Application Security for Developers and DevOps Professionals

Module 3 Glossary: OWASP Application Security Risks

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 in other certificate programs.

Estimated reading time: 6 minutes

Term	Definition
Blind cross-site scripting	Injects a script that has a payload to be executed on the backend 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.
Code injection	One of the four pervasive types of SQL injection attacks.
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	Can deface websites by replacing or removing images or content.
Function call injection	One of the four pervasive types of SQL injection attacks.
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.
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.
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.
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.
OWASP	Open Web Application Security Project, launched in 2001 and formally formed in 2004, is a foundation that focuses on software security. OWASP supports the security industry with the OWASP Top 10.
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.
Principle of Least Privilege (or PoLP)	Users should only have the minimum permissions necessary to perform their tasks.
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.
Server-side request forgeries (SSRF)	A server site attack that results in sensitive information being disclosed or leaked from the backend server of the application.
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.
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.
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.

Author(s)

- Gagandeep Singh