Sonatype

WHITEPAPER

Understanding & Addressing OWASP's Newest Top Ten Threat: Using Components with Known Vulnerabilities

OVERVIEW

Many organizations turn to the Open Web Application Security Project (OWASP) to help ensure that their code and applications are secure. Recently OWASP's Top Ten list of application security risks was updated to include "A9: Using components with known vulnerabilities."

The full description from OWASP states "Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts."

Why has managing and securing components become a priority? Simply put, components have become a rich attack vector because of their pervasive reuse. Reuse that makes it easy for hackers to propagate their attack across multiple applications and multiple organizations.

This means organizations need to expand their security approach to accommodate components – which are re-usable blocks of code that are assembled together to create an application. Components can be created and re-used within an organization's development team – but most often they are downloaded from public repositories such as the Central Repository. These re-usable components now comprise approximately 90% of an average application thus exposing organizations to potential security, license and quality risks.

Why has managing and securing components become a priority? Simply put, components have become a rich attack vector because of their pervasive reuse. Reuse that makes it easy for hackers to propagate their attack across multiple applications and multiple organizations. This component challenge is exacerbated by the fact that the application is the threat vector of choice – and hackers can increase their exploit rate by going after vulnerable components. Instead of identifying an exploit in individual applications (which can't be reused for exploits against other applications), once a component vulnerability is discovered, a hacker can blast that exploit across the web looking for other applications that use that same component.

CHALLENGE

Existing approaches are not designed for how applications are constructed today. For example:

- Most existing application security tools are designed for source code, not open source components. Components are binaries so attempts to scan them using traditional application security tools often yield false positives which drag down development velocity.
- Managing components in a development environment is generally a manual, cumbersome effort. Attempts to govern usage often fail to keep up with the variety, complexity and release cadence of components used in an agile environment.
- Even though applications have become a primary threat vector, organizations generally focus more budget and energy on network and perimeter defenses.

Process and communication need to be re-engineered to ensure trusted applications. Ideas include:

- Ensuring developers are educated with respect to security, and that they place a high priority on delivering secure applications.
- Ensuring the security team works effectively with the development team and other constituents on timely collaboration and communication.
- Ensuring the integrity of the components that are downloaded (that they have not been compromised – they are what you think they are, they came from who you think they came from).

Component usage introduces the need for new development requirements, such as:

- Standardizing usage of components based on acceptable security, license and quality risks. However, without the proper tools and processes this is difficult to enforce.

OWASP Top Ten, updated 2013

A1-Injection

A2-Broken Authentication and Session Management

A3-Cross-Site Scripting (XSS)

A4-Insecure Direct Object References

A5-Security Misconfiguration

A6-Sensitive Data Exposure

A7-Missing Function Level Access Control

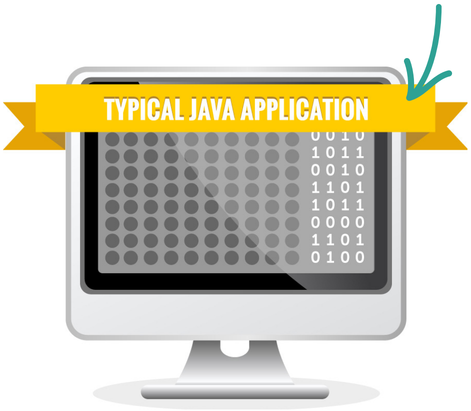
A8-Cross-Site Request Forgery (CSRF)

A9-Using Components with Known Vulnerabilities

A10-Unvalidated Redirects and Forwards

71% of all applications contain a critical flaw in at least one open source component.

These days, 80% of an application is assembled from open source components.



Yet, only 57% of organizations have policies governing component usage.

- Understanding which components have been used - and where - so that risk can be assessed and remediation efforts are possible.
- Updating components as new versions are released and making those revisions in live production applications.
- Monitoring risk to determine which components have vulnerabilities. However, this is generally a manual and time-consuming effort since public sources do not provide intelligence in a standard, searchable way and it is often hard to find information for a specific version number.

Continuous monitoring is needed to assure long-term trust. For example:

- Hackers are not complacent. Today's trusted component may be tomorrow's vulnerability.
- Newer component versions not only improve security, but generally also improve overall quality and functionality.

OWASP is the tip of the iceberg – it is referenced by other standards, some of which require actual certification. Therefore:

- Meeting OWASP guidelines is not only a best practice, but also may be mandatory if your organization is governed by PCI, SANS, BSIMM, NIST and others who rely on OWASP guidelines to be met as part of their certification.

SOLUTION

Sonatype specializes in open source governance, management and compliance and, therefore, is ideally suited to guide organizations through the new A9 guideline.

Sonatype Component Lifecycle Management (CLM) is the first solution to deliver component information, controls, and remediation options directly into the tools that developers use every day. By uniquely identifying components, making it easy to fix flaws early, and enforcing policy at every phase of the software development lifecycle, Sonatype CLM eliminates security and other risks in open source software.

