Security Misconfiguration Prevention in PHP

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly-descriptive errors which may reveal vulnerabilities in the application. This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.

Prevention:

1. Preventing directory listing, using (.htaccess):

When an online directory doesn't have an index page. Files inside that directory (if any) can be listed and viewed to the public which allows intruders to analyze files and codes and try to get their hands on the server.

i. First the toolkit checks the existence of the ".htaccess" in the project's root
ii. Then it makes sure that this line exists in it:
    1. Options –Indexes
iii. Above line of code prevents listing of empty directory on Apache Web Server.

To read more, go here:
https://www.thesitewizard.com/apache/prevent-directory-listing-htaccess.shtml

2. Error handling

The toolkit will check the web/app if it has error handling or not, which means an application shouldn't reveal enough info to the outside world when an error happens during production, because it helps the attackers to analyze the system easily.

So `error_reporting(0);` must be called in every page, you can include it, in the config file which will guarantees its calling on every request.

To read more, go here:
https://www.php.net/manual/en/function.error-reporting.php

All Above Explained ideas will be Scanned in the Toolkit.

3. Some Verbal Advices

a. Disable any unused Services or Libraries in your Web Site/Application
b. Close all unused ports and services in your Server
c. Make sure your Libraries and Services are up to date with the most security patches.
d. Make sure all default configurations and credentials are changed in your Web Site/App and Server.

To read more about Sensitive Data Exposure:
https://www.youtube.com/watch?v=JuGSUMtKTPU
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration