Application Security for Developers and DevOps Professionals

Glossary: Application Security for Developers and DevOps Professionals

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: 20 minutes

Term	Definition
Access control	A security measure employed to govern and control the access and permissions provided to users, processes, or entities operating within a system or network.
Ad hoc testing	Random, informal testing without a plan for the discovery of a vulnerability.
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.
BDD-Security	A security testing framework that uses behavior-driven development.
Blind cross-site scripting	Injects a script that has a payload to be executed on the back-end of an application by the user or the administrator without their knowing about it.
Broken access control	When attackers can access, modify, delete, or perform actions outside of an application or system's intended permissions.
Buffer overflows	One of the four pervasive types of SQL injection attacks. This happens when a program allocates more data in a buffer than the buffer can store. A buffer overflow causes a system or program to crash or execute malicious code.
Burp Suite	A vulnerability scanner that is popular for scanning web applications. You can set up automated scans of a website or perform manual scanning by crawling the overall structure of a website or web application.
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.
Click	A framework for writing command line applications.
Code injection	One of the four pervasive types of SQL injection attacks.
Code practices	They are part of the software development process for secure software development.
Code review	In code review, you use automated static analysis security testing and perform manual code inspection.
Code scanners	Provide vulnerability reporting and insights after they scan code in your repositories.
CodeSonar	A static code analysis tool from GrammaTech is 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.
Credential stuffing	Occurs when an attacker has a list of legitimate usernames and passwords. The attacker employs automation to use those passwords in an attack.
Cross-site scripting	When an application takes untrusted data and then sends it to a web browser without proper validation or escaping. You may see cross-site scripting represented as "XSS."
Cross-site scripting attack	It can deface websites by replacing or removing images or content.
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.
DAST	Dynamic application security testing (or DAST) evaluates the application from the outside in through the front end.
Data link layer	The second layer of the OSI model transforms the transmitted raw data into a line free from undetected errors.
Dependencies	It adds features and functionality to the software without writing it from scratch. Dependencies are reusable codes found in a library (package or module) that your code makes calls to.
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.
Dynamic analysis	Dynamic analysis is the process of testing and evaluating an application as it is executing.
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.
Exploratory testing	Takes place outside of formal testing.
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.
Flask	It is a web framework written in Python that provides you with tools, libraries, and other features for building web applications.
Function call injection	One of the four pervasive types of SQL injection attacks.
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.
GitHub SCA	It is for viewing dependency packages and vulnerabilities while using GitHub.
GPL	General Public License.
Guantlt	A security framework that hooks into security tools for simplified integration.
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.

Term	Definition
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.
HTTP Host header injection	When creating URIs for links in web applications, developers typically use the HTTP host header available in the HTTP request that is sent from the client side. An attacker can exploit this practice by sending a fake header that contains a domain name that, for example, can be used to corrupt the web cache or password reset emails.
Hypertext Transport Protocol Secure (HTTPS)	Used for secure communication between computers over the World Wide Web (WWW).
IAST	Interactive Application Self-testing (or IAST) scans for vulnerabilities during testing.
Identification and Access Management (IAM)	Important security mechanisms to grant permissions to applications and systems within cloud infrastructures.
Insecure development environment	It is an environment where production systems are secure, but the development environment where coding is built and deployed is a free-for-all with direct connections to the production infrastructure.
Integration tests	For testing the integration of several coded classes within an application.
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.
ItsDangerous	A secure data integrity dependency.
Jinja	A template language for rendering web pages.
JSON	JavaScript Object Notation.
LDAP	Lightweight Directory Access Protocol
Lightweight Directory Access Protocol (LDAP) injection	Exploits websites that construct LDAP statements from data provided by users. In this type of attack, an attacker might modify LDAP statements using a local proxy in order to execute arbitrary commands (granting permissions to unauthorized queries) or modify the content of the LDAP tree.
Linux kernel	A core component of an operating system that provides a platform for running programs and various services on top of it.
Logstash	A data processing pipeline that collects, parses, and stores logs for future use. IBM Financial Crimes Alerts Insight with Watson (FCAI) uses Logstash to collect and normalize log files.
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.
MarkupSafe	A security dependency for untrusted input.
Message digests	Cryptographic hash functions are used to compute checksums of data blocks. It can also be used to sign and verify signatures.
Mittn	Popular tool suite to include in continuous integration.
Multi-factor authentication (MFA)	It is an identity verification method that requires users to provide at least one authentication factor in addition to a password, or at least two authentication factors instead of a password, to gain access to a website, application, or network.
Nessus	It is a vulnerability scanner that scans operating systems, network devices, and critical infrastructure for vulnerabilities, threats, and compliance violations.
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.
Operating system command injection	OS command injection, also termed shell injection, is a web security vulnerability where an attacker can execute arbitrary operating system (OS) commands on a server running an application and can fully compromise it along with all its data.
Orchestration	The automated configuration, management, and coordination of computer systems, applications, and services.
OWASP	Open Web Application Security Project, launched in 2001 and formally formed in 2004, is a foundation that focuses on software security.
OWASP Dependency-Check	It is an SCA for checking for vulnerabilities within project dependencies.
OWASP Dependency-Track	It is an SCA for identifying any risks within the software supply chain.
OWASP Software Component Verification Standard	It is a community-supported effort to build a sustainable framework for reducing risk within a software supply chain.
OWASP Top 10	A report that identifies current software security vulnerability concerns and represents a consensus from the OWASP core team, security analysts, security organizations, and other security experts. The OWASP Top 10 is used globally as a standard check for web application security.
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.
Principle of Least Privilege (PoLP)	Users should only have the minimum permissions necessary to perform their tasks.
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 is 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.
RASP	Runtime Application Self-Protection (or RASP) looks for assaults in the production environment.
Reflected cross-site scripting attack	A reflected cross-site scripting attack injects a script to be reflected from the attacked server to users on a system.
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.
Runtime protection	Runtime protection is a modern security mechanism that shields applications against threats while the applications are running.
SALSA	Supply-chain Levels for Software Artifacts (or SALSA) provides a security framework for improving integrity and preventing tampering by implementing standards and controls.
SAST	Static application security testing (or SAST) examines source code to identify security flaws that render your organization's applications vulnerable to attack.
SCA	Software component analysis (or SCA) is the process of determining which open-source components and dependencies are used in your application.
SCM	Source control management.
Scrum framework	A framework under which individuals may handle complicated adaptive challenges while producing high-value goods in a productive and creative manner.

Term	Definition
Secure development environment	A secure development environment is an ongoing process of securing the network, compute resources and storage devices on-premises and in the cloud.
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.
Security testing	Security testing provides a secure code baseline for development. It should be performed on all new codes to reduce the risk of impacts.
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.
Server-side request forgeries (SSRF)	A server site attack results in sensitive information being disclosed or leaked from the back-end server of the application.
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	A developer security platform for securing code, dependencies, containers, and infrastructure as code.
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.
SQL	Structured Query Language
SQL injection	Takes advantage of the SQL syntax to inject commands that can read or modify a database or compromise the meaning of the original SQL query. In this type of attack, an attacker can spoof an identity; expose, tamper with, destroy, or make existing data unavailable; or become the administrator of the database server.
SQL injection attacks	Attempt to exploit web application vulnerabilities by concatenating user input with SQL queries. If successful, these attacks can execute malicious SQL commands using a legitimate web application connection.
SQL manipulation	One of the most common types of SQL injection and an attack that modifies an SQL statement of set operations.
Static analysis	Static analysis examines all code or runtime binaries to help detect common vulnerabilities without executing code or running programs.
Static Reviewer	Eliminates well-known vulnerabilities.
Stored cross-site scripting	A stored cross-site scripting attack injects a script that becomes permanently stored in a database or on a targeted server.
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.
SWID Tags	Software Identification Tags (or SWID Tags) are standard to track software installed on managed devices.
Symmetric ciphers	Cryptographic algorithms 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.
Unit testing	For testing classes and methods to evaluate application programming interface (or API) contracts, you can perform unit testing on individual classes with limited scope.
Validating input	Validating input means checking (on the server side) that the input provided by the user or attacker is what you expect it to be.
Vault	Developed by HashiCorp, Vault is a token-based storage solution for managing secrets. This tool provides policies that constrain user access and privileges when users interact with a Vault server.
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 analysis	It is a method of identifying possible application flaws that could jeopardize your application.
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.
Werkzeug	A web server gateway interface.
XML	Extensible Markup Language.
ZAP	Zed Attack Proxy (or Zap) is a vulnerability scanner. It is an OWASP tool and open-source software that uses spiders to crawl web applications.

Author(s)

- Gagandeep Singh