ZeroDay

AIAST Quick-start Guide

Advanced Interactive Application Security Testing

Abstract

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.

Easy-to-use 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 https://tomcat.apache.org/download-80.cgi, please choose the download link as the figure below. For the installation , please refer to the official Tomcat instructions https://dlcdn.apache.org/tomcat/tomcat-8/v8.5.83/README.html.

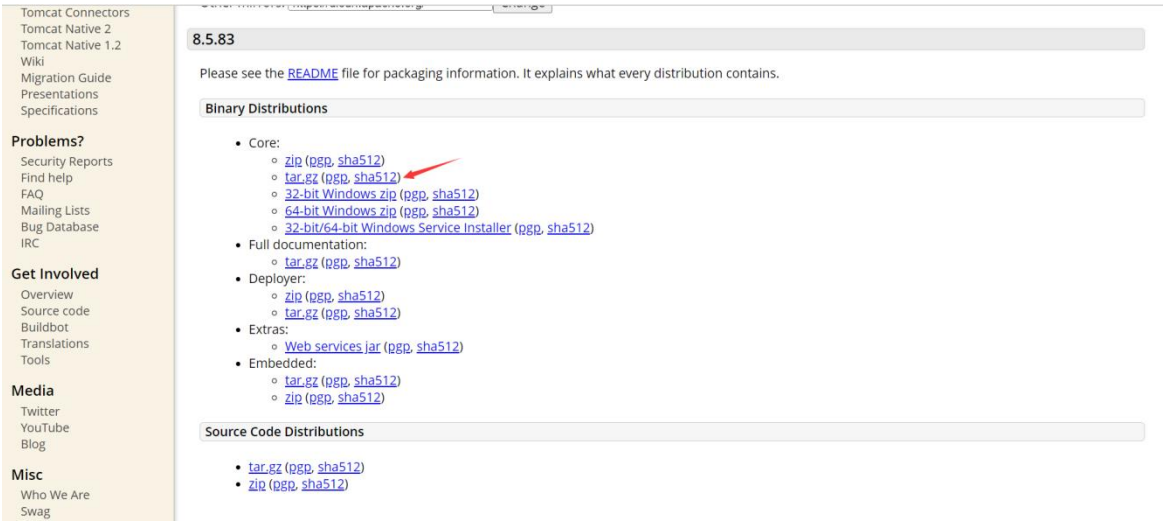


Figure 1 Tomcat download page

Download Agent

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;

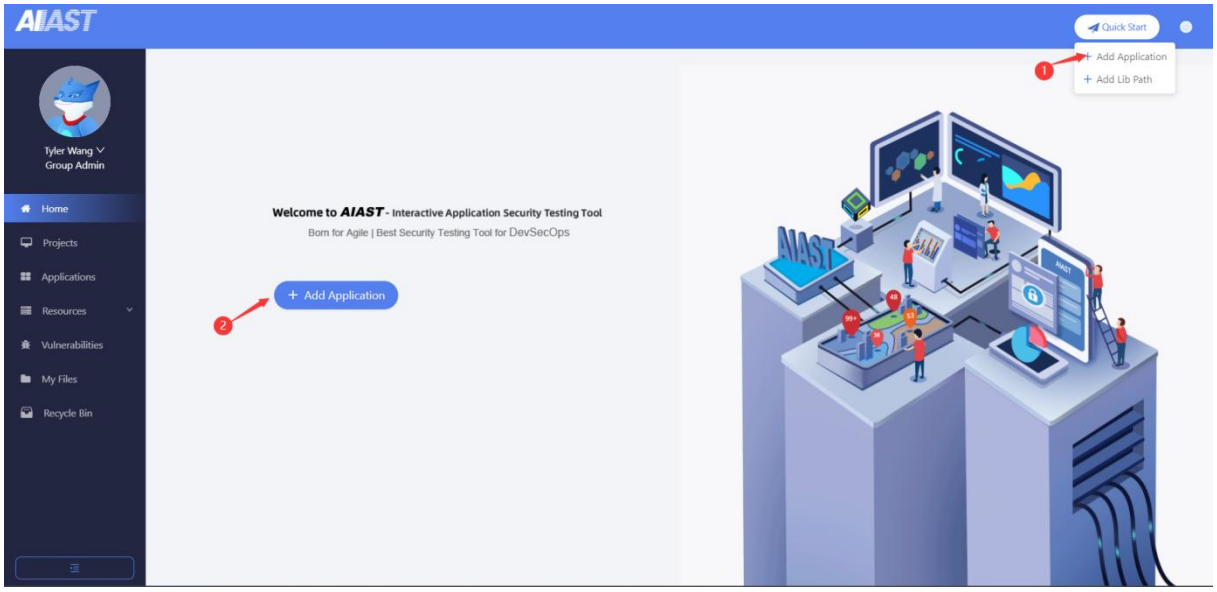


Figure 2 Download Agent on the Homepage (method #1 & #2)

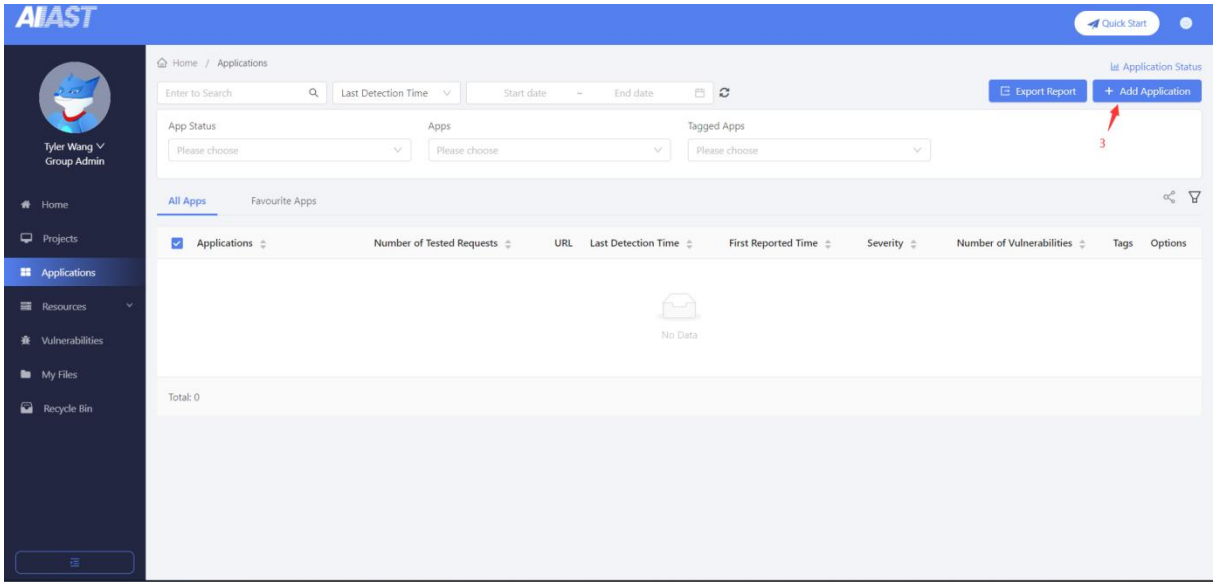


Figure 3 Download Agent on the Applications page (method #3)

