WHY BUSINESSES NEED APPLICATION SECURITY

kiuwan

APP SECURITY ESSENTIALS

Today, businesses cannot run without applications that allow customers to instantly interact with the applications they have at their fingertips. Customers want apps that perform perfectly every time they're used.

Web application exploits continue to be the most common form of external attack. In a recent survey on application security conducted by Forrester Research, 39% of companies reported they were victims of a data security breach as a result of web application exploits.

To improve a company's ability to shield itself, application security must constantly evolve to protect against data breaches and the latest web application threats. Application security can help avoid the potential negative business outcomes and instead focus on what matters:

- **Reduce risks of security infiltration**
- **Protect brand image**
- **Safeguard data against major and minor breaches**
- **Eliminate loss of revenue**
- **Avoid expensive downtime**
- **Address security and quality defects early**
- **Improve trust from customers/investors/lenders**

The Verizon 2020 Data Breach Investigations Report indicates that cloud-based data is continually a target for cybercrime, with web application attacks doubling to 43% in less than a year.

This article provides an overview of why businesses need application security.

WHAT IS APPLICATION SECURITY TESTING?

Application security testing is designed to protect software applications from external threats throughout the entire application life cycle. One of the main goals of application security testing is to protect the confidentiality of data within the application.

A web application attack is defined as any attempt by a malicious party to infiltrate and compromise the security of a web-based application. Attacks may either target the application itself to gain access to sensitive data or use the application as a foundation to launch attacks against users.

Attackers can use many different paths to get to your application with the ultimate goal of harming your organization. Each of these potential attacks represents a risk serious enough to warrant attention.

To guard against vulnerabilities that attackers can exploit, testing all your applications with basic vulnerability scanning throughout the entire software development life cycle is a necessity. This timeline encompasses the application life cycle through early requirements analysis, design, implementation, verification, and maintenance.

ASSESSING RISKS

Performing an initial security assessment should always be the first step to improving your company's security. This includes an application security code review, which is the manual review of source code with the developers to identify code-level issues that may enable an attacker to compromise an application, system, or business functionality.

To identify possible software and security vulnerabilities across all your web applications, a complete risk assessment should be performed. A risk assessment can reveal the most valuable IT assets at your company, the probability of an exploit, and the potential impact of a data breach on customers and the company itself.

This process is crucial because it's necessary to know the value of the information that may be compromised. This in-depth assessment can be performed by an in-house IT or security team. The assessment can also come from purchased external security tools that can come into play the moment a security breach is detected.

When effective testing methods are used to secure web applications, vulnerabilities in the source code or weaknesses in external software can be detected, remedied, and acted upon before the software is deployed.

DEVSECOPS PRACTICE

DevOps is the incorporation of tools and practices that strengthen a company's capacity to deliver applications and services at high speed. This practice leads to developing and enhancing products at a faster pace than traditional software development.

It makes sense to develop a security operations process (DevSecOps) that includes both operational teams and creates security testing methods that can monitor applications daily. These methods can include:

- **Dynamic application security testing (DAST).** Improves the detection of gaps and security vulnerabilities by changing the perspective of managers and placing them in the role of an attacker or hacker. This focuses on the behavioral testing of applications.

- **Static application security testing (SAST).** By inspecting the static source code of an application locally, vulnerabilities can be identified to reveal possible weaknesses in the system's internal operations.

- **Software composition analysis.** Manages the use of open-source solutions by performing automated scans of an application's codebase.

- **Runtime application self-protection.** Uses real-time application data to catch and kill attacks as they occur.

- **Interactive application security testing.** Combines DAST and SAST to use software to monitor application performance. It supports finding a broader range of security weaknesses in order to provide important information on the root cause of vulnerabilities, particularly specific lines of problematic code.

THE RISKS ASSOCIATED WITH WEAK APPLICATION SECURITY

Applications are a primary target for attackers, and threats to applications have become one of the most significant risks to business success. Consistently guarding against attacks can be challenging for security teams.

The risks to companies have never been greater. Despite the well-known and well-publicized security and data breaches that severely impact businesses on every level, web application exploits and attacks continue to occur every day, damaging some businesses beyond repair due to the loss of revenue and customer trust.

Developers, security teams, IT departments, and web companies must create a plan to ward off cyberthreats and attackers. Without a security solution in place, your company's web applications may succumb to the torrent of attacks and threats they continually face.

