

[← Back to all topics](#)

SQL injection

Cross-site scripting

Cross-site request forgery (CSRF)

Clickjacking

DOM-based vulnerabilities

Cross-origin resource sharing (CORS)

XML external entity (XXE) injection

Server-side request forgery (SSRF)

HTTP request smuggling

OS command injection

Server-side template injection

Path traversal

Access control vulnerabilities

Authentication

WebSockets

Cross-site scripting

LAB

APPRENTICE

Reflected XSS into HTML context with nothing encoded →

✓ Solved

APPRENTICE

Stored XSS into HTML context with nothing encoded →

✓ Solved



APPRENTICE

DOM XSS in `document.write` sink using `source`
`location.search` →

✓ Solved

LAB

APPRENTICE

DOM XSS in `innerHTML` sink using source `location.search` →

✓ Solved

Track your progress

1 Nasdaq 100
-2.12%

Q Search

ENG
IN

21:08
03-09-2024

< Back to all topics

SQL injection

Cross-site scripting

Cross-site request forgery (CSRF)

Clickjacking

DOM-based vulnerabilities

Cross-origin resource sharing (CORS)

XML external entity (XXE) injection

Server-side request forgery (SSRF)

HTTP request smuggling

OS command injection

Server-side template injection

Path traversal

Access control vulnerabilities

Authentication

WebSockets

LAB

PRACTITIONER

DOM XSS in `document.write` sink using source
`location.search` inside a select element →

✓ Solved

LAB

PRACTITIONER

DOM XSS in AngularJS expression with angle brackets and double
quotes HTML-encoded →

✓ Solved

LAB

PRACTITIONER

Reflected DOM XSS →

✓ Solved

LAB

PRACTITIONER

Stored DOM XSS →

✓ Solved

All labs | Web Security Academ

portswigger.net/web-security/all-labs#cross-site-scripting

< Back to all topics

SQL injection

Cross-site scripting

Cross-site request forgery (CSRF)

Clickjacking

LAB

EXPERT

Reflected XSS with AngularJS sandbox escape without strings →

Solved

LAB

EXPERT

Reflected XSS with AngularJS sandbox escape and CSP →

Solved