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

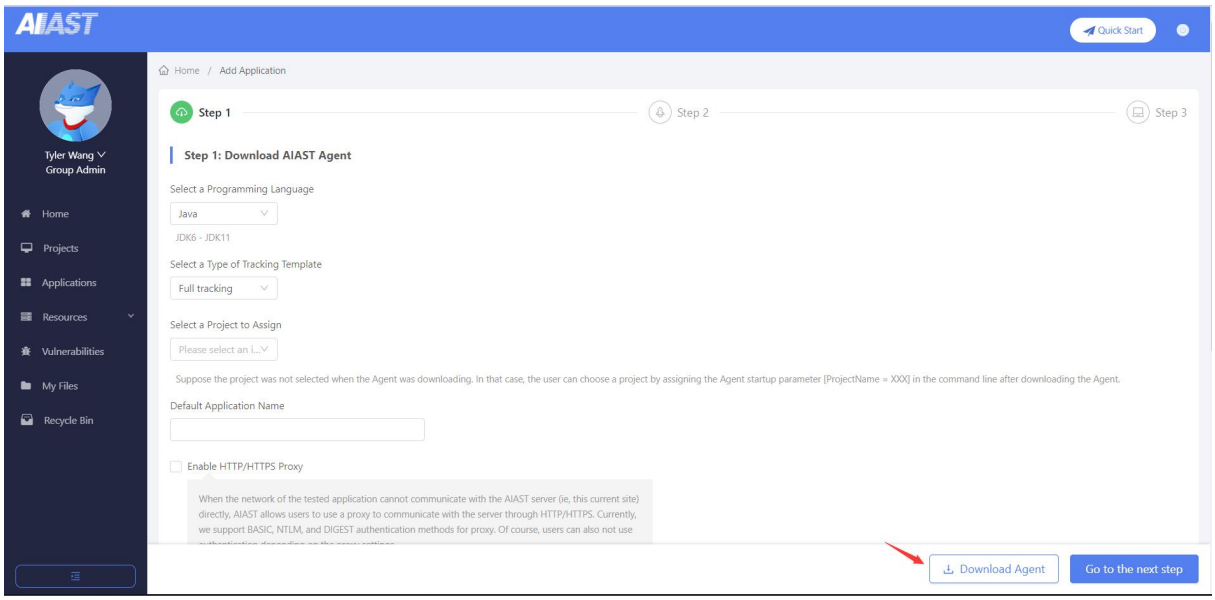


Figure 4 Steps of downloading Agent

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:

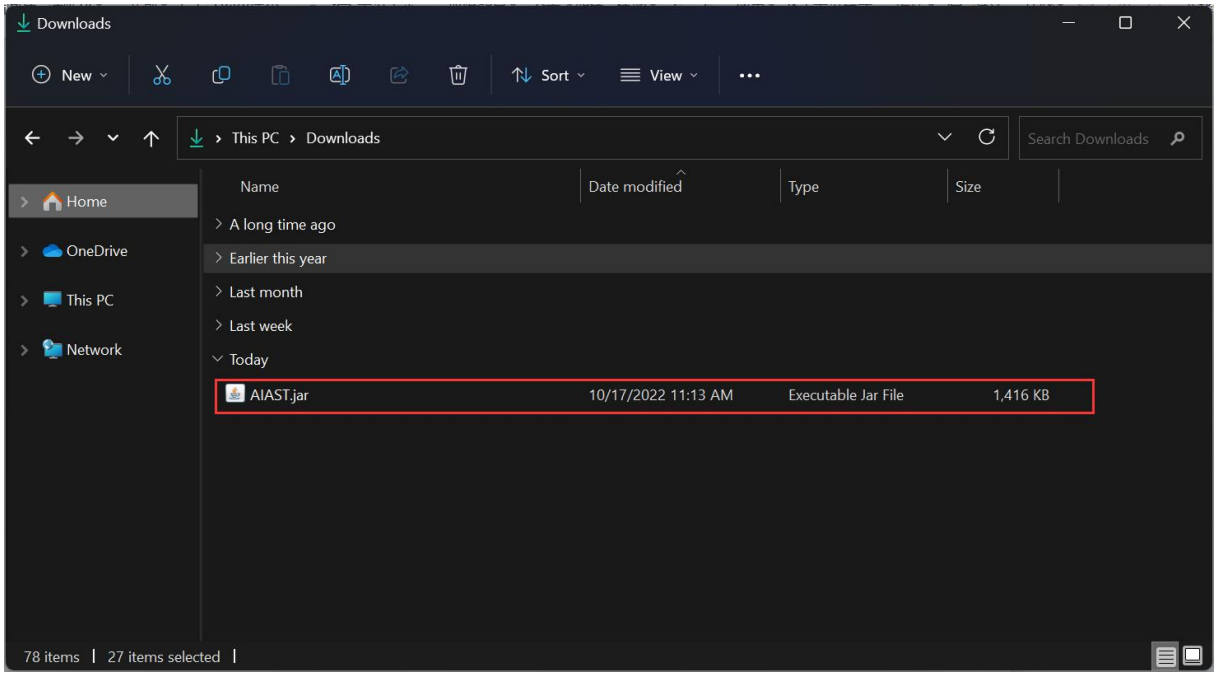


Figure 5 AIAST.jar is displayed in the folder

Configure Agent

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:

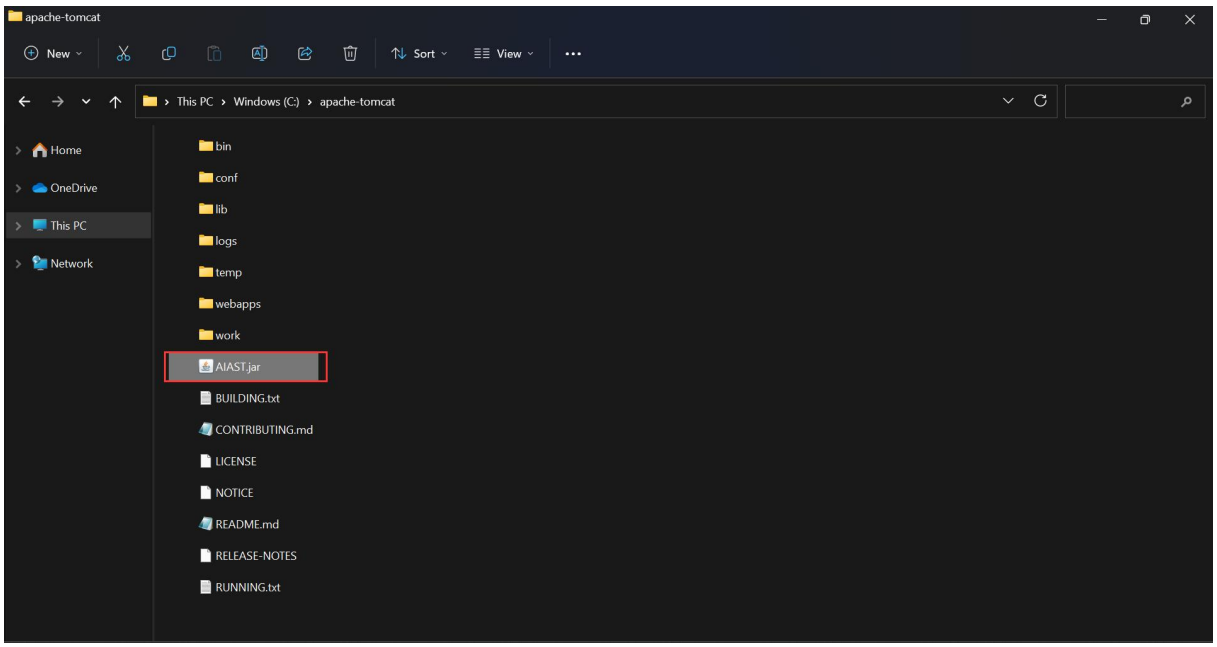


Figure 6 Place AIAST.jar in the apache-tomcat folder

The Tomcat installation directory used in the example is: C:\apache-tomcat

In the Tomcat root directory, enter the bin subdirectory:

