Get Started with Application Security in 3 Easy Steps

Ensuring your applications are secure doesn't have to be a cumbersome process. With the right program and tools, you can improve your organization's security without getting in the way of developer productivity.

Guide

opentext™

Introduction

Think about the applications you use every day in your organization from emails to browsers, business applications, and office productivity tools such as Google apps and Microsoft Office. Companies rely more than ever on mobile and web applications to communicate with customers and partners. And as development teams struggle to keep up with the growing demand for rapid delivery of new business applications, security is often neglected.

Fortify's Software Security Research team has found that 80% of web applications contain at least one critical or high vulnerability. According to the 2017 Verizon Data Breach Investigations Report (DBIR), web applications are under attack even more so than last year. In over half of the reported breaches, personal data was compromised. It has become common to read about large data breaches caused by application vulnerabilities on company websites. These breaches affect millions of consumers as criminals gain access to sensitive data including Social Security Numbers, birth dates, addresses, and driver's license numbers.

It's not a surprise that application-layer attacks are a leading cause of breaches. Since development is highly competitive and driven by speed, security is often sidelined, increasing unintended flaws or weaknesses in the software. By exploiting these flaws in the application, cybercriminals enter the system and steal sensitive data. Also, many organizations continue to wrongly assume that their perimeter security such as Web Application Firewalls (WAFs) and Secure Web Gateways are sufficient in protecting against cyberattacks. But building higher walls isn't enough to protect your "crown jewels"—your applications and sensitive data. You need an application security program that ensures the security of your web and mobile applications.

Creating a Flexible, Comprehensive Application Security Program

Sometimes it seems that creating an application security program is fraught with hurdles, and to some it might seem too daunting to start. But starting is easier than you think.

Before discussing how to create a program, we should understand what application security entails. Application security (AppSec) encompasses measures you must take to improve the security of your applications by identifying, remediating and preventing software vulnerabilities.

There are two important approaches to secure an application: Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST).

Static Application Security Testing (SAST)

SAST, also known as white-box testing, is usually performed as part of a code review and should be integrated into the software development lifecycle (SDLC). With SAST, you scan source code to find known patterns of weaknesses, which developers can use to weed out security flaws. It's important to check that the SAST solution you are considering fits into your development process by providing support for a variety of programming languages and tools such as PHP, C# and Java; IDEs including Eclipse and Visual Studio; and build servers such as Ant, Maven and Gradle. Web and mobile applications often use third-party open source components, which can be unsafe and outdated, so a SAST solution should be able to analyze third-party components. SAST can be invaluable in eliminating vulnerabilities early in the development lifecycle.

Dynamic Application Security Testing (DAST)

DAST, also referred to as black-box testing, identifies vulnerabilities in running applications in a pre-production environment before the application is deployed. With DAST, applications are subjected to simulated attacks in real time to find flaws that attackers could exploit. It explores and tests web applications and services via HTTP and HTTPs. DAST doesn't require any knowledge or access to source code or binaries. Using the types of attacks that hackers might use to penetrate application security,

According to the 2017 Verizon DBIR, web applications are under attack even more so than last year. In over half of the reported breaches, personal data was compromised.

DAST assessments are helpful in finding a broad range of flaws such as server configuration mistakes and input/output validation problems.

DAST tools can search the network for applications, identifying ones you didn't even know existed such as legacy marketing pages or shadow IT and development applications, and testing those applications for vulnerabilities. This process helps the security teams stay on top of all applications and give them quick wins in identifying and remediating vulnerabilities.

A solution that offers SAST and/or DAST must be fast and flexible enough to keep up with your Continuous Integration (CI) or development practices such as Agile and DevOps, while providing results with minimal false positives and negatives. Also, if your organization has any compliance mandates including PCI DSS and HIPAA or a desire to adhere to standards such as OWASP Top 10, you should ensure that the solution you choose can assess vulnerabilities based on those requirements.

SAST or DAST: Which One Should You Choose?

Deciding whether to adopt static or dynamic analysis testing depends on your organization's requirements. While source code or static analysis gives software developers feedback on their code and even educates them in real time, dynamic analysis gives your security team quick wins by finding exploitable vulnerabilities in running applications.

In most cases, mature organizations run both. Static and dynamic work hand in hand to give you the best protection against application-layer attacks. It is often preferable to find a technology that provides both testing methods so that you have a single, comprehensive view into the security of your application from design to delivery.

Cloud Versus On-Premises Security Solutions

At some point in your program, you will have to consider whether you'd prefer to perform assessments with on-premises SAST and DAST tools or through a cloud-based service. With cloud-based services, on-site implementations are not required, and the application security provider manages your assessments. With on-premises tools, your organization's security team maintains and manages the process in-house. Many organizations nowadays prefer cloud-based services, while others must use on-premises tools or a combination of the two. Whatever path you choose, it should align with your organization's business objectives.

Ensuring your applications are secure doesn't have to be a cumbersome process. With the right program and tools, you can improve your organization's security posture without ever getting in the way of developer productivity.

Get Started in 3 Easy Steps

Step 1: Understand the "Lay of the Land"

Start by dedicating time to understanding the "lay of the land" and the key players, along with their objectives and motivations. For example, is the development team on board with an application security program? Spend time with the parts of the organization that you are least familiar with such as operations, so you can see how they should be included in the decision-making process. Identify the security mandate as defined by your business. Does your organization need to achieve compliance with mandates such PCI DSS, NIST or HIPAA? Business drivers may originate from industry compliance obligations or internal policies, and your application security programs should align with it. Take a risk-based approach by identifying areas of highest-risk and then mitigating those risk. By getting the "lay of the land" you can answer questions such as:

- What are your most critical web and mobile applications?
- What security tools and services does my organization currently use?
- Where does security fit into the software development lifecycle?
- Which assessment type should we perform?

To make this process easier, you can start by taking a self-assessment test designed to give you an understanding of the status of your application security program and provide you with improvement suggestions..

Step 2: Start Small. Start Now.

The main hurdle that stops most organizations from embarking on an application security program is knowing how to start. The easiest way to get started is to pick one of your organization's web applications and run it through an assessment. You can do this by using the Fortify on Demand free trial, which helps you quickly identify any potential vulnerabilities and see if the results from the scan line up with the self-assessment you just performed.

Putting your application through a trial scan enables you to get lightning-fast results and gain knowledge about the status of your application and how to proceed with your program.

Step 3: Measure Success and Outline Next Steps

Once you have tested the application, you can revisit your self-assessment and modify the requirements of your project. Use reports gathered from the trial to share what was discovered during the assessment with other stakeholders. You can communicate relevant metrics via a

Take a self-assessment test

Connect with Us
OpenText CEO Mark Barrenechea's blog

management dashboard or by filtering by severity, and quickly show identified critical vulnerabilities, even drilling down to the actual line of code and providing remediation recommendation along with example code.

This information not only helps you get a quick win at identifying vulnerabilities, it can set the stage for your plan to scale the program and secure all your applications.

Concluding Remarks

As recent cyberattacks have shown, applications are under attack more than ever and in at least half of these attacks sensitive data has been compromised. With the alarmingly high number of vulnerabilities found in web and mobile applications, it is imperative that organizations are prepared to defend themselves. A flexible, comprehensive application security program which includes SAST and DAST and fits into your business and development process is key to your Defense-in-Depth strategy and improving your organizational security posture.

Run your application through a quick assessment with an on-demand free trial.

Start Now!

About Us

OpenText™ is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from OpenText™ Data Security, ArcSight by OpenText™, and Fortify by OpenText™, the OpenText™ Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Fortify offers the most comprehensive static and dynamic application security testing technologies, along with runtime application monitoring and protections, backed by industry-leading security research. Solutions can be deployed in-house or as a service to build a scalable, nimble Software Security Assurance program that meets the evolving needs of today's IT organization.

Learn more at
www.microfocus.com/appsecurity
www.microfocus.com/opentext

264-000011-001 | O | 06/23 | © 2023 Open Text

opentext™