International Journal of Management, IT & Engineering
Vol. 13 Issue 04, April 2023,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Secure Software, Secure Future: The Benefits of Product Security

Sunil Kumar Rangineni

Abstract

In this article, we will discuss Product security– DevSecOps practices and its benefits, and best practices to be followed:

A Seasoned Cybersecurity professional with 15 plus years of experience in the Information Security domain, with profound knowledge, focusing on solving organizations' pain points in the Cyber Threat landscape.

Proven track record in securing critical infrastructure, such as global financial markets and pharmaceutical Industries, against evolving cyber risks. I have a deep knowledge of security standards and regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and have experience in developing and implementing security policies.

As a Cybersecurity Enthusiast, my sole intent is to bring Cybersecurity Awareness around organizations and train Engineers to handle them. With this Intent,I actively participate in serving multiple Cybersecurity forums and organizations. As a participant,I aim to serve, assist and improve the security awareness of participants. The outcome of such sessions is to train the participants to protect themselves from constantly evolving threats.

1. Introduction:

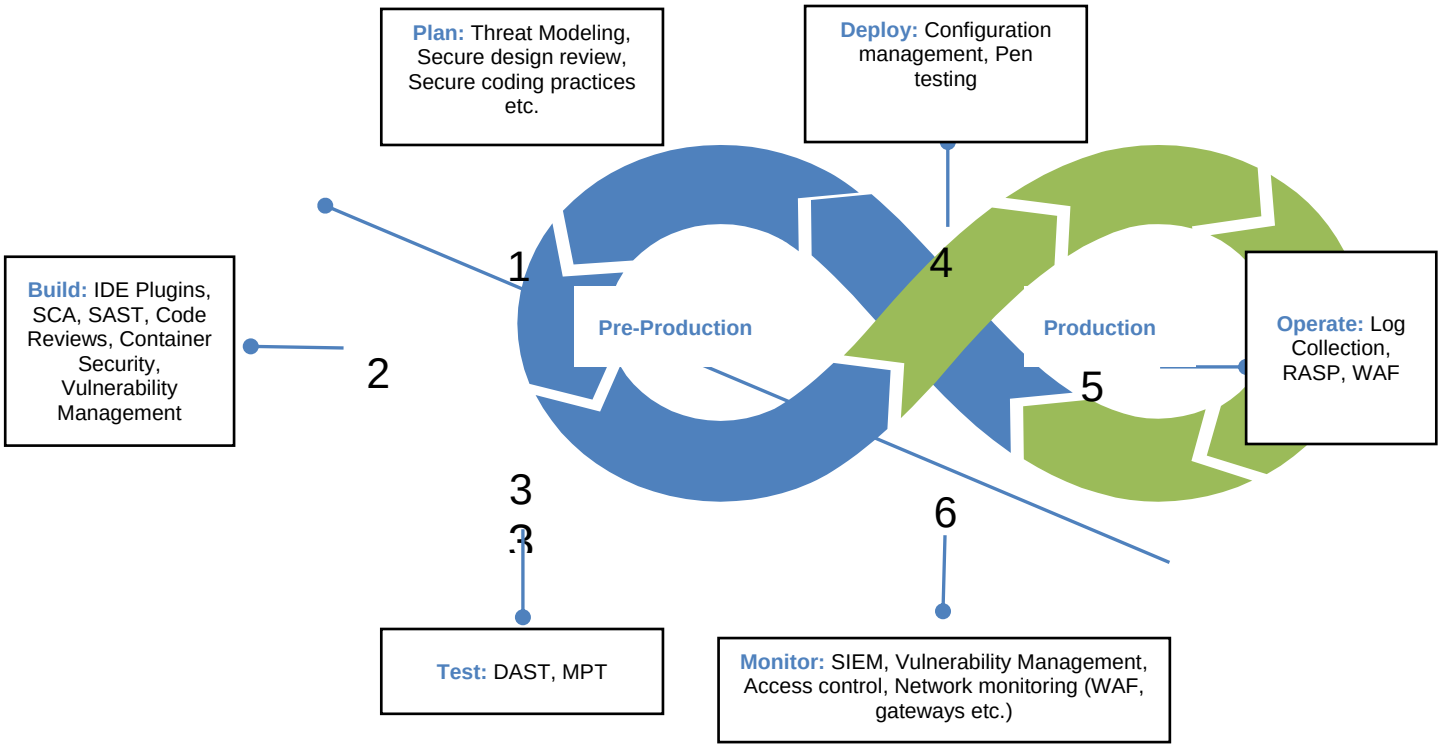
Product Security is an evolving field, which refers to measures taken to ensure that a product, it can be software or hardware, is developed through a security-conscious approach, incorporating security into every aspect of the design, development, testing, and maintenance process. The primary focus of our article is on the software (Web applications, Webservices, Mobile applications, and Associated IT Infrastructure devices). In recent times we are seeing multiple advancements made to technology, building multiple APIs, and increase in the number of connected devices to an application or product has increased. The primary mission is to avoid sensitive data theft and protect products from security threats, ensuring the security of these products has become a top priority.This is achieved by ensuring security is added to every stage of the product lifecycle.By implementing strong product security measures, companies can mitigate the risk of security breaches and safeguard their customers' data and assets.

