THE ACUNETIX BLOG (/BLOG/) ›
WEB SECURITY ZONE (HTTPS://WWW.ACUNETIX.COM/BLOG/CATEGORY/WEB-SECURITY-ZONE/)

What Are Injection Attacks (https://www.acunetix.com/blog/articles/injection-attacks/)

Ian Muscat (https://www.acunetix.com/blog/author/ianmuscat/) | April 18, 2019

Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation.

This attack type is considered a major problem in web security. It is listed as the number one web application security risk in the OWASP Top 10 (https://www.acunetix.com/blog/articles/owasp-top-10-2017/) – and for a good reason. Injection attacks, particularly SQL Injections (SQLi attacks) and Cross-site Scripting (XSS), are not only very dangerous but also widespread, especially in legacy applications.

What makes injection vulnerabilities particularly scary is that the attack surface is enormous (especially for XSS and SQL Injection vulnerabilities). Furthermore, injection attacks are a very well understood vulnerability class. This means that there are many freely available and reliable tools that allow even inexperienced attackers to abuse these vulnerabilities automatically.

Types of Injection Attacks

SQL injection (SQLi) and Cross-site Scripting (XSS) are the most common injection attacks but they are not the only ones. The following is a list of common injection attack types.

Injection attack	Description	Potential impact

Injection attack	Description	Potential impact
Code injection (https://www.acunetix.com/blog/articles/code-injection/)	The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full web server compromise.	Full system compromise

Injection attack	Description	Potential impact
CRLF injection (https://www.acunetix.com/websitesecurity/crlf-injection/)	The attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence. This sequence is used to split an HTTP response header and write arbitrary contents to the response body. This attack may be combined with Cross-site Scripting (XSS).	Cross-site Scripting (XSS)
Cross-site Scripting (XSS) (https://www.acunetix.com/websitesecurity/cross-site-scripting/)	The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application. This script is then executed inside the victim's browser.	• Account impersonatior • Defacement • Run arbitrary JavaScript in the victim's browser

Injection attack	Description	Potential impact
Email Header Injection (https://www.acunetix.com/blog/articles/email-header-injection-web-vulnerability-detection/)	This attack is very similar to CRLF injections. The attacker sends IMAP/SMTP commands to a mail server that is not directly available via a web application.	• Spam relay • Information disclosure
Host Header Injection (https://www.acunetix.com/blog/articles/automated-detection-of-host-header-attacks/)	The attacker abuses the implicit trust of the HTTP Host header to poison password-reset functionality and web caches.	• Password-reset poisoning • Cache poisoning
LDAP Injection (https://www.acunetix.com/vulnerabilities/web/ldap-injection)	The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands. They can gain permissions and modify the contents of the LDAP tree.	• Authentication bypass • Privilege escalation • Information disclosure

Injection attack	Description	Potential impact
OS Command Injection (https://www.acunetix.com/blog/web-security-zone/os-command-injection/)	The attacker injects operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full system compromise.	Full system compromise

Injection attack	Description	Potential impact
SQL Injection (SQLi) (https://www.acunetix.com/websitesecurity/sql-injection/)	The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.	• Authentication bypass • Information disclosure • Data loss • Sensitive data theft • Loss of data integrity • Denial of service • Full system compromise.
XPath injection (https://www.acunetix.com/vulnerabilities/web/xpath-injection-vulnerability)	The attacker injects data into an application to execute crafted XPath queries. They can use them to access unauthorized data and bypass authentication.	• Information disclosure • Authentication bypass

It's easy to test if your website or web application is vulnerable to all the injection attacks listed above. All you need to do is run an automated web scan using the Acunetix vulnerability scanner. Take a demo (https://www.acunetix.com/web-vulnerability-scanner/demo/) and find out more about running scans against your website or web application.

Frequently asked questions

What are injection attacks?

What are the common types of injection attacks?

How to detect injection vulnerabilities?

How to avoid injection attacks?

Subscribe

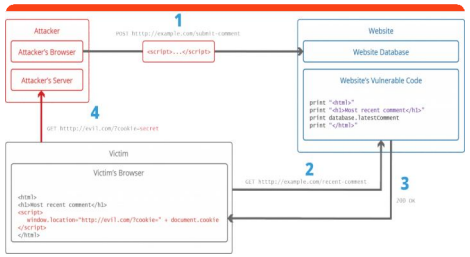
SHARE THIS POST

THE AUTHOR

Ian Muscat

Acunetix developers and tech agents regularly contribute to the blog. All the Acunetix developers come with years of experience in the web security sphere.