These attacks can include not only malicious code and vulnerability scanning, but also penetration testing (pen testing), distributed denial-of-service (DDoS) attacks, SQL injection attacks, buffer overflow, and more. The global cost of online crime is expected to reach $6 trillion by 2021, with the average cost of a data breach amounting to $3.92 million.

WHAT HAPPENS WHEN A BREACH OCCURS

When a threat is detected at your company, what happens next? What safety rules are in place and immediately available when a breach occurs? Who is accountable for web-based attacks and responsible for security testing? What protocol has your company implemented in the event of anattack?

These are important questions for your company's DevOps and DevSecOps teams. A strong security stance means you have the requisite means in place to protect your web applications from vulnerabilities and threats.

DETECTED VULNERABILITIES

A powerful security solution, whether created in-house or purchased externally, can and most likely will protect against an attack at some point in the life cycle of the application. Dynamic and static application security testing helps detect and identify vulnerabilities by examining code locally and in the process of deployment.

- **Uninitialized variables**
- **Application misconfiguration**
- **Credential/session prediction**
- **Directory indexing**
- **Insufficient authorization/authentication**
- **Automatic reference counting**
- **Cross-site request forgery**
- **Information leakage**
- **Insufficient transport layer protection**
- **Free non-heap variable**
- **Double free/close**
- **Insufficient binary protection**
- **Cross-site scripting**
- **Injection attacks**
- **Interprocess communication**
- **OS commanding**
- **Insecure cryptography**
- **SQL injection**
- **Cryptographic related attacks**
- **Buffer overrun**
- **Format string vulnerability**
- **Return pointer to local**

These may include a range of varying web application exploits and application vulnerabilities, including:
Cyberthreats Enabled by Poor App Security
Every phase of a company's application system is a potential target for hackers. Web and mobile applications now represent a significant portion of a company's vulnerability. For example, an app on an employee's cell phone with a connection to your network can become an open door for hackers. Whether you are creating apps for in-house use, buying apps for employee use, or selling apps, security is a critical step in the process.

Different industries are vulnerable to selected cyberthreats. For example, in 2020 in the retail industry, 99% of incidents were financially motivated, with payment data and personal credentials continuing to be prized. Web applications, rather than point-of-sale devices, are now the main focus of retail breaches.

For the financial and insurance industries, 30% of breaches were caused by web application attacks, primarily driven by external actors using stolen credentials to get access to sensitive data stored in the cloud. The move to online services is a key factor in generating the increased interest in these attacks.

A Facebook incident recently leaked information for half a billion users. Numerous sources disclosed the discovery of a pool of Facebook records, including information on more than 530 million users. The leaked data included personal information and was posted to a known website for hackers.

Once breaches emerge, they cannot be recalled or canceled, so it is essential for businesses to take a pre-emptive approach to security-forward designs, implementation, and testing prior to release.

COMMON TYPES OF WEB APPLICATION EXPLOITS

MALWARE

Malware describes malicious software, including viruses, spyware, worms, and ransomware. When a user clicks an infected link or email attachment, malware can breach a network through a vulnerability not discovered by security teams. Malware can do the following once it is inside a system:

- **Block admittance to key parts of the network (in the form of ransomware)**
- **Obtain sensitive information and transmit that data from the hard drive without the user's knowledge or awareness (as spyware)**
- **Install harmful software into the system**
- **Disrupt certain components to render the system inoperable**

PHISHING

Phishing starts with a fraudulent email or other communication that is intended to entice a victim to provide sensitive information. The communication appears to have come from a highly reliable source or an application that the victim either frequently uses or has used at least once in the past. The victim is manipulated into providing confidential information, such as login and password credentials or credit card numbers, often through a scam website.

FORM-JACKING

This is a type of attack where cybercriminals inject malicious JavaScript code into a targeted application or the form page of a website to take over the functionality of the page and covertly collect sensitive user information. It is most often targeted to a payment page form, where the data can be collected and reused or sold for nefarious purposes.

MAN-IN-THE-MIDDLE ATTACK

Sometimes referred to as eavesdropping attacks, man-in-the-middle attacks occur when hackers insert themselves between a device and the network it seeks to access. Once the hackers interrupt online access, they can steal data, including Social Security numbers, addresses, credit card data, and confidential banking information.

This is standard practice on unsecured public Wi-Fi connections when, without knowing, the victim passes all information through the attacker. In addition to stealing sensitive information, once the breach has occurred, an attacker can install malware to process all of the victim's information.

