



OFFICE OF THE SENIOR VICE PRESIDENT –  
BUSINESS AND FINANCE

OFFICE OF THE PRESIDENT  
1111 Franklin Street  
Oakland, California 94607-5200

September 19, 2008

BEATRICE CARDONA  
WEN TANG

BARBARA VANDEN BORRE  
SUNGSOO YANG

Re:	Release:	1837
	Error Reports:	2180
	Programs:	None
	Copy Members:	None
	Include Members:	None
	DDL Members:	None
	Bind Members:	None
	CICS Maps:	None
	CICS Help:	None
	Forms:	None
	Table Updates:	None
	Java Access Beans:	None
	Java Display Beans:	None
	Java Event Handlers:	MainMenuHandler.java, RosterHandler.java
	Java Parameters:	None
	JavaScript:	None
	Web Pages:	DisplayCbuc.jsp, DisplayPerfEvalCodes.jsp, DisplayRangeRateTable.jsp, DisplayStatusCode.jsp, DisplayStepRateTable.jsp, DisplaySubLoc.jsp, Error.jsp, MeritMenu.jsp, SendMail.jsp
	Urgency:	Urgent (see Timing of Installation below)

This release addresses the following Error Report:

**Error Report 2180**

UCLA identified that a malicious user can enter special characters into a URL string of Web Merit system to perform SQL Injection and Cross-Site Scripting.

The following security-related enhancements are needed to the Web Merit online application:

1. Prevent direct access to the files in the web content section of Web Merit system.
2. Display the “failed attempt” message, if userid or sessionid or authid is changed in the main menu URL.

## **Java Event Handlers**

### **RosterHandler.java**

RosterHandler.java is the Event handler program for the roster related events.

It was modified to check the http session to stop direct invocation of the following JSP pages without a proper login:

- Range based download JSP page - RosterRangeBasedDownload.jsp
- Step based download JSP page - RosterStepBasedDownload.jsp

### **MainMenuHandler.java**

MainMenuHandler.java is the Event handler program for the main menu related events. When this event handler is called first time, User Id, Session Id, and Auth Id from the input query string are stored in the session attributes.

It was modified to disallow change of User Id or Session Id or Auth Id in the input query string, if the session values are established.

## **Web Pages**

### **DisplayCbuc.jsp**

This is the web page for the CBUC display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplayCbuc.jsp page.

### **DisplayPerfEvalCodes.jsp**

This is the web page for the performance evaluation codes display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplayPerfEvalCodes.jsp page.

### **DisplayRangeRateTable.jsp**

This is the web page for the range rate table display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplayRangeRateTable.jsp page.

### **DisplayStatusCode.jsp**

This is the web page for the status codes display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplayStatusCode.jsp page.

### **DisplayStepRateTable.jsp**

This is the web page for the step rate table display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplayStepRateTable.jsp page.

#### DisplaySubLoc.jsp

This is the web page for the sub location display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of DisplaySubLoc.jsp page.

#### Error.jsp

This is the web page for the error display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of Error.jsp page.

#### MeritMenu.jsp

This is the web page for the merit menu display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of MeritMenu.jsp page.

#### SendMail.jsp

This is the web page for the send mail status display.

It was modified to include CheckSession.include method that checks http session for a valid login to stop direct invocation of SendMail.jsp page.

#### **Installation Instructions**

Download and install the .ear or .war file from the release dataset PAYDIST.R1837.MERITEAR or MERITWAR using binary FTP. For details on installation, please see the documentation for releases 1485 and 1668.

#### **Test Plan**

On the Merit Menu page, use the "view source" option of your browser to confirm that the release 1837 version of the application has been installed.

#### **Timing of Installation**

The timing of this release is **urgent**. Installing this release is critical because by performing SQL Injection and Cross-Site Scripting, a malicious user can get into the Web Merit system and manipulate the merit database.

As usual, campuses are encouraged to install this release in as timely a fashion as possible and in the normal numeric sequence.

If there are any questions, please send electronic mail to baskar.chitravel@ucop.edu, or call 510-987-0692.

Baskar Chitravel