Automated Source Code Review

pentestlab.blog/category/general-lab-notes/page/9

November 27, 2012

Manual source code review is task that requires a lot of time and good understanding of the application source code that is being reviewed.So the use of automated tools is often necessary in order to help the penetration tester to identify fast and more easily vulnerabilities on the code.However you cannot fully rely on the automated tools and you have to validate the results by checking the code as the majority of them produces a large number of false positives and in some cases they might even not found a vulnerability on the code that exists.So the penetration tester still needs to manual review the source code in order to do the job properly but tools exist and are here to help.In this article we will see some of the tools that we can use for performing automated source code review on applications.

Yet Another Source Code Analyzer (YASCA)

YASCA is a tool that can analyze php,java,C/C++ and javascript code for security vulnerabilities and code quality issues.One of the main advantages of this tool is that it can integrate other tools and plugins in order to scan many programming languages.YASCA runs through the command line and can generate the reports in HTML,XML and CSV formats.

Author: Michael Scovetta

Languages: Multi

URL: http://www.scovetta.com/yasca.html

Platforms: Windows and Linux

Pixy

Pixy is a tool that runs in Java and can scan PHP4 code in order to identify XSS and SQL injection vulnerabilities.Pixy is considered one of the best tools for discovering SQL injection vulnerabilities in PHP code however it supports only PHP4 code.

Author: Nenad Jovanovic

Languages: PHP4

URL: http://pixybox.seclab.tuwien.ac.at/pixy/

Platforms: Windows and Linux

AppCodeScan

AppCodeScan users regular expression string matching to identify dangerous functions and strings in the code.The vulnerabilities that this tool can discover includes XSS,SQL injections,poor validation and many more.The AppCodeScan is a GUI based tool and runs on the .NET framework.

Languages: Multi

URL: http://www.blueinfy.com/

Platform: Windows

LAPSE

Lapse is a security scanner for Java 2EE applications that can discover common vulnerabilities.The vulnerabilities that can discover includes Cookie Poisoning,SQL Injection,XSS,XML Injection etc.LAPSE is a project of OWASP.

Author: Benjamin Livshits

Languages: Java J2EE

URL: http://suif.stanford.edu/~livshits/work/lapse/

Platforms:Windows,Linux and OSX

IDE: Eclipse

SWAAT

SWAAT scans the source code and tries to discover common vulnerabilities by using XML based signature files.SWAAT is a command line tool.

URL: https://www.owasp.org/index.php/Category:OWASP_SWAAT_Project

Languages: PHP,JSP and ASP.NET

Platforms: Windows,Linux,OSX

Microsoft Source Code Analyzer for SQL Injection

Microsoft source code analyzer is a tool that it can be used when reviewing .asp code for the discovery of SQL injection vulnerabilities.This tool have not been designed for ASP.NET code and it only scans ASP code.

URL: http://www.microsoft.com/en-us/download/details.aspx?id=16305

Languages: ASP

Platforms: Windows

Microsoft Code Analysis Tool (CAT.NET)

CAT.NET is a binary code analysis tool that can identify vulnerabilities like XSS,Xpath injection and SQL injection in applications that have been written in C#,Visual Basic.NET and J#.CAT.NET discover these vulnerabilities by checking the binary of the application and traces the data flow among its statements and methods.

URL: http://www.microsoft.com/en-gb/download/details.aspx?id=19968

Languages: C#,Visual Basic.NET and J#

Platform: Windows

IDE:Visual Studio

Conclusion

Automated tools can never replace the human factor in penetration testing.The reason that automated tools exists is for helping the penetration tester to perform his task effectively and on the time-frame that he has.Even with the use of that automated tools the penetration tester stills needs to look at the code and to see if the vulnerability exists or it’s a false positive.However the use of such tools can make the source code review of an application more easier task.