DISTRIBUTED DENIAL-OF-SERVICE ATTACK

Using the DDoS method, a hacker can flood networks, servers, or systems with enough heavy traffic to drain resources and bandwidth. When the application or system is unable to fulfill rightful requests, it becomes vulnerable to infiltration. Multiple compromised devices can be used to launch this attack.

SQL INJECTION

In what sounds like a complicated process, an attacker could carry out a SQL injection attack simply by presenting malicious code into a defenseless website search box. Malicious code can be inserted by an attacker into a server that uses a structured query language (SQL). It forces that server to reveal information that under normal circumstances would be protected.

ZERO-DAY EXPLOIT

Before a patch or solution can be implemented, a zero-day exploit swoops in after a network vulnerability is announced. During this window of time, attackers target the disclosed vulnerability in hopes of gaining information.

CREDENTIAL STUFFING

Credential stuffing is a cyberattack method where attackers use lists of compromised or stolen user credentials to breach into a system. These lists usually contain email IDs or usernames (thousands to millions) along with matching passwords and are used to gain illegal access to real user accounts using bots for automation and scale. It is based on the theory that many users reuse usernames and passwords across multiple devices and services.

HOW TO ENHANCE APPLICATION SECURITY

MAKE SECURITY ASSESSMENT YOUR TOP PRIORITY

As noted earlier, assessing risk should always be the first step to improving your comprehensive security methods. A risk assessment serves to reveal the most valuable and essential IT assets at your company's disposal and determine the probability of an exploit.

This in turn would reveal the probable impact of a data breach and point to the next steps in enhancing your security infrastructure. This assessment can be performed by an in-house IT or security team or conducted by a third-party security tool like Kiuwan that can help implement this process for you.

MAKE THREAT DETECTION AND REMEDIATION AN AUTOMATIC PROCESS

Incorporate technology that accommodates automated threat detection in order to keep application security continually proactive instead of reactive. With the plethora of modern applications, it's not possible to cover all possible threats. Human error is a huge factor in software vulnerabilities. The best approach is to have the application recognize and remediate threats without the need for continual human intervention.

MAKE PERIODIC CHECKS AND IMPLEMENT UPDATES AS NEEDED

To maintain a strong security protocol, don't allow your security tools and practices to become outdated. They have to be regularly renewed and adjusted to maintain optimal results.

IT and security teams should make frequent changes and corrections to stay a step ahead of modern threats. Moreover, they need to stay current with advancements in security technology and organize updates and reassessments regularly to ensure that corrupt parties are not taking advantage of outmoded technologies in your web applications.

LET BUSINESS IMPACT GUIDE YOUR DECISIONS

By prioritizing and fixing the risks that will have the largest influence on your business, you can save time and money. Determining the effect of these risks on business-critical applications will serve you well in the effort to prioritize what must be patched and remediated.

DEVSECOPS PRACTICE

Implementing a developmental security testing operation should help you integrate security into daily application monitoring. This is critical as approaches for new attacks and breaches are created every day. Waiting to do security audits at the end of the quarter provides too much of an opportunity for attackers to gain access to your system before you can examine it.

CREATE AND USE AN INCIDENT MANAGEMENT PLAN

An incident management plan is a pivotal component of being proactive in your company's security. This plan empowers the IT and security teams to know what to do when they encounter a security breach. It will manage your time and efforts more efficiently. You may want to conduct a test security breach to check the effectiveness of your incident management plan.

BEST PRACTICES AND BENEFITS OF APPLICATION SECURITY TESTING

Web security can benefit businesses that leverage software, especially companies in the banking, financing, and insurance industries. For these businesses, application security testing is a business imperative. The best testing protocols allow organizations to prioritize security issues based on high-impact threats and the financial cost of immediately designating the resources needed for remediation. Of particular concern to the banking and financial industries is the revelation that financially motivated attacks and data breaches account for 91% of cases in North America. 75% of banking and finance software developers struggle to detect vulnerabilities across a range of development environments.

With the Kiuwan platform, DevSecOps teams can easily identify vulnerabilities in their software and rapidly remediate them to prevent challenges in the deployment. Even if you implement a robust password-changing protocol, this does not solve your data breach problems. A full 33% of breaches were associated with either phishing or pretexting to gain stolen credentials, which is more of an internal dilemma as ackers essentially gain access to your code by permission.

