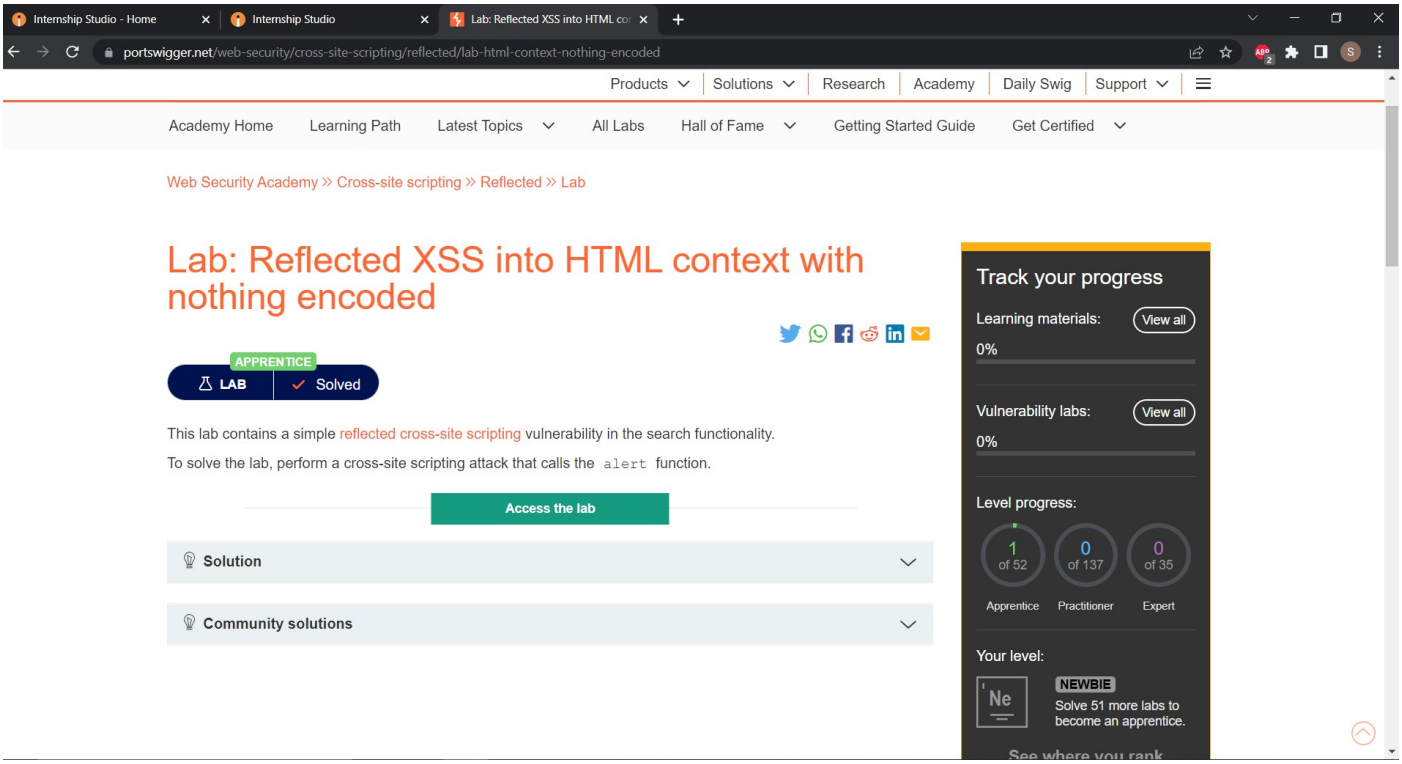
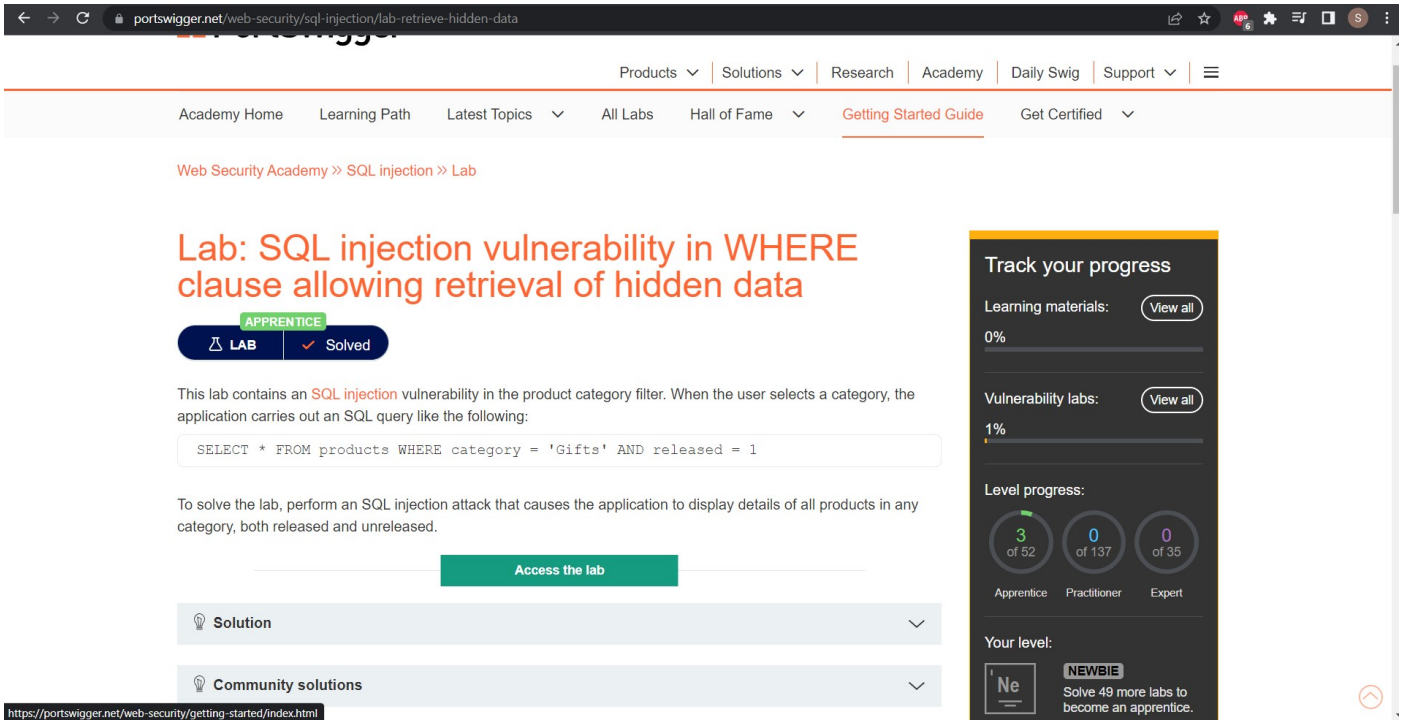
ETHICAL HACKING PROJECT REPORT