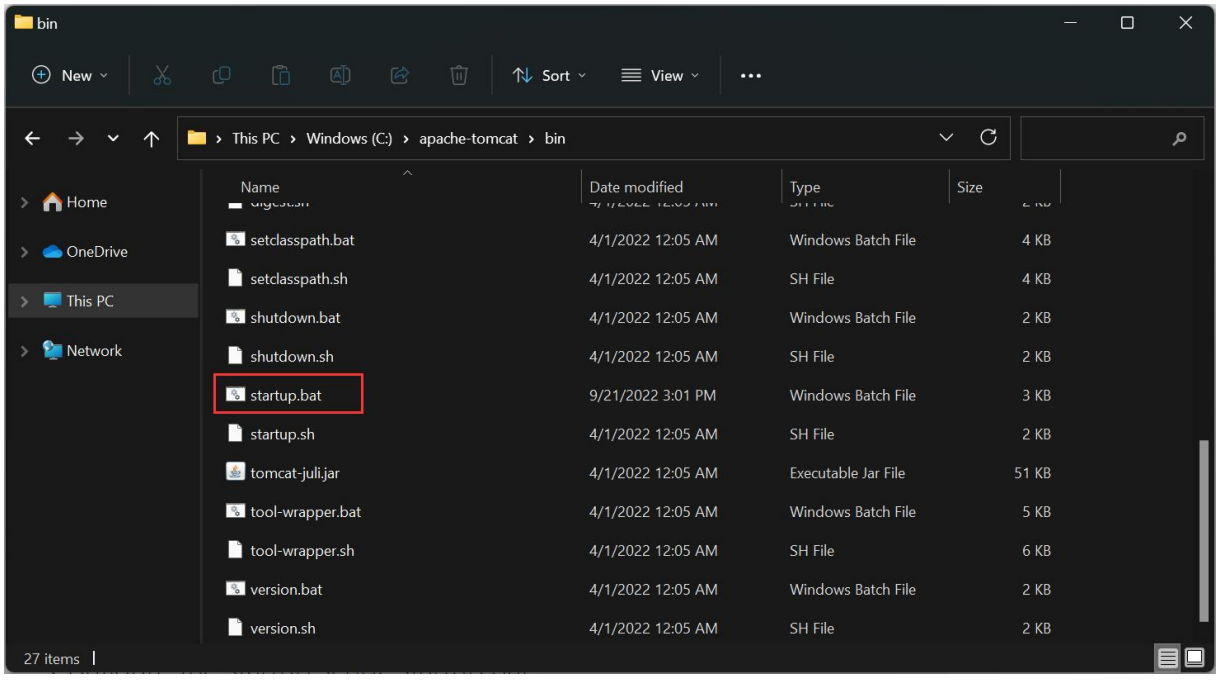


Figure 7 startup script of Tomcat in the bin subdirectory

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.

```
rem
rem Unless required by applicable law or agreed to in writing, software
rem distributed under the License is distributed on an "AS IS" BASIS,
rem WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
rem See the License for the specific language governing permissions and
rem limitations under the License.

rem -----------------------------------------------------------------------------
rem Start script for the CATALINA Server
rem -----------------------------------------------------------------------------

setlocal

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

rem Guess CATALINA_HOME if not defined
set "CURRENT_DIR=%cd%"
if not "%CATALINA_HOME%" == "" goto gotHome
set "CATALINA_HOME=%CURRENT_DIR%"
if exist "%CATALINA_HOME%\bin\catalina.bat" goto okHome
cd ..
set "CATALINA_HOME=%cd%"
cd "%CURRENT_DIR%"
:gotHome
if exist "%CATALINA_HOME%\bin\catalina.bat" goto okHome
echo The CATALINA_HOME environment variable is not defined correctly
echo This environment variable is needed to run this program
goto end
:okHome

set "EXECUTABLE=%CATALINA_HOME%\bin\catalina.bat"

rem Check that target executable exists
if exist "%EXECUTABLE%" goto okExec
echo Cannot find "%EXECUTABLE%"
echo This file is needed to run this program
goto end
:okExec
```

Figure 8 Contents of startup.bat

Save and exit.

Deploy Application

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-war-exec.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:

