**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](#_Toc508804192)

[2. Details of different functionality 4](#_Toc508804193)

[2.1 Struts Upgrade 4](#_Toc508804194)

[2.2 JDK Upgrade 5](#_Toc508804195)

[2.3 Return Inactive IACMS STA associations 5](#_Toc508804196)

[2.4 Security-Related Fixes 10](#_Toc508804197)

[2.4.1 Configuration settings (CM-6) Body parameters accepted in query 10](#_Toc508804198)

[2.4.2 Input Validation Cross Site Forgery 11](#_Toc508804199)

[2.5 508 Compliance Related Fixes 12](#_Toc508804200)

[2.5.1 508 remediation – Keyboard accessibility 12](#_Toc508804201)

[2.5.2 508 remediation – Web form 13](#_Toc508804202)

# 

# **Overview**

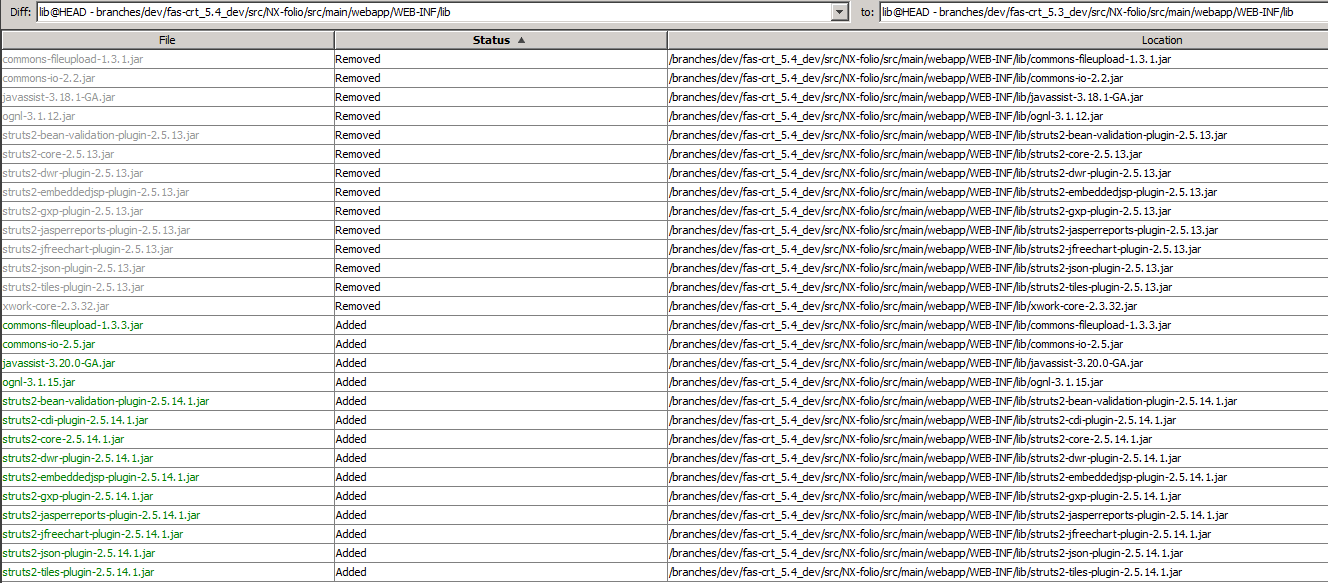
The purpose of this document is to describe the release highlights for FAS Release 5.4.

# 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

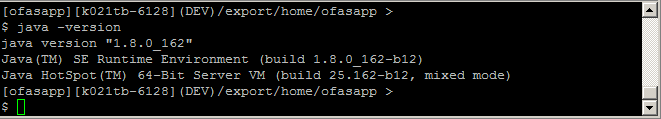
*Summary Description:* Removed all struts2 2.5.13 jar files and dependencies and upgraded to version struts2 2.5.14.1

