Grepping the source code is a classic method to perform security code review.

OmGrep is based on grepping with a GUI to list down potential SQL Injection, OS Command Injection, Server side request Forgery, Cookie set without http only flag, vulnerable javascript and few other third parties using “Retire js” utility and insecure file upload.

How it finds security issues?

(a) Sql Injection: The most recommended way to write secure sql queries in php is going parameterized way. OmGrep will list down all the sql queries not written in parameterized way and potentially vulnerable to sql injection attack
(b) It will list all the instance where os system command functions are used with a variable.
(c) It will list all the instance where functions are used with a variable which can lead to server side request forgery vulnerability
(d) It will list all the instances where cookies are being set with a chance of not having httponly flag
(e) It’s recommended to have one central service for file upload so that every developer is not writing her own set of validation. This service should be properly tested manually. OmGrep will list down all the instances where file is being uploaded probably without this secure service(developers negligence)
(f) Third Party Vulnerabilities using retire-js utility at backend.

Important Pointers:

User can suppress an issue on the result page so that it does not appear again.

Users can run the docker container with mounted source code directory or can provide the source code to be scanned by a git url

Intended Users: Developers, InfoSec people not having much budget for expensive commercial security code review solutions.

Coming in next releases: PDF Report, other vulnerabilities checks.

Usage instructions:

Pre-requisites: Docker

Mkdir codereview

cd codereview

Git clone https://github.com/sandeepgit1900/OmGrep.git

docker build “absolute path of directory/codereview” –t codereview

Mounting codebase:

docker run --name codereview -v **/tmp**:/tmp/codebase -d -p **8091**:80 codereview:latest

Replace the “/tmp” in bold with the code repository (to be scanned).

8091 can be replaced with any port which can be opened on host machine.

After running the docker container, select “Code Mounted” option on main page.

Provide the name of central file upload service which is manual tested for security, if there is no such service, leave blank and go.

If user wishes to provide code repository by git url, run the docker container as:

docker run --name codereview -d -p **8091**:80 codereview:latest

Provide the git url on main page.