**Security Scan Remediation for FAS**

Release 5.4

3/6/18

DHS Systems Engineering

Life Cycle

**Transportation Security Administration**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 3/6/18 | 1.0 | Initial Document | Tracy Ho |

Table of Contents

[1. Overview 4](#_Toc508266835)

[2. Details of different functionality 4](#_Toc508266836)

[2.1 Struts Upgrade 4](#_Toc508266837)

[2.2 JDK Upgrade 5](#_Toc508266838)

[2.3 Return Inactive IACMS STA associations 5](#_Toc508266839)

[2.4 Security-Related Fixes 10](#_Toc508266840)

[2.4.1 Configuration settings (CM-6) Body parameters accepted in query 10](#_Toc508266841)

[2.4.2 Input Validation Cross Site Forgery 10](#_Toc508266842)

[2.5 508 Compliance Related Fixes 10](#_Toc508266843)

[2.5.1 508 remediation – Keyboard accessibility 10](#_Toc508266844)

[2.5.2 508 remediation – Web form 11](#_Toc508266845)

# 

# **Overview**

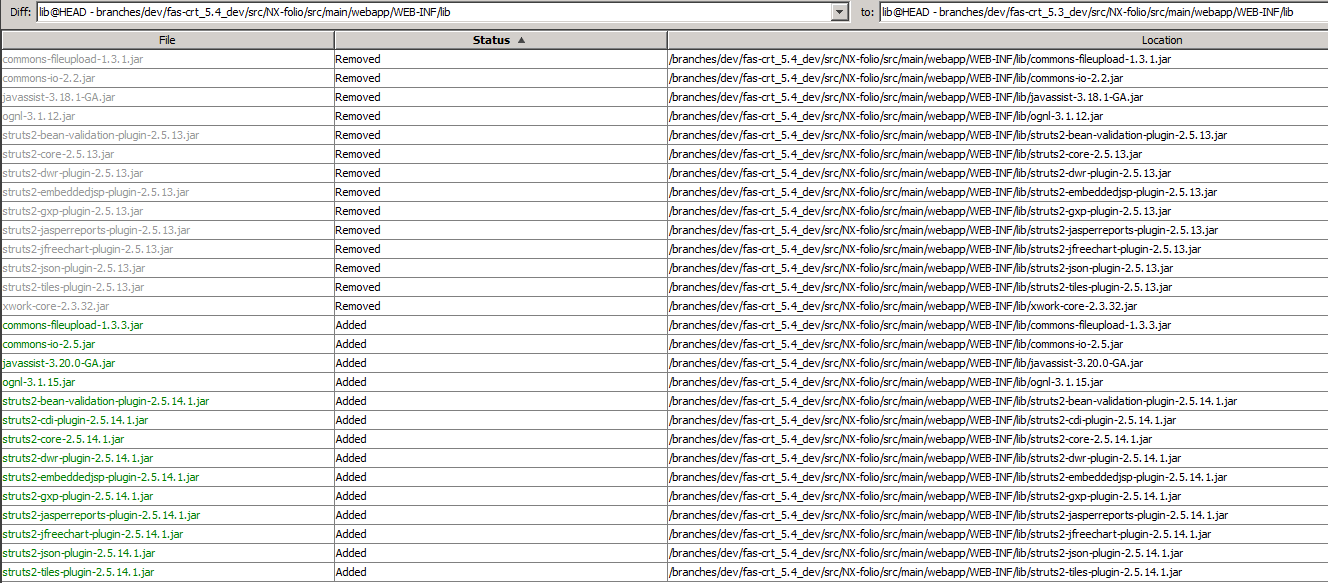
The purpose of this document is to describe the release highlights for FAS Release 5.4.

# Details of different functionality

## Struts Upgrade

*Finding:* To address security concerns, current version of Struts used in FAS needs to be upgraded to latest version 2.5.14.1

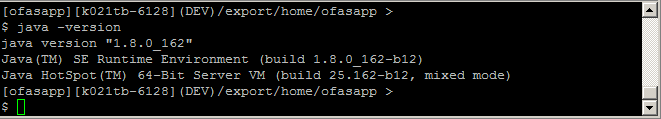
*Summary Description:* Removed all struts2 2.5.13 jar files and dependencies and upgraded to version struts2 2.5.14.1

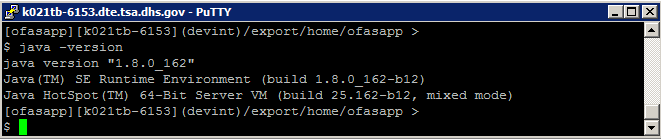


## JDK Upgrade

*Finding:* To address security concerns, current version of JDK used in FAS needs to be upgraded to latest version 8u162

*Summary Description:* JDK 8u162 are upgraded in both DEV servers

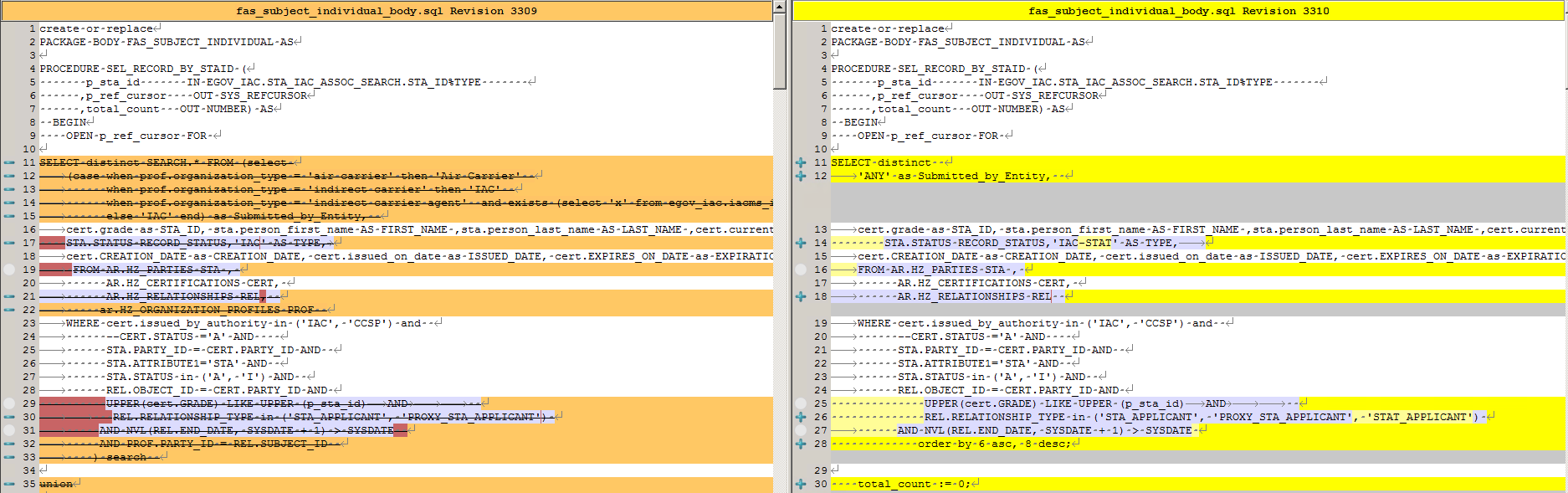


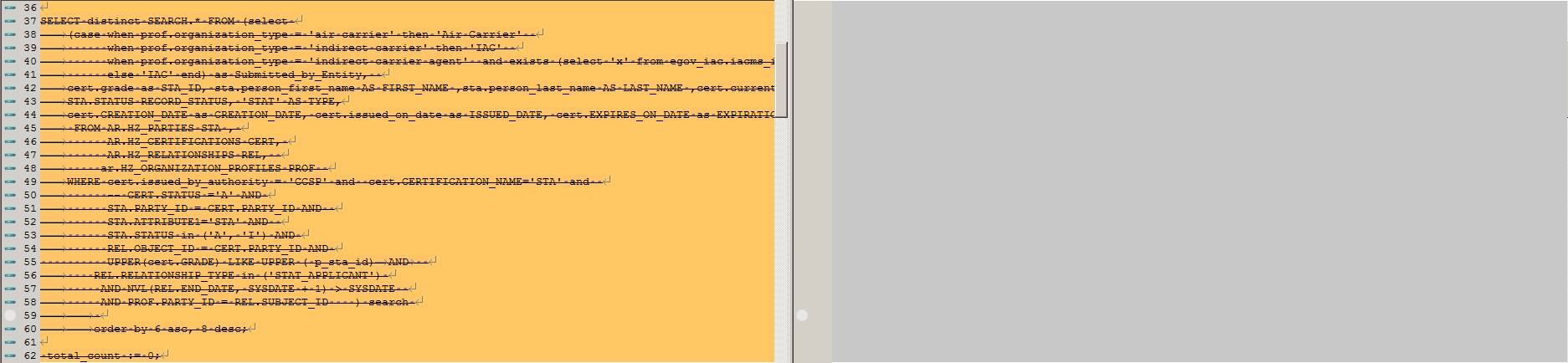


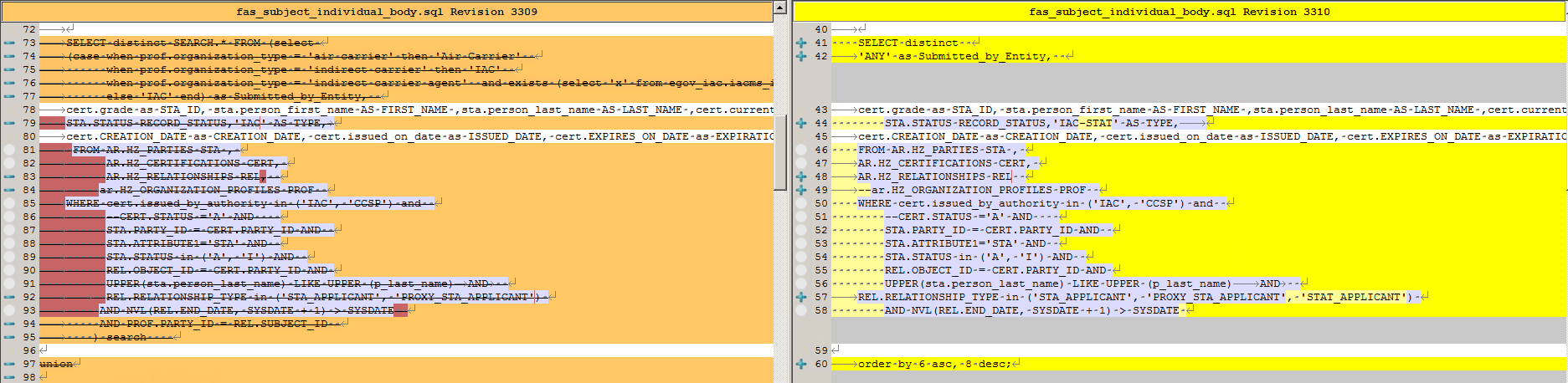
## Return Inactive IACMS STA associations