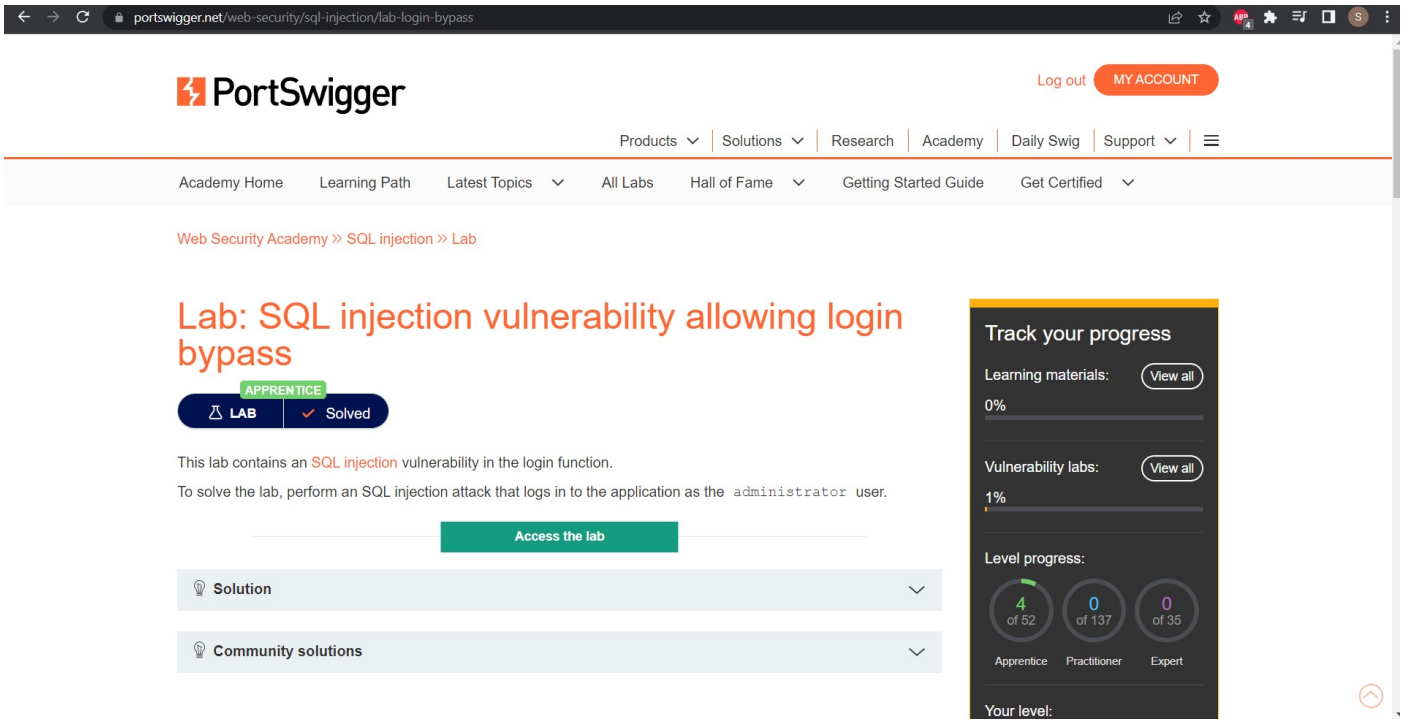
Steps for Task-1:

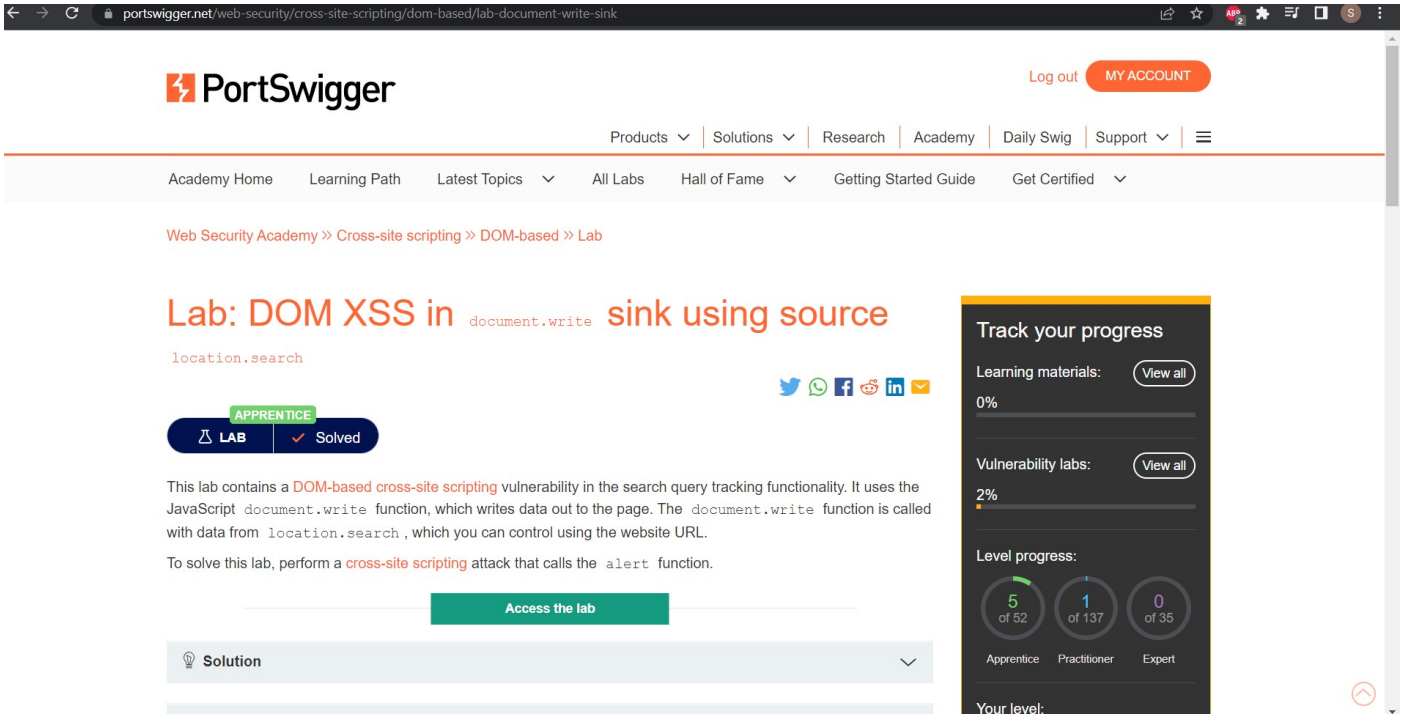
1) Open Portswigger website and login.
2) Click on ‘All labs’ icon.
3) Select any 5 labs in the list shown.
4) Read the problem statement in each lab
5) For help and hints see the solution