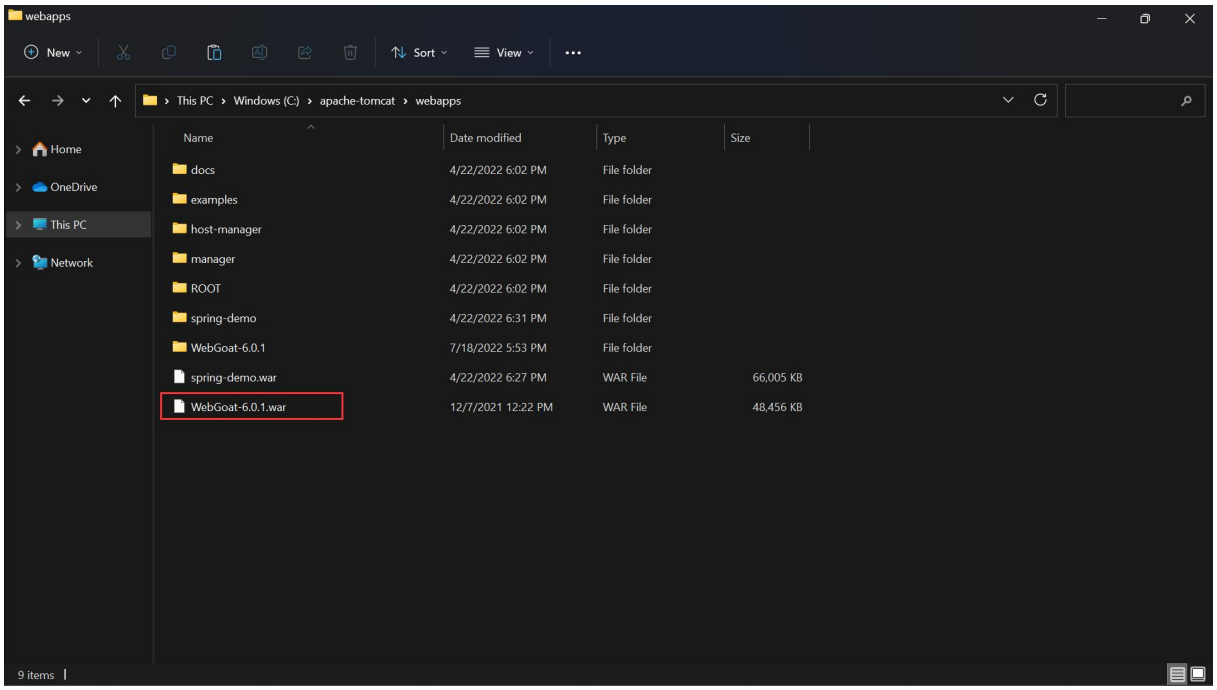


Figure 9 WebGoat in the webapps directory

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

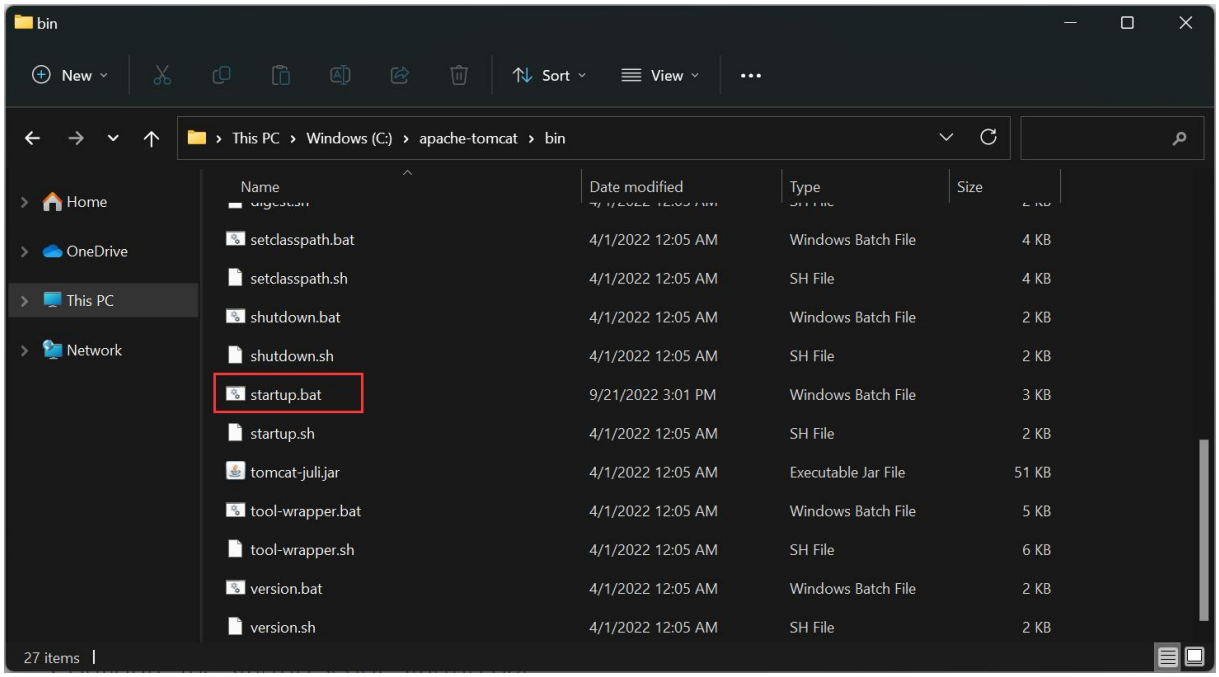


Figure 10 Execute the startup.bat

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

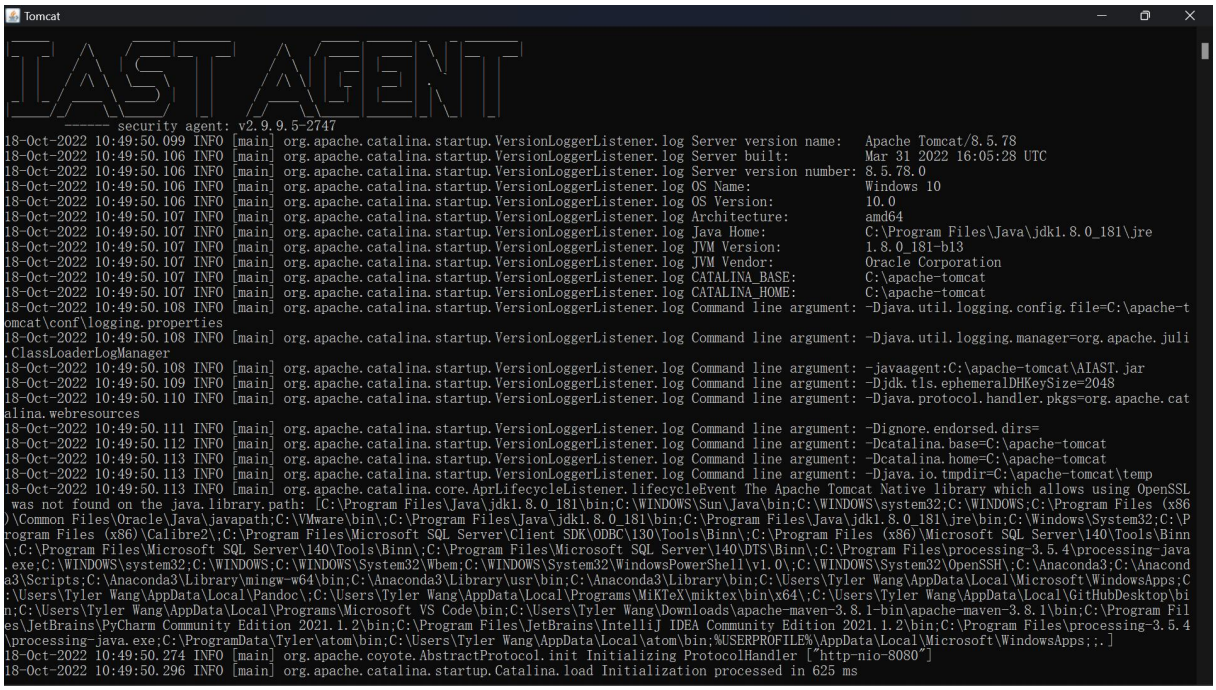
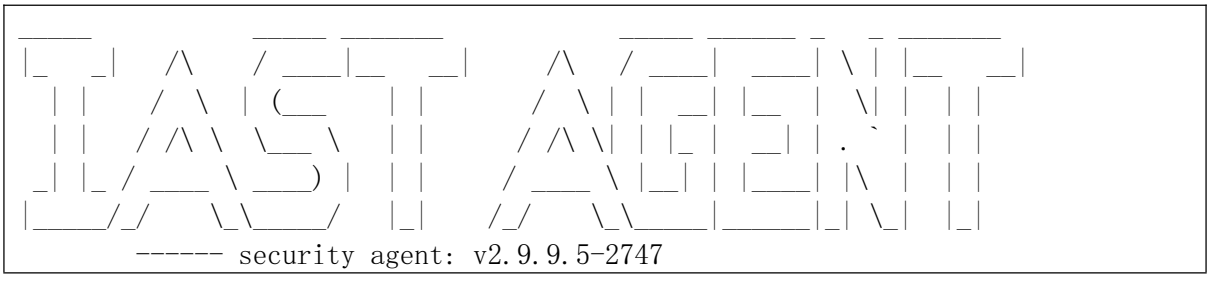


Figure 11 Starting the server

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



Test Application

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:

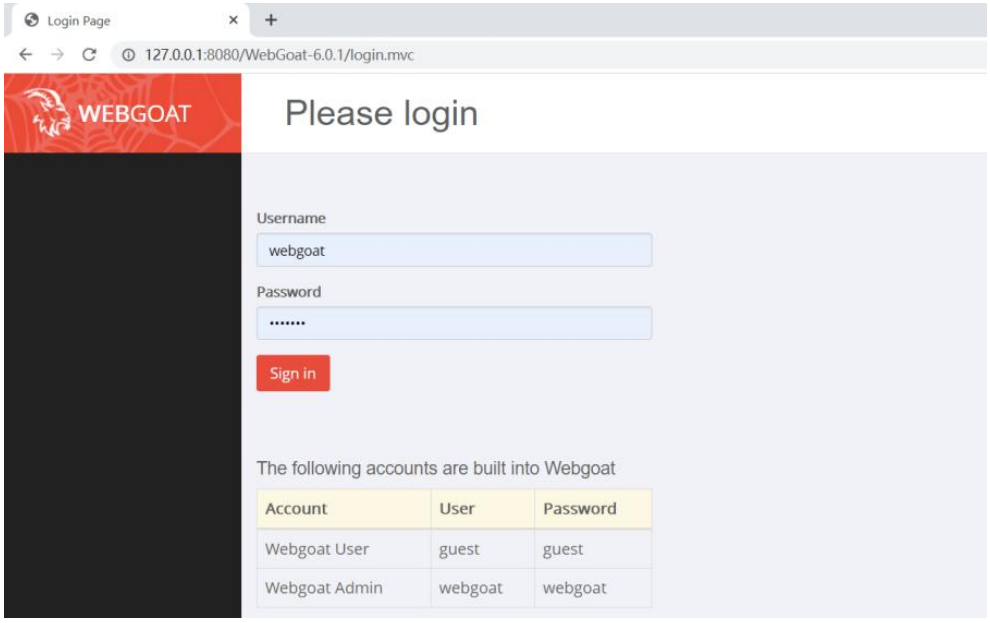


Figure 12 WebGoat login page

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:

