SimpleRisk Release Notes

Version 20140224-001

This version provides several minor bug fixes, a couple of UI enhancements, and several security updates. If you are not already running SimpleRisk, then follow the standard installation instructions. If you are currently running the 20131231-001 release of SimpleRisk, then you will need to extract the new files over the old ones (back up your config.php first) and then run the /admin/upgrade.php script to upgrade your database.

The complete list of changes for this release is below:

- New Functionality
    - Created a new report showing all risks sorted by risk scoring method that includes Classic, CVSS, DREAD, OWASP, and Custom.
- User Interface Enhancements
    - Updated the Extras page in the Configuration menu to show which Extras are enabled.
    - Added the new header to the reviews.php page.
    - Configured the LDAP option when creating a new user to only show if the custom authentication extra is enabled.
- Security Enhancements
    - Added an auto-complete restriction to all HTML password fields.
    - Added nonces to prevent Cross-Site Request Forgery (CSRF) in all authenticated forms.
    - Updated the Announcements page in the Configuration menu to use HTTPS instead of HTTP to fetch the announcements.
    - Updated the About page in the Configuration menu to use HTTPS instead of HTTP to fetch the latest version information.
    - Added a proper unique salt for each user. This value will take effect for each user at their next password update.
- Bug Fixes
    - Fixed an issue preventing a mitigation or management review where the Team-Based Separation Extra was enabled.
    - Fixed an issue where the reviews.php page was not properly stripping slashes.
    - Fixed an issue where Javascript was attempting to execute when fields were populated with a specific function. This lead to "object not found" messages when clicking drop downs on the IE risk submission screen.
- Database Changes
    - Added a new "salt" column to the user table in order to provide each user with a unique and random salt value.
- Notes
    - In performing some testing with a newer version of PHP, it appears that PHP has removed the standard JSON extension as of PHP 5.5rc2 due to a license conflict. This functionality is used in SimpleRisk's graphing library. If you notice that your pie charts

are not displaying properly, you may need to install the "php5-json" package for these charts to work as expected.

- o If you see "PHP Notice: Use of undefined constant" messages in your error log file, you should check your config.php file to ensure that the first line reads "<?php" instead of "<?". This is because in newer versions of PHP, short tags are turned off by default. This should only affect adopters of SimpleRisk prior to this release as the new config.php file has the non-short tag included now.

- o A SimpleRisk user noted that they were having difficulty logging in with the default username of "admin" with password of "admin". Upon investigation, it was discovered that PHP was enforcing secure cookies, but the application was not using SSL, so the session values were not set. This may be an isolated instance, but if you experience this issue, try installing a SSL certificate and run SimpleRisk over HTTPS to fix it.