VERACODE

INFOSHEET

What Is Application Security?

Every enterprise's application landscape is now both business critical and rapidly expanding.

Mobile and cloud computing are dramatically changing the way we do business. Today, the world runs on applications, and, as a result, every company is becoming a software company — regardless of its primary business.

And enterprises are producing these applications faster than ever before, often using DevOps processes and then augmenting their internal development programs with open source libraries and components.

Defining Application Security

Gartner describes application security with the analogy of a crown jewel in a treasure chest; the sensitive information is the crown jewel, and the applications are the treasure chest. To get at the jewels, attackers need to attack vulnerabilities in the application "container" — meaning it's imperative that enterprises keep that application "container" secure.

How can organizations ensure the security of their critical and fluid application landscapes? That's where application security comes in. Application security, or "AppSec," is what an organization does to protect its critical data from external threats by ensuring the security of all of the software used to run the business, whether built internally, bought or downloaded. Application security helps identify, fix and prevent security vulnerabilities in any kind of software application.

A software "vulnerability" is an unintended flaw or weakness in the software that leads it to process critical data in an insecure way. By exploiting these "holes" in applications, cybercriminals can gain entry into an organization's systems and steal confidential data. Common software vulnerabilities include SQL injection, CRLF Injection and Cross-Site Scripting (XSS).

And almost every application has vulnerabilities. Veracode's State of Software Security Report revealed that about 77 percent of all applications had at least one vulnerability classified as one of the top 10 web vulnerability types. Commercial software, financial services software,software written by government agencies… all are vulnerable.

"Web applications are the leading source of breaches within the information industry (41%). SQL injection is one of the top two hacking breaches involved in web application attacks."

FOR MORE INFO

About the application security landscape:

Gartner 2018 Magic Quadrant for Application Security Testing

On what a mature application security program looks like:

Everything You Need to Know About Maturing Your Application Security Program

"Businesses aren't asking for SAST, SCA, DAST — they're asking, how do I solve my problem? And the right answer is: with a little bit of everything, depending on your environment."

Chris Wysopal
Veracode Co-founder, CTO & CISO

COMMON APPLICATION VULNERABILITIES

SQL Injection exploits an application vulnerability that allows an attacker to submit a database SQL command, exposing the back-end database, where the attacker can create, read, update, alter or delete data.

Cross Site Scripting (XSS) is an attack that occurs when "malicious scripts are injected into otherwise benign and trusted websites" (according to OWASP). XSS stems from the security weaknesses of client-side scripting languages, such as HTML and JavaScript.

CRLF Injection includes any vulnerability that enables any kind of Carriage Return Line Feed (CRLF) injection attack. It encompasses flaws involving improper output neutralization for logs and improper neutralization of CRLF in HTTP headers.

Application Security Solutions

Although many companies first turn to tools and technologies to address application security, a successful solution will always start with a strong strategy. At a high level, the strategy should address, and continuously improve, these basic steps: identification of vulnerabilities, assessment of risk, fixing flaws, learning from mistakes and better managing future development processes.

There are a variety of application security technologies available to help with this endeavor, but no one is a silver bullet. You need to gather the strengths of multiple analysis techniques along the entire application lifetime to drive down application risk.

The end goal for any organization should be a mature, robust application security program that:

- Assesses every application, whether built in-house, purchased or compiled
- Enables developers to find and fix vulnerabilities while they are coding
- Takes advantage of automation and cloud-based services to more easily incorporate security into the development process and scale the program

TECHNOLOGIES AVAILABLE TO ASSESS APPLICATIONS FOR SECURITY VULNERABILITIES INCLUDE THE FOLLOWING:

Static Analysis (SAST), or "white-box" testing, analyzes applications without executing them.

Dynamic Analysis (DAST), or "black-box" testing, identifies vulnerabilities in running web applications.

Software Composition Analysis (SCA) analyzes open source and third-party components.

Manual Penetration Testing (or "pen testing") uses the same methodology cybercriminals use to exploit application weaknesses.

GET MORE INFO

On the different application security testing methods in

Your Guide to Application Security Solutions

VERACODE

Veracode delivers the application security solutions and services today's software-driven world requires. Veracode's unified platform assesses and improves the security of applications from inception through production so that businesses can confidently innovate with the web and mobile applications they build, buy and assemble as well as the components they integrate into their environments. Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 500, three of the top four U.S. commercial banks and more than 20 of Forbes' 100 Most Valuable Brands.