Skills Network

Application Security for Developers and DevOps Professionals

Module 1 Glossary: Introduction to Security for Application Development

Welcome! This alphabetized glossary contains many of the terms in this course. This comprehensive glossary also includes additional industry-recognized terms not used in course videos. These terms are essential for you to recognize when working in the industry, participating in user groups, and participating in other certificate programs.

Estimated reading time: 12 minutes

Term	Definition
Access control	Security measures employed to govern and control the access and permissions provided to users, processes, or entities operating within a system or network.
Alerting	Responsive component of a monitoring system that performs actions based on changes in metric values.
Application layer	The seventh and topmost layer of the OSI model is used by developers for building and deploying applications.
Application Programming Interface (API)	A collection of guidelines, protocols, and tools that allow diverse software applications to communicate with each other.
Asymmetric encryption	When different keys are used to encrypt and decrypt.
Authentication	Process of verifying a user's identity.
Authorization	Process of determining a user's access rights.
Checksums	Derived values from data employed to identify errors that may have occurred during the transmission or storage of that data.
CI/CD	CI/CD, which stands for continuous integration (CI) and continuous delivery (CD), creates a faster and more precise way of combining the work of different people into one cohesive product.
CI/CD pipeline	The continuous integration/continuous delivery (CI/CD) pipeline is an agile DevOps workflow focused on a frequent and reliable software delivery process.
Code scanners	Provide vulnerability reporting and insights after they scan code in your repositories.
CodeSonar	A static code analysis tool from GrammaTech used to find and fix bugs and security vulnerabilities in source and binary code.
Container scanning	Scans code deployed to containers, which may contain vulnerabilities and security threats.
Containers	Executable software units in which application code is packaged along with its libraries and dependencies in common ways to run the code anywhere, whether it be on a desktop, traditional IT, or the cloud.
Coverity	An incremental analysis scanner for programming languages such as C, C++, Java, and Python.
Cryptographic keys	Essential tools used to secure data from cyberattacks during transmission and storage.
Cryptographic service	A confidentiality service that keeps data secret. Its purpose is to secure data from others, even when the data traverses a non-secure network without the necessary credentials.
Data link layer	The second layer of the OSI model transforms the transmitted raw data into a line free from undetected errors.
DevSecOps	DevSecOps (DevOps with an emphasis on security) is a set of practices that automate security integration across the software development lifecycle (or SDLC), from original design to integration, testing, deployment, and software delivery.
Dialog control	Refers to the management and coordination of communication sessions between two devices or systems.
E-commerce transactions	Refer to the buying and selling of goods and services over the internet.
Encryption	Process of encoding information so that only those users with authorized access can decode it.
Endpoint security	Detects application and system anomalies and protects systems, servers, and various types of devices connected to a network.
Exhaustive documentation	Security pattern documentation that is accessible, precise, easy to read, and follow through. Software developers are inclined to refer to such documentation.
eXtensible Access Control Markup Language (XACML)	A standard used to define and implement access control policies. It offers a comprehensive framework for managing and enforcing access control decisions across different systems, applications, and services. This empowers organizations to regulate resource access and specific actions based on established policies.
eXtensible Markup Language (XML)	A widely utilized markup language created to organize, transport, and structure data in a format that is human-readable and platform-independent.
Firewall	A network security device or software that acts as a barrier between a trusted internal network and an untrusted external network like the internet.
Functional Verification Test (FVT)	Validates the software's functionality using the solution specification document, design papers, and use case documents.
GitHub	An online platform that offers version control for software development projects, enabling developers to collaborate on code, monitor changes, and manage their source code repositories in a distributed manner.
Hash algorithms	A hash algorithm, also referred to as a hash function, is a mathematical procedure that accepts input of any size and generates a fixed-size output called the hash value or hash code.
Hashicorp's Vault	An open-source, identity-based secret and encryption management tool.
Hijacking	A type of cyberattack in which an unauthorized person or entity intercepts and manipulates communication between two parties who believe that they are directly communicating with each other.
Hypertext Transport Protocol Secure (HTTPS)	Used for secure communication between computers over the World Wide Web (WWW). It ensures that the data exchanged between the browser and the website remains confidential and protected from unauthorized access.
Identification and Access Management (IAM)	Important security mechanisms to grant permissions to applications and systems within cloud infrastructures.
Integrity	A cryptographic service that guarantees data has not been modified or tampered with during or after reception and helps support the anti-tampering of data for users needing data verification between sender and receiver.
Interoperable	The ability of diverse systems, software, or components to collaborate, function cohesively, and exchange information effectively and seamlessly.
Intrusion detection	The ongoing detection of any cyberattacks, threats, or intrusions that may compromise an application or system.
Linux kernel	Core component of an operating system that provides a platform for running programs and various services on top of it.
Man-in-the-middle attacks	A type of cyberattack wherein the attacker covertly intercepts and potentially modifies the communication between two parties who are under the impression that they are directly communicating with each other.
Message digests	Cryptographic hash functions used to compute checksums of data blocks. It can also be used to sign and verify signatures.
Network firewall	A security device or software that serves as a protective barrier between an internal network, like a corporate network, and an external network, such as the internet. Its role is to regulate and observe incoming and outgoing network traffic.
Network layer	The third layer of the OSI model handles data transmission and control of the subnet.
Network mapper (Nmap)	Used to discover hosts and services on a computer network by sending packets and analyzing responses.
Network security	Detects application and system anomalies and monitors a network using a network tool such as Nmap or Snort.
Open Systems Interconnection (OSI model)	Enables communication between diverse communication systems using standard protocols.