CLM is the first practical way to automate governance of open-source component usage throughout the software lifecycle and eradicate flawed components from production applications. Sonatype CLM addresses each of the OWASP A9 recommendations for avoiding the use of insecure components head-on. These include:

1. Identify the components and their versions you are using, including all dependencies. (e.g., the versions plugin).
2. Monitor the security of these components in public databases, project mailing lists, and security mailing lists, and keep them up-to-date.
3. Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and meeting license guidelines.

Sonatype CLM goes beyond these recommendations and is designed to manage the entire component lifecycle. CLM integrates security, licensing and quality information about the components directly in the tools that developers use (repository manager, IDE, build/CI environment), provides early and quick remediation capabilities, and continuously monitors your production applications.

OWASP New Top 10 List Includes Secure Component Requirement

"OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted… We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas."

OWASP has recognized the critical role that components play in today's applications. OWASP updated their Top 10 list to include A9, which states that applications should avoid using components with known vulnerabilities. The standard includes these best practices:

- Identify the components and the versions you are using, including all dependencies.
- Monitor the security of these components in public databases, project mailing lists, and security mailing lists, and keep them up-to-date.
- Establish security policies governing component use, such as requiring certain software development practices, passing security tests, and acceptable license.

According to Jeff Williams, founding member of OWASP and CEO of Aspect Security.

"The performance, time and cost advantages of agile, open-source development comes at a price - you have to ensure the components you use are up-to-date and secure.

. . .

Unfortunately, it's not trivial to figure out what components you applications are using, and even harder to figure out which vulnerabilities apply to those components.

. . .

The new OWASP Top Ten has detailed recommendations for locking down your software supply chain, and Sonatype's tools make them much easier."

Although Sonatype CLM is closely identified with A9, it provides the ability to support the entirety of the OWASP Top 10 as it relates to the components that are being used to construct applications. Sonatype CLM does this since the vulnerabilities that are discovered for the components include those documented in the Top 10. For example, Injection, Cross-Site Scripting (SXX), Insecure References, etc., that are discovered in the components are identified and managed by the CLM solution.

WHY SONATYPE?

Sonatype CLM is uniquely designed to support component-based, agile development.

- Instead of automating the approval workflow, Sonatype CLM automates the actual policies so that organizations can keep pace with the volume, variety, complexity and release cadence of components.
- Sonatype CLM uses automation to guide and enforce action in the tools that developers use today, freeing up humans to focus on building policies and managing exceptions.

Sonatype CLM is effective throughout the entire software lifecycle.

- Sonatype CLM is naturally integrated in the tools that developers use to build applications – out of the box, we don't just give you an API and an SDK and tell you to build your own integration.
- Sonatype CLM produces results that are available instantaneously – developers have the information they need to select the best component from the start, and information necessary to assess their builds or continuous integration efforts. The information is available without the delay associated with tools that are dependent on intensive and time-consuming scans.

Nearly 2/3 of organizations don't know which components are used in their applications.

In manufacturing we call this a "Bill of Materials"

Sonatype CLM provides guidance that prevents problems and remediates flaws that are discovered.

- Sonatype CLM aggregates, and augments vulnerability data by leveraging multiple sources and doing additional research that pinpoints the vulnerability to specific version numbers. This information is then presented using an intuitive, graphical display directly in the tools that are used to develop, build and release the applications.
- Sonatype CLM doesn't stop with problem identification, it prevents and remediates flawed components. Problems are prevented from the start by providing information in the IDE to empower developers to pick the best components from the start. And if policy violations are found, Sonatype CLM provides the information necessary to pick the best replacement version and to migrate to that version with a single click directly in the IDE.

Continuous trust for production applications

- Sonatype CLM extends support to applications that are in production. Sonatype CLM monitors the application inventory non-invasively and notifies the appropriate individuals if a new security vulnerability has been detected. It provides information to help triage the flaw, remediation support, and the ability to help manage the release process to get the new application version deployed as quickly as possible.
- Sonatype CLM provides a complete view of enterprise risk for component-based applications by providing dashboards that include summary and detailed views. Organizations can assess their overall risk exposure and stay abreast of new vulnerabilities.

Most application security methods can't see components.

Today's popular application "scanning" tools don't assess components (or their dependencies).

Sonatype provides information to help triage the flaw, provides remediation support, and provides the ability to help manage the release process to get the new application version deployed as quickly as possible.

ADDITIONAL INFORMATION

OWASP Press Release - http://www.sonatype.com/news/software-component-vulnerability-cited-as-latest-application-security-threat-in-owasp-top-ten-list-sonatype-first-to-provide-comprehensive-solution#.Umkui2RAQ_A

CLM Press Release - http://www.sonatype.com/news/sonatype-ushers-in-new-era-of-application-security-aimed-at-eliminating-risk-in-the-modern-software-supply-chain#.UmkuuGRAQ_A

Sonatype's OWASP A9 Blog Post - http://blog.sonatype.com/people/2013/06/a9_nexusclm/#.Um_ThezD99M

OWASP Website - https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities

Sonatype's software protects the world's enterprise software applications from security, compliance, and licensing threats. Every day, millions of developers build software applications from open source building blocks, or components. Customers rely on the Sonatype family of products to accurately identify and analyze component usage and proactively fix flawed components throughout the software development lifecycle so applications are secure and comply with licensing and regulatory requirements. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures.