Web exploitation, explained by the pentesters who do it.

This section covers the server-side web vulnerabilities that most often escalate to serious impact: injection into templates, queries, and shells; parsers that betray trust; and request-boundary confusion. Each explainer names the technique, shows how it is detected and abused, and gives the control that closes it. For the client-side and access-control classes, see the Application Security section.

HOW IT WORKS

01 Related classes elsewhere

Web attacks span more than this section. The client-side and access-control classes live under Application Security:

- SQL Injection: breaking out of SQL syntax to read and alter data.
- Cross-Site Scripting (XSS): running script in the victim's browser.
- SSRF: coercing the server into making attacker-chosen requests.
- IDOR: reaching another user's objects through a predictable reference.

02 How to read this section

Every explainer follows the same shape: what the flaw is, how it is detected and abused with real payloads shown for defensive context, and how to close it. The payloads are here to help defenders recognize and reproduce the issue, not to weaponize it. If you want these tested against your own application with reproducible evidence and a developer-ready report, that is what web application penetration testing delivers.

SOURCES

[1] OWASP Web Security Testing Guide

[2] PortSwigger Web Security Academy

Have these tested against your real application.
securelayer7.net/learn/web-exploitation

Open online