Open-source software library (OpenSSL)	A library of software that implements the Secure Socket Layer (or SSL) protocol. It is an open-source toolkit to ensure secure communication with cryptography for all types of communication, from personal to commercial and e-commerce transactions.
Orchestration	The automated configuration, management, and coordination of computer systems, applications, and services.
OWASP	Open Web Application Security Project
PGP	Pretty good privacy
Physical layer	The lowest layer of the OSI model transmits bits of raw information.
Presentation layer	The sixth layer of the OSI model focuses on the syntax and semantics of data being transmitted from one point to another.
Private key	A confidential piece of information utilized to demonstrate ownership of digital assets.
Process for Attack Simulation and Threat Analysis (PASTA)	A risk-based model that connects to business objectives and technical requirements.
Public key	A cryptographic key used for the encryption and validation of digital signatures.
Public key cryptography	A public cryptographic algorithm that uses public and private keys. Rivest, Shamir, and Adleman (or RSA) is the most popular implementation of public key cryptography. RSA provides secrecy, authentication, and encryption for anyone to use. It is also used to implement prime number generation to generate private keys using different sizes of key lengths depending upon the level of encryption needed.
Role-based access control (RBAC)	An access control framework that regulates resource access according to predefined roles. In an RBAC system, users are allocated specific roles, each linked to a set of permissions that determine the actions or resources accessible to users within that role.
Scrum framework	A framework under which individuals may handle complicated adaptive challenges while producing high-value goods in a productive and creative manner.
Secure shell (SSH)	Secure connection protection for connecting with remote devices, such as physical and cloud servers.
Secure Socket Layer (SSL)	A protocol based on encryption technology that provides secure data transmission over the internet. It ensures that data exchanged between a web browser and a web server remains confidential and protected from unauthorized access during transit.
Security Assertion Markup Language (SAML)	Facilitates the exchange of authentication and authorization data among various entities. It enables smooth and secure authentication across diverse domains, empowering users to access multiple applications and services using a single set of credentials.
Security pattern	A set of rules that represent and define a reusable solution to recurring security threats or issues. By following security patterns, organizations establish robust security frameworks while ensuring the confidentiality, integrity, and availability of the system's data.
Security pattern catalog	Empowers software developers to review and choose security patterns for developing necessary and additional security features for their application code. When developing for deployment, a well-classified security pattern catalog enables developers to reuse security patterns across multiple applications. Software developers also rely on security pattern catalogs to become more aware of the associated security mechanisms.
Serverless computing	A cloud application development and execution model that lets developers build and run code without managing servers or paying for idle cloud infrastructure.
Session layer	The fifth OSI model layer establishes multiple sessions from different machines while establishing consistent sessions if a crash occurs.
Snort	A network intrusion detection and prevention system that provides real-time analysis of network traffic.
Snyk Code	An integrated development tool that performs semantic analysis to discover coding and security bugs throughout the development phase.
Software Development Lifecycle (SDLC)	A framework that specifies the steps involved in software development at each stage. It details the strategy for developing, deploying, and maintaining a program.
Spoofing	A form of network attack that involves manipulating network traffic or data to gain unauthorized access to systems, services, or users.
Static Reviewer	Eliminates well-known vulnerabilities. It is a component within the Security Reviewer suite, compliant with frameworks including the Open Web Application Security Project (or OWASP), Common Vulnerabilities and Exposures (or CVEs), and the National Institute of Standards and Technology (or NIST).
STRIDE	STRIDE means Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privileges. STRIDE, which came from Microsoft, evaluates applications and systems to find threats and vulnerabilities.
Subnets	A subnetwork (or subnet) is a smaller portion of a larger network partitioned to create more feasible segments of the network with higher efficiency.
Symmetric ciphers	Cryptographic algorithms that use the same key for both encryption and decryption of data.
Symmetric encryption	When the same key is used for both encrypting and decrypting.
System-call auditing	The retrieval and review of system-call information from a kernel, such as the Linux kernel.
Threat modeling	Provides a process to analyze ongoing threats and eliminate the potential for software coding weaknesses and vulnerabilities.
Threat monitoring	Scanning code repositories and containers to find security issues. Password mishandling, protocol insecurities, and incorrect permissions are examples of issues that you can discover with threat monitoring.
Token management	Involves the procedures and protocols employed in handling and controlling tokens, which are unique pieces of data or strings used in diverse systems and applications.
Transport layer	The fourth layer of the OSI model accepts transmissions or data from the network layer and chops them into smaller units or packets for passing them back to the network layer.
Transport Layer Security (TLS)	A protocol based on encryption technology used to secure communications over a computer network. It is the successor to SSL and is designed using an advanced encryption algorithm.
Two-factor authentication	This added security measure is employed to safeguard user accounts and digital data. It demands that users present two distinct forms of identification before obtaining access to a system, service, or application.
Unified Modelling Language (UML)	Can visually model and represent a system for a better understanding of the system's architecture and design.
Visual, Agile, and Simple Threat (VAST)	An agile methodology with application and operational threat models. VAST uses process-flow diagrams to represent the architectural perspective.
Vulnerability patching	The distribution of security updates or patches improves functionality or eliminates vulnerabilities in an IT system or service.
Vulnerability scanner	A specialized software tool designed to detect and evaluate security ineffectiveness in computer systems, networks, applications, and other digital assets.
Vulnerability scanning	The search for security vulnerabilities from within the code and outside of an application.
Web services security	A set of measures and protocols implemented to ensure confidentiality, integrity, and authentication of data exchanged between web services and their clients over the internet.

Author(s)

- Gagandeep Singh

Changelog

Date	Version	Changed by	Change Description
08-08-2023	0.1	Gagandeep Singh	Initial version created