HARMONY PURPLE

Harmony Purple Web Scanning Release Notes

Release Date: January 2022

Copyright

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

The Orchestra Group Ltd logo and all Orchestra Group Ltd product and service names listed herein are either registered trademarks or trademarks of Orchestra Group Ltd or its subsidiaries. All other marks are the property of their respective owners.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

New Features and Changes

The ability to scan web applications for the Open Web Application Security Project (OWASP) vulnerabilities is being added to Harmony Purple. The release of the web scanning feature is scheduled for January, 2022. The purpose of this feature is to enable security and IT teams to determine if their internal and internet-facing web applications are vulnerable to attacks identified by the OWASP.

Web Scanning Feature Details

Vulnerability Coverage

Details of the vulnerabilities covered by this feature are listed in the appendix of this document. The scanning capability includes many vulnerability classes. Please see the appendix for details.

Deployment

The feature is enabled by deploying a web-scanning server that is connected to the Harmony Purple management server. The connection to the web scanner is established by entering its IP address in the Harmony Purple management UI. The web scanner is controlled from the Harmony Purple management server.

Web Scanning Operation

Once the web scanning server has been set up and configured, scanning is performed as follows:

1. Navigate to the **WebScan** tab.
2. Enter the following configuration parameters:
    - **Targets as IP or URLs**: There is no limit to the number of targets.
    - **Credentials** and authentication method per target. If required.
    - **URLs to exclude** in the process of crawling: Logout page, for example.
    - **Maximum scan time** (optional).
3. Trigger the scan selecting a designated button.

    Note: Progress of the scan is presented as a percentage of completion. You can abort the current scan, if desired.
4. When scan is completed, select **`Download`** to download the results. The file is downloaded to your browser's default download folder.

Scan Results

The CSV file contains the following information:

- URL tested
- Test name
- General description of the test
- Status: Failed (vulnerable)/ Passed (not vulnerable)
- Run time: The date and time when this test occurred
- Suggested remediation
- External references for more information
- OWASP Top10 category
- Additional information: Information such as affected users, data found, etc.

Feature Notes:

- Scanning data will only be presented in the CSV file and not in the UI. Presentation of the data in the UI is planned for a subsequent release.
- The ability to define a scan configuration and save it for future use is planned for a subsequent release.
- There can only be one scan at a specific time.
- The system only keeps the latest scan for download. The ability to provide scan history is planned for a subsequent release.

Appendix: Supported Scans

- SQL Injections (Error based, Boolean based, time based) and XPath Injections
- Cross Site Scripting (XSS) reflected and permanent
- File disclosure detection (local and remote include, require, fopen, readfile...)
- Command Execution detection (eval(), system(), passtru()...)
- XXE (Xml eXternal Entity) injection
- CRLF Injection
- Search for potentially dangerous files on the server
- Bypass of weak htaccess configurations
- Search for copies (backup) of scripts on the server
- Shellshock
- Folder and file enumeration (DirBuster like)
- Server Side Request Forgery
- Open Redirects
- Detection of uncommon HTTP methods (like PUT)
- Basic CSP Evaluator
- Brute Force login form (using a dictionary list)
- Checking HTTP security headers
- Checking cookie security flags (secure and httponly flags)
- Cross Site Request Forgery (CSRF) basic
- Fingerprinting of web applications using the Wappalyzer database
- Enumeration of WordPress and Drupal modules
- Subdomain takeovers detection