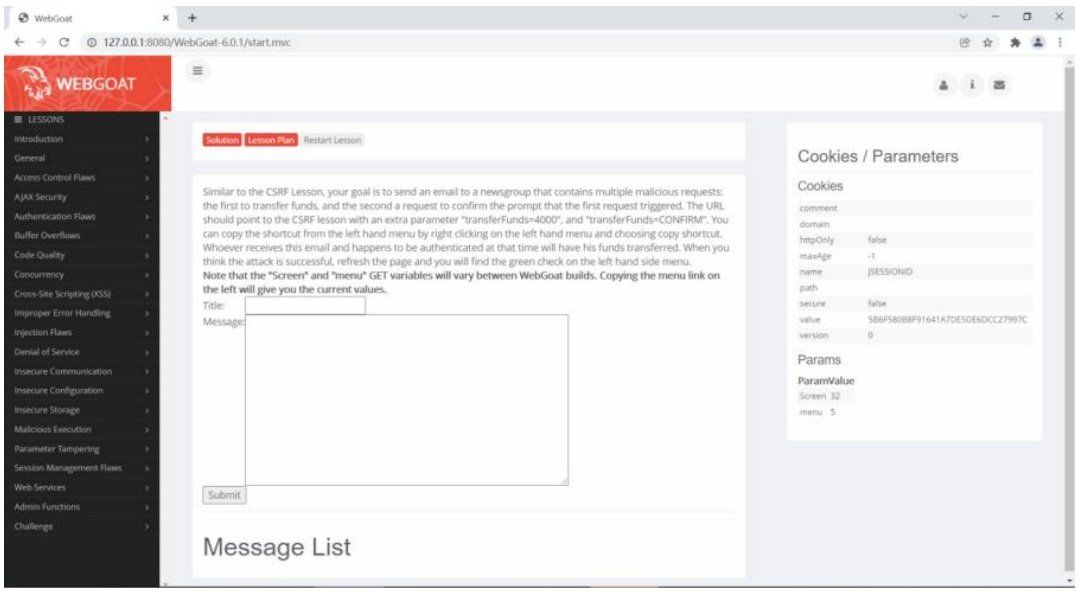


Figure 13 WebGoat Homepage

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

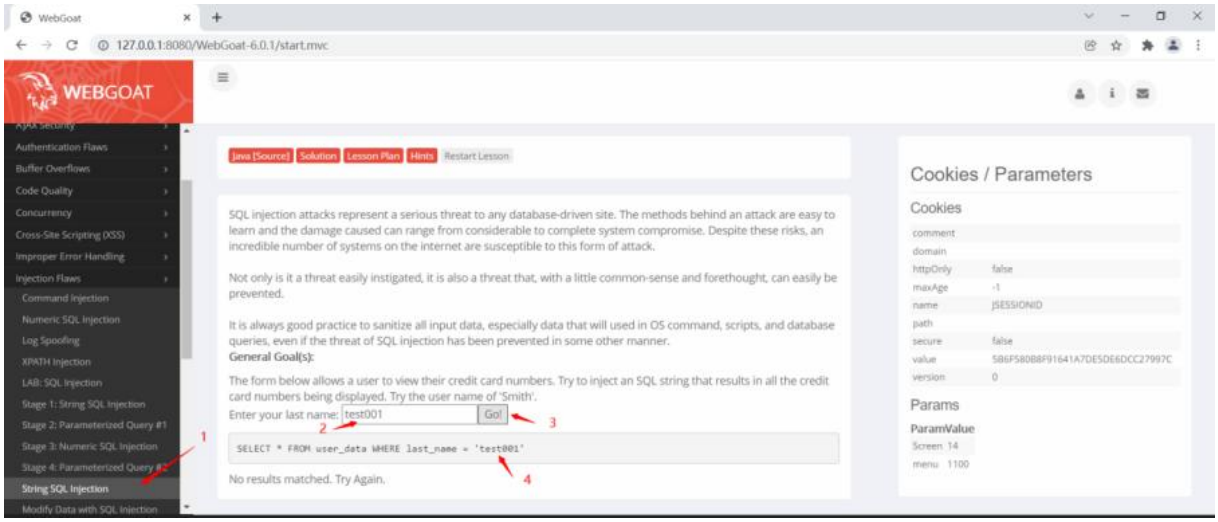


Figure 14 exploit SQL Injection in WebGoat

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

View Results

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:

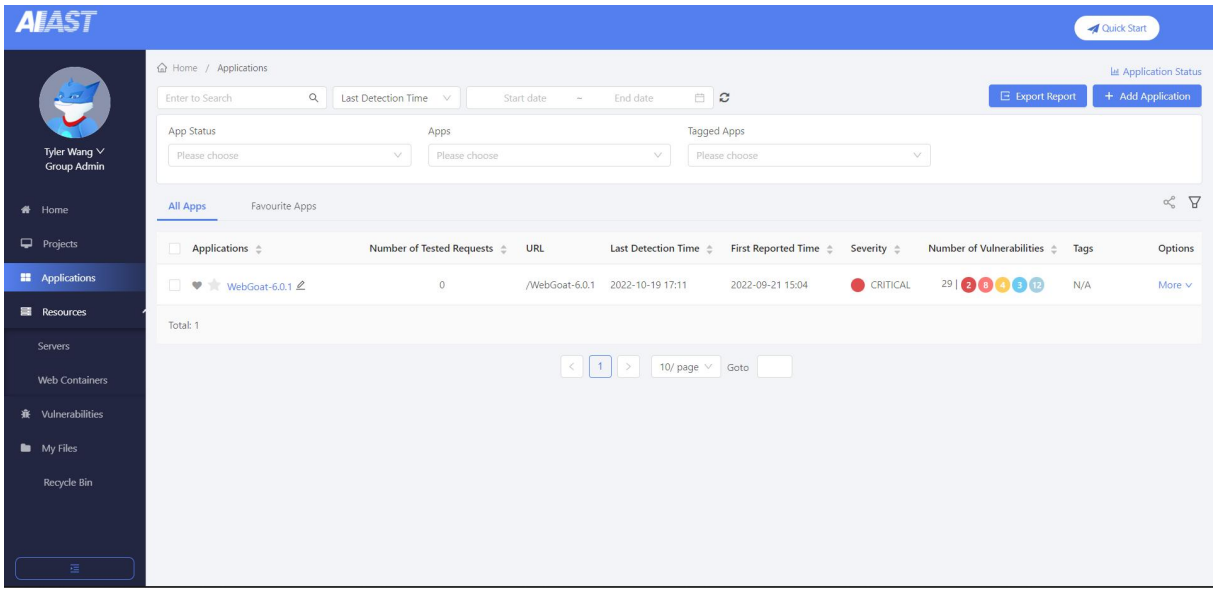


Figure 15 Cyber range’s Info

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

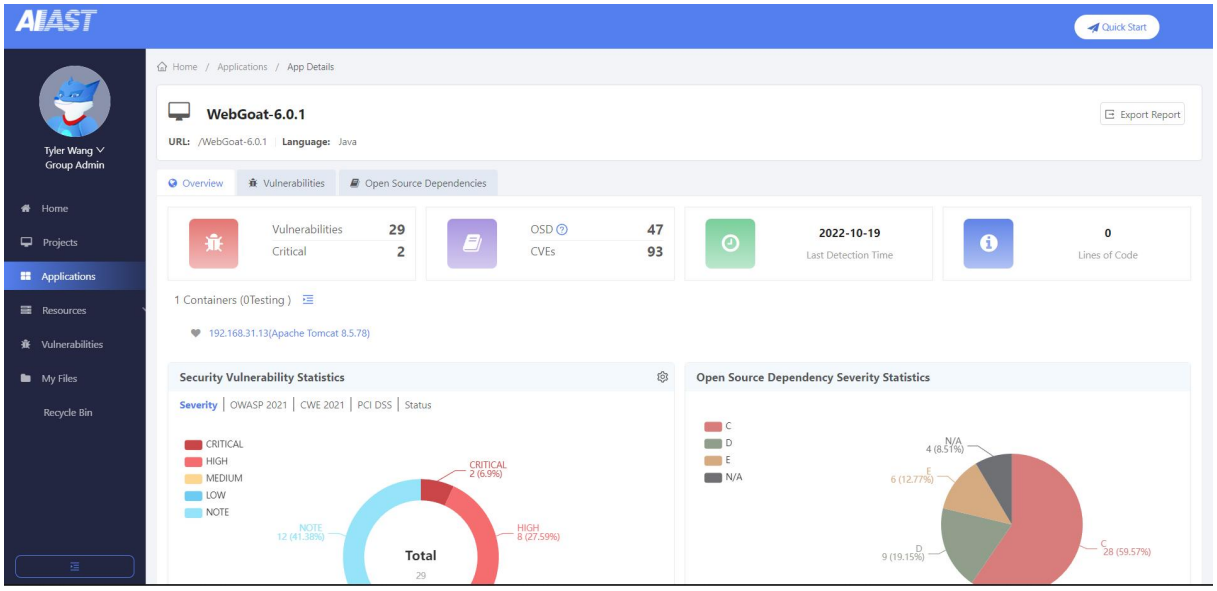


Figure 16 Application Overview

Click on the [Vulnerabilities]:

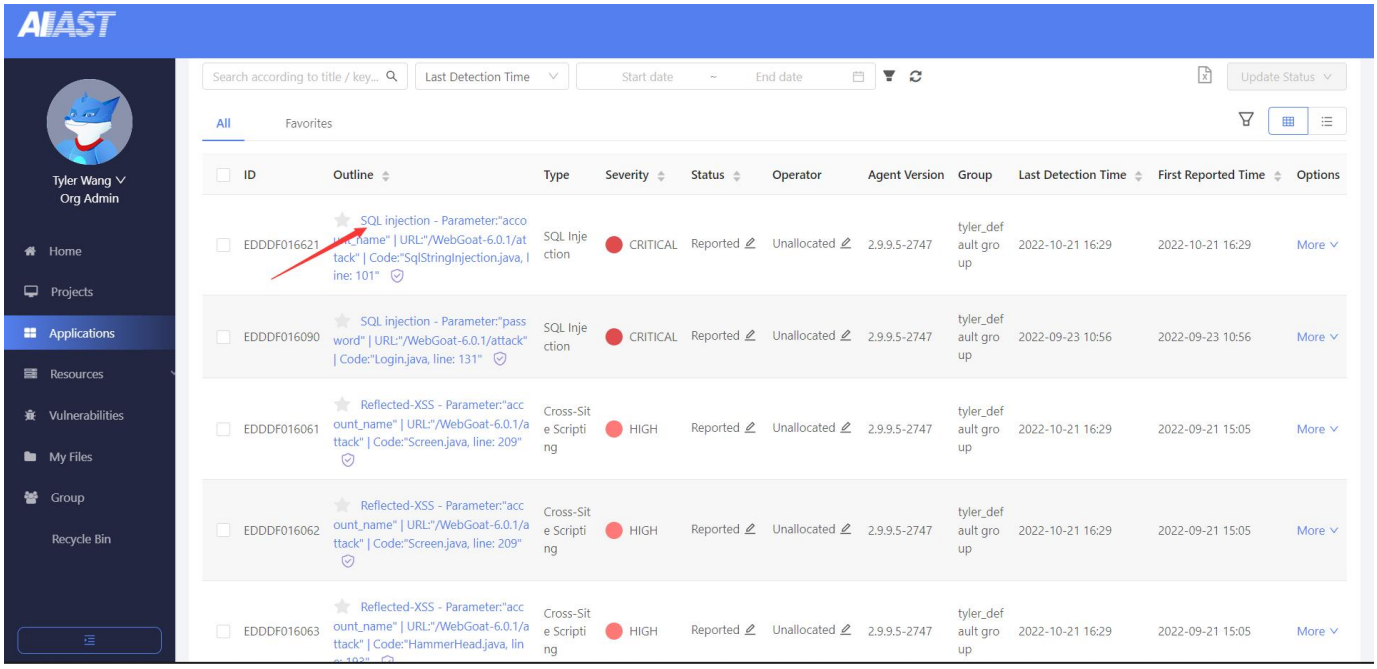


Figure 17 SQL Injection

Click on a specific vulnerability to view the data flow:

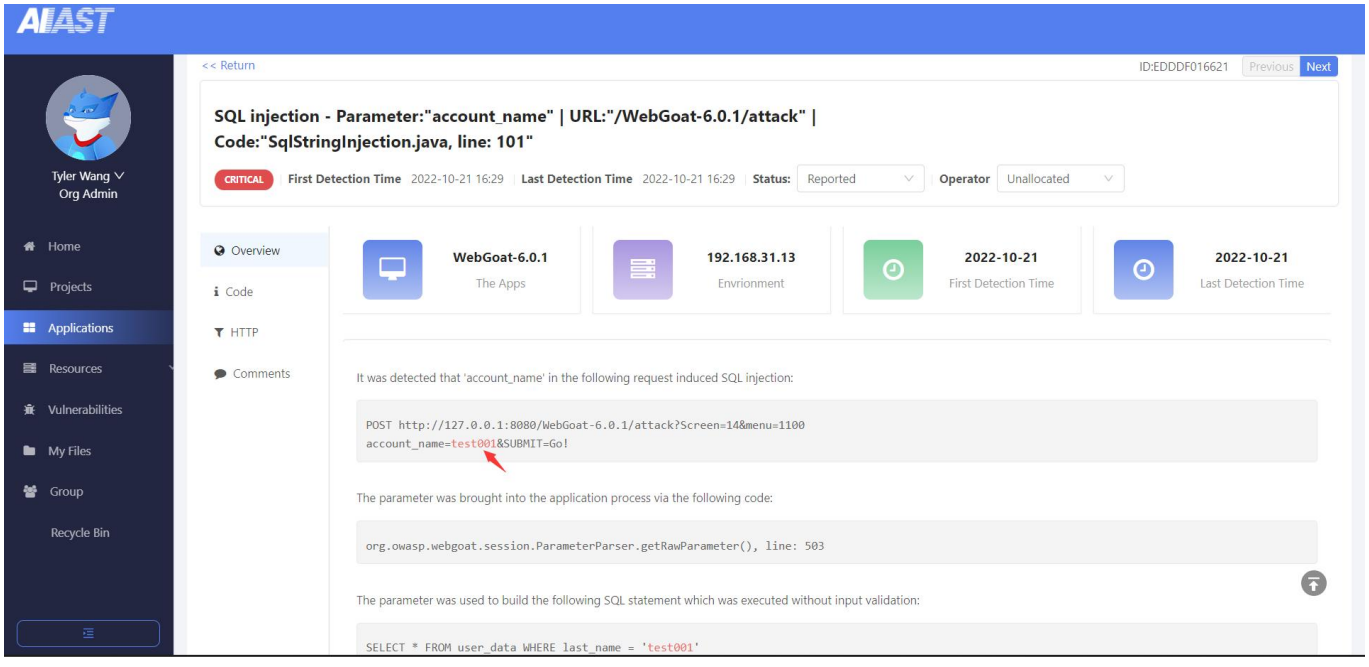


Figure 18 User Input is shown as below

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:

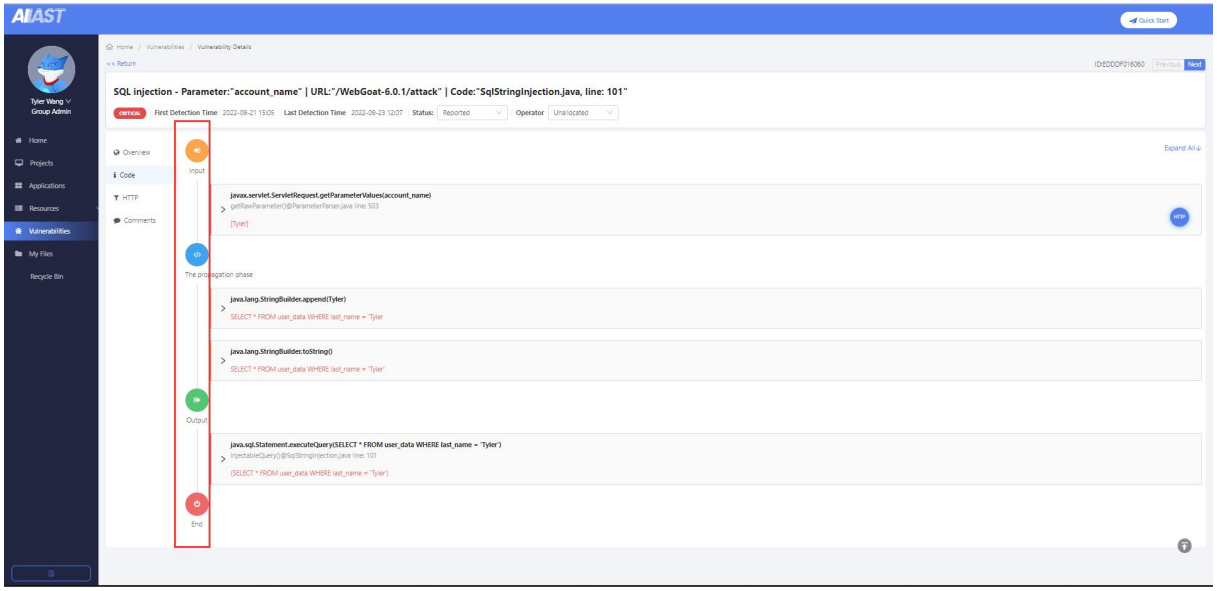


Figure 19 Taint propagation process

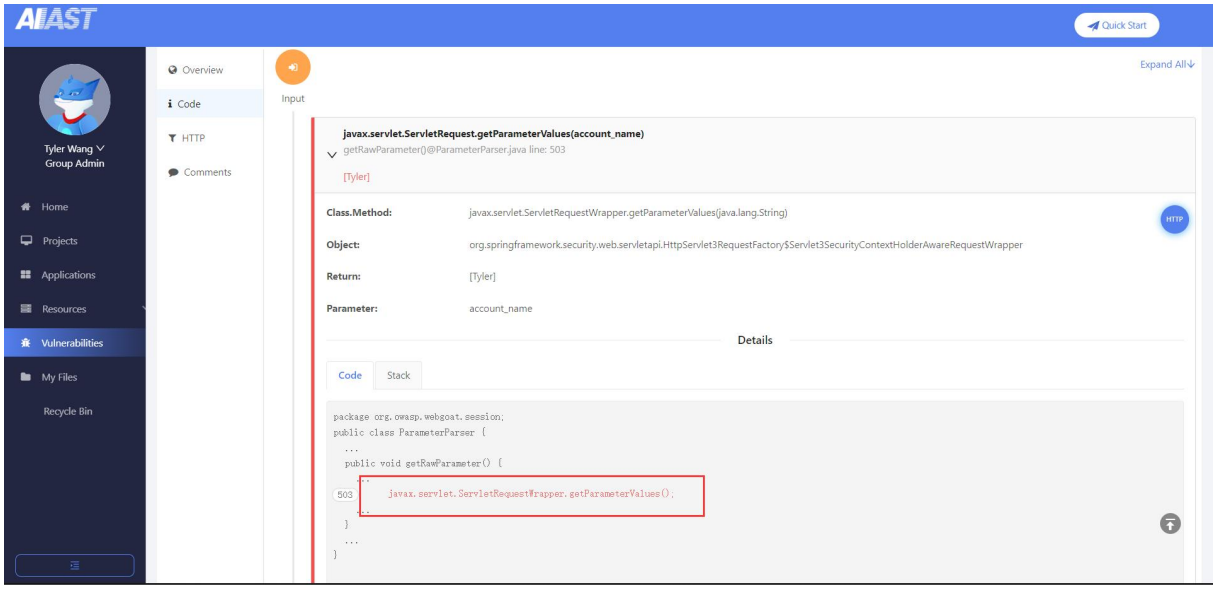


Figure 20 locate the vulnerability in specific code line

Export Report

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

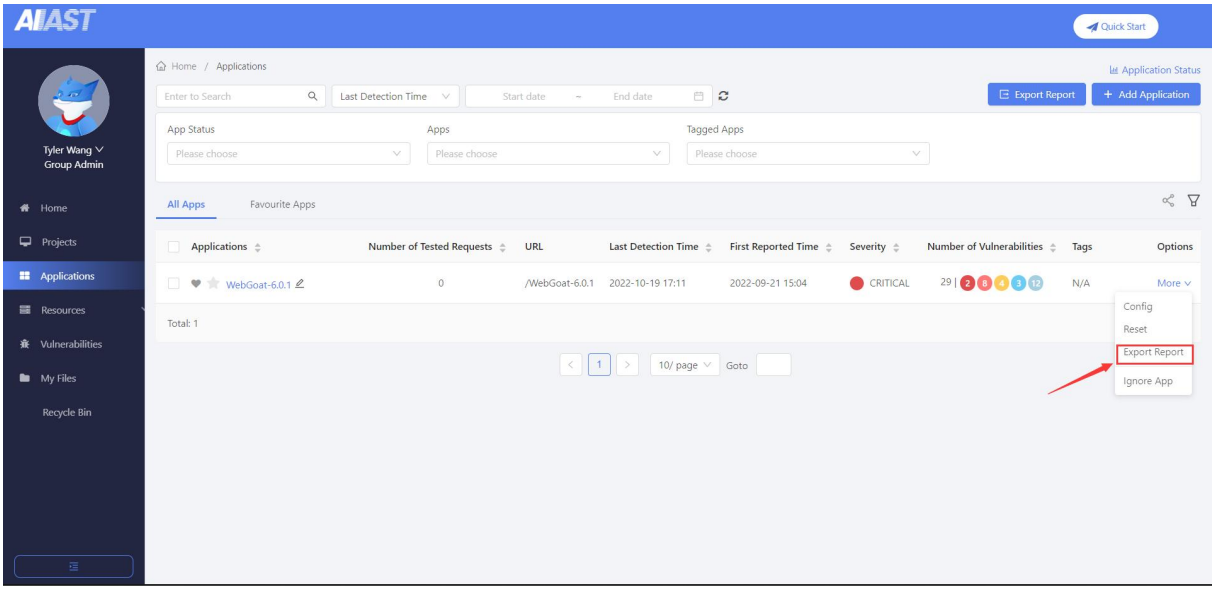


Figure 21 Export Report

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

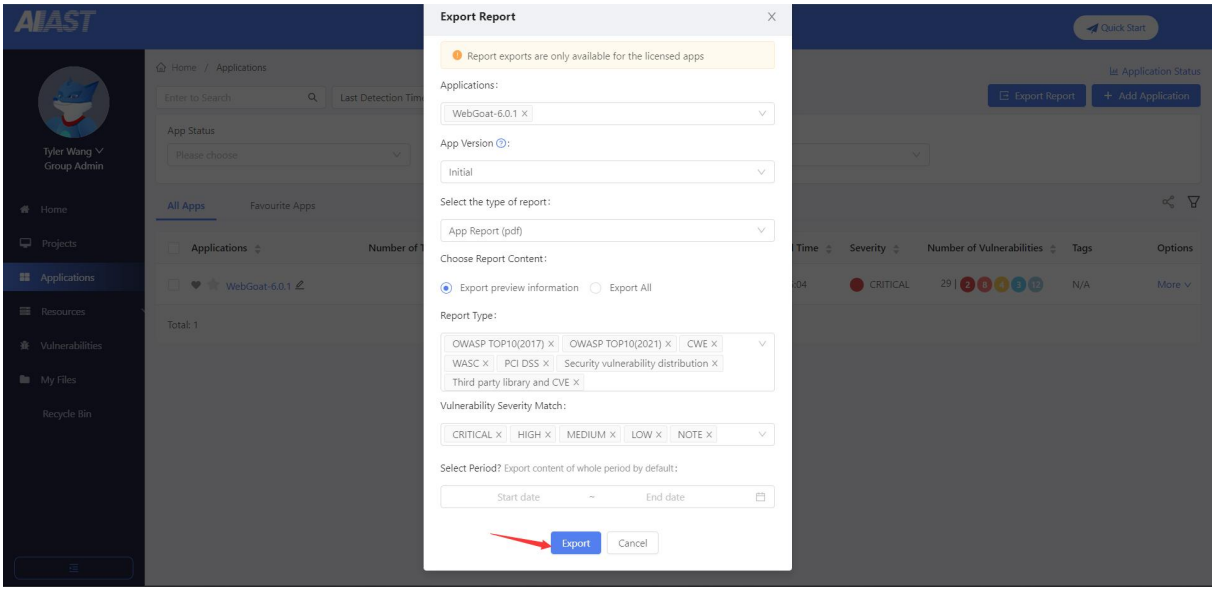


Figure 22 Select generated report to export

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

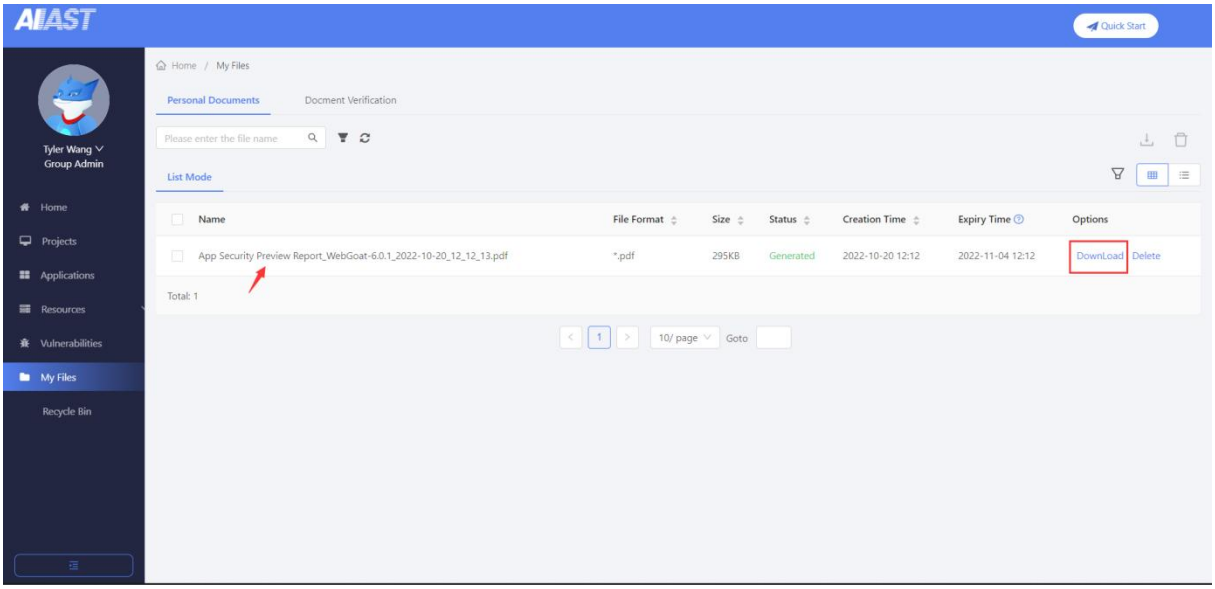


Figure 23 Report generated in [My Files]

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

