86)\Callbre2\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\J30\Tools\Binn\;C:\Program Files \C:\Program Files\Microsoft SQL Server\140\Tools\Binn\;C:\Program Files\Microsoft SQL Server\140\TS\Binn\;C:\Program Files .exe:C:\WINDOWS\system32\C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\v1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;C:\WINDOWS\System32\VindowsPowerShell\V1.0\;Vindows\VINDOWS\System32\VindowsPowerShell\V1.0\;Vindows\VINDOWS\System32\VINDOWS\VINDOWS\System32\VINDOWS\VINDOWS\System32\VINDOWS\VINDOWS\System32\VINDOWS\VINDOWS\VINDOWS\System32\VINDOWS\VINDOWS\System32\VINDOWS\VINDOW</pre>	81\jre\bin;C:\Windows\System32;C:\P Microsoft SQL Server\140\Tools\Binn es\processing-3.5.4\processing-java M32\OpenSSH\;C:\Anaconda3;C:\Anacond MData\Local\Microsoft\WindowsApps;C Wang\AppBtata\Local\GitHubDeskton\bi mache-maven-3.8.1\bin;C:\Program Fil n;C:\Program Files\processing-3.5.4 Microsoft\WindowsApps;;]

#### Figure 11 Starting the server

When you view the keywords "IAST AGENT", it means the Agent has been started:





Using a browser (Chrome), visit the URL of the application:

http://127.0.0.1:8080/WebGoat-6.0.1/login.mvc

The interface is displayed as follows:

S Login Page	+			
← → C ① 127.0.0.1:8080	)/WebGoat-6.0.1/login.mvo			
WEBGOAT	Please I	ogin		
	Username			
	webgoat			
	Password			
	Sign in The following accou	ints are built ir	ito Webgoat	
	Account	User	Password	
	Webgoat User	guest	guest	
	Webgoat Admin	webgoat	webgoat	

Figure 12 WebGoat login page

Use the account and password shown on this page to log in, and enter the system to perform the function tests. The Agent will collect and report the traffic generated during the tests to the AIAST server. Finally, the results will be displayed to you.

WebGoat homepage is displayed as below:

🕲 WebGost	×	+	✓ - □ ×			
← → C © 127.0	.0.1:8080/	WebGoat-6.0.1/start.mvc	@ 🛧 ≱ 🚨 !			
WEBGOA	г	8	A i 35			
E LESSONS	-					
		Solution Lesson Plan - Restart Lesson				
			Cookies / Parameters			
			Cookies			
	1.0	Similar to the CSRF Lesson, your goal is to send an email to a newsgroup that contains multiple malicious requests:	Coonica			
	1.0	should point to the CSRF lesson with an extra parameter "transferFunds=4000", and "transferFunds=CONFIRM". You	comment			
	1.1	can copy the shortcut from the left hand menu by right clicking on the left hand menu and choosing copy shortcut.	http://http://www.second			
		Whoever receives this email and happens to be authenticated at that time will have his funds transferred. When you think the attack is supported in a second data ways that the attack is a the left hand side mean.	maxAge -1			
		Note that the "Screen" and "menu" GET variables will vary between WebGoat builds. Copying the menu link on	name JSESSIONIO			
		the left will give you the current values.	path			
Improper Error Handling		Title:	secure false			
		Message:	value S66PS6088P91641A7DE5DE6DCL27997C			
	1.0		Params			
Insecure Configuration			ParamValue			
Insecure Stocage			Screen 32			
Malicious Execution	100		termine to			
Parameter Tamperine	1.00					
Session Management Flaws	100					
Web Services						
Admin Functions		Submit				
Challeroon						
Come de la		Manageralist				
		wessage List				

#### Figure 13 WebGoat Homepage

Here is an example of SQL injection. For other examples, please refer to the official tutorial.



Figure 14 exploit SQL Injection in WebGoat

Process of exploitation:

- 1. Select the Injection Flaws / String SQL Injection tab;
- 2. Enter the specified string in the input box, enter test001 as example here;
- 3. Click [go] to execute the operation;
- 4. The display part shows the executed SQL statement.

You could choose to manually perform function tests as described above to generate data traffic or else can also use DAST tools like AppScan to automatically generate traffic, then detect and report vulnerabilities efficiently



After performing the function tests, you can log in to the AIAST SaaS platform to view the details of the security vulnerabilities.