2. What is Product Security?

Product Security is a process within the Cybersecurity function, which aims to deliver a secure product, which includes the organization’s Web applications, Web services, Mobile applications, or any hardware manufactured. This focuses on considering security at every stage, starting from Design, development, implementation, maintain. This is a continuous process that requires collaboration across teams and stakeholders.

Product Security involves multiple activities, including threat modeling, Security testing (Static application security testing (SAST), Dynamic application security testing (DAST), Penetration Testing, Secure coding practices, Incident response, and Continuous monitoring. The primary goal of product security is to protect the CIA (Confidentiality, Integrity, and Availability).

Standards used: In my opinion, multiple standards apply to secure a product, some of them are SDL (Microsoft Security Development Lifecycle), CIS Controls, National Institute of Standards and Technology (NIST) Cybersecurity Framework, Secure Software Development Framework (SSDF), OWASP Top 10, SAN 25, Penetration testing standards, etc.,



Product Security: DevSecOps, Shift Left (Securing the product throughout SDLC cycle)

3. Why do we need product Security?

We need product security to defend the products from security threats/risks posed by the threat actors. Some of the common routes observed for product security are:

Injection Issues: This is a Security vulnerability, where it allows a threat actor to inject malicious code / untrusted data when the application fails to validate or sanitize the input.

Security Misconfigurations: Opening up the unused or unsecured ports, which results in compromising the application or a product i.e., Unauthorized access to an application and its data.

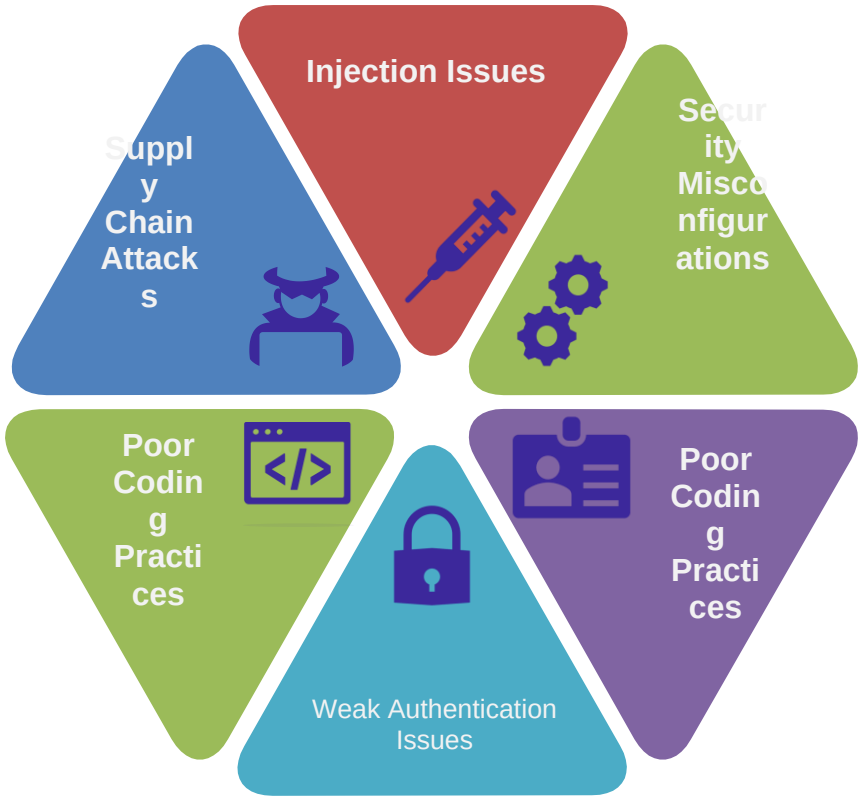
Security updates (OS and 3rd Party application library Vulnerabilities): When the systems, applications, or products are not patched or updated with the security vulnerabilities

Weak Authentication mechanism: Applications or systems still use the easily guessable username and passwords / using the default credentials.

Poor Coding Practices: Following poor/insecure coding practices

Supply Chain Attacks: Attack which compromises a product or its associated components, this works by carrying the malicious software or a component via a supplier or vendor.

To overcome these issues vectors and to deliver a secure product, we need to consider them at every stage of your SDLC (Software Development Lifecycle) process.



4. Product Security Threats

Below listed are some of the common product security vulnerabilities reported:

- **Cross-Site Scripting (XSS):** Malicious scripts are injected into trusted websites
- **SQL Injection:** Used to exploit a vulnerability in a web application that uses a database. Allowing the attacker to inject malicious code into the database
- **Remote Code Execution:** Attackers remotely execute commands to place malware or other malicious code on your computer or network
- **Denial of service:**An attack that attempts in making an application or any infrastructure resources to be unavailable
- **Buffer overflow:** A vulnerability that occurs when a program tries to write more data to a buffer than it can hold

5. Best practices to be considered for Product Security

Below listed are some of the best practices to be followed for a successful product security program.

