This release addresses the following Error Reports:

**Error Report 2137**

Release 1792 addressed a cross-site scripting vulnerability in the PPS net.data web code. Error Report 2137 reports an additional cross-site script vulnerability when one of the programs transfers control to the logout page. When the web programs detect certain errors, such as a timeout condition, control is transferred to the logout screen with a message. Previously, the application passed the text of the message on the URL, which provides the potential for malicious code to be inserted and sensitive data to be transmitted to a hacker's server.

This release contains modifications to prevent that cross-site scripting.

**Table Updates**

**System Messages Table**

The following messages which were previously hard-coded in the net.data programs have been added to the System Messages Table.

Messages WA-015 and 016 will be displayed together when a session timeout occurs:

WA-015 Session timed out.

WA-016 Your session was canceled due to inactivity.
Messages WA-017, 18 and 19 will be displayed together when the EDB inquiry subsystem is unavailable:

WA-017 Subsystem Unavailable.
WA-018 EDB Inquiry is currently unavailable due to system maintenance.
WA-019 Please try your request again later.

Messages WA-020 and 021 will be displayed when the user is not authorized for EDB inquiry:

WA-020 Not authorized.
WA-021 Your user ID is not authorized for Web EDB Inquiry.

Message WA-022 will be displayed when RACF returns an unknown code when trying to verify the user:

WA-022 Your access to EDB Inquiry could not be verified due to error=

**Net.data Macros**

**ppschgpw.d2w**

ppschgpw.d2w is the change password screen program. It passes a message on the URL to the exit screen program when the user's session has expired. It has been modified as follows:

- Message numbers WA015 and WA016 is now passed to the logout screen program in place of message text, when the user's session has expired.

**ppsexit.d2w**

ppsexit.d2w is the logoff screen program. It displays messages passed on the URL from other programs. It has been modified as follows:

- Code to translate spaces and commas in the message text has been removed.
- Previously, this screen displayed messages sent in the URL from other programs. It has been changed to take the message number from the URL and obtain the message text via call to the get_message utility.

**ppsmenu.d2w**

ppsmenu.d2w is the menu screen program. It passes a message on the URL to the exit screen program when the user's session has expired. It has been modified as follows:

- Code to translate spaces and commas in the message text has been removed.
- Message numbers WA015 and WA016 is now passed to the logout screen program in place of message text, when the user's session has expired.

**ppsrouter.d2w**

ppsrouter.d2w is the main navigation driver for EDB Inquiry. It passes messages on the URL to the exit screen program. It has been modified as follows:

- Code to translate spaces and commas in the message text has been removed.
- Message numbers are now passed to the screen programs in place of message text. Additional data needed by the message is appended to the message number after an asterisk.
Installation Instructions
A separate Installation Instructions document is provided for this release.

Test Plan
A separate Test Plan document is provided for this release.

Timing of Installation
The timing of this release is urgent. The web applications will remain vulnerable to cross-site scripting until this release is installed.

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