acunetix

Finding the right web application scanner; why black box scanning is not enough.

Acunetix AcuSensor Technology is a new security technology that allows you to identify more vulnerabilities than a traditional Web Application Scanner, whilst generating less false positives. In addition it indicates exactly where in your code the vulnerability is and reports also debug information.

The increased accuracy is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code while the source code is executed. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. Therefore combining these techniques together achieves more relevant results than using source code analyzers and black box scanning independently.

AcuSensor Technology does not require .NET source code; it can be injected in already compiled .NET applications! Thus there is no need to install a compiler or obtain the web applications' source code, which is a big advantage when using a third party .NET application. In case of PHP web applications, the source is already available.

To date, Acunetix is the leading and only Web Vulnerability Scanner to implement this technology.

Advantages of using Acunetix AcuSensor Technology

1. Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query.

2. We can significantly reduce false positives when scanning a website because we can internally understand better the behaviour of the web application.

3. Can alert you of web application configuration problems which could result in a vulnerable application or expose internal application details. E.g. If 'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.

4. Detect many more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported or via other common techniques.

5. Ability to detect SQL Injection vulnerabilities in all SQL statements, including in SQL INSERT statements. With a black box scanner such SQL injections vulnerabilities cannot be found.

6. Ability to know about all the files present and accessible though the web server. If an attacker will gain access to the website and create a backdoor file in the application directory, the file will be found and scanned when using the AcuSensor Technology and you will be alerted.

7. AcuSensor Technology is able to intercept all web application inputs and builds a comprehensive list will all possible inputs in the website and tests them.

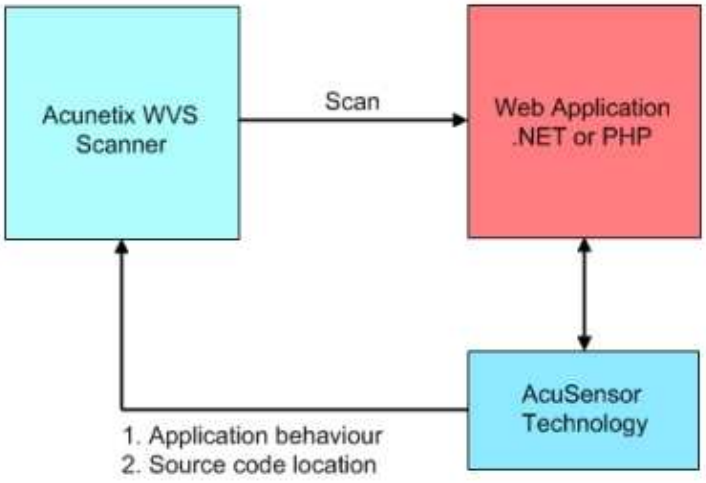
8. No need to write URL rewrite rules when scanning web applications which use search engine friendly URL's! Using AcuSensor Technology the scanner is able to rewrite SEO URL's on the fly.

9. Ability to test for arbitrary file creating and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.

10. Ability to test for email injection. E.g. A malicious user may append additional information such as a list or recipients or additional information to the message body to a vulnerable web form, to spam a large number of recipients anonymously.

How it works

When AcuSensor Technology is used, it communicates with the web server to find out about the web application configuration and the web application platform (such as PHP and .NET) configuration. Once triggered from the Acunetix WVS scanner, the sensor gets a listing of all the files present in the web application directory, even of those which are not linked to through the website. It also gathers a list of all the web application inputs. Since it knows what kind of inputs the application expects, it can launch a broader range of tests against the application.



Screenshot 1 – AcuSensor Technology functionality diagram

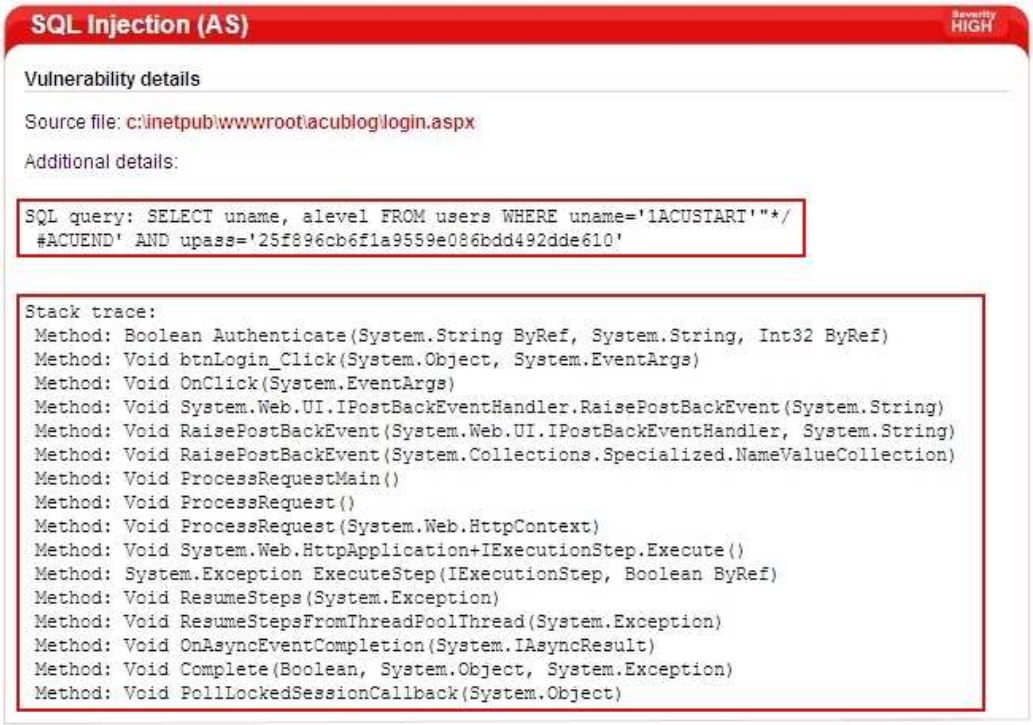
It has also the ability to scan all SQL transactions taking place between the web application and the database when the web application is being scanned. It hooks between the web application and the database and is able to trace SQL injection vulnerabilities in the code without relying on database errors like other typical scanners do.

AcuSensor Technology vulnerability Reporting

Unlike other vulnerabilities found by typical scans, a vulnerability reported from the AcuSensor Technology contains much more detailed information. As seen in the examples below, it can contain details such as source code line number, stack trace, affected SQL query etc. Each vulnerability found by AcuSensor Technology, will be marked with '(AS)' in the title.

Example 1: SQL Injection reported by Acunetix AcuSensor Technology

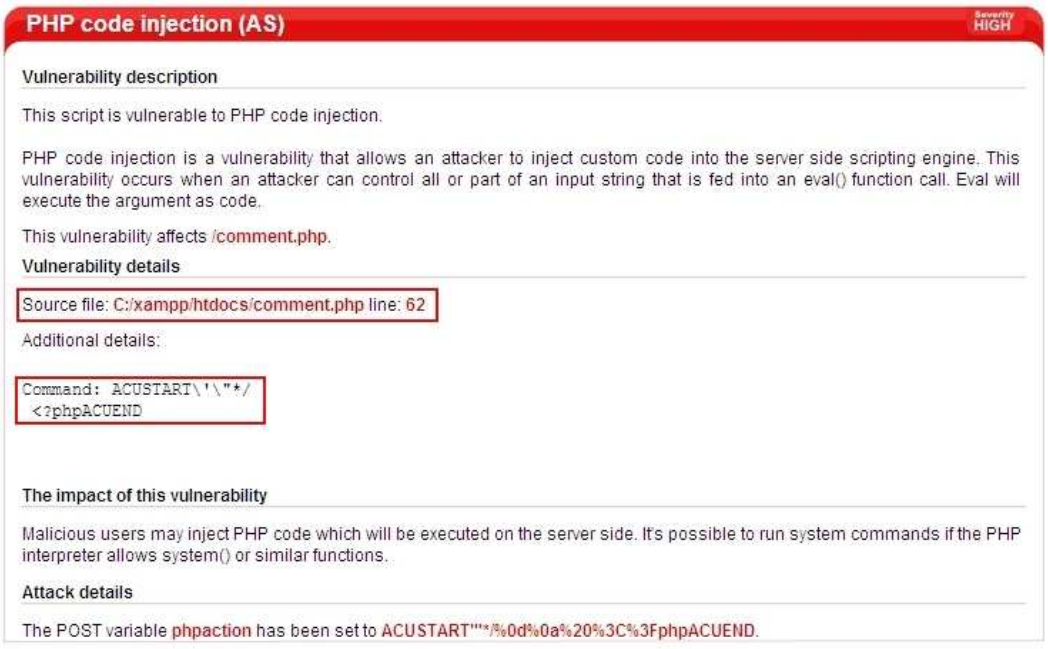
For the reported SQL injection featured in the screenshot below, the SQL query including the injected content which results into an SQL injection vulnerability is shown. The stack trace information is also displayed, to guide the developer where exactly the problem is.



Screenshot 2 – SQL Injection reported by AcuSensor Technology

Example 2: Code Injection reported by Acunetix AcuSensor Technology

For the reported PHP code injection featured in the screenshot below, the vulnerable file name is displayed including the line number of the code which leads to the reported vulnerability. The injected code is also displayed under 'Attack details'.



Screenshot 3 – PHP code injection reported by AcuSensor Technology

Conclusion

As seen above, using the AcuSensor Technology has many advantages. Apart from the above mentioned advantages, information provided by the AcuSensor Technology helps the developer trace the vulnerability and fix it in a much shorter time. It also helps them understand what was wrong in the code to allow such vulnerability to happen. From this, developers proactively learn more about vulnerabilities and it helps them in writing more secure code for future web applications and increases web security awareness.

Download and test the Trial version of Acunetix Web Vulnerability Scanner Version 6 today and see for yourself how Acunetix AcuSensor Technology goes beyond black box scanning!