Check the [Applications] page to view if there is web application' s info:

ALAST	A Quick Star	t
	الله Home / Applications الله Appli	ication Status
	Enter to Search Q Last Detection Time V Start date ~ End date 🗇 🔁 🕒 Export Report	Application
	App Status Apps Tagged Apps	
Tyler Wang ∨ Group Admin	Please choose     V     Please choose     V	
🖀 Home	All Apps Favourite Apps	~ 8
Projects	Applications $\Diamond$ Number of Tested Requests $\Diamond$ URL Last Detection Time $\Diamond$ First Reported Time $\Diamond$ Severity $\Diamond$ Number of Vulnerabilities $\Diamond$ Tags	Options
Applications	🗌 🖤 🍿 WebGoat-6.0.1 🖉 0 / WebGoat-6.0.1 2022-10-19 17:11 2022-09-21 15:04 🕒 CRITICAL 29   💈 🗿 🕐 N/A	More V
Resources ·	Total: 1	
Servers		
Web Containers	< 1 > 10/ page $\lor$ Goto	
策 Vulnerabilities		
My Files		
Recycle Bin		
Ē		

Figure 15 Cyber range's Info

Click on the name of the web application to enter the sub-page:

Alast		Quick Start
	Home / Applications / App Details	
Tyler Wang ∨	WebGoat-6.0.1 URL: /WebGoat-6.0.1 Language: Java	E Export Report
Group Admin	Q Overview         ★ Vulnerabilities         Ø         Open Source Dependencies	
🖶 Home	Vulnerabilities 29 OSD () 47 2022-10-19	0
Projects	Critical 2 CVEs 93 O Last Detection Time	Lines of Code
Applications	1 Containers (Mastino) 🗵	
Resources	101160.2112/Asseks Toward 9.570)	
¥ Vulnerabilities	▲ I3C1002113(Hadre Mirver0210)	
🖿 My Files	Security Vulnerability Statistics 🛞 Open Source Dependency Severity Statistics	
Recycle Bin	Severity   OWASP 2021   CWE 2021   PCI DSS   Status	
	CRITICAL D 4(85/9)	
	HIGH CRITICAL 2 (599) 6 (12.77%) 6 (12.77%)	
	NOTE	c
Ξ	Total 9(9,15%)	28 (59.57%)



#### Click on the [Vulnerabilities]:

A	IAST												
		Sear	ch according to ti	itle / key Q Last Detection Time	× ]	Start date	~ E	nd date 🛛 🗄	T C			L Update S	tatus 🗸
	7	All	Favorite	S								7	
	Tyler Wang ∨		ID	Outline 👙	Туре	Severity \$	Status 👙	Operator	Agent Version	Group	Last Detection Time 👙	First Reported Time 👙	Options
*	Org Admin Home Projects		EDDDF016621	SQL injection - Parameter:"acco Inc.name"   URL:"/WebGoat-6.0.1/at tack"   Code:"SqlStringInjection.java,   ine: 101"	SQL Inje ction	CRITICAL	Reported 🖉	Unallocated 🖉	2.9.9.5-2747	tyler_def ault gro up	2022-10-21 16:29	2022-10-21 16:29	More ∨
	Applications Resources		EDDDF016090	SQL injection - Parameter:"pass word"   URL:"/WebGoat-6.0.1/attack"   Code:"Login.java, line: 131" 💮	SQL Inje ction		Reported 🖉	Unallocated 🖉	2.9.9.5-2747	tyler_def ault gro up	2022-09-23 10:56	2022-09-23 10:56	More ⊻
*	Vulnerabilities My Files		EDDDF016061	Reflected-XSS - Parameter:"acc ount_name"   URL:"/WebGoat-6.0.1/a ttack"   Code:"Screen.java, line: 209"	Cross-Sit e Scripti ng	HIGH	Reported 🖉	Unallocated 🖉	2.9.9.5-2747	tyler_def ault gro up	2022-10-21 16:29	2022-09-21 15:05	More ∽
*	Group Recycle Bin		EDDDF016062	Reflected-XSS - Parameter:"acc ount_name"   URL:"/WebGoat-6.0.1/a ttack"   Code:"Screen.java, line: 209" ©	Cross-Sit e Scripti ng	HIGH	Reported 🖉	Unallocated 🖉	2.9.9.5-2747	tyler_def ault gro up	2022-10-21 16:29	2022-09-21 15:05	More ¥
	E		EDDDF016063	Reflected-XSS - Parameter:"acc ount_name"   URL:"/WebGoat-6.0.1/a ttack"   Code:"HammerHead.java, lin	Cross-Sit e Scripti ng	HIGH	Reported 🖉	Unallocated 🖉	2.9.9.5-2747	tyler_def ault gro up	2022-10-21 16:29	2022-09-21 15:05	More ∨

Figure 17 SQL Injection

Click on a specific vulnerability to view the data flow:

ALAST								
	<< Return	ID:EDDDF016621 Previous Next						
7	SQL injection - Parameter:"account_name"   URL:"/WebGoat-6.0.1/attack"   Code:"SqlStringInjection.java, line: 101"							
Tyler Wang ∨ Org Admin	CRITICAL First Det	Birst Detection Time       2022-10-21       Last Detection Time       2022-10-21       Status:       Reported       Image: Constraint of the state of the						
🏶 Home	Overview	WebGoat-6.0.1 192.168.31.13 2022-10-21 2022-10-21						
Projects	i Code	The Apps Envrionment First Detection Time Last Detection Time						
Applications	<b>Т</b> НТТР							
🗮 Resources 🕚	Comments	It was detected that 'account_name' in the following request induced SQL injection:						
資 Vulnerabilities		POST http://127.0.0.1:8080/WebGoat-6.0.1/attack?Screen=14&menu=1100						
My Files		account_name=test001&SUBMIT=Go!						
嶜 Group		The parameter was brought into the application process via the following code:						
Recycle Bin		org.owasp.webgoat.session.ParameterParser.getRawParameter(), line: 503						
		The parameter was used to build the following SQL statement which was executed without input validation:						
		SELECT * FROM user_data WHERE last_name = 'test001'						

Figure 18 User Input is shown as below

It can be seen that this vulnerability is the vulnerability we exploit in the WebGoat application.

In addition, you can view other pages such as details, HTTP information, fix suggestions, and discussion boards, etc., to learn more about all aspects of the vulnerabilities.

More details about the vulnerability are shown as follows:

AIAST				A Quick Start
yer Wang ∨ Group Admin	Home / Vulnarabil Keturn KQL injection Correct: First E	- Parame	nexeting Davies	EDD0F016060 Previous Nett
🖶 Home 🖵 Projects	Overview	Input		Bipand All 4
Applications     Resources     Automatilities	♥ HTTP ● Comments		jarasserkel.SerkelBequest.pethrameterWaterstoorunt_name > pottow/barneter/Diffiximeter/barseptina line 333 [7]ver]	(TP)
My Files Regicte Bin		The prop	Applied or price imalies ShingShingShingShingShingShingShingShing	
		Output	Inc. of Statement.executeQueryGHLCT * ROM war, data WHER Int, anne = "yter")     StateStateCom/d StateStateQueryGHLCT * ROM war, data WHER Int, anne = "yter")     GELCT * ROM war, data WHERI Int, serie = "yter")	
			1	0



Alast			Quick Start
	Overview		Expand All↓
- <u>-</u>	i Code Input		
Tyler Wang ∨ Group Admin	HTTP     Comments	javax.servlet.ServletRequest.getParameterValues(account_name) v getRawParameter()@ParameterParser.java line: 503 [Tyler]	
🖀 Home		Class.Method: javax.servlet.ServletRequestWrapper.getParameterValues(java.lang.String)	нпр
Projects		Object: org.springframework.security.web.servletapi.HttpServlet3RequestFactorySServlet3SecurityContextHolderAwareRequestWrapper	-
Applications		Return: [Tyler]	
Resources		Parameter: account_name	
¥ Vulnerabilities		Details	
🖿 My Files		Code Stack	
Recycle Bin		package org.owap, webgoat.session; public class ParameterParser {  public void getRamParameter() { (503 ) javax.servlet.ServletRequestWrapper.getParameterValues(); }	Ō
E		)	

Figure 20 locate the vulnerability in specific code line



Click the [Applications] tab, select the application you want to take action on, then click [More]-

[Export Report]:



Figure 21 Export Report

Select the desired report type, report granularity, compliance criteria, and vulnerability severity

for report export:



Figure 22 Select generated report to export

After exporting the report, then select the generated report to download.

AIAST							Quick Start
Tyler Wang V Group Admin							± 0 V
	Name	File Format 👙	Size 👙	Status 😄	Creation Time 👙	Expiry Time 💿	Options
Projects     Applications	App Security Preview Report_WebGoat-6.0.1_2022-10-20_12_12_13.pdf	*.pdf	295KB	Generated	2022-10-20 12:12	2022-11-04 12:12	DownLoad Delete
Resources	Total: 1	1 > 10/ pag	e ∨ Goto				
My Files							
Recycle Bin							

Figure 23 Report generated in [My Files]

After the report is downloaded, the report is shown locally as below:



Figure 24 Downloaded Report

Taking the Application Security Report as an example, the preview is as follows:



Figure 25 Preview of the report

Vulnerabilities classified by various compliance standards will be presented in the form of subsections. By reading the report, security managers can be aware of the general application security posture.

The AIAST has the ability to assist security managers in arranging work based on reports. It can help developers schedule and perform the bug-fixing, development, and test work according to the reports. It also offers insights and suggested solutions for vulnerability fixing.

		Technical Specifications
--	--	--------------------------

## Supported language

Supported platform

Java
Node.js
C#/.NET
PHP
Python

## Windows Linux MacOS Unix like

# Supported web server/applicationframework

#### Java

### - Tomcat

- WebLogic
- Spring Boot
- Jetty
- WebSphere
- JBoss
- WildFly
- Resin
- WebSphere Liberty

N	od	e.	js
N	od	e.	js

- Express
- .Net
- .NET Framework

## .PHP

- Nginx
- Apache



Founded in 2016, ZeroDay aims to make software development more secure and application security work simpler, saving your precious time and workforce.

Spearheaded by AIAST, our product portfolio will include software component analysis, static application security testing, dynamic application security testing, fuzz testing, and more in the coming days.

For more information about	160 The Edge, Clowes Street Salford,	Sales: + 44-16-1350-8028
ZeroDay, visit us online at	Manchester, M3 5NE	
www.zeroday.co.uk	U.K.	