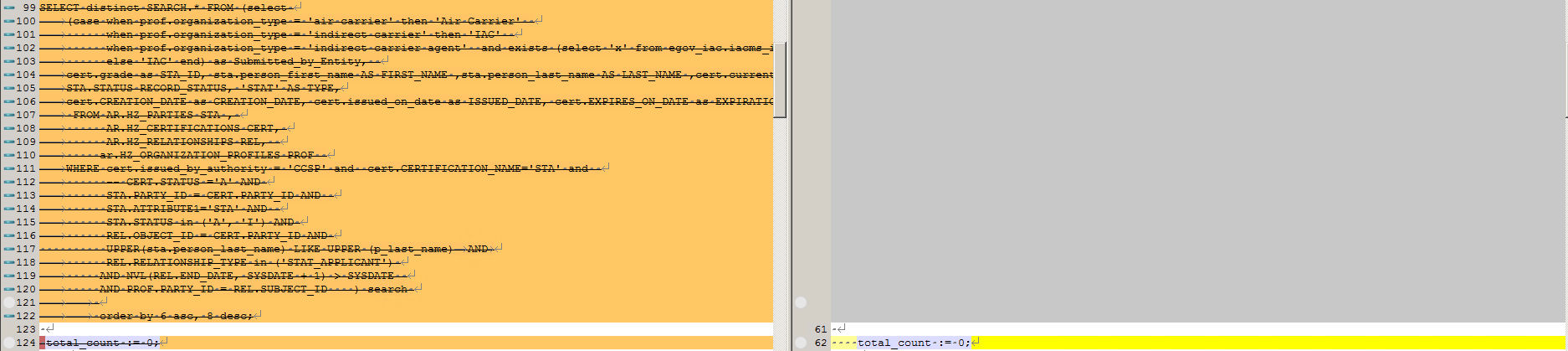
*Finding:* To address the inactive STA pulled issues.

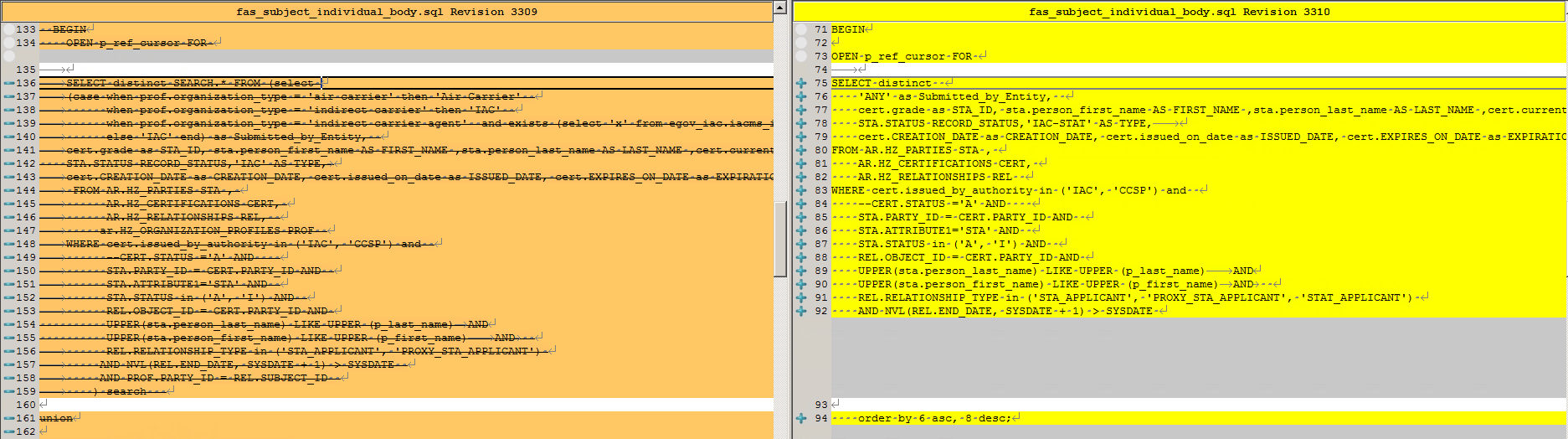
*Summary Description:* Tuned up the fas\_subject\_individual\_body.sql query

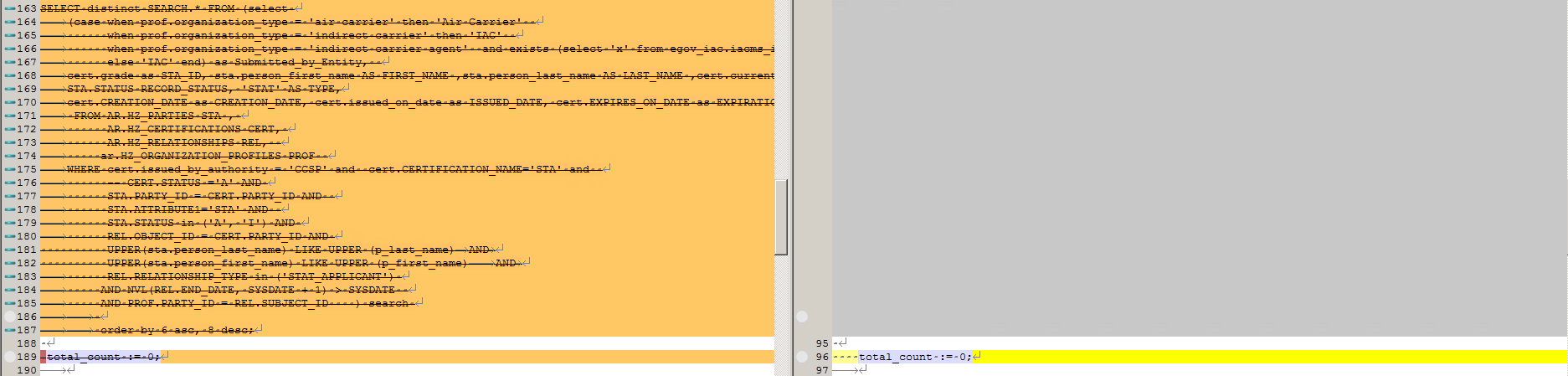


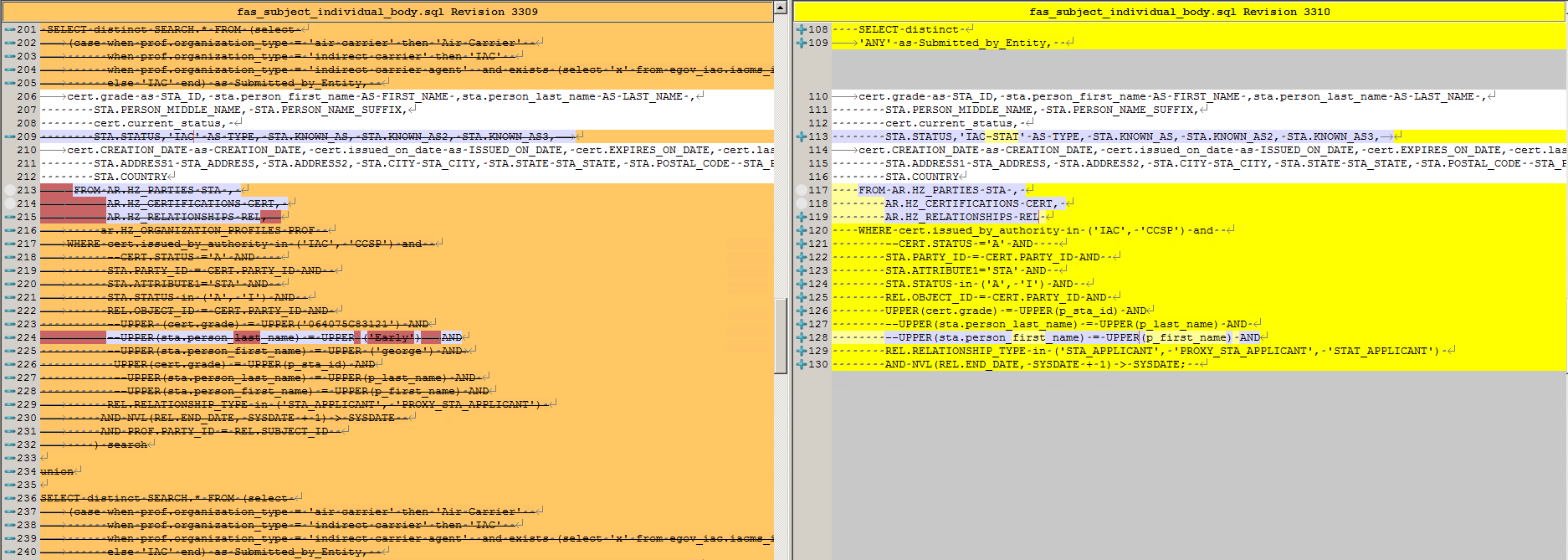


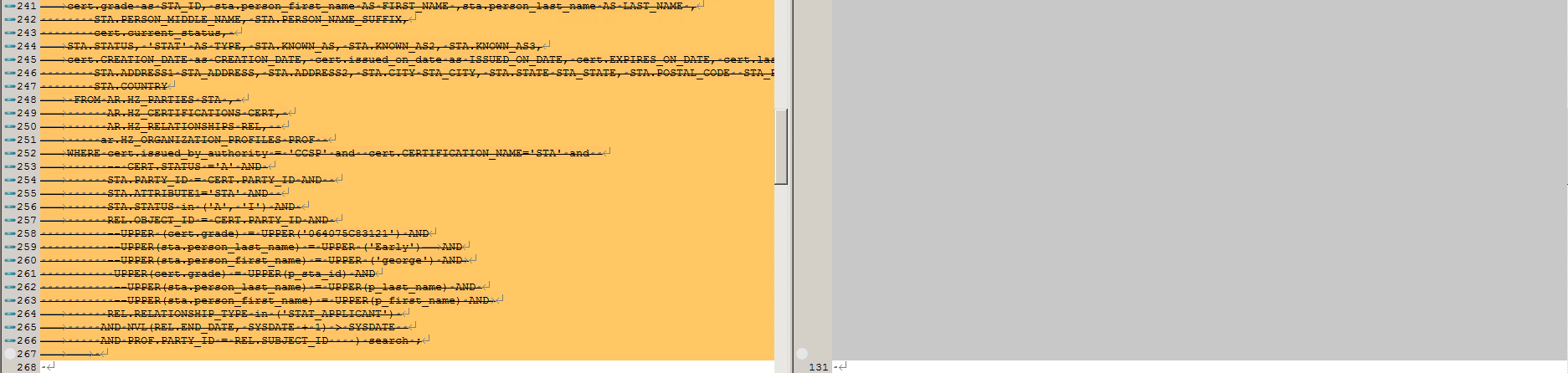










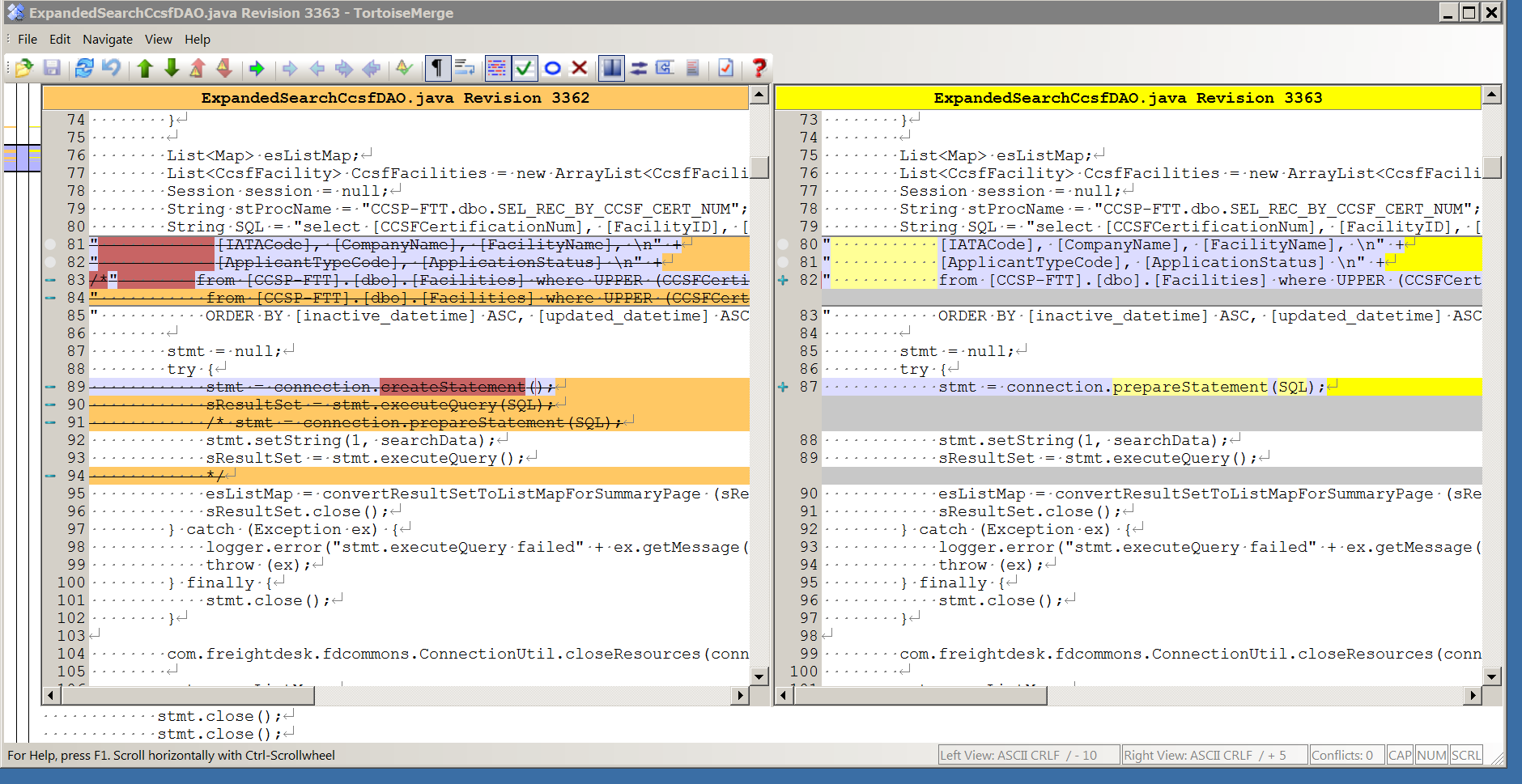


## Security-Related Fixes

### Configuration settings (CM-6) Body parameters accepted in query

*Finding*: Application processed body parameters that were submitted in the query.

*Summary Description:* Use prepareStatement instead of createStatement. The prepareStatement can bind the parameters to avoid the sql injection.



### Input Validation Cross Site Forgery

*Finding:* When remote requests are sent to your Apache web server, by default, some valuable information such as the web server version number, server operating system details, installed Apache modules plus more, are sent along in server-generated documents back to the client. This is a good deal of information for attackers to exploit vulnerabilities and gain access to your web server. To avoid showing Web server information, this information should be turned off or removed.

