Web Application Security Consortium
www.webappsec.org | contact@webappsec.org

Last update: February 23, 2004

Web Security Glossary

The Web Security Glossary is an alphabetical index of terms and terminology relating to web application security. The purpose of the Glossary is to clarify the language used within the community.

Abuse of Functionality: An attack technique that uses the features and functionality of a web site to consume, defraud, or circumvent the site's access controls. See also "Denial of Service".

ActiveX controls: ActiveX controls are software based on the Component Object Model (COM) and formerly known as OLE controls. ActiveX controls are portable, reusable, and can be utilized by many development languages. They are widely used by web-based applications to extend their functionality (ie: Windows Update site, etc.) See also "Java", "Java Applets", "JavaScript", "Web Browser".

Application Server: A software server, normally using HTTP, which has the ability to execute dynamic web applications. Also known a middleware, this piece of software is normally installed on or near the web server where it can be called upon. See also "Web Application", "Web Server".

Anti-Automation: Security measure that prevents automated programs from exercising web site functionality by administering the Turing Test to a user, which only a human could pass. See also "Visual Verification".

Authentication: The process of verifying the identity or location of a user, service or application. Authentication is performed using at least one of three mechanisms: "something you have", "something you know" or "something you are". The authenticating application may provide different services based on the location, access method, time of day, etc. See also "Insufficient Authentication".

Authorization: The determination of what resources a user, service or application has permission to access. Accessible resources can be URL's, files, directories, servlets, databases, execution paths, etc. See also "Insufficient Authorization".

Backup File Disclosure: (Obsolete) See "Predictable File Location".

Basic Authentication: A simple form of client-side authentication supported in HTTP. The http-client sends a request header to the web server containing a Base64 encoded username and password. If the username/password combination is valid, the web server grants the client access to the requested resource. See also "Authentication", "Insufficient Authentication".

Brute Force: An automated process of trial and error used to guess the "secret" protecting a system. Examples of these secrets include usernames, passwords or cryptographic keys. See also "Authentication", "Insufficient Authentication", "Password Recovery System", "Weak Password Recovery Validation".

Buffer Overflow: An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer Overflows are a common cause of malfunctioning software. If the data written into a buffer exceeds its size, adjacent memory space will be corrupted and normally produce a fault. An attacker may be able to utilize a buffer overflow situation to alter an application's process flow. Overfilling the buffer and rewriting memory-stack pointers could be used to execute arbitrary operating-system commands.

CGI Scanner: Automated security program that searches for well-known vulnerabilities in web servers and off-the-shelf web application software. Often CGI Scanners are not very "stateful" in their analysis and only test a series HTTP requests against known CGI strings. See also, "Web Application Vulnerability Scanner."

CGI Security: (Obsolete) See "Web Application Security".

Client-Side Scripting: Web browser feature that extends the functionality and interactivity of static HyperText markup language (HTML) web pages. Examples of Client-Side Scripting languages are JavaScript, JScript and VBScript. See also “ActiveX controls”, “Java Applets”.

Common Gateway Interface: (Acronym - CGI) Programming standard for software to interface and execute applications residing on web servers. See also “Web Application”, “Application Server”, “Web Server”.

Configuration File Disclosure: (Obsolete) See “Predictable File Location”.

Content Spoofing: An attack technique used to trick a user into thinking that fake web site content is legitimate data.

Cookie: Small amount of data sent by the web server, to a web client, which can be stored and retrieved at a later time. Typically cookies are used to keep track of a users’ state as they traverse a web site. See also “Cookie Manipulation”.

Cookie Manipulation: Altering or modification of cookie values, on the client’s web browser, to exploit security issues within a web application. Attackers will normally manipulate cookie values to fraudulently authenticate themselves to a web site. This is an example of the problem of trusting the user to provide reasonable input. See also “Cookie”.

Cookie Poisoning: (Obsolete) See “Cookie Manipulation”.

Cross-Site Scripting: (Acronym – XSS) An attack technique that forces a web site to echo client-supplied data, which execute in a user’s web browser. When a user is Cross-Site Scripted, the attacker will have access to all web browser content (cookies, history, application version, etc). See also “Client-Side Scripting”.

Debug Commands: Application debugging features or commands that assist in identifying programming errors during the software development process.

Denial of Service: (Acronym – DoS) An attack technique that consumes all of a web site's available resources with the intent of rendering legitimate use impossible. Resources include CPU time, memory utilization, bandwidth, disk space, etc. When any of these resources reach full capacity, the system will normally be inaccessible to normal user activity. See also "Abuse of Functionality".

Directory Browsing: (Obsolete) See "Directory Indexing".

Directory Enumeration: (Obsolete) See "Predictable File Location".

