All labs

Mystery lab challenge

Try solving a random lab with the title and description hidden. As you'll have no prior knowledge of the type of vulnerability that you need to find and exploit, this is great for practicing recon and analysis.

Take me to the mystery lab challenge →

SQL injection

LAB APPRENTICE **SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →** ✓ Solved

LAB APPRENTICE **SQL injection vulnerability allowing login bypass →** ✓ Solved

LAB PRACTITIONER **SQL injection attack, querying the database type and version on Oracle →** ✓ Solved

LAB PRACTITIONER **SQL injection attack, querying the database type and version on MySQL and Microsoft →** ✓ Solved

LAB PRACTITIONER **SQL injection attack, listing the database contents on non-Oracle databases →** ✓ Solved

LAB PRACTITIONER **SQL injection attack, listing the database contents on Oracle →** Not solved

LAB PRACTITIONER **SQL injection UNION attack, determining the number of columns returned by the query →** Not solved

LAB PRACTITIONER **SQL injection UNION attack, finding a column containing text →** Not solved

LAB	PRACTITIONER	SQL injection UNION attack, retrieving data from other tables →	Not solved
LAB	PRACTITIONER	SQL injection UNION attack, retrieving multiple values in a single column →	Not solved
LAB	PRACTITIONER	Blind SQL injection with conditional responses →	Not solved
LAB	PRACTITIONER	Blind SQL injection with conditional errors →	Not solved
LAB	PRACTITIONER	Visible error-based SQL injection →	Not solved
LAB	PRACTITIONER	Blind SQL injection with time delays →	Not solved
LAB	PRACTITIONER	Blind SQL injection with time delays and information retrieval →	Not solved
LAB	PRACTITIONER	Blind SQL injection with out-of-band interaction →	Not solved
LAB	PRACTITIONER	Blind SQL injection with out-of-band data exfiltration →	Not solved
LAB	PRACTITIONER	SQL injection with filter bypass via XML encoding →	Not solved

Cross-site scripting

LAB	APPRENTICE	Reflected XSS into HTML context with nothing encoded →	Not solved
LAB	APPRENTICE	Stored XSS into HTML context with nothing encoded →	Not solved

LAB APPRENTICE
DOM XSS in `document.write` sink using source `location.search` →
Not solved

LAB APPRENTICE
DOM XSS in `innerHTML` sink using source `location.search` →
Not solved

LAB APPRENTICE
DOM XSS in jQuery anchor `href` attribute sink using `location.search` source →
Not solved

LAB APPRENTICE
DOM XSS in jQuery selector sink using a hashchange event →
Not solved

LAB APPRENTICE
Reflected XSS into attribute with angle brackets HTML-encoded →
Not solved

LAB APPRENTICE
Stored XSS into anchor `href` attribute with double quotes HTML-encoded →
Not solved

LAB APPRENTICE
Reflected XSS into a JavaScript string with angle brackets HTML encoded →
Not solved

LAB PRACTITIONER
DOM XSS in `document.write` sink using source `location.search` inside a select element →
Not solved

LAB PRACTITIONER
DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded →
Not solved

LAB PRACTITIONER
Reflected DOM XSS →
Not solved

LAB PRACTITIONER
Stored DOM XSS →
Not solved

LAB PRACTITIONER
Reflected XSS into HTML context with most tags and attributes blocked →
Not solved

LAB PRACTITIONER
Reflected XSS into HTML context with all tags blocked except custom ones →
Not solved

LAB
PRACTITIONER
Reflected XSS with some SVG markup allowed →
Not solved

LAB
PRACTITIONER
Reflected XSS in canonical link tag →
Not solved

LAB
PRACTITIONER
Reflected XSS into a JavaScript string with single quote and backslash escaped →
Not solved

LAB
PRACTITIONER
Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped →
Not solved

LAB
PRACTITIONER
Stored XSS into `onclick` event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped →
Not solved

LAB
PRACTITIONER
Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped →
Not solved

