This release addresses the following Error Report:

**Error Report 2126**

Error Report 2126 reports that the net.data screen programs are vulnerable to "cross-site scripting", in which malicious JavaScript code can be inserted into the ErrMsg variable on the URL between screens. This can allow sensitive data to be transmitted to a hacker's server.

This release contains modifications to prevent cross-site scripting.

**Table Updates**

**System Messages Table**

One new message, WA-014,. has been added to the message table which was previously hard-coded in the PAN application.

**Net.data Macros**

**ppsauth.d2w**

ppsauth.d2w contains the authorization code for the login process. It passes error messages on the URL to screen programs. 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.

**ppsbframe.d2w**

ppsbframe.d2w is the EDB Inquiry footer frame for all EDB Inquiry screens. It displays messages, but does not generate any. 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.

**ppschgpw.d2w**

ppschgpw.d2w is the change password screen program. It displays messages, but does not generate any. 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.

**ppslogon.d2w**

ppslogon.d2w is the login screen program. It displays messages, but does not generate any. 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 displays messages, but does not generate any. 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.
- The program has also been modified to create a new session ID so it doesn't time out too soon.

**ppsrouter.d2w**

ppsrouter.d2w is the main navigation driver for EDB Inquiry. It passes error messages on the URL to screen programs. 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.

**Net.data Include Members**

ppsutil.d2w

ppsutil.d2w contains utilities used by other net.data programs, including the get_message utility. It has been modified as follows:

- Code to translate spaces and commas in the message text has been removed.
- If there is additional data provided with the message number (following an asterisk), up to 5 characters of this data are now appended to the message text obtained from PPPMSG.
Java Properties Files

ApplicationResources.properties

- This file contains the parameter settings for the Web PAN application. Previously, this file contained message texts to be passed in the url back to the (net.data) main menu. These have been replaced by message numbers to prevent cross-site scripting.

Installation Instructions

A separate Installation Instructions document is provided for this release.

Test Plan

A separate Installation Instructions 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 p510-987-0422.

Maxine Gerber