DEFENSECODE Ltd
27 Cork Road, Midleton
County Cork
Ireland
www.defensecode.com
defensecode@defensecode.com

DefenseCode

APPLICATION SECURITY TESTING

THE PROBLEM – SECURITY VULNERABILITIES

In the modern interconnected world we rely heavily on technology. We use various software solutions and applications to perform our daily tasks – sometimes for business and sometimes for pleasure. We use desktop, web and mobile applications to help us build our business upon, achieve our business goals, communicate with our peers, share our experiences and sometimes to relax after a busy day.

It is safe to say that our digital identity, our most valuable data and our privacy is handled and entrusted to technology. And what is technology these days? Hardware and software are often mentioned, but hardware is merely a tool to access software and applications. Data itself is processed by the software.

QUESTION: WHERE DOES ALL THAT SOFTWARE AND APPLICATIONS COME FROM? ANSWER: FROM PEOPLE WHO BUILD THEM. ORDINARY PEOPLE LIKE YOU OR ME, PEOPLE WHO MAKE MISTAKES.

As we all know, human being is prone to make mistakes and errors in life. Well, pretty much the same goes for people building a software - developers. Developers who build the software, applications that we rely upon, make mistakes and shortcomings. Sometimes those mistakes are tiny and benign and go unnoticed, but sometimes they can have a huge impact and negative consequences. Those mistakes that developers make and software errors can sometimes lead to a broken software and that is pretty obvious – software doesn't work as it should. But what about more subtle problems and errors that do not pop up immediately, more dangerous mistakes – **security vulnerabilities**.

HACKERS SIMPLY LOVE SECURITY VULNERABILITIES!

If we take aside human mistakes in handling data, **software security vulnerabilities lie behind every system compromise and every data security breach that ever happened**. Hi-tech criminals ("**hackers**") exploit these vulnerabilities to compromise the security of organizations, steal information, money, abuse company resources, and disrupt business operations

Security incidents are **time consuming** and **costly**. They can cause direct and **indirect damages**, including **negative PR** and **loss of customer confidence.**

Hackers are creative, they are very creative. They will analyze your system and your applications upside down and inside out looking for even the smallest weak spots that they can abuse for their purposes. That can be just **a single vulnerable line of code** in your application. That's all that they need to compromise your application, your system and your data.

THE SOLUTION – APPLICATION SECURITY TESTING

Applications should be properly tested for security vulnerabilities before being pushed into the production and later, during their time in production every time they are upgraded. Applications can be tested manually for security vulnerabilities by the security testers. The problem with this approach is **scalability**. It takes a lot of time to manually test complex applications and even then security vulnerabilities can be missed due to the complexity of the application. Moreover, it is advisable to test the application for security vulnerabilities on every significant code change because it can introduce new vulnerabilities. It is needless to say that is time-consuming and requires a dedicated team that would analyze applications in development around the clock.

SOLUTION: AUTOMATIZE THE WHOLE APPLICATION SECURITY TESTING PROCESS WITH THE SECURITY TESTING TOOLS

Good news is that application security testing can be automatized. There are two security testing approaches that automatized tools can do for you:

- **BLACKBOX SECURITY TESTING – DYNAMIC APPLICATION SECURITY TESTING (DAST)**
- **WHITEBOX SECURITY TESTING – STATIC APPLICATION SECURITY TESTING (SAST)**

In the **Blackbox** (**D**ynamic **A**pplication **S**ecurity **T**esting), application is tested dynamically from "the outside" as the real hackers would do it. That way, "live and running", applications can be tested for security vulnerabilities.

In the **Whitebox** (**S**tatic **A**pplication **S**ecurity **T**esting), application is tested statically on the source code level. Each line of source code is inspected for the presence of the security vulnerabilities.

DefenseCode products can test your applications with both **SAST** and **DAST** application security testing approach with deployment of **ThunderScan SAST** and **Web Security Scanner DAST** security products.