LAB
PRACTITIONER
Exploiting cross-site scripting to steal cookies →
Not solved

LAB
PRACTITIONER
Exploiting cross-site scripting to capture passwords →
Not solved

LAB
PRACTITIONER
Exploiting XSS to perform CSRF →
Not solved

LAB
EXPERT
Reflected XSS with AngularJS sandbox escape without strings →
Not solved

LAB
EXPERT
Reflected XSS with AngularJS sandbox escape and CSP →
Not solved

LAB
EXPERT
Reflected XSS with event handlers and `href` attributes blocked →
Not solved

LAB EXPERT Reflected XSS in a JavaScript URL with some characters blocked → Not solved

LAB EXPERT Reflected XSS protected by very strict CSP, with dangling markup attack → Not solved

LAB EXPERT Reflected XSS protected by CSP, with CSP bypass → Not solved

Cross-site request forgery (CSRF)

LAB APPRENTICE CSRF vulnerability with no defenses → Not solved

LAB PRACTITIONER CSRF where token validation depends on request method → Not solved

LAB PRACTITIONER CSRF where token validation depends on token being present → Not solved

LAB PRACTITIONER CSRF where token is not tied to user session → Not solved

LAB PRACTITIONER CSRF where token is tied to non-session cookie → Not solved

LAB PRACTITIONER CSRF where token is duplicated in cookie → Not solved

LAB PRACTITIONER SameSite Lax bypass via method override → Not solved

LAB PRACTITIONER SameSite Strict bypass via client-side redirect → Not solved

LAB PRACTITIONER SameSite Strict bypass via sibling domain → Not solved

LAB PRACTITIONER SameSite Lax bypass via cookie refresh → Not solved

LAB PRACTITIONER CSRF where Referer validation depends on header being present → Not solved

LAB PRACTITIONER CSRF with broken Referer validation → Not solved

Clickjacking

LAB APPRENTICE Basic clickjacking with CSRF token protection → Not solved

LAB APPRENTICE Clickjacking with form input data prefilled from a URL parameter → Not solved

LAB APPRENTICE Clickjacking with a frame buster script → Not solved

LAB PRACTITIONER Exploiting clickjacking vulnerability to trigger DOM-based XSS → Not solved

LAB PRACTITIONER Multistep clickjacking → Not solved

DOM-based vulnerabilities

LAB PRACTITIONER DOM XSS using web messages → Not solved

LAB PRACTITIONER DOM XSS using web messages and a JavaScript URL → Not solved

LAB PRACTITIONER DOM XSS using web messages and `JSON.parse` → Not solved

LAB PRACTITIONER DOM-based open redirection → Not solved

LAB	PRACTITIONER	DOM-based cookie manipulation →	Not solved
LAB	EXPERT	Exploiting DOM clobbering to enable XSS →	Not solved
LAB	EXPERT	Clobbering DOM attributes to bypass HTML filters →	Not solved

Cross-origin resource sharing (CORS)

LAB	APPRENTICE	CORS vulnerability with basic origin reflection →	Not solved
LAB	APPRENTICE	CORS vulnerability with trusted null origin →	Not solved
LAB	PRACTITIONER	CORS vulnerability with trusted insecure protocols →	Not solved
LAB	EXPERT	CORS vulnerability with internal network pivot attack →	Not solved

XML external entity (XXE) injection

LAB	APPRENTICE	Exploiting XXE using external entities to retrieve files →	Not solved
LAB	APPRENTICE	Exploiting XXE to perform SSRF attacks →	Not solved
LAB	PRACTITIONER	Blind XXE with out-of-band interaction →	Not solved
LAB	PRACTITIONER	Blind XXE with out-of-band interaction via XML parameter entities →	Not solved
LAB	PRACTITIONER	Exploiting blind XXE to exfiltrate data using a malicious external DTD →	Not solved

LAB	PRACTITIONER	Exploiting blind XXE to retrieve data via error messages →	Not solved
LAB	PRACTITIONER	Exploiting XInclude to retrieve files →	Not solved
LAB	PRACTITIONER	Exploiting XXE via image file upload →	Not solved
LAB	EXPERT	Exploiting XXE to retrieve data by repurposing a local DTD →	Not solved

Server-side request forgery (SSRF)

LAB	APPRENTICE	Basic SSRF against the local server →	Not solved
LAB	APPRENTICE	Basic SSRF against another back-end system →	Not solved
LAB	PRACTITIONER	Blind SSRF with out-of-band detection →	Not solved
LAB	PRACTITIONER	SSRF with blacklist-based input filter →	Not solved
LAB	PRACTITIONER	SSRF with filter bypass via open redirection vulnerability →	Not solved
LAB	EXPERT	Blind SSRF with Shellshock exploitation →	Not solved
LAB	EXPERT	SSRF with whitelist-based input filter →	Not solved

HTTP request smuggling

LAB PRACTITIONER
HTTP request smuggling, confirming a CL.TE vulnerability via differential responses →
Not solved

LAB PRACTITIONER
HTTP request smuggling, confirming a TE.CL vulnerability via differential responses →
Not solved

LAB PRACTITIONER
Exploiting HTTP request smuggling to bypass front-end security controls, CL.TE vulnerability →
Not solved

LAB PRACTITIONER
Exploiting HTTP request smuggling to bypass front-end security controls, TE.CL vulnerability →
Not solved

LAB PRACTITIONER
Exploiting HTTP request smuggling to reveal front-end request rewriting →
Not solved

LAB PRACTITIONER
Exploiting HTTP request smuggling to capture other users' requests →
Not solved

LAB PRACTITIONER
Exploiting HTTP request smuggling to deliver reflected XSS →
Not solved

LAB PRACTITIONER
Response queue poisoning via H2.TE request smuggling →
Not solved

LAB PRACTITIONER
H2.CL request smuggling →
Not solved

LAB PRACTITIONER
HTTP/2 request smuggling via CRLF injection →
Not solved

LAB PRACTITIONER
HTTP/2 request splitting via CRLF injection →
Not solved

LAB PRACTITIONER
CL.0 request smuggling →
Not solved

LAB PRACTITIONER
HTTP request smuggling, basic CL.TE vulnerability →
Not solved

LAB	PRACTITIONER HTTP request smuggling, basic TE.CL vulnerability →	✓ Solved
LAB	PRACTITIONER HTTP request smuggling, obfuscating the TE header →	Not solved
LAB	EXPERT Exploiting HTTP request smuggling to perform web cache poisoning →	Not solved
LAB	EXPERT Exploiting HTTP request smuggling to perform web cache deception →	Not solved
LAB	EXPERT Bypassing access controls via HTTP/2 request tunnelling →	Not solved
LAB	EXPERT Web cache poisoning via HTTP/2 request tunnelling →	Not solved
LAB	EXPERT Client-side desync →	Not solved
LAB	EXPERT Server-side pause-based request smuggling →	Not solved

OS command injection

LAB	APPRENTICE OS command injection, simple case →	Not solved
LAB	PRACTITIONER Blind OS command injection with time delays →	Not solved
LAB	PRACTITIONER Blind OS command injection with output redirection →	Not solved
LAB	PRACTITIONER Blind OS command injection with out-of-band interaction →	Not solved

LAB	PRACTITIONER	Blind OS command injection with out-of-band data exfiltration →	Not solved

Server-side template injection

LAB	PRACTITIONER	Basic server-side template injection →	Not solved
LAB	PRACTITIONER	Basic server-side template injection (code context) →	Not solved
LAB	PRACTITIONER	Server-side template injection using documentation →	Not solved
LAB	PRACTITIONER	Server-side template injection in an unknown language with a documented exploit →	Not solved
LAB	PRACTITIONER	Server-side template injection with information disclosure via user-supplied objects →	Not solved
LAB	EXPERT	Server-side template injection in a sandboxed environment →	Not solved
LAB	EXPERT	Server-side template injection with a custom exploit →	Not solved