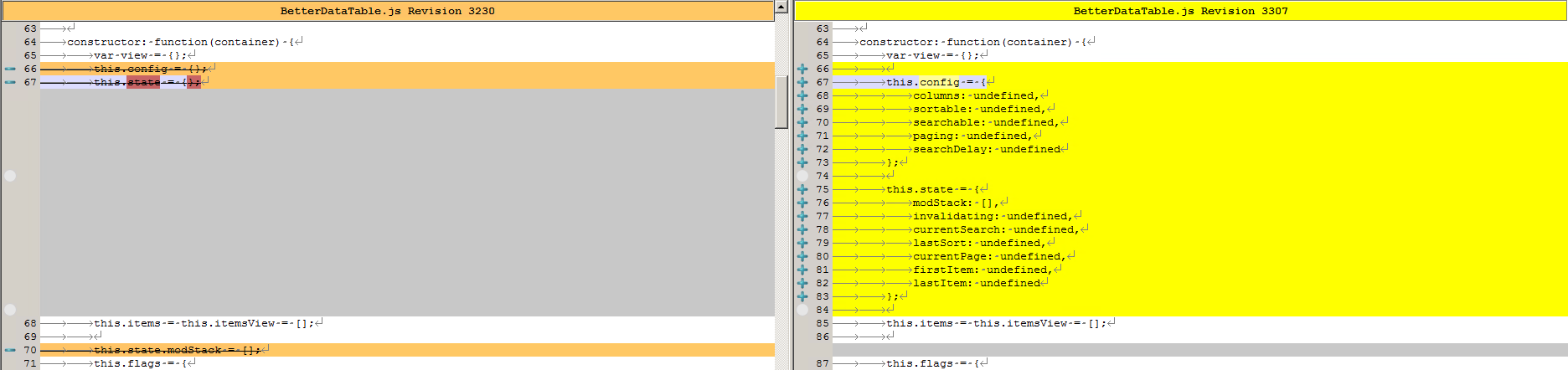
*Summary Description:* The standalone.xml file within JBoss server needs to be modified to turn off the ‘**X-Powered-By: JSP/2.2**’ displays by inserting the lines below

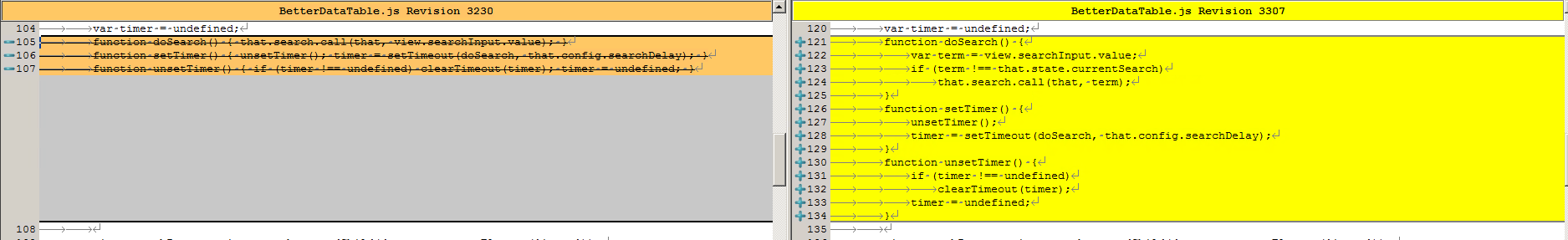
## 508 Compliance Related Fixes

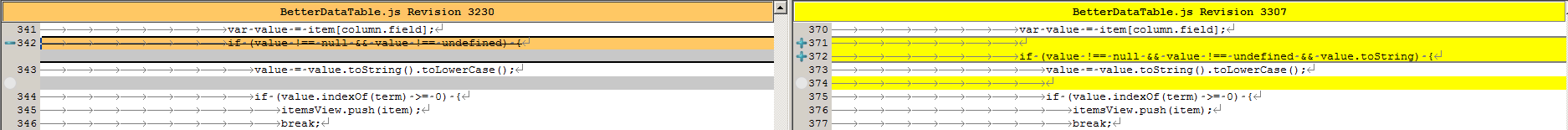
### 508 remediation – Keyboard accessibility

*Finding:* An interactive element or function cannot be accessed or activated by keyboard

*Summary Description:* Added scope=col and scope=row tags to <th> and <td> in all tables







### 508 remediation – Web form

*Finding:* Data table’s row or column headers have to be identified programmatically.

*Summary Description:* Added scope=col and scope=row tags to <th> and <td> in all tables