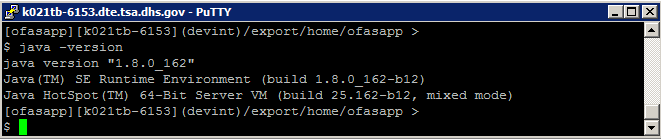


## JDK Upgrade

*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

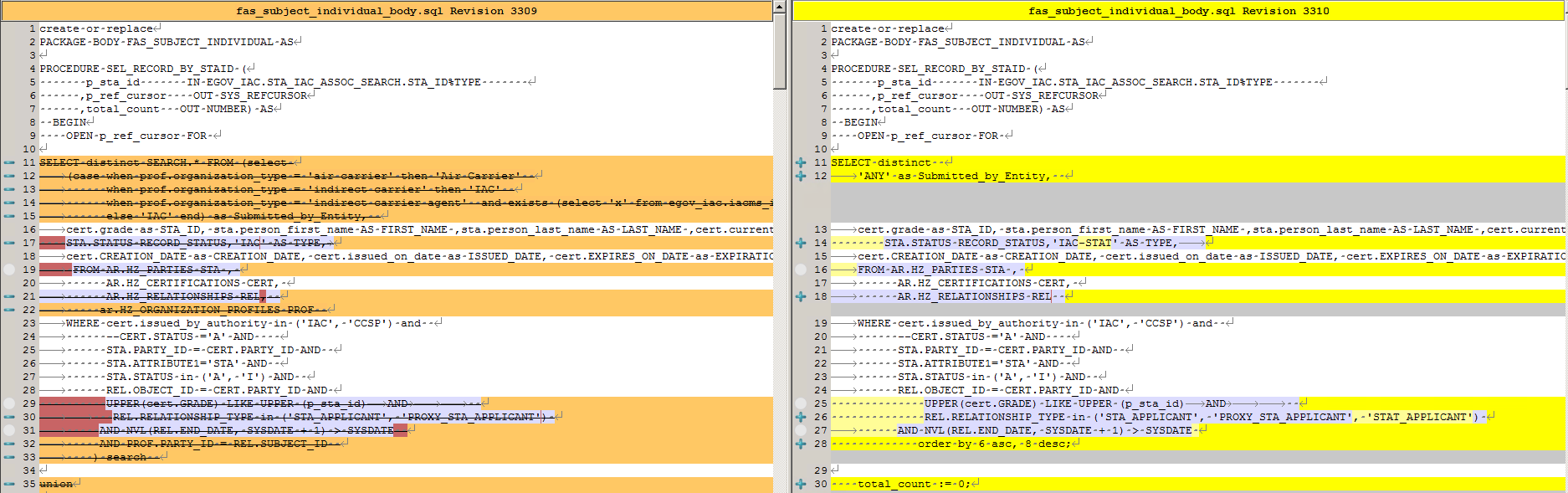


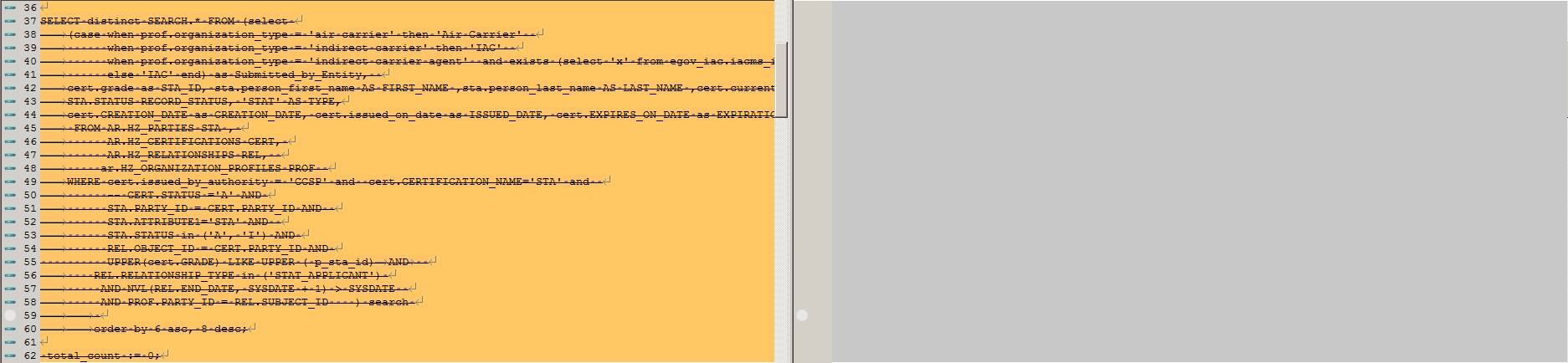