Path traversal

LAB	APPRENTICE	File path traversal, simple case →	Not solved
LAB	PRACTITIONER	File path traversal, traversal sequences blocked with absolute path bypass →	Not solved
LAB	PRACTITIONER	File path traversal, traversal sequences stripped non-recursively →	Not solved
LAB	PRACTITIONER	File path traversal, traversal sequences stripped with superfluous URL-decode →	Not solved

LAB | PRACTITIONER | File path traversal, validation of start of path → | Not solved

LAB | PRACTITIONER | File path traversal, validation of file extension with null byte bypass → | Not solved

Access control vulnerabilities

LAB | APPRENTICE | Unprotected admin functionality → | ✓ Solved

LAB | APPRENTICE | Unprotected admin functionality with unpredictable URL → | ✓ Solved

LAB | APPRENTICE | User role controlled by request parameter → | ✓ Solved

LAB | APPRENTICE | User role can be modified in user profile → | ✓ Solved

LAB | APPRENTICE | User ID controlled by request parameter → | ✓ Solved

LAB | APPRENTICE | User ID controlled by request parameter, with unpredictable user IDs → | ✓ Solved

LAB | APPRENTICE | User ID controlled by request parameter with data leakage in redirect → | ✓ Solved

LAB | APPRENTICE | User ID controlled by request parameter with password disclosure → | ✓ Solved

LAB | APPRENTICE | Insecure direct object references → | ✓ Solved

LAB | PRACTITIONER | URL-based access control can be circumvented → | Not solved

LAB	PRACTITIONER	Method-based access control can be circumvented →	Not solved
LAB	PRACTITIONER	Multi-step process with no access control on one step →	Not solved
LAB	PRACTITIONER	Referer-based access control →	Not solved

Authentication

LAB	APPRENTICE	Username enumeration via different responses →	✓ Solved
LAB	APPRENTICE	2FA simple bypass →	✓ Solved
LAB	APPRENTICE	Password reset broken logic →	✓ Solved
LAB	PRACTITIONER	Username enumeration via subtly different responses →	Not solved
LAB	PRACTITIONER	Username enumeration via response timing →	Not solved
LAB	PRACTITIONER	Broken brute-force protection, IP block →	Not solved
LAB	PRACTITIONER	Username enumeration via account lock →	Not solved
LAB	PRACTITIONER	2FA broken logic →	Not solved
LAB	PRACTITIONER	Brute-forcing a stay-logged-in cookie →	Not solved
LAB	PRACTITIONER	Offline password cracking →	Not solved

LAB PRACTITIONER
Password reset poisoning via middleware →
Not solved

LAB PRACTITIONER
Password brute-force via password change →
Not solved

LAB EXPERT
Broken brute-force protection, multiple credentials per request →
✓ Solved

LAB EXPERT
2FA bypass using a brute-force attack →
Not solved

WebSockets

LAB APPRENTICE
Manipulating WebSocket messages to exploit vulnerabilities →
Not solved

LAB PRACTITIONER
Cross-site WebSocket hijacking →
Not solved

LAB PRACTITIONER
Manipulating the WebSocket handshake to exploit vulnerabilities →
Not solved

Web cache poisoning

LAB PRACTITIONER
Web cache poisoning with an unkeyed header →
Not solved

LAB PRACTITIONER
Web cache poisoning with an unkeyed cookie →
Not solved

LAB PRACTITIONER
Web cache poisoning with multiple headers →
Not solved

LAB PRACTITIONER
Targeted web cache poisoning using an unknown header →
Not solved

LAB PRACTITIONER Web cache poisoning via an unkeyed query string → Not solved

LAB PRACTITIONER Web cache poisoning via an unkeyed query parameter → Not solved

LAB PRACTITIONER Parameter cloaking → Not solved

LAB PRACTITIONER Web cache poisoning via a fat GET request → Not solved

LAB PRACTITIONER URL normalization → Not solved

LAB EXPERT Web cache poisoning to exploit a DOM vulnerability via a cache with strict cacheability criteria → Not solved

