


PortSwigger Completed Lab List

M.Gobi Shankar
CB.SC.P2CYS23019

Your level



Ne

NEWBIE

Solve 28 more labs to become an apprentice.

See where you rank

- Check out our [Hall of Fame](#)

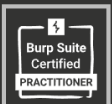
Hall of Fame high flyers

- Read three of our [user journeys](#)

Find your next topic

- [View all topics](#)

Your certifications



Burp Suite Certified PRACTITIONER

NOT READY

You're not ready to take the Burp Suite certification exam.

Level progress

30 of 58

Apprentice

47 of 168

Practitioner

1 of 38

Expert

Vulnerability labs

29%

[VIEW ALL](#)

Exam preparation steps

NOT READY

The labs you choose to complete must be "Practitioner" level or higher.

9 of 23

Lab from all topics

[Read more](#)

1 of 8

Specific labs

[Read more](#)

0 of 5

Mystery labs

[Read more](#)

0 of 1

Practice exam

[Read more](#)

SQL Injection

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

**PRACTITIONER**

SQL injection attack, listing the database contents on non-Oracle databases →

✓ Solved

**PRACTITIONER**

SQL injection attack, listing the database contents on Oracle →

✓ Solved

**PRACTITIONER**

SQL injection UNION attack, determining the number of columns returned by the query →

✓ Solved

**PRACTITIONER**

SQL injection UNION attack, finding a column containing text →

✓ Solved

**PRACTITIONER**

SQL injection UNION attack, retrieving data from other tables →

✓ Solved

**PRACTITIONER**

SQL injection UNION attack, retrieving multiple values in a single column →

✓ Solved

**PRACTITIONER**

Blind SQL injection with conditional responses →

✓ Solved

**PRACTITIONER**

Blind SQL injection with conditional errors →

✓ Solved

**PRACTITIONER**

Visible error-based SQL injection →

✓ Solved

**PRACTITIONER**

Blind SQL injection with time delays →

✓ Solved



PRACTITIONER

Blind SQL injection with time delays and information retrieval →

✓ Solved



PRACTITIONER

Blind SQL injection with out-of-band interaction →

Not solved



PRACTITIONER

Blind SQL injection with out-of-band data exfiltration →

Not solved



PRACTITIONER

SQL injection with filter bypass via XML encoding →

Not solved

Cross-Site Scripting

Cross-site scripting



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



APPRENTICE

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

✓ Solved



APPRENTICE

DOM XSS in jQuery anchor `href` attribute sink using
`location.search` source →

✓ Solved



APPRENTICE

DOM XSS in jQuery selector sink using a hashchange event →

✓ Solved



APPRENTICE

Reflected XSS into attribute with angle brackets HTML-encoded →

✓ Solved



APPRENTICE

Stored XSS into anchor `href` attribute with double quotes HTML-
encoded →

✓ Solved



APPRENTICE

Reflected XSS into a JavaScript string with angle brackets HTML
encoded →

✓ Solved



PRACTITIONER

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

✓ Solved



PRACTITIONER

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

✓ Solved



PRACTITIONER

Reflected DOM XSS →

✓ Solved



PRACTITIONER

Stored DOM XSS →

✓ Solved



PRACTITIONER

Reflected XSS into HTML context with most tags and attributes
blocked →

✓ Solved

**PRACTITIONER**

Reflected XSS into HTML context with all tags blocked except custom ones →

✓ Solved

**PRACTITIONER**

Reflected XSS with some SVG markup allowed →

✓ Solved

**PRACTITIONER**

Reflected XSS in canonical link tag →

✓ Solved

**PRACTITIONER**

Reflected XSS into a JavaScript string with single quote and backslash escaped →

✓ Solved

**PRACTITIONER**

Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped →

✓ Solved

**PRACTITIONER**

Stored XSS into `onclick` event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped →

✓ Solved

**PRACTITIONER**

Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped →

✓ Solved

**PRACTITIONER**

Exploiting cross-site scripting to steal cookies →

Not solved

**PRACTITIONER**

Exploiting cross-site scripting to capture passwords →

Not solved





**PRACTITIONER**

Exploiting XSS to perform CSRF →

✓ Solved






Cross-Origin Resource Sharing (CORS)

Cross-origin resource sharing (CORS)

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

XML External Entity (XXE) Injection

XML external entity (XXE) injection

 LAB	APPRENTICE Exploiting XXE using external entities to retrieve files →	✓ Solved
 LAB	APPRENTICE Exploiting XXE to perform SSRF attacks →	✓ 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

**PRACTITIONER**

Exploiting blind XXE to retrieve data via error messages →

✓ Solved

**PRACTITIONER**

Exploiting XInclude to retrieve files →

✓ Solved

**PRACTITIONER**

Exploiting XXE via image file upload →

✓ Solved

**EXPERT**

Exploiting XXE to retrieve data by repurposing a local DTD →

Not solved

Server-Side Request Forgery (SSRF)

Server-side request forgery (SSRF)

**APPRENTICE**

Basic SSRF against the local server →

✓ Solved

**APPRENTICE**

Basic SSRF against another back-end system →

✓ Solved

**PRACTITIONER**

Blind SSRF with out-of-band detection →

Not solved

**PRACTITIONER**

SSRF with blacklist-based input filter →

✓ Solved

**PRACTITIONER**

SSRF with filter bypass via open redirection vulnerability →

✓ Solved

**EXPERT**

Blind SSRF with Shellshock exploitation →

Not solved

**EXPERT**

SSRF with whitelist-based input filter →

✓ Solved

OS Command Injection

OS command injection

**APPRENTICE**

OS command injection, simple case →

✓ Solved

**PRACTITIONER**

Blind OS command injection with time delays →

✓ Solved

**PRACTITIONER**

Blind OS command injection with output redirection →

✓ Solved

**PRACTITIONER**

Blind OS command injection with out-of-band interaction →

Not solved

**PRACTITIONER**

Blind OS command injection with out-of-band data exfiltration →

Not solved

Path Traversal

Path traversal

🔬 LAB

APPRENTICE

File path traversal, simple case →

✓ Solved

🔬 LAB

PRACTITIONER

File path traversal, traversal sequences blocked with absolute path bypass →

✓ Solved

🔬 LAB

PRACTITIONER

File path traversal, traversal sequences stripped non-recursively →

✓ Solved

🔬 LAB

PRACTITIONER

File path traversal, traversal sequences stripped with superfluous URL-decode →

✓ Solved

🔬 LAB

PRACTITIONER

File path traversal, validation of start of path →

✓ Solved

🔬 LAB

PRACTITIONER

File path traversal, validation of file extension with null byte bypass →

✓ Solved


Access Control Vulnerabilities

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 →

✓ Solved



PRACTITIONER

Method-based access control can be circumvented →

✓ Solved



PRACTITIONER

Multi-step process with no access control on one step →

✓ Solved



PRACTITIONER

Referer-based access control →

✓ Solved

File Upload Vulnerabilities

File upload vulnerabilities



APPRENTICE

Remote code execution via web shell upload →

✓ Solved



APPRENTICE

Web shell upload via Content-Type restriction bypass →

✓ Solved



PRACTITIONER

Web shell upload via path traversal →

✓ Solved



PRACTITIONER

Web shell upload via extension blacklist bypass →

✓ Solved



PRACTITIONER

Web shell upload via obfuscated file extension →

✓ Solved



PRACTITIONER

Remote code execution via polyglot web shell upload →

✓ Solved



EXPERT

Web shell upload via race condition →

Not solved