AppSec Cheat Sheet

Fortify

Glossary of terms frequently used in application security.

Application Programming Interface (API)
A software intermediary that lets a product or service interact with other products or services without having to know how they are implemented. APIs allow two applications to talk to each other.

API Security
A process to find possible vulnerabilities in APIs, getting them fixed, and protecting APIs from potential exploits.

Binary Code Analysis
A threat assessment and vulnerability testing at the binary code level.

Breach
Any incident that results in data, applications, networks, or devices being accessed without authorization.

Container Security
The process of implementing security tools and policy to protect the container against cybersecurity threats and ensure that the container is running as intended.

Common Vulnerability and Exposure (CVE)
A system that identifies and catalogues vulnerabilities in software or firmware for publicly known information-security vulnerabilities and exposures.

Compliance Standards
A set of government-mandated or corporate-defined guidelines. Examples include HIPAA or Europe's GDPR.

Data Security
The process of protecting data from unauthorized access and data corruption throughout its lifecycle. It includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms.

DevOps
A culture, movement, or practice that provides a vehicle for organizational transformation from siloed, traditionally adversarial groups to collaborative, shared ownership teams. Its common goal is to support the practices of automating software delivery and infrastructure changes and create a culture and environment where building, testing, and releasing software happens rapidly, frequently, and more reliably.

DevSecOps
An extension of DevOps with the goal of continuously integrating security within the development environment (IDE). The tools and process must be able to automate some security gates to keep from slowing down the DevOps workflow.

Dynamic Application Security Testing (DAST)
An application security tool that analyzes a web application from the "outside in," through the front-end, to find vulnerabilities through simulated attacks.

Exploit
Taking a particular action or set of actions that cause software to behave in a manner that deviates from its designed intent.

Firewall
A network security system that monitors traffic to and from your network based on predetermined security rules.

Interactive Application Security Testing (IAST)
A combination of SAST and DAST techniques that provide faster and more accurate results. IAST analyzes code for security vulnerabilities while the application is running, gathers information to continuously monitor how the application is performing, and identifies vulnerabilities in real time.

Issue Severity
The impact that a defect has on the development or use of a program. There are four categories:
Critical: Intruders can potentially gain access to the host or leak highly sensitive information. The exploitation is usually straightforward.
High: Intruders might be able to gain access to specific information stored on the host; it can result in significant data loss or downtime.
Medium: Intruders usually manipulate individual victims to obtain access to sensitive information or exploit known vulnerabilities to software versions.
Low: Intruders can collect information about the host and might be able to find other vulnerabilities to exploit. These vulnerabilities usually have low impact on the business.

Malicious Code
An application security threat designed to perform an unauthorized process that will create system vulnerabilities that can impact the confidentiality, integrity, or availability of an information system.

Microservice
A decentralized approach to software development, where larger applications are broken down into smaller components, or microservices, and developed separately and concurrently.

Mitigate
Establish a plan to handle threats on a computer, server, or network by eliminating or reducing their possible impact through corrective actions, prevention, or remedies.

Mobile Application Security Testing (MAST)
The process of finding and fixing security issues in mobile application across devices, networks, and servers.

National Vulnerabilities Database (NVD)
The U.S. government repository of standards-based vulnerability management data, represented using the Security Content Automation Protocol (SCAP).

AppSec Cheat Sheet

Fortify

Open Source Software
Code that is designed to be publicly accessible. The copyright holder grants anyone the rights to see, use, modify, and distribute the code.

OWASP Top 10
A list of the most critical security risks to web applications, globally recognized by developers as the first step towards more secure coding.

Patching
A patch is a set of code inserted into an executable program to repair a vulnerability or flaw identified after the release of an application or a software program.

Patch Management
The process of distributing and applying updates to software in a network of computers.

Penetration Testing (Pen Testing)
A technique to find vulnerabilities in a computer system by simulating a cyberattack against a computer system to check for exploitable vulnerabilities.

Quality Assurance
The process of ensuring that all software complies with defined standards to ensure proper quality of the software and avoid problems when delivering products or services to customers.

Remediate
The process by which organizations identify and resolve threats to their systems by addressing existing vulnerabilities.

Runtime Application Self-Protection (RASP)
A technology that detects attacks on an application in real time. It directly measures attacks from the inside and prevents exploits from within.

Secure Coding
A set of practices that applies security considerations to how software will be coded and encrypted to best defend against cyber-attacks or vulnerabilities.

Security Information and Event Management (SIEM)
A software solution that collects, aggregates, and analyzes activity throughout the organization's technology infrastructure and generates reports on security-related incidents and events to alert them of a potential security issue.

Social Engineering
An attempt to manipulate people to give up confidential information that can be used to attack systems or networks.

Software as a Service (SaaS)
A software delivery and licensing method that is based on a subscription and is centrally hosted, rather than being purchased and installed on individual computers.

Software Vulnerability
A mistake in software that can be directly used by a hacker to gain access to a system or network.

Software Weakness
Flaws, faults, bugs, vulnerabilities, and other errors in software implementation, code, design, or architecture that, if left unaddressed, could result in systems and networks being vulnerable to attack.

Source Code
A human-readable list of commands that a programmer compiles into an executable computer program.

Static Application Security Testing (SAST)
An AppSec tool that analyzes the application from the "inside out" by scanning an application's source, binary, or byte code.

Software Composition Analysis
A methodology that provides users better visibility into the open source inventory of their applications by identifying potential areas of risk from the use of third-party and open-source components.

Threat
A potential negative action or event facilitated by a vulnerability, with the potential of adversely impacting organizations through an information system.

Threat Modeling
A process to identify potential threats or lack of appropriate safeguards to prioritize mitigations.

Vulnerability Management
The ongoing process of identifying, classifying, and remediating security holes.

Web Application Firewall (WAF)
A solution (either hardware or software) that sits between your app and the public internet and tries to identify and block those inevitable attacks.

Zero Day
A currently unknown flaw to the software maker or to antivirus vendors.