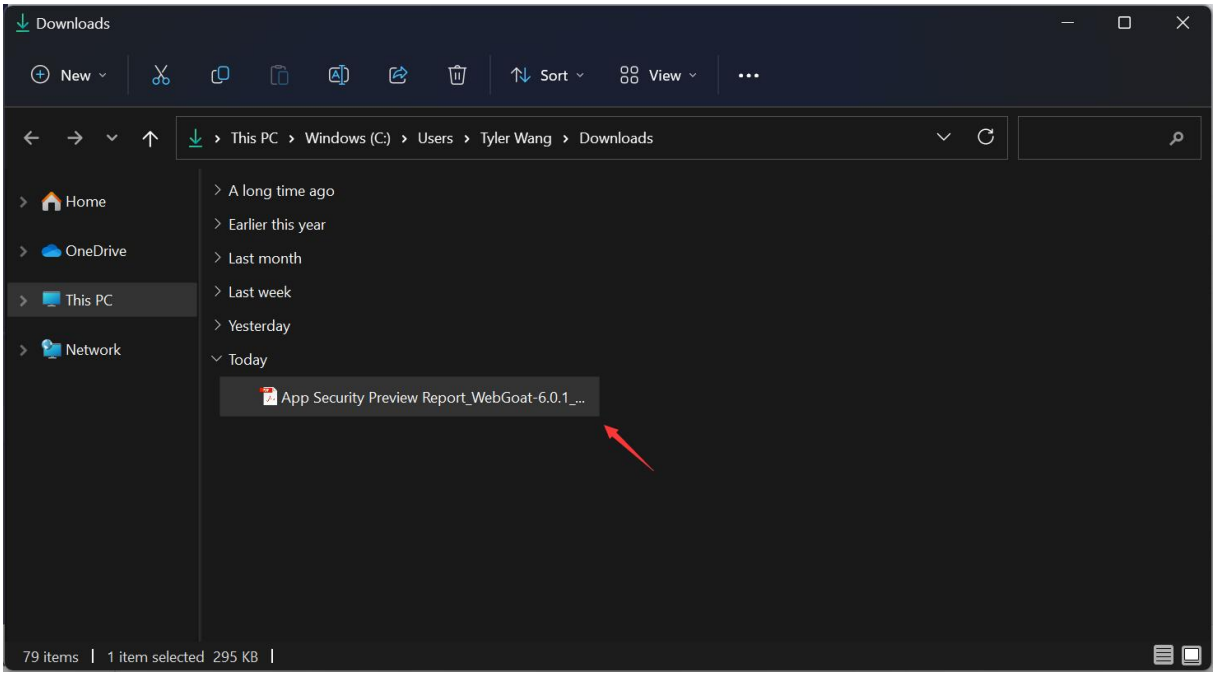


Figure 24 Downloaded Report

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.

AIAST | Technical Specifications

Supported language

Java

Node.js

C#/.NET

PHP

Python

Supported platform

Windows

Linux

MacOS

Unix like

Supported web server/application framework

Java

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

Node.js

- Express

.Net

- .NET Framework

.PHP

- Nginx
- Apache

About ZeroDay

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 ZeroDay, visit us online at www.zeroday.co.uk

160 The Edge, Clowes Street Salford, Manchester, M3 5NE
U.K.

Sales: + 44-16-1350-8028