







Web Security Completed Labs

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
 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 →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, determining the number of columns returned by the query →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, finding a column containing text →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, retrieving data from other tables →	✓ Solved

Web Security Completed Labs

 LAB	PRACTITIONER SQL injection UNION attack, retrieving multiple values in a single column →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with conditional responses →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with conditional errors →	✓ Solved
 LAB	PRACTITIONER Visible error-based SQL injection →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with time delays →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with time delays and information retrieval →	✓ Solved

OS Command Injection

 LAB	APPRENTICE OS command injection, simple case →	✓ Solved
 LAB	PRACTITIONER Blind OS command injection with time delays →	✓ Solved
 LAB	PRACTITIONER Blind OS command injection with output redirection →	✓ Solved

Web Security Completed Labs

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

File Upload


LAB	APPRENTICE Remote code execution via web shell upload →	✓ Solved
LAB	APPRENTICE Web shell upload via Content-Type restriction bypass →	✓ Solved
LAB	PRACTITIONER Web shell upload via path traversal →	✓ Solved
LAB	PRACTITIONER Web shell upload via extension blacklist bypass →	✓ Solved
LAB	PRACTITIONER Web shell upload via obfuscated file extension →	✓ Solved
LAB	PRACTITIONER Remote code execution via polyglot web shell upload →	✓ Solved

Web Security Completed Labs

Access Control

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


Web Security Completed Labs

 LAB

PRACTITIONER

Method-based access control can be circumvented →


✓ Solved

 LAB

PRACTITIONER

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

✓ Solved


 LAB

PRACTITIONER

Referer-based access control →

✓ Solved


Cross Site Scripting

 LAB

APPRENTICE

Reflected XSS into HTML context with nothing encoded →


✓ Solved

 LAB

APPRENTICE

Stored XSS into HTML context with nothing encoded →


✓ Solved

 LAB

APPRENTICE

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

✓ Solved

 LAB

APPRENTICE

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

✓ Solved

 LAB

APPRENTICE







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

✓ Solved




Web Security Completed Labs

LAB	APPRENTICE DOM XSS in jQuery selector sink using a hashchange event →	✓ Solved
LAB	APPRENTICE Reflected XSS into attribute with angle brackets HTML-encoded →	✓ Solved
LAB	APPRENTICE Stored XSS into anchor href attribute with double quotes HTML-encoded →	✓ Solved
LAB	APPRENTICE Reflected XSS into a JavaScript string with angle brackets HTML encoded →	✓ Solved
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
LAB	PRACTITIONER Reflected XSS into HTML context with most tags and attributes blocked →	✓ Solved
LAB	PRACTITIONER Reflected XSS into HTML context with all tags blocked except custom ones →	✓ Solved

Web Security Completed Labs

 LAB	PRACTITIONER Reflected XSS with some SVG markup allowed →	✓ Solved
 LAB	PRACTITIONER Reflected XSS in canonical link tag →	✓ Solved
 LAB	PRACTITIONER Reflected XSS into a JavaScript string with single quote and backslash escaped →	✓ Solved
 LAB	PRACTITIONER Reflected XSS into a JavaScript string with angle brackets and double quotes HTML-encoded and single quotes escaped →	✓ Solved
 LAB	PRACTITIONER Stored XSS into <code>onclick</code> event with angle brackets and double quotes HTML-encoded and single quotes and backslash escaped →	✓ Solved
 LAB	PRACTITIONER Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped →	✓ Solved

Cross-Side Request Forgery







 LAB	APPRENTICE CSRF vulnerability with no defenses →	✓ Solved
 LAB	PRACTITIONER CSRF where token validation depends on request method →	✓ Solved
 LAB	PRACTITIONER CSRF where token validation depends on token being present →	✓ Solved

Web Security Completed Labs

Server-Side Request Forgery

-  LAB APPRENTICE Basic SSRF against the local server →  Solved
-  LAB APPRENTICE Basic SSRF against another back-end system →  Solved
-  LAB PRACTITIONER SSRF with blacklist-based input filter →  Solved
-  LAB PRACTITIONER SSRF with filter bypass via open redirection vulnerability →  Solved
-  LAB EXPERT SSRF with whitelist-based input filter →  Solved

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 →  Solved

Web Security Completed Labs

LAB	PRACTITIONER Exploiting blind XXE to retrieve data via error messages →	✓ Solved
LAB	PRACTITIONER Exploiting XInclude to retrieve files →	✓ Solved
LAB	PRACTITIONER Exploiting XXE via image file upload →	✓ Solved

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