- Ensure proper threat modeling, Security Architecture, and design reviews are performed.
- Training or empowering the developers on secure coding practices
    - Create a culture of security within your organization by offering security training and awareness programs, and by emphasizing the importance of security throughout the entire development and deployment process. By doing so, you can help ensure that everyone involved in the product development lifecycle is aware of the potential security risks and is equipped to address them. This can help mitigate vulnerabilities and reduce the risk of security incidents.
- Following the established coding standards and frameworks, sSDL (Microsoft Security Development Lifecycle), CIS Controls, National Institute of Standards and Technology (NIST) Cybersecurity Framework, Secure Software Development Framework (SSDF), OWASP Top 10, SAN 25, Penetration testing standards, etc., to ensure that your code and product is secure
- Integrating Spell checkers to the Developer IDE's (e.g.: Secure Code warrior) identifies the vulnerabilities within the code as the developer types their code
- Secrets management allows organizations to remove these hard-coded secrets from DevOps tools within the CI/CD pipeline.
- Ensure the developed code is fully tested, and adequate security testing is performed (E.g.: SAST, DAST, and Manual Penetration testing)
- Proper access controls and authorization to be setup
- Data Encryption: Ensure data is encrypted both in transit and at rest
- Monitoring and logging: To continuously monitor which helps in the detection or response to security incidents
- Setting up strong Vulnerability management and configuration management programs
- Follow the principle of least privilege, to prevent unauthorized access.
- Implementing strong network controls (WAF, IDS, IPS,etc.)

6. Benefits of Product Security

- Protects the applications / Products from unauthorized access, sensitive data exposure
- Reduces the cost of the security incidents
- Great saving of remediation timelines, as we implement the security at every stage of this process
- Maintains customer trust and loyalty
- Great brand reputation
- Protects from financial losses

7. Key components of Product Security (Testing Standards)

Multiple security frameworks are in use, some of the common frameworks are:

Center for Internet Security (CIS) Controlsframework which provides securitycontrols that organizations can implement to improve their overall security posture.

National Institute of Standards and Technology (NIST) Cybersecurity Framework:a framework that outlines standards, guidelines, and best practices to help organizations manage and mitigate cybersecurity risks. This framework includes a specific emphasis on product security and offers a versatile approach to managing cybersecurity risks.

Open Web Application Security Project (OWASP):Framework for developing secure web applications. I wanted to emphasize more related to this framework as securing the application or products at the build stages will avoid multiple security breaches and exploitations. In my opinion, I see this as a base or starting point for product security.

The **OWASP Top 10**serves as a guide for developers and organizations to prioritize and address security risks in their products.

Below listed is the **OWASP TOP 10 standards list**:

Injection flaws: Attackers can exploit these vulnerabilities by injecting malicious code into an application's input fields. Once injected, this code can be executed by the application's backend, potentially allowing the attacker to take control of the system or steal sensitive information.

Broken authentication and session management: The application fails to adequately manage user authentication and session tokens; it can create vulnerabilities that enable unauthorized access to sensitive information or functionality.These vulnerabilities can pose a significant threat to the security and integrity of an application and its users' data.

Improper input validation: The application fails to perform sufficient validation of input data; it can create vulnerabilities that attackers can exploit by submitting malicious input. This leads to various injection attacks, cross-site scripting attacks, and other types of data manipulation. These vulnerabilities can be especially dangerous because they can allow attackers to take control of the application or gain access to sensitive data.

Security misconfiguration: Vulnerabilities can arise when an application is not properly configured, attackers can exploit the vulnerabilities and gain unauthorized access to sensitive data or systems. This may lead to complete control of the system.

Insecure communication: This occurs when an application communicates through a secure channel (Plain text), This enables the threat actor to intercept and extract the data.

Poor access control: The application fails or does not properly restrict access to sensitive functionality or data, allowing unauthorized users to access or modify information they should not have access to.

Insecure design: vulnerabilities occur when an application is designed with security flaws.

Insufficient logging and monitoring: Vulnerabilities occur when the application does not properly log security events or monitor for suspicious activity which makes it difficult to respond to threat attacks.

Software and data integrity failures: When an application doesn't check that it is software and data are correct and haven't been changed by attackers, it can create vulnerabilities that allow attackers to manipulate or damage the system. This can lead to data breaches or other types of security incidents that could cause significant harm.

Server-side request forgery (SSRF): Vulnerabilities can arise when an application handles URLs supplied by users. Attackers can take advantage of these vulnerabilities by sending malicious requests to internal resources, which could result in data theft or unauthorized access. These types of attacks can be particularly dangerous because they

may allow attackers to gain access to sensitive data or systems that are not intended to be accessible from the outside.

8. Conclusion

In conclusion, implementing product security is key for any organization to secure applications or products from external threat attacks. Allows Organizations to measure, detect identify, prevent, and mitigate security risks. By adopting product security culture organizations can protect their assets and clients.

Reference: https://owasp.org/www-project-top-ten/