

# Changes or new features - 8.3.25

- [Mainframe Analyzer](#)
  - Support for IMS MFS Maps
  - Improved support for JCL Dataset sub types
  - Rule documentation updates
- [SQL Analyzer embedded in AIP](#)
- [User Input Security](#)
  - Improved violation type coverage
  - Improvement to support for Apache Struts 2 applications
- [CAST Database Extractor](#)
- [CAST Storage Service/PostgreSQL admin](#)
  - [CSS Upgrade Wizard](#)
  - [CombinedTransfer.bat](#)
- [Miscellaneous](#)
- [CAST AIC Portal](#)
  - [CAST Management Studio - Create application option](#)



**Summary:** CAST AIP 8.3.25 introduces a number of features and changes as listed below.

## Mainframe Analyzer




### Support for IMS MFS Maps

Support has been implemented for **IMS MFS Maps** to improve [IMS/DC support](#) so that it is possible to find out which Cobol programs use an MFS Map:

- MFS Maps are contained in files with the extension \*.mfs.
- FMT macro defines the map (called "format" in IMS vocabulary).
- MSG macro defines MID and MOD messages. MID are those that have the INPUT type and MOD are those that have the OUTPUT type.
- MID and MOD identifiers are specified in the IO-PCB.
- In the MID/MOD structure, there is a field that contains the name of the transaction. This information allows the analyzer to create links between MFS Maps and transactions

As a result, some changes have been implemented:

- The [Mainframe Discoverer](#) will detect a project (and therefore automatically create an Analysis Unit) for each \*.mfs file discovered in a folder.
- \*.mfs files have been added to the list of files that will be automatically analyzed - see for example [Mainframe - Analysis configuration](#)
- New **object types** will be resolved - see [Mainframe - Analysis results](#):

	IMS Message Format Service
	IMS Message Input Descriptor
	IMS Message Output Descriptor

### Improved support for JCL Dataset sub types

The Mainframe Analyzer is now able to detect the following specific types of **JCL Dataset**, which will now be visible in CAST Enlighten, Architecture Checker and CAST Transaction Configuration. See [Mainframe - Technical notes](#) for more details.

- GDG datasets
- PDS datasets
- DBD datasets
- GSAM datasets
- VSAM datasets
- Temporary datasets

In addition, a new **prototype link** has been implemented between **DBD objects** and **JCL Datasets (DBD)**.

### Rule documentation updates

The documentation for the following rules has been updated

Rule ID	Description	Change
8468	Program semantic should respect the logic of flow execution	Rationale has been updated.

## SQL Analyzer embedded in AIP

The SQL Analyzer embedded in AIP now supports:

- (by reference) the analysis of databases hosted on:
  - **Microsoft SQL Server 2016, 2017 and 2019**, however no new syntax or features introduced in these newer releases are supported.
  - **Sybase ASE 16**, however no new syntax or features introduced in this newer release are supported.

## User Input Security

### Improved violation type coverage

The following new rules have been implemented:

Rule ID	CWE ID	Rule name	Input name	Target name	.NET support	JEE support
8482	79	Cross-site scripting through API requests	Network.readAPI	Network.write	NO	LIMITED
8484	113	HTTP response splitting through API requests	Network.readAPI	Network.http	NO	LIMITED
8486	99	Resource injection through API requests	Network.readAPI	Resource.write	NO	LIMITED
8488	99	Resource URL manipulation through API requests	Network.readAPI	Resource.writeURL	NO	LIMITED
8490	89	SQL injection through API requests	Network.readAPI	Database.write	NO	LIMITED
8492	90	LDAP injection through API requests	Network.readAPI	LDAP.filter	NO	LIMITED
8494	78	OS command injection through API requests	Network.readAPI	Runtime.exec	NO	LIMITED
8496	114	Process control through API requests	Network.readAPI	Runtime.load	NO	LIMITED
8498	78	Denial of service threat through API requests	Network.readAPI	Thread.sleep	NO	LIMITED
8500	94/95	Code injection through API requests	Network.readAPI	Script.eval	NO	LIMITED
8502	470	Reflection injection through API requests	Network.readAPI	Reflection.write	NO	LIMITED
8504	91	XPath injection through API requests	Network.readAPI	XPath.write	NO	LIMITED
8506	73	Path manipulation through API requests	Network.readAPI	File.open	NO	LIMITED
8508	117	Log forging through API requests	Network.readAPI	Log.write	NO	LIMITED
8510	134	Uncontrolled format string through API requests	Network.readAPI	String.format	NO	LIMITED
8512	501	Request parameters in session through API requests	Network.readAPI	Network.writeSession	NO	LIMITED
8514	89	NoSQL injection through API requests	Network.readAPI	Nosql.write	NO	LIMITED
8516	601	Open redirect through API requests	Network.readAPI	Network.redirect	NO	LIMITED