Directory Indexing: A feature common to most popular web servers, that exposes contents of a directory when no index page is present. See also "Predictable File Location".

Directory Traversal: A technique used to exploit web sites by accessing files and commands beyond the document root directory. Most web sites restrict user access to a specific portion of the file-system, typically called the document root directory or CGI root directory. These directories contain the files and executables intended for public use. In most cases, a user should not be able to access any files beyond this point.

Encoding Attacks: An exploitation technique that aids an attack by changing the format of user-supplied data to bypass sanity checking filters. See also "Null Injection".

Extension Manipulation: (Obsolete) See "Filename Manipulation".

File Enumeration: (Obsolete) See "Predictable File Location".

Filename Manipulation: An attack technique used to exploit web sites by manipulating URL filenames to cause application errors, discover hidden content, or display the source code of an application. See also “Predictable File Location”.

Filter-Bypass Manipulation: See “Encoding Attacks”.

Forced Browsing: See “Predictable File Location”.

Form Field Manipulation: Altering or modification of HTML Form-Field input values or HTTP post-data to exploit security issues within a web application. See also “Parameter Tampering”, “Cookie Manipulation”.

Format String Attack: An exploit technique that alters the flow of an application by using string formatting library features to access other memory space.

Frame Spoofing: (Obsolete) See “Content Spoofing”.

HyperText Transfer Protocol: (Acronym – HTTP) A protocol scheme used on the World Wide Web. HTTP describes the way a web client requests data and how a web server responds to those requests. See also “Web Server”, “Web Browser”.

Information Leakage: When a web site reveals sensitive data, such as developer comments or error messages, which aids an attacker in exploiting the system. See also “Verbose Messages”,.

Insufficient Authentication: When a web site permits an attacker to access sensitive content or functionality without verifying their identity. See also “Authentication”.

Insufficient Authorization: When a web site permits an attacker to access sensitive content or functionality that should require increased access control restrictions. See also “Authorization”.

Insufficient Session Expiration: When a web site permits an attacker to reuse old session credentials or session ID's for authorization. See also "Session Replay", "Session Credential", "Session ID", "Session Manipulation".

Insufficient Process Validation: When a web site permits an attacker to bypass or circumvent the intended flow control of an application.

Java: A popular programming language developed by Sun Microsystems(tm). See also "ActiveX conrols", "Web Browser", "JavaScript", "Client-Side Scripting".

Java Applets: An applet is a program written in the Java programming language that can be included in a web page. When a Java enabled web browser views a page containing an applet, the code is executed by the Java Virtual Machine (JVM). See also "Web Browser", "Java", "ActiveX", "JavaScript", "Client-Side Scripting".

JavaScript: A popular web browser client-side scripting language used to create dynamic web page content. See also "ActiveX", "Java Applets", "Client-Side Scripting".

Known CGI file: See "Predictable File Location".

Known Directory: See "Predictable File Location".

LDAP Injection: A technique for exploiting a web site by altering backend LDAP statements through manipulating application input. Similarly to the methodology of SQL Injection. See also "Parameter Tampering", "Form Field Manipulation".

Meta-Character Injection: An attack technique used to exploit web sites by sending in meta-characters, which have special meaning to a web application, as data input. Meta-characters are characters that have special meaning to programming languages, operating system commands, individual program procedures, database queries, etc.

These special characters can adversely alter the behavior of a web application. See also “Null Injection”, “Parameter Tampering”, “SQL Injection”, “LDAP Injection”, “Cross-Site Scripting”.

Null Injection: An exploitation technique used to bypass sanity checking filters by adding URL encoded null-byte characters to user-supplied data. When developers create web applications in a variety of programming languages, these web applications often pass data to underlying lower level C-functions for further processing and functionality. If a user-supplied string contains a null character (\0), the web application may stop processing the string at the point of the null. Null Injection is a form of a meta-character Injection attack. See also “Encoding Attacks”, “Parameter Tampering”, “Meta Character Injection”.

OS Command Injection: See “OS Commanding”.

OS Commanding: An attack technique used to exploit web sites by executing operating-system commands through manipulating application input. See also “Parameter Tampering”, “Form Field Manipulation”.

Page Sequencing: (Obsolete) See “Insufficient Process Validation”.

Parameter Tampering: Altering or modification of the parameter name and value pairs in a URL. Also known as “URL Manipulation”. See also “Uniform Resource Locator”.

Password Recovery System: An automated process that allows a user to recover or reset his password in the event that it has been lost or forgotten. See also “Weak Password Recovery Validation”.

Predictable File Location: A technique used to access hidden web site content or functionality by making educated guesses, manually or automatically, of the names and locations of files. Predictable file locations may include directories, CGI’s, configuration files, backup files, temporary files, etc.

