Release 1792
Error Report 2126
Prevent Cross-site Scripting in Web Applications

Test Plan

November 14, 2007
Prepared by Maxine Gerber
Information Resources & Communications
Office of the President
University of California
Testing Overview

This test plan addresses the test runs and cases constructed to verify the correct installation of Release 1792.

The test is made up of the following components:

1. Web Testing
Web Testing

1. Attempt to log on to the PPS Web application using an invalid user ID.
   
   **Verification:** The login screen is re-displayed with the message "Unknown userid" (WA008). Note that the message text does not appear in the URL, just the message number. This confirms that the changes to the authorization program have been correctly installed.

2. Perform the following steps:
   - Log on to the PPS Web application.
   - From the main menu, select "Change Password"
   - On the Change Password screen, in the "old password" field, enter an incorrect password
   
   **Verification:** The Change Password screen is re-displayed with the message "Invalid Old Password" (WA012). Note that the message text does not appear in the URL, just the message number. This confirms that the changes to the Change Password screens have been correctly installed.

3. This step requires that a user ID be set up in ARSM with limited access to EDB data. The following shows a record in the UC0ASC table which has been set up to access data only in one department. Note that this user ID does not appear in the UC0GRP table.

<table>
<thead>
<tr>
<th>IDENTIFIER</th>
<th>ACCESS_RULE</th>
<th>SEQ_NUMBER</th>
<th>ASSOCIATION_DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAR(8)</td>
<td>CHAR(8)</td>
<td>SMALLINT</td>
<td>CHAR(18)</td>
</tr>
<tr>
<td>PRIMARY---</td>
<td>PRIMARY----</td>
<td>---PRIMARY</td>
<td>------------------</td>
</tr>
<tr>
<td>PAYTST3</td>
<td>HMEDEPT</td>
<td>1</td>
<td>827701</td>
</tr>
</tbody>
</table>

   Perform the following steps:
   - Log on to the PPS Web application using a user ID with limited EDB access.
   - From the main menu, select "EDB Inquiry"
   - From the browse screen, select an employee to which the user ID does not have access.
   
   **Verification:** The browse screen is re-displayed with the message "Not authorized to see data for selected employee" (WA001). Note that the message text does not appear in the URL. This confirms that the changes to the web inquiry programs have been correctly installed.

4. This step requires that a user ID be set up in RACF with limited access to PAN screens. Perform the following functions:
   - Log on to the PPS Web application using a user ID with limited PAN access.
   - From the main menu, select a screen for which the user is not authorized.
   
   **Verification:** The main menu is re-displayed with the message "Not authorized to view the requested page" (WA003). Note that the message text does not appear in the URL. This confirms that the changes to the Web PAN properties file and the PPS main menu have been correctly installed.