All of the above new rules are based on "injection through API requests" - the list of supported APIs is as follows:

- [javax.ws.rs-api-2.1](#)
- [jersey-client-1.19.4](#)
- [resteasy-client](#)
- [cxf-rt-frontend-jaxrs-2.7.18](#)
- [wink-client-1.4](#)
- [resthub-web-client-2.2.0](#)

### Improvement to support for Apache Struts 2 applications

The following truncated manglings are now supported:

- `com.opensymphony.xwork2.DefaultTextProvider.getText`
- `com.opensymphony.xwork2.ActionSupport.getText`
- `com.opensymphony.xwork2.validator.DelegatingValidatorContext.getText`
- `com.opensymphony.xwork2.CompositeTextProvider.getText`
- `com.opensymphony.xwork2.TextProviderSupport.getText`
- `com.opensymphony.xwork2.TextProvider.getText`

This is an improvement to "AIPCORE-1705 - User Input Security is now able to detect security violations in Apache Struts 2 applications" added in **CAST AIP 8.3.21**.

# CAST Database Extractor

The [CAST Database Extractor](#) now supports:

- (by reference) the extraction of databases hosted on:
  - **Microsoft SQL Server 2016, 2017 and 2019**, however the extractor will handle the databases as **Microsoft SQL Server 2014** databases and no new syntax or features introduced in these newer releases are supported.
  - **Sybase ASE 16**, however the extractor will handle the databases as **Sybase ASE 15.x** databases and no new syntax or features introduced in this newer release are supported.

# CAST Storage Service/PostgreSQL admin

## CSS Upgrade Wizard

The CSS Upgrade Wizard (CSSUpgrade.exe) used to move schemas from one CAST Storage Service/PostgreSQL instance to another is now deprecated.

## CombinedTransfer.bat

A new batch file called CombinedTransfer.bat has been created as a replacement for the CSS Upgrade Wizard. It is a wrapper batch file for the [CSS Backup and Restore Tools](#), provided as part of the **CAST AIP 8.3.x**, and involves a **fully automated process** of dumping the required schemas to file and then restoring the dumps on the new server. The CAST Storage Services/PostgreSQL do not need to be installed on the same host, and both can be remote to the machine on which you are executing the batch file.

The **CombinedTransfer.bat** batch file is located in the following folder and **must be executed from within the context of this folder**:

```
<CAST AIP installation>\CSSAdmin\CSSUpgrade\
```

See [CAST Storage Service - Moving existing schemas to new hosts](#) for more information.

# Miscellaneous

## CAST AIC Portal

[CAST AIC Portal](#) is now **deprecated** and official support for this web application will cease at the **end of 2020**. CAST encourages users to **switch** to [AIP Console](#) where possible.

## CAST Management Studio - Create application option

If you need to onboard new Applications and are not yet using [AIP Console](#) or are having issues using [CAST AIC Portal](#), then it is now possible to create new Applications directly in CAST Management Studio for all user audiences ("regular" through to "expert"). This is a "stop gap" solution until such time as you are ready to switch to AIP Console.