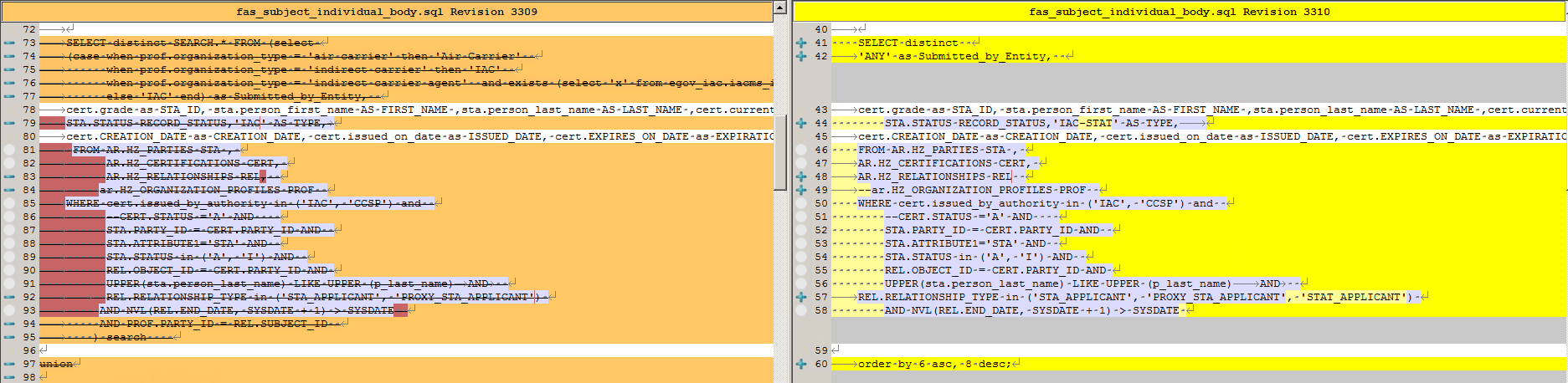
## Return Inactive IACMS STA associations

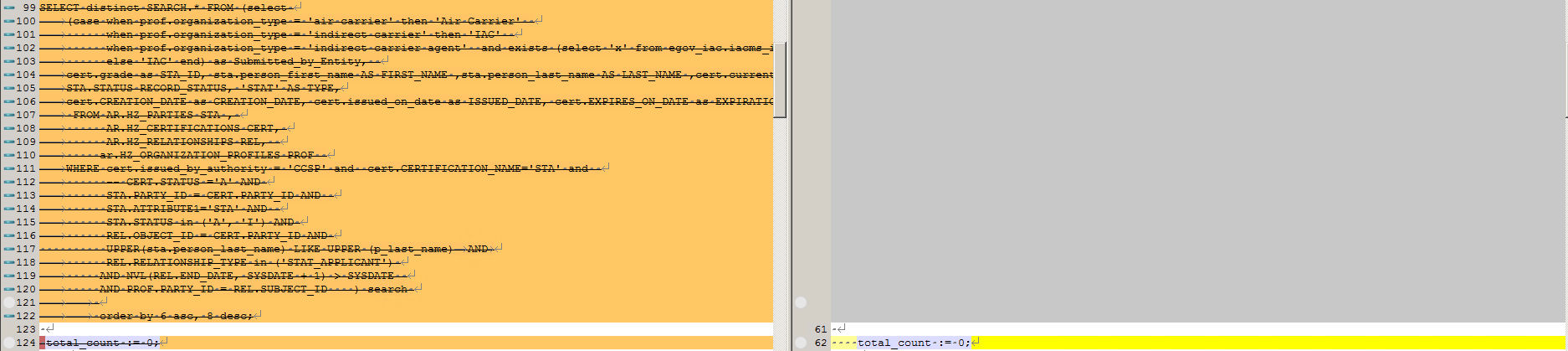
*Finding:* To address the inactive STA pulled issues.