DEFENSECODE THUNDERSCAN SAST

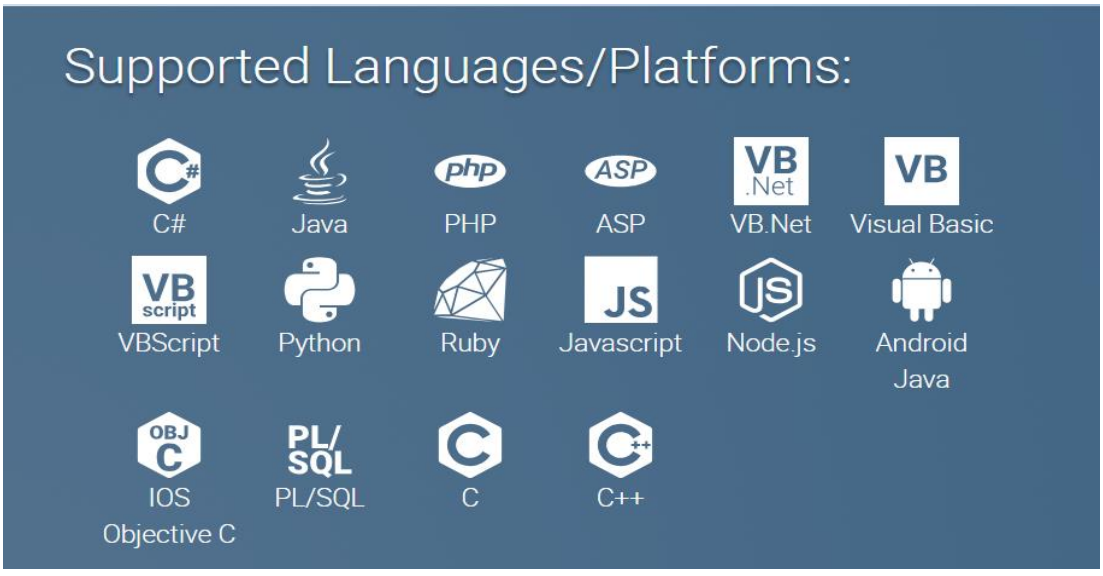
DefenseCode ThunderScan SAST is a static source code security analyzer tool that is able to inspect the application on the source code level for the security vulnerabilities. That way an application can be tested during the development and after the development process to identify the vulnerabilities as soon as possible. ThunderScan SAST source code security analyzer can identify vulnerabilities buried deeply in the source code and detect even the very subtle backdoors hidden in the application source code.

THE ADVANTAGES OF AUTOMATIZED SOURCE CODE SECURITY ANALYZER TOOL?

Automatized static source code security analysis **tools are fast**. They are really fast. **DefenseCode ThunderScan SAST** is capable of analyzing **50,000 lines of code under two minutes**. Imagine how much time would be needed for a security analyst (person) to manually analyze 50,000 lines of code just by reading them. Moreover that process need to be repeated on every significant source code change.

DefenseCode ThunderScan SAST is very simple to use and **can be used by the developers** to identify security vulnerabilities before pushing the code into the production or **by security analysts to analyze third-party source code** for the presence of the security vulnerabilities. ThunderScan itself can be installed on-premise (with easy integration into CI/CD pipeline) or in the cloud. ThunderScan SAST can be used as a Windows desktop application, as a server based REST API or as a web oriented Web User Interface application directly from the internet browser.

THUNDERSCAN SUPPORT A WIDE RANGE OF DEVELOPMENT/PROGRAMMING LANGUAGES



THUNDERSCAN SAST – VULNERABILITY COVERAGE

DefenseCode ThunderScan SAST can find all sorts of nasty application security vulnerabilities that could lurk in your applications. Dangerous **SQL Injections** can lead to database compromise, various **Code Injections** can lead to complete web application and system takeover, **Cross Site Scripting** vulnerabilities can be abused to attack your application users and hijack application session, **Weak encryption** could expose your sensitive passwords to prying eyes and many more. All of the **OWASP TOP 10** vulnerabilities are covered together with **50+ other vulnerability classes**.

THUNDERSCAN DETAILED CODE FLOW COVERAGE – IT'S NOT A "GREP"

ThunderScan SAST will simulate the real inner working and data flows of the application that is tested, and it will deeply analyze code flow for potential security vulnerabilities. This makes ThunderScan scanning approach incomparable to the simple grep/pattern matching tools that just trigger an alarm on any occurrence of the pattern they are searching for. ThunderScan really understands the application that is tested.

Following the code flow from untrusted user input down to the potentially vulnerable sinks in the application itself, ThunderScan can differentiate whether a vulnerability is really exploitable or if it just belongs to a normal, benign code flow.

In previous code flow chart we can see that user input is coming from getParameter() function, passed as an argument to CustomFunc() and ends up in executeQuery() SQL function. If user input is not properly validated and filtered for special SQL characters, that situation could easily lead to an SQL Injection vulnerability in the application.