Secure Sockets Layer: (Acronym – SSL) An industry standard public-key protocol used to create encrypted tunnels between two network-connected devices. See also “Transport Layer Security”.

Session Credential: A string of data provided by the web server, normally stored within a cookie or URL, which identifies a user and authorizes them to perform various actions. See also “Session ID”.

Session Fixation: An attack technique that forces a user’s session credential or session ID to an explicit value. See also “Session Credential”, “Session ID”.

Session Forging: See “Session Prediction”.

Session Hi-Jacking: The result of a user’s session being compromised by an attacker. The attacker could reuse this stolen session to masquerade as the user. See also “Session Prediction”, “Session Credential”, “Session ID”.

Session ID: A string of data provided by the web server, normally stored within a cookie or URL. A Session ID tracks a user’s session, or perhaps just his current session, as he traverse the web site.

Session Manipulation: An attack technique used to hi-jack another user’s session by altering a session ID or session credential value. See also “Session Prediction”, “Session Hi-Jacking”, “Session Credential”, “Session ID”.

Session Prediction: An attack technique used to create fraudulent session credentials or guess other users current session ID’s. If successful, an attacker could reuse this stolen session to masquerade as another user. See also “Session Credential”, “Session ID”, “Session Hi-Jacking”.

Session Replay: When a web site permits an attacker to reuse old session credentials or session ID’s for authorization. See also

“Session ID”, “Session Credential”, “Insufficient Session Expiration”.

Session Tampering: See “Session Manipulation”

SQL Injection: An attack technique used to exploit web sites by altering backend SQL statements through manipulating application input. See also “Parameter Tampering”, “Form Field Manipulation”.

SSI Injection: A server-side exploit technique that allows an attacker to send code into a web application, which will be executed by the web server. See also “Meta-Character Injection”, “Parameter Tampering”, “Form Field Manipulation”.

Transport Layer Security: (Acronym – TLS) The more secure successor to SSL. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. TLS is based on the SSL protocol, but the two systems are not interoperable. See also “Secure Sockets Layer”.

Universal Resource Locator: (Acronym – URL) A standard way of specifying the location of an object, normally a web page, on the Internet. See also “Parameter Tampering”.

Unvalidated Input: When a web application does not properly sanity-check user-supplied data input.

URL Manipulation: Altering or modification of a web applications parameter name and value pairs. Also known as “Parameter Tampering”.

User-Agent Manipulation: A technique used to bypass web site browser requirement restrictions by altering the value sent within an HTTP User-Agent header. See also “Cookie Manipulation”.

Verbose Messages: Detailed pieces of information revealed by a web site, which could aid an attacker in exploiting the system.

Visual Verification: Visual oriented method of anti-automation that prevents automated programs from exercising web site functionality by determining if there is presence of mind. See also “Anti-Automation”.

Weak Password Recovery Validation: When a web site permits an attacker to illegally obtain, change or recover another user’s password. See also “Password Recovery System”.

Web Application: A software application, executed by a web server, which responds to dynamic web page requests over HTTP. See also “Web Server”, “Web Application”, “Web Service”.

Web Application Scanner: See “Web Application Vulnerability Scanner”.

Web Application Security: Theory and practice of information security relating to the World Wide Web, HTTP and web application software. Also known as “Web Security”.

Web Application Firewall: An intermediary device, sitting between a web client and a web server, analyzing OSI Layer-7 messages for violations in the programmed security policy. A web application firewall is used as a security device protecting the web server from attack. See also “Web Application Security”, “Web Server”.

Web Application Vulnerability Scanner: An automated security program that searches for software vulnerabilities within web applications. See also “Web Application Security.

Web Browser: A program used to display HyperText markup language (HTML) web pages sent by a web server. See also “ActiveX”, “Cookie”, “Java Applets”, “JavaScript”, “Client-Side Scripting”.

Web Security: See “Web Application Security”.

Web Security Assessment: A process of performing a security review of a web application by searching for design flaws, vulnerabilities and inherent weaknesses. See also “Web Application Security”.

Web Security Scanner: See “Web Application Vulnerability Scanner”.

Web Server: A general-purpose software application that handles and responds HTTP requests. A web server may utilize a web application for dynamic web page content. See also “Web Application”, “Application Server”, “HyperText Transfer Protocol”.

Web Service: A software application that uses Extensible Markup Language (XML) formatted messages to communicate over HTTP. Typically, software applications interact with web services rather than normal users. See also “Web Server”, “Web Application”, “Application Server”, “HyperText Transfer Protocol”.

Contributors

Robert Auger
Cesar Currudo
Jeremiah Grossman
Dennis Groves
Sverre H. Huseby
Aaron C. Newman
Ray Pompon
Ivan Ristic