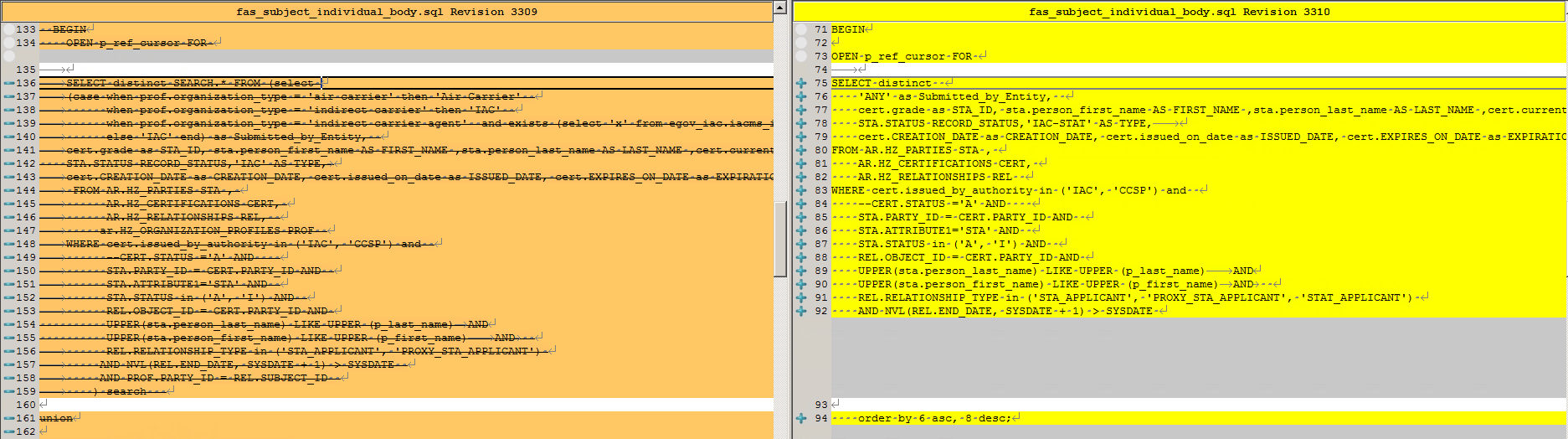
*Summary Description:* Tuned up the fas\_subject\_individual\_body.sql query

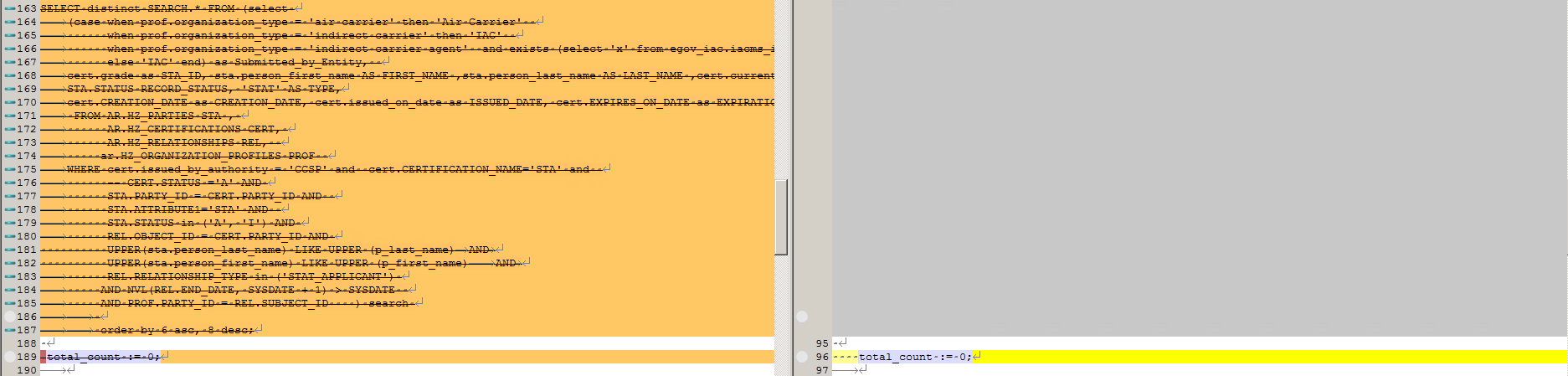


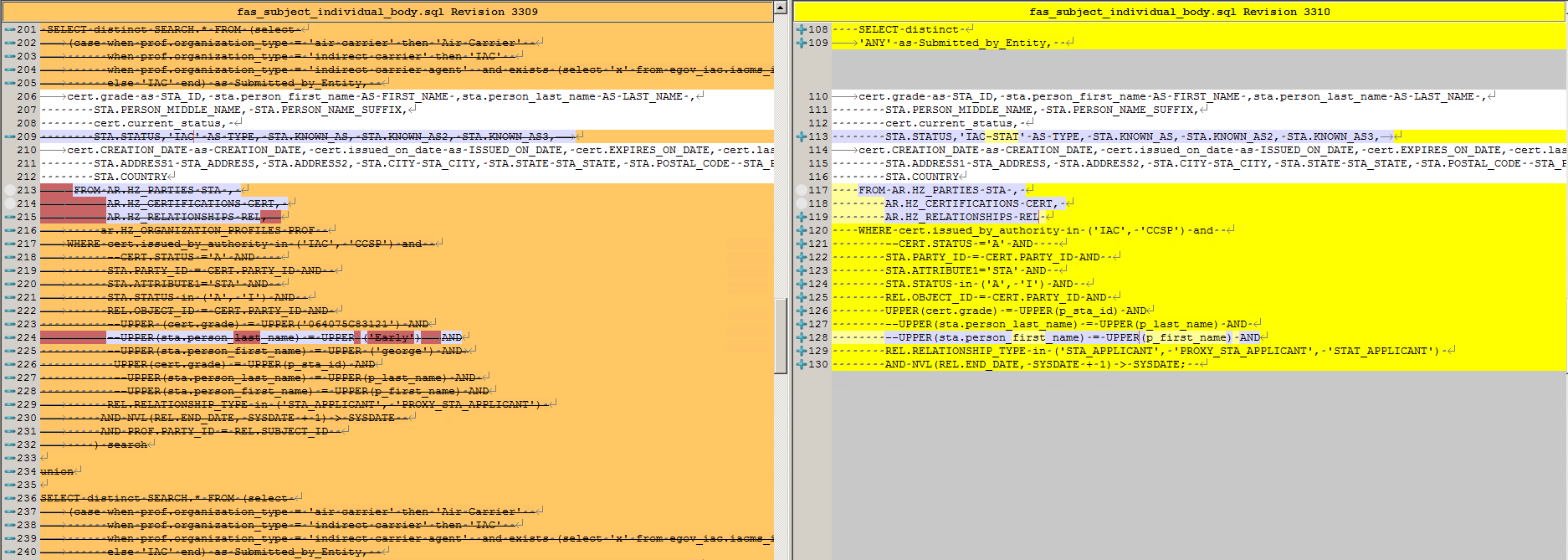


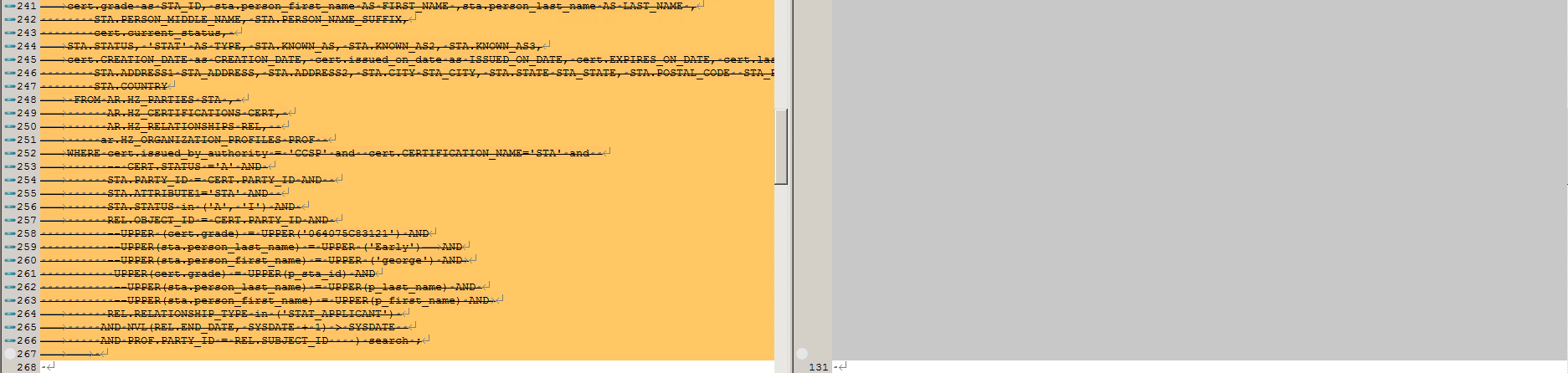










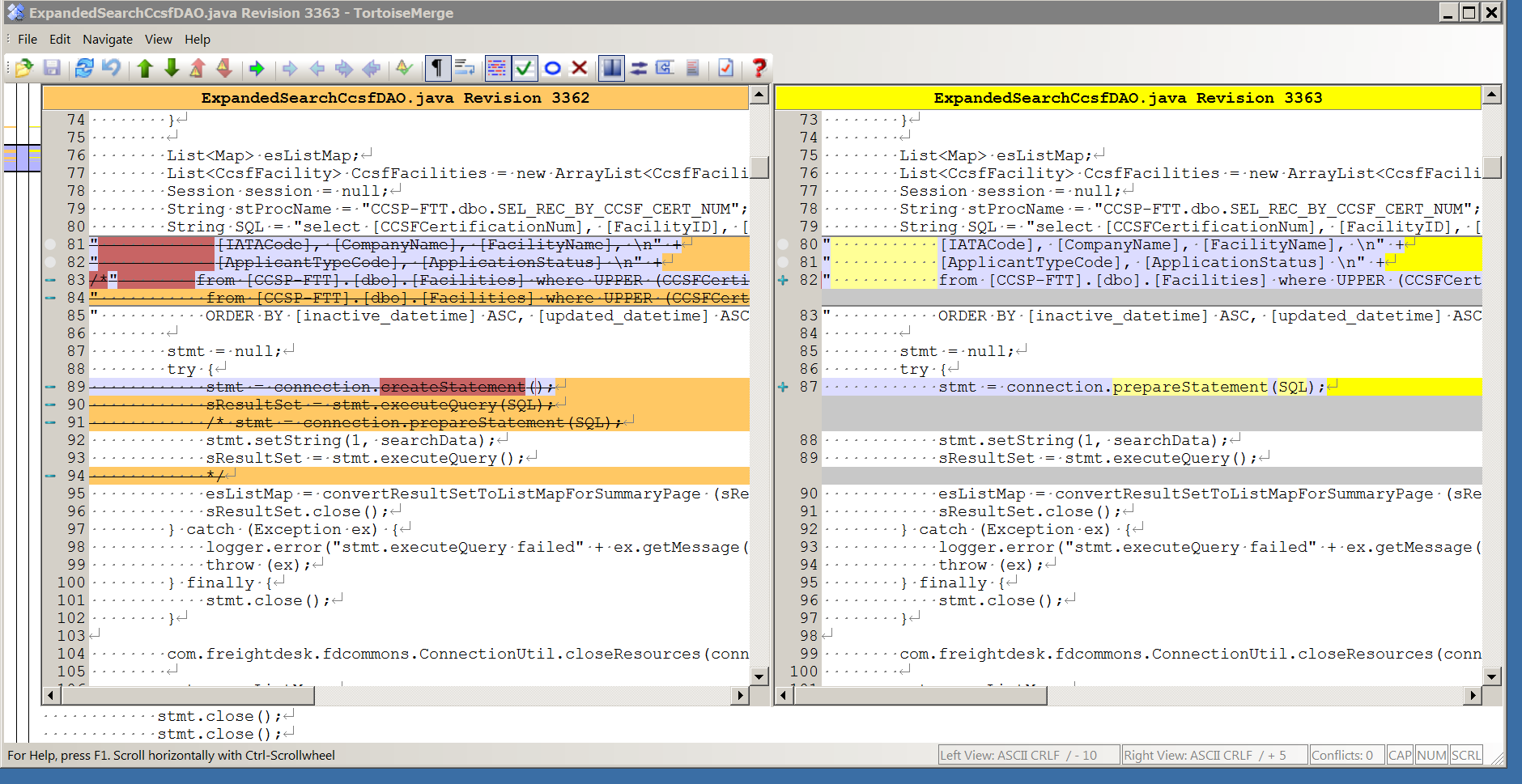


## Security-Related Fixes

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

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

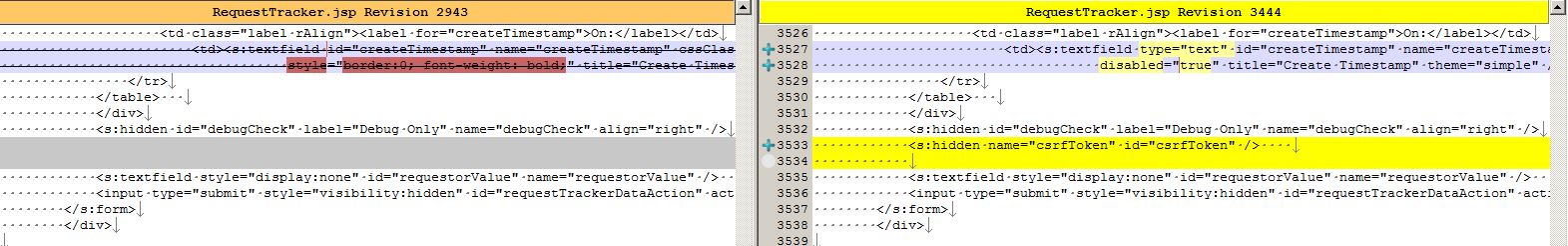