With such a vast threat landscape, testing all critical systems should be a fundamental and primary concern to IT and security teams in all industries, large or small, publicly or privately owned. The best practice approach is obtaining data from multiple scanning tools to produce actionable information that will inform the four most problematic issues facing application security in the banking, financing, and insurance industries:

VISIBILITY

Determining who is responsible for the app security of your business is an issue of visibility and accountability. No one can be held responsible for data breaches or web attacks when managers or |security team leaders don't have the visibility they need into risk and security gaps.

DEVSECOPS PRACTICES

For web application security to get the type of comprehensive coverage needed by your company, application security teams must work with DevOps teams. DevSecOps is rooted in the need to execute security measures at the speed and scale of DevOps. This practice should occur at all stages of the software development life cycle. Security must be tightly integrated into DevOps for true and accurate DevSecOps to be realized.

MANAGEMENT OF SECURITY TOOLS

No individual tool can do everything a company requires with regard to the safety of its web applications. Many companies use several security tools to test their code. These tools can sometimes generate vast amounts of dissimilar vulnerability data, and it can be challenging to wade through the different formats and assessments.

Selecting an all-encompassing platform like Kiuwan can make a difference in your company's security stance or posture by making security data accessible and understood by all interested parties.

SECURE PRIORITIES

It can't be stressed enough that a comprehensive real-time view of risk is what separates you from your competitors. Sorting through data to prioritize what really matters is what allows you to make business and operational decisions based on clear information. Security is an ongoing process, and every breach must be evaluated using legitimate data to build and measure priorities.

SMALL AND MEDIUM-SIZED BUSINESSES ARE ALSO UNDER ATTACK

The increased implementation of cloud and web-based applications in all industry types has made small and medium-sized businesses vulnerable to attack, and they are now a high-level target for cyberthreats and web application infiltration.

Phishing is the most prominent threat for small businesses and accounts for over 30% of data breaches, followed at 27% by the use of stolen credentials. Stolen credentials were also found in over 20% of attacks against web applications. Attackers targeted login credentials and personal data containing sensitive materials such as payment information and medical records.

THE ROLE OF KIUWAN CODE SECURITY

Kiuwan provides effective static application security testing and source code analysis as a fully integrated security solution for your DevSecOps process.

Sensitive data is continually at risk of being compromised by malicious actors. Strengthening security against external threats should take precedence over other IT and security operations. Kiuwan offers affordable solutions for teams of all sizes.

Static application security testing (SAST) is the most effective way to detect vulnerabilities in application source code. This approach allows businesses to remediate vulnerabilities early in the software development process before security flaws make it into the build and deployment pipeline. This can significantly reduce the cost of remediation.

Moreover, a SAST solution integrated into the development environment facilitates a DevSecOps approach that makes security everyone's responsibility. The best approach is one that helps drive productivity and collaboration by automating infrastructure and workflows as well as evaluating performance.

CUSTOM SECURITY BUILDS

Build custom configurations with the intuitive features of Kiuwan Code Security. Automatically generate action plans to remediate the defects found based on either the effort required by the development teams or the rating you want to achieve.

You can determine the way you view the criticality of your applications, either distributed by files or vulnerabilities. Kiuwan compliance reports meet all well-known market standards (OWASP, CWE, MISRA, NIST, PCI, and CERT, among others), and we are the only platform to support 30-plus programming languages.

INCREASE SECURITY — AND LOWER YOUR COSTS

Today, most companies need software to support their business, whether a pivotal point of contact with customers or a SAST that runs behind the scenes facilitating work. Methods of code security can be developed internally or purchased from a third-party solution like Kiuwan.

The decision to integrate Kiuwan code security in your development process will reduce risk and cost, thanks to the early detection and correction of newly introduced vulnerabilities. Kiuwan code security enforces a rigorous approach in the detection of security vulnerabilities.

Remember that all companies have similar needs concerning security:

- **To detect web application vulnerabilities and remedy those issues before deployment**
- **To identify safety protocols while the application is deployed**
- **To gain more significant management and control of web application development**
- **To manage the costs connected to development, maintenance, and remediation**
- **To reduce the number of corrupt attacks affecting the performance and efficiency of their software**

The Kiuwan code security platform can address all the above needs, regardless of the size and level of complexity of the development process.
DON'T WAIT FOR AN ATTACK REQUEST A **FREE TRIAL** OR A **DEMO** TODAY

GET IN TOUCH

Headquarters
2950 N Loop Freeway W, Ste 700
Houston, TX 77092, USA

United States: **+1 732 895 9870**
Asia-Paciifc, Europe, Middle-East and Africa: **+ 44 1628 684407**

contact@kiuwan.com
Partnerships: **partners@kiuwan.com**