LAB EXPERT Combining web cache poisoning vulnerabilities → Not solved

LAB EXPERT Cache key injection → Not solved

LAB EXPERT Internal cache poisoning → Not solved

Insecure deserialization

LAB APPRENTICE Modifying serialized objects → Not solved

LAB PRACTITIONER Modifying serialized data types → Not solved

LAB PRACTITIONER Using application functionality to exploit insecure deserialization → Not solved

LAB PRACTITIONER Not solved

	Arbitrary object injection in PHP →	
LAB	PRACTITIONER Exploiting Java deserialization with Apache Commons →	Not solved
LAB	PRACTITIONER Exploiting PHP deserialization with a pre-built gadget chain →	Not solved
LAB	PRACTITIONER Exploiting Ruby deserialization using a documented gadget chain →	Not solved
LAB	EXPERT Developing a custom gadget chain for Java deserialization →	Not solved
LAB	EXPERT Developing a custom gadget chain for PHP deserialization →	Not solved
LAB	EXPERT Using PHAR deserialization to deploy a custom gadget chain →	Not solved

Information disclosure

LAB	APPRENTICE Information disclosure in error messages →	Not solved
LAB	APPRENTICE Information disclosure on debug page →	Not solved
LAB	APPRENTICE Source code disclosure via backup files →	Not solved
LAB	APPRENTICE Authentication bypass via information disclosure →	Not solved
LAB	PRACTITIONER Information disclosure in version control history →	Not solved

Business logic vulnerabilities

LAB	APPRENTICE	Excessive trust in client-side controls →	Not solved
LAB	APPRENTICE	High-level logic vulnerability →	Not solved
LAB	APPRENTICE	Inconsistent security controls →	Not solved
LAB	APPRENTICE	Flawed enforcement of business rules →	Not solved
LAB	PRACTITIONER	Low-level logic flaw →	Not solved
LAB	PRACTITIONER	Inconsistent handling of exceptional input →	Not solved
LAB	PRACTITIONER	Weak isolation on dual-use endpoint →	Not solved
LAB	PRACTITIONER	Insufficient workflow validation →	Not solved
LAB	PRACTITIONER	Authentication bypass via flawed state machine →	Not solved
LAB	PRACTITIONER	Infinite money logic flaw →	Not solved
LAB	PRACTITIONER	Authentication bypass via encryption oracle →	Not solved

HTTP Host header attacks

LAB	APPRENTICE	Basic password reset poisoning →	Not solved
LAB	APPRENTICE	Host header authentication bypass →	Not solved

LAB	PRACTITIONER	Web cache poisoning via ambiguous requests →	Not solved
LAB	PRACTITIONER	Routing-based SSRF →	Not solved
LAB	PRACTITIONER	SSRF via flawed request parsing →	Not solved
LAB	PRACTITIONER	Host validation bypass via connection state attack →	Not solved
LAB	EXPERT	Password reset poisoning via dangling markup →	Not solved

OAuth authentication

LAB	APPRENTICE	Authentication bypass via OAuth implicit flow →	Not solved
LAB	PRACTITIONER	SSRF via OpenID dynamic client registration →	Not solved
LAB	PRACTITIONER	Forced OAuth profile linking →	Not solved
LAB	PRACTITIONER	OAuth account hijacking via redirect_uri →	Not solved
LAB	PRACTITIONER	Stealing OAuth access tokens via an open redirect →	Not solved
LAB	EXPERT	Stealing OAuth access tokens via a proxy page →	Not solved

File upload vulnerabilities

LAB	APPRENTICE	Remote code execution via web shell upload →	Not solved
LAB	APPRENTICE	Web shell upload via Content-Type restriction bypass →	Not solved
LAB	PRACTITIONER	Web shell upload via path traversal →	Not solved
LAB	PRACTITIONER	Web shell upload via extension blacklist bypass →	Not solved
LAB	PRACTITIONER	Web shell upload via obfuscated file extension →	Not solved
LAB	PRACTITIONER	Remote code execution via polyglot web shell upload →	Not solved
LAB	EXPERT	Web shell upload via race condition →	Not solved

