

SQL Injection

LAB 1: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

The screenshot shows the PortSwigger Web Security Academy interface. The main heading is "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". Below the heading, it says "APPRENTICE" and "LAB Solved". The description states: "This lab contains an SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out an SQL query like the following: SELECT * FROM products WHERE category = 'Gifts' AND released = 1. To solve the lab, perform an SQL injection attack that causes the application to display details of all products in any category, both released and unreleased." There is a button "Access the lab" and a "Solution" dropdown menu. On the right, a "Track your progress" sidebar shows 0% completion for learning materials and vulnerability labs, and a level progress of 1 of 32 for the Apprentice level.


LAB 2: SQL injection UNION attack, finding a column containing text


The screenshot shows the PortSwigger Web Security Academy interface for Lab 2. The main heading is "Lab: SQL injection UNION attack, finding a column containing text". Below the heading, it says "PRACTITIONER" and "LAB Solved". The description states: "This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. To do this, you need to find a column containing text data. The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform an SQL injection UNION attack that returns an additional row containing the value provided." There is a button "Access the lab" and a "Solution" dropdown menu. On the right, a "Track your progress" sidebar shows 1% completion for vulnerability labs, and a level progress of 1 of 88 for the Practitioner level.

LAB 3: SQL injection UNION attack, determining the number of columns returned by the query

The screenshot shows the PortSwigger Web Security Academy interface for Lab 3. The main heading is "Lab: SQL injection UNION attack, determining the number of columns returned by the query". Below the heading, it says "PRACTITIONER" and "LAB Solved". The description states: "This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables. To do this, you first need to determine the number of columns that are being returned by the query. To solve the lab, perform an SQL injection UNION attack that returns an additional row containing null values." There is a button "Access the lab" and a "Solution" dropdown menu. On the right, a "Track your progress" sidebar shows 2% completion for vulnerability labs, and a level progress of 2 of 88 for the Practitioner level.







LAB 4: SQL injection UNION attack, retrieving multiple values in a single column



Products | Solutions | Research | Academy | Daily Swig | Support | 

Web Security Academy » SQL injection » UNION attacks » Lab


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



PRACTITIONER

LAB


Solved



This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The database contains a different table called users, with columns called username and password.

To solve the lab, perform an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the administrator user.

 Read more

SQL injection cheat sheet »

Access the lab

Track your progress

Learning materials:

View all

0%

Vulnerability labs:

View all

2%

Level progress:

1 of 32

3 of 88

0 of 18

Apprentice Practitioner Expert


Your level:


Ne

NEWBIE

Solve 31 more labs to become an apprentice.







LAB 5: SQL injection vulnerability allowing login bypass



Products | Solutions | Research | Academy | Daily Swig | Support | 

Web Security Academy » SQL injection » Lab


Lab: SQL injection vulnerability allowing login bypass



APPRENTICE

LAB

Solved



This lab contains an SQL injection vulnerability in the login function.

To solve the lab, perform an SQL injection attack that logs in to the application as the administrator user.

Access the lab

Solution

Track your progress

Learning materials:

View all

0%

Vulnerability labs:

View all

0%

Level progress:

1 of 32

0 of 88

0 of 18

Apprentice Practitioner Expert

Your level:


Ne


NEWBIE

Solve 31 more labs to become an apprentice.

Cross-site scripting







LAB 1: DOM XSS in jQuery anchor href attribute sink using location.search source



Products | Solutions | Research | Academy | Daily Swig | Support | 

Web Security Academy » Cross-site scripting » DOM-based » Lab


Lab: DOM XSS in jQuery anchor href attribute sink using location.search source



APPRENTICE

LAB

Solved



This lab contains a DOM-based cross-site scripting vulnerability in the submit feedback page. It uses the jQuery library's `$` selector function to find an anchor element, and changes its href attribute using data from `location.search`.

To solve this lab, make the "back" link alert `document.cookie`.

Access the lab

Solution

Track your progress

Learning materials:

View all

0%

Vulnerability labs:

View all

7%

Level progress:

6 of 32

5 of 88

0 of 18

Apprentice Practitioner Expert

Your level:

Ne

NEWBIE

Solve 26 more labs to become an apprentice.

LAB 2: DOM XSS in innerHTML sink using source location.search

Web Security Academy » Cross-site scripting » DOM-based » Lab

Lab: DOM XSS in innerHTML sink using source location.search

APPRENTICE

LAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the search blog functionality. It uses an innerHTML assignment, which changes the HTML contents of a div element, using data from location.search. To solve this lab, perform a cross-site scripting attack that calls the alert function.

Access the lab

Solution

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

7%

Level progress:

5 of 32 Apprentice 5 of 68 Practitioner 0 of 18 Expert

Your level:

LAB 3: DOM XSS in document.write sink using source location.search inside a select element

PORTSWIGGER
WEB SECURITY

Log out

My account

Products | Solutions | Research | Academy | Daily Swig | Support |

Web Security Academy » Cross-site scripting » DOM-based » Lab

Lab: DOM XSS in document.write sink using source location.search inside a select element

PRACITIONER

LAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the stock checker functionality. It uses the JavaScript document.write function, which writes data out to the page. The document.write function is called with data from location.search which you can control using the website URL. The data is enclosed within a select element.

To solve this lab, perform a cross-site scripting attack that breaks out of the select element and calls the alert function.

Access the lab

Solution

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

0%

Level progress:

4 of 32 Apprentice 5 of 68 Practitioner 0 of 18 Expert

Your level:

NEWBIE Solve 28 more labs to become an apprentice.

See where you rank on our Hall of Fame >

LAB 4: DOM XSS in document.write sink using source location.search

PORTSWIGGER
WEB SECURITY

Log out

My account

Products | Solutions | Research | Academy | Daily Swig | Support |

Web Security Academy » Cross-site scripting » DOM-based » Lab

Lab: DOM XSS in document.write sink using source location.search

APPRENTICE

LAB Solved

This lab contains a DOM-based cross-site scripting vulnerability in the search query tracking functionality. It uses the JavaScript document.write function, which writes data out to the page. The document.write function is called with data from location.search, which you can control using the website URL.

To solve this lab, perform a cross-site scripting attack that calls the alert function.

Access the lab

Solution

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

5%

Level progress:

4 of 32 Apprentice 4 of 68 Practitioner 0 of 18 Expert

Your level:

NEWBIE Solve 28 more labs to

LAB 5: Reflected XSS into HTML context with nothing encoded

PORTSWIGGER
WEB SECURITY

Log out

My account

Products | Solutions | Research | Academy | Daily Swig | Support |

Web Security Academy » Cross-site scripting » Reflected » Lab

Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

LAB Solved

This lab contains a simple reflected cross-site scripting vulnerability in the search functionality. To solve this lab, perform a cross-site scripting attack that calls the alert function.

Access the lab

Solution

Track your progress

Learning materials: [View all](#)

0%

Vulnerability labs: [View all](#)

5%

Level progress:

3 of 32 Apprentice 4 of 68 Practitioner 0 of 18 Expert

Your level:

Cross-site request forgery (CSRF)

LAB 1: CSRF with broken Referer validation

PORTSWIGGER

WEB SECURITY

[Products](#) | [Solutions](#) | [Research](#) | [Academy](#) | [Daily Swig](#) | [Support](#) | [Menu](#)

Web Security Academy » CSRF » Lab

Lab: CSRF with broken Referer validation

PRACITIONER

LAB Solved

This lab's email change functionality is vulnerable to CSRF. It attempts to detect and block cross domain requests, but the detection mechanism can be bypassed.

To solve the lab, use your exploit server to host an HTML page that uses a **CSRF attack** to change the viewer's email address.

You have an account on the application that you can use to help design your attack. The credentials are: carlos / montoya.

Access the lab

Solution

Track your progress

Learning materials: 0% [View all](#)

Vulnerability labs: 4% [View all](#)

Level progress:

2 of 32

4 of 88

0 of 18

Apprentice Practitioner Expert

Your level:

Ne NEWBIE

Solve 30 more labs to

LAB 2: CSRF vulnerability with no defenses

PORTSWIGGER

WEB SECURITY

[Products](#) | [Solutions](#) | [Research](#) | [Academy](#) | [Daily Swig](#) | [Support](#) | [Menu](#)

Web Security Academy » CSRF » Lab

Lab: CSRF vulnerability with no defenses

APPRENTICE

LAB Solved

This lab's email change functionality is vulnerable to CSRF.

To solve the lab, craft some HTML that uses a **CSRF attack** to change the viewer's email address and upload it to your exploit server.

You have an account on the application that you can use to help design your attack. The credentials are: carlos / montoya.

Access the lab

Solution

Track your progress

Learning materials: 0% [View all](#)

Vulnerability labs: 3% [View all](#)

Level progress:

2 of 32

3 of 88

0 of 18

Apprentice Practitioner Expert

Your level:

Ne NEWBIE

Solve 30 more labs to become an apprentice