*Summary Description:* Use prepareStatement instead of createStatement. The prepareStatement can bind the parameters to avoid the sql injection.

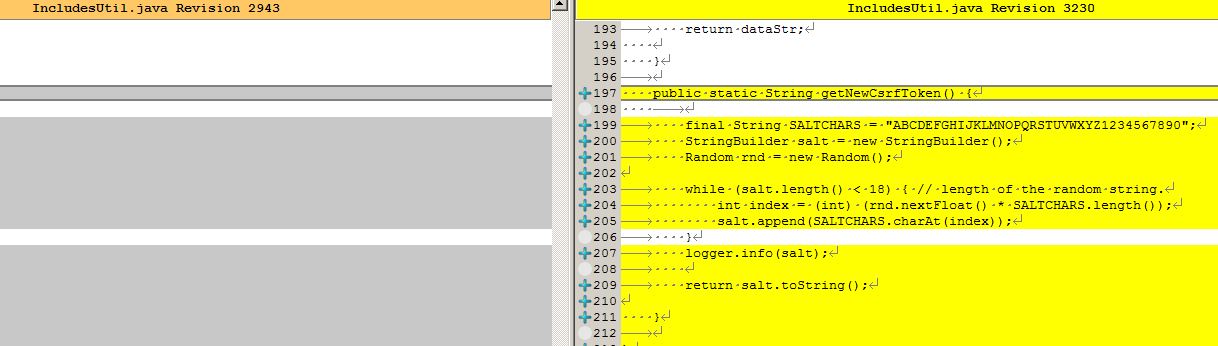


### Input Validation Cross Site Forgery

*Finding:* Cross-site request forgery (CSRF) is a type of website exploit carried out by issuing unauthorized commands from a trusted website user. CSRF exploits a website’s trust for a particular user's browser, as opposed to cross-site scripting, which exploits the user’s trust for a website. This term is also known as session riding or a one-click attack.

*Summary Description:* The predefined CSRF\_TOKEN value is validated in the vulnerable code to ensure the inputs are originated from legitimate pages.



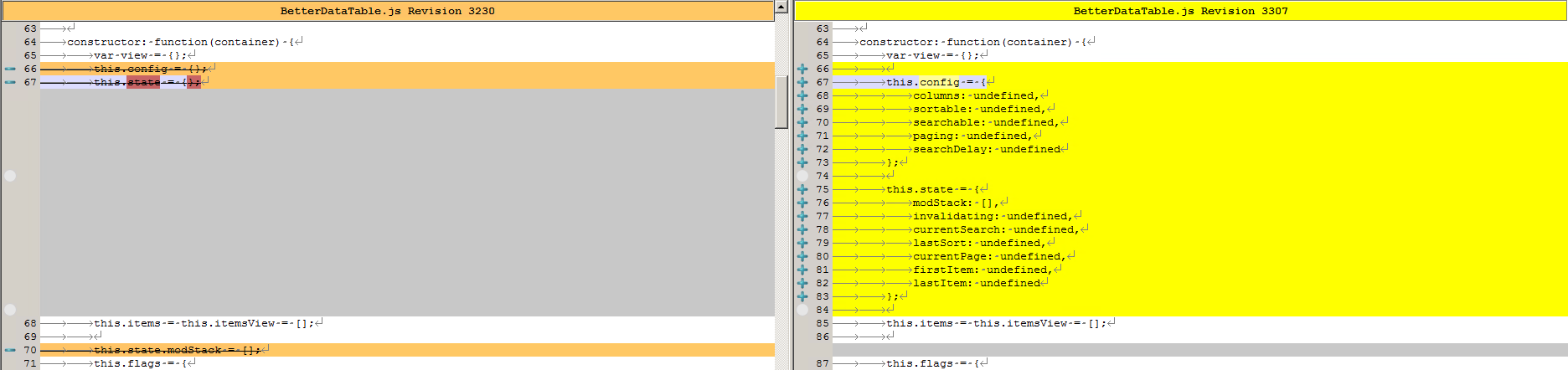


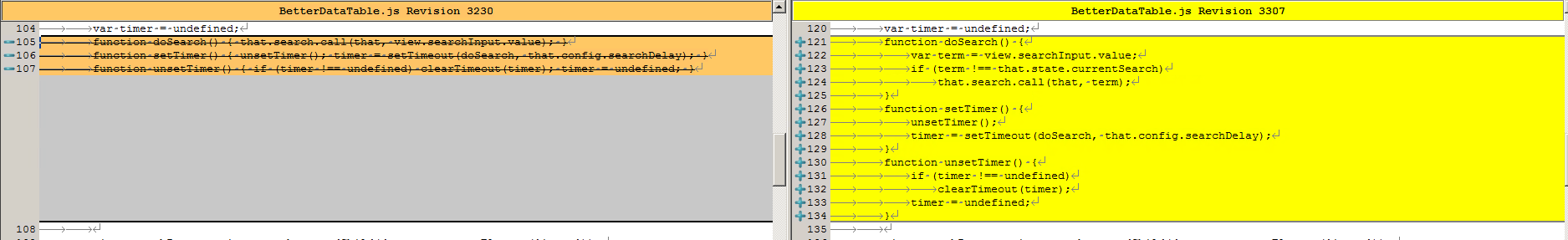
## 508 Compliance Related Fixes

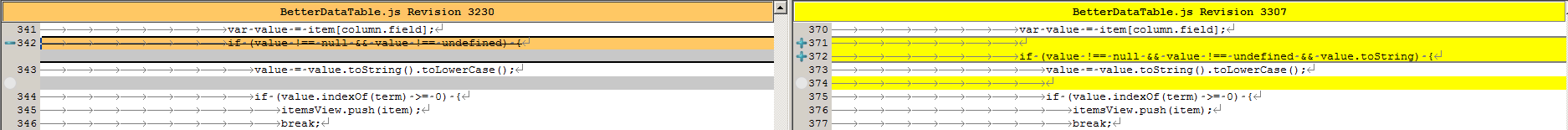
### 508 remediation – Keyboard accessibility

*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