JWT

LAB	APPRENTICE	JWT authentication bypass via unverified signature →	Not solved
LAB	APPRENTICE	JWT authentication bypass via flawed signature verification →	Not solved
LAB	PRACTITIONER	JWT authentication bypass via weak signing key →	Not solved
LAB	PRACTITIONER	JWT authentication bypass via jwk header injection →	Not solved
LAB	PRACTITIONER	JWT authentication bypass via jku header injection →	Not solved
LAB	PRACTITIONER	JWT authentication bypass via kid header path traversal →	Not solved

LAB
EXPERT
JWT authentication bypass via algorithm confusion →
Not solved

LAB
EXPERT
JWT authentication bypass via algorithm confusion with no exposed key →
Not solved

Essential skills

LAB
PRACTITIONER
Discovering vulnerabilities quickly with targeted scanning →
Not solved

LAB
PRACTITIONER
Scanning non-standard data structures →
Not solved

Prototype pollution

LAB
PRACTITIONER
Client-side prototype pollution via browser APIs →
Not solved

LAB
PRACTITIONER
DOM XSS via client-side prototype pollution →
Not solved

LAB
PRACTITIONER
DOM XSS via an alternative prototype pollution vector →
Not solved

LAB
PRACTITIONER
Client-side prototype pollution via flawed sanitization →
Not solved

LAB
PRACTITIONER
Client-side prototype pollution in third-party libraries →
Not solved

LAB
PRACTITIONER
Privilege escalation via server-side prototype pollution →
Not solved

LAB
PRACTITIONER
Detecting server-side prototype pollution without polluted property reflection →
Not solved

LAB
PRACTITIONER
Not solved

Bypassing flawed input filters for server-side prototype pollution →

LAB PRACTITIONER
Remote code execution via server-side prototype pollution → Not solved

LAB EXPERT
Exfiltrating sensitive data via server-side prototype pollution → Not solved

GraphQL API vulnerabilities

LAB APPRENTICE
Accessing private GraphQL posts → Not solved

LAB PRACTITIONER
Accidental exposure of private GraphQL fields → Not solved

LAB PRACTITIONER
Finding a hidden GraphQL endpoint → Not solved

LAB PRACTITIONER
Bypassing GraphQL brute force protections → Not solved

LAB PRACTITIONER
Performing CSRF exploits over GraphQL → Not solved

Race conditions

LAB APPRENTICE
Limit overrun race conditions → Not solved

LAB PRACTITIONER
Bypassing rate limits via race conditions → Not solved

LAB PRACTITIONER
Multi-endpoint race conditions → Not solved

LAB PRACTITIONER
Single-endpoint race conditions → Not solved

LAB PRACTITIONER Exploiting time-sensitive vulnerabilities → Not solved

LAB EXPERT Partial construction race conditions → Not solved

NoSQL injection

LAB APPRENTICE Detecting NoSQL injection → Not solved

LAB APPRENTICE Exploiting NoSQL operator injection to bypass authentication → Not solved

LAB PRACTITIONER Exploiting NoSQL injection to extract data → Not solved

LAB PRACTITIONER Exploiting NoSQL operator injection to extract unknown fields → Not solved

API testing

LAB APPRENTICE Exploiting an API endpoint using documentation → Not solved

LAB PRACTITIONER Exploiting server-side parameter pollution in a query string → Not solved

LAB PRACTITIONER Finding and exploiting an unused API endpoint → Not solved

LAB PRACTITIONER Exploiting a mass assignment vulnerability → Not solved

LAB EXPERT Exploiting server-side parameter pollution in a REST URL → Not solved

Track your progress

Vulnerability labs: View all

7%

Level progress:

14 of 57	4 of 166	1 of 37
Apprentice	Practitioner	Expert

Your level:

Ne

NEWBIE

Solve 43 more labs to become an apprentice.

See where you rank on our Hall of Fame →

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research

PortSwigger

Follow us