Related Posts:



Cross-site Scripting (XSS)

(https://www.acunetix.com/wel

What is SQL Injection (SQLi) and How to Prevent It

(https://www.acunetix.com/wel

What Are CRLF Injection Attacks

(https://www.acunetix.com/v

Read more → (https://www.acun Read more → (https://www.acunetix.com/v Read more → (https://www

← Older (https://www.acunetix.com/blog/articles/code-injection/)

Newer → (https://www.acunetix.com/blog/docs/why-are-some-vulnerabilities-marked-as-verified/)

Subscribe by Email

Get the latest content on web security in your inbox each week.

Enter E-Mail Subscribe

Learn More

IIS Security (https://www.acunetix.com/websitesecurity/iis-security/)

Apache Troubleshooting (https://www.acunetix.com/websitesecurity/troubleshooting-tips-for-apache/)

Security Scanner (https://www.acunetix.com/websitesecurity/security-scanner/)

DAST vs SAST (https://www.acunetix.com/blog/articles/dast-dynamic-application-security-testing/)

Threats, Vulnerabilities, & Risks (https://www.acunetix.com/blog/articles/cyber-threats-vulnerabilities-risks/)

Vulnerability Assessment vs Pen Testing (https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/)

Server Security (https://www.acunetix.com/websitesecurity/webserver-security/)

Google Hacking (https://www.acunetix.com/websitesecurity/google-hacking/)

Blog Categories

Articles (https://www.acunetix.com/blog/category/articles/)

Web Security Zone (https://www.acunetix.com/blog/category/web-security-zone/)

News (https://www.acunetix.com/blog/category/news/)

Events (https://www.acunetix.com/blog/category/events/)

Product Releases (https://www.acunetix.com/blog/category/releases/)

Product Articles (https://www.acunetix.com/blog/category/docs/)

PRODUCT INFORMATION

AcuSensor Technology (https://www.acunetix.com/vulnerability-scanner/acusensor-technology/)

AcuMonitor Technology (https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/)

Acunetix Integrations (https://www.acunetix.com/vulnerability-

USE CASES

Penetration Testing Software (https://www.acunetix.com/vulnerability-scanner/penetration-testing-software/)

Website Security Scanner (https://www.acunetix.com/vulnerability-scanner/website-security-scanner/)

External Vulnerability Scanner (https://www.acunetix.com/vulnerability-

WEBSITE SECURITY

Cross-site Scripting (https://www.acunetix.com/websitesecurity/cross-site-scripting/)

SQL Injection (https://www.acunetix.com/websitesecurity/sql-injection/)

Reflected XSS (https://www.acunetix.com/websitesecurity/xss/)

scanner/acunetix-integrations/)

Vulnerability Scanner (/vulnerability-scanner/)

Support Plans (https://www.acunetix.com/support-plans/)

scanner/external-vulnerability-scanner/)

Web Application Security (https://www.acunetix.com/vulnerability-scanner/web-application-security/)

Vulnerability Management Software (https://www.acunetix.com/vulnerability-scanner/vulnerability-management-software/)

CSRF Attacks (https://www.acunetix.com/websitesecurity/csrf-attacks/)

Directory Traversal (https://www.acunetix.com/websitesecurity/directory-traversal/)

LEARN MORE

White Papers (https://www.acunetix.com/white-papers/)

TLS Security (https://www.acunetix.com/blog/articles/tls-security-what-is-tls-ssl-part-1/)

WordPress Security (https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/)

Web Service Security (https://www.acunetix.com/websitesecurity/web-services-wp/)

Prevent SQL Injection (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)

COMPANY

About Us (https://www.acunetix.com/about/)

Customers (https://www.acunetix.com/vulnerability-scanner/customers/)

DOCUMENTATION

Case Studies (https://www.acunetix.com/case-studies/)

Support (https://www.acunetix.com/support/)

Become a Partner (https://www.acunetix.com/partners/)

Careers (https://www.acunetix.com/careers/)

Contact (https://www.acunetix.com/contact/)

Videos (https://www.acunetix.com/support/videos/)

Vulnerability Index (/vulnerabilities)

Webinars (https://www.acunetix.com/webinars/)

Login (https://online.acunetix.com)

Subscription Services Agreement (https://www.acunetix.com/ssa/)

Data Protection Policy (https://www.acunetix.com/data-protection-policy/)

Information Security Policy (https://www.acunetix.com/isp/)

Privacy Policy (https://www.acunetix.com/privacy-policy/)

Sitemap (https://www.acunetix.com/sitemap/)