



OFFICE OF THE SENIOR VICE PRESIDENT –
BUSINESS AND FINANCE

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

December 9, 2009

BEATRICE CARDONA
WEN TANG

BARBARA VANDEN BORRE

Re: Release: 1894
Error Reports: 2235
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 Classes: AdminCycleUpdate.java, ARSMAccessBean.java, BaseDataAccessBean.java,
CycleIdDetailAccessBean.java, RosterEmpDetAccessBean.java,
RosterHandler.java
Web Pages: FAQ.html
Urgency: Urgent (see Timing of Installation below)

This release addresses the following Error Report:

Error Report 2235

An automated security scan identified SQL injection vulnerabilities in the web merit application.

Java Classes

AdminCycleUpdate.java

AdminCycleUpdate.java is the event handler for cycle id maintenance events for the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

ARSMAccessBean.java

ARSMAccessBean.java invokes the ARSM (Application Resources Security Manager) security rules for the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

BaseDataAccessBean.java

BaseDataAccessBean.java contains the basic data access methods for the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

CycleIdDetailAccessBean.java

CycleIdDetailAccessBean.java contains data access code for the maintenance of merit cycle id data for the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

RosterEmpDetAccessBean.java

RosterEmpDetAccessBean.java contains data access methods for employee detail data for the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

RosterHandler.java

RosterHandler.java is the event handler for roster update related events in the web merit application. It was modified to remove instances where query parameters were concatenated to the query string itself, replacing those with code to set the query parameters in prepared statements.

Web Pages

FAQ.html

FAQ.html is the Frequently Asked Questions page for the web merit application. The following lines were added at the bottom of the page so that the release number can be seen to verify installation.

University of California
Release 1894 12/09/09

Installation Instructions

Download and install the .ear or .war file from the release dataset PAYDIST.R1894.MERITEAR or MERITWAR using binary FTP. For details on installation, please see the documentation for releases 1485 and 1668.

Test Plan

1. Log into the main menu and access the web merit application.
2. In the application menu in the upper right, select "FAQ".
3. Scroll to the bottom of the FAQ page, and confirm that the following appears:

University of California
Release 1894 12/09/09

Timing of Installation

The timing of this release is **urgent**.

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 maxine.gerber@ucop.edu, or call 510-987-0422.

Maxine Gerber