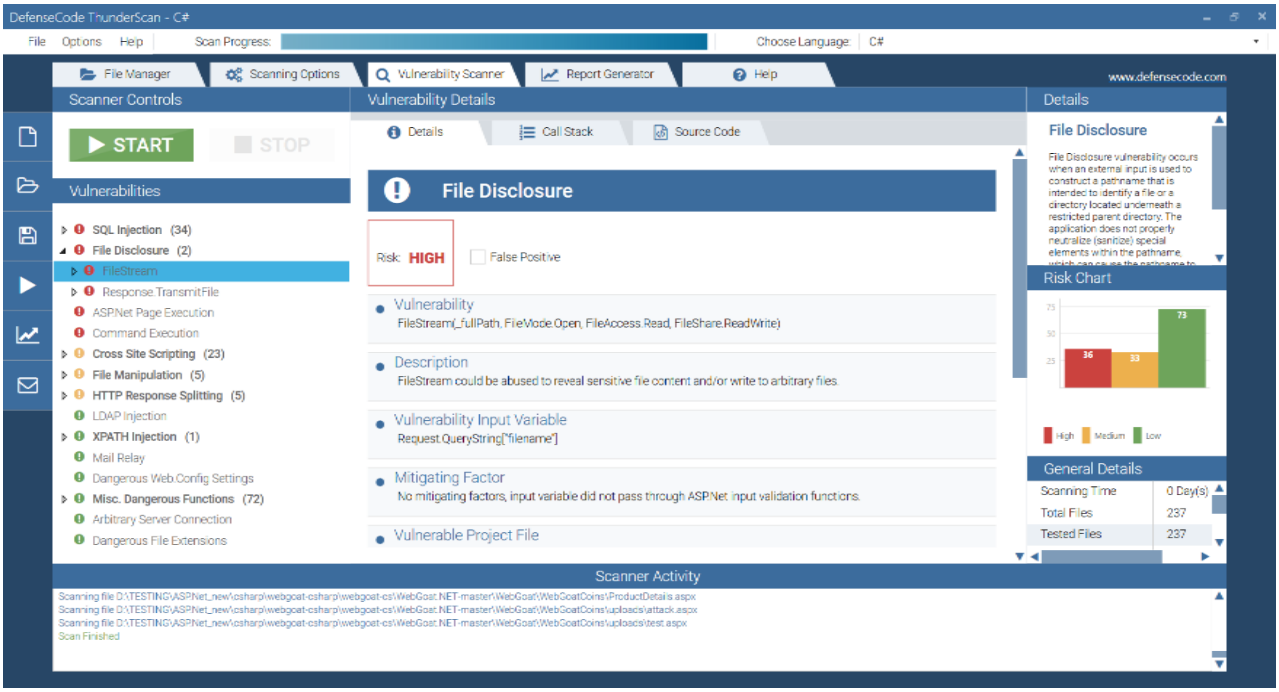
MORE THAN 3000+ VULNERABILITY RULES

ThunderScan SAST incorporates more than **3000+ vulnerability detection rules** to identify all sorts of security vulnerabilities in the most popular programming languages at the source code level. Customization features enable you to add your own custom rules to the scanning engine.

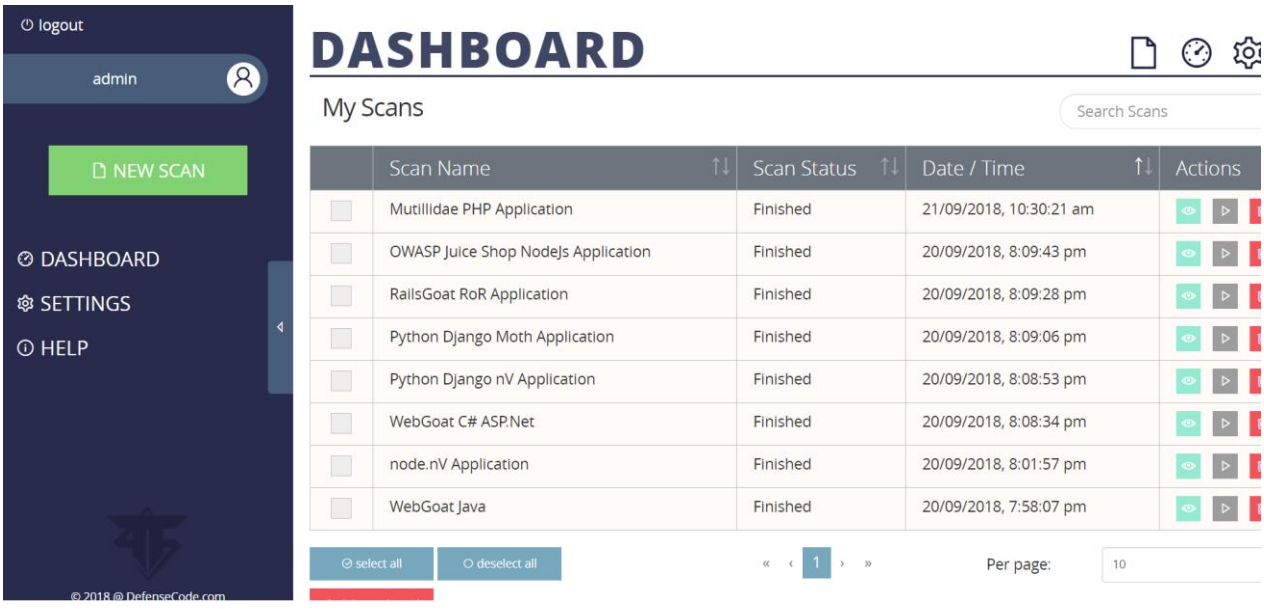
POWERFUL REST API AND WEB USER INTERFACE

ThunderScan can be deployed as a desktop GUI solution, as a powerful REST API interface that can be accessed using already prepared CLI clients for Windows, Linux and MacOS, and as a Web Application available from the internet browser.

THUNDERSCAN HAS A VERY POWERFUL DESKTOP INTERFACE



SAME OPTIONS BUT MORE MULTI-USER AND MULTI-DEVELOPER ORIENTED ARE AVAILABLE IN THE WEB APPLICATION VERSION OF THE THUNDERSCAN SAST



DEFENSECODE WEB SECURITY SCANNER DAST

DefenseCode Web Security Scanner DAST is a dynamic application security testing product that is capable to perform a security scan of the "live" web applications and web sites. Web applications are very popular these days and almost everything is web-oriented. This makes security testing of the web applications very important. When hackers probe your web application, they will try to "play" with every single aspect of the web application to see how it behaves and if there is anything unusual or worth attention in their malicious endeavor.

WHAT DOES WEB SECURITY SCANNER DO?

Web Security Scanner will mimic all the efforts of hackers when trying to penetrate a live web site or web application. Web scanner will first crawl your web site (as the internet search engines would do) and create a database of your web site structure. Later it will use this structure to identify data entry points where untrusted user input comes into the web application for processing. After that, it will try to probe each and every single data entry point with security testing data that could result in application misbehavior and potentially lead to a security vulnerability. Along with the probe oriented security testing, web scanner will search for data leaks, easily guessable file names that could contain valuable data or various web site errors that could reveal sensitive information, as well as many other things.

THE ADVANTAGES OF WEB SECURITY SCANNING?

Sole purpose of the web security scanner is to mimic and automate the work of the hackers as much as possible. It would take a hacker quite a lot of time to probe each and every data input vector on the web site to identify security vulnerabilities. Well, web security scanner automatize that. Web security scanner is very fast. **It can send millions HTTP requests within couple of hours** (depending on the web site speed and internet bandwidth limitations). You can think of the web security scanner as of an army of hackers trying to penetrate your website or web application in each and every possible way. But in this case, those "automated hackers" are under your control.

SUPPORTED TECHNOLOGIES

DefenseCode Web Security Scanner can scan and analyze any HTTP oriented web application. It has support for **HTTP, HTTPS, HTML, HTML5, AJAX, Web 2.0, jQuery** and more. One very important thing is that the technology in which the web application is developed is completely irrelevant for the successful scan. You can have a web application written in the Cobol, and the web security scanner will still be able to analyze it and find security defects.

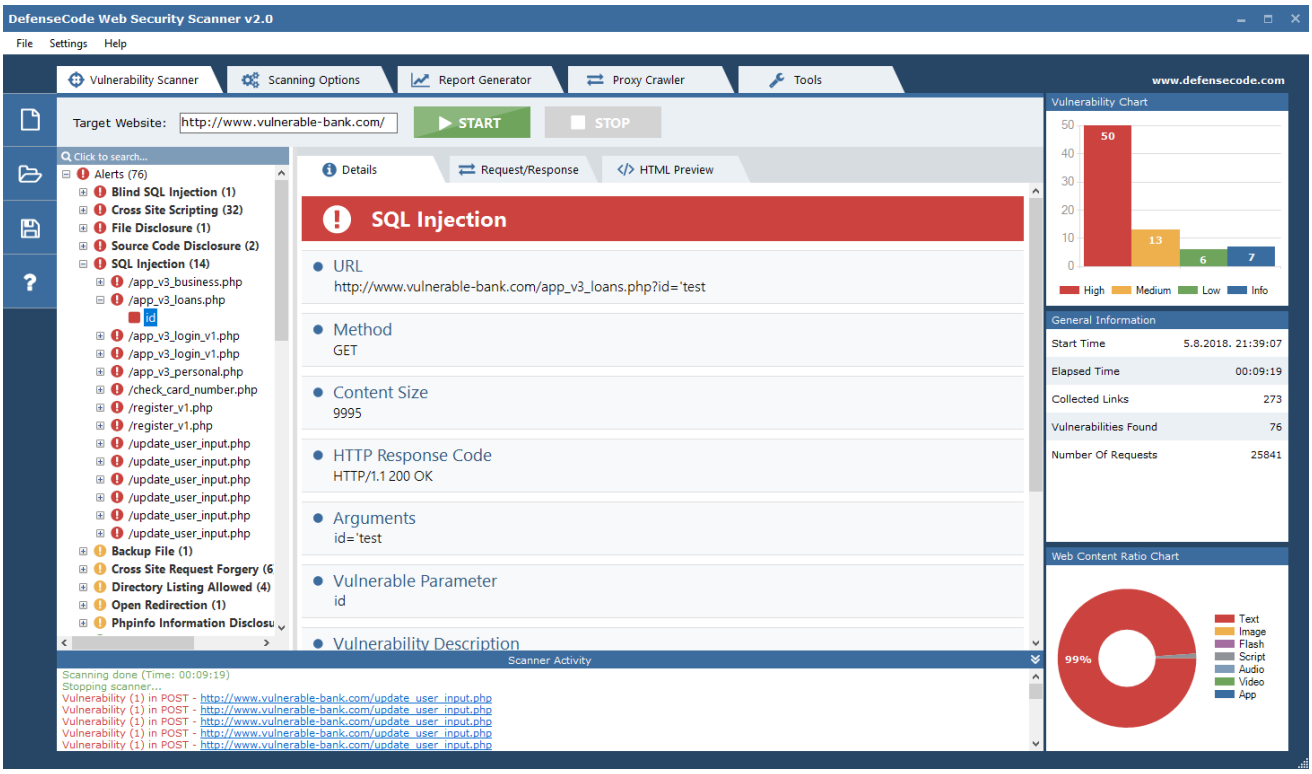
DEFENSECODE WEB SECURITY SCANNER DAST – VULNERABILITY COVERAGE

DefenseCode Web Security Scanner is capable of finding all **OWASP TOP 10** vulnerabilities along with **50+** more vulnerability classes and **5,000+ CVE-defined vulnerabilities**. Web security scanner can identify very wide range of security vulnerabilities in the live web applications. Some of them are **SQL Injection, Cross Site Scripting, Path Traversal, Source Code Disclosure, Code Injection** and many other. Web security scanner will search for vulnerabilities in various parts of **HTTP** protocol like **GET, POST, HEADERS, COOKIES, JSON based data, XML based data and URL path parts**.

WHO SHOULD USE DEFENSECODE WEB SECURITY SCANNER?

DefenseCode Web Security Scanner is very simple to use and can be used as a "point and click" software to analyze the security of the web site or web application. Scanning results are very easy to interpret so **it can be used by an average IT specialist**. However, DefenseCode Web Security Scanner is a very powerful tool that can be configured in many ways and used as a starting point for various web application **penetration testing engagements by security specialists and penetration testers**.

DEFENSECODE WEB SECURITY SCANNER WINDOWS DESKTOP APPLICATION



DEFENSECODE APPLICATION SECURITY TESTING - CONCLUSION

In the modern interconnected world threats to our critical digital infrastructure and information systems are lurking from everywhere. **Just one single vulnerability in your application can have devastating consequences** resulting in **direct loss of money, data and company reputation**. You can see newspaper headlines about cybersecurity incidents almost every day. In order to prevent you becoming a part of the negative cyber incident trend statistics, it is necessary to take appropriate measures to protect your critical infrastructure. **Application Security Testing** is a great start and a step in the right direction.

CONTACT US

DEFENSECODE LTD
27 Cork Road, Midleton
County Cork
Ireland
www: https://www.defensecode.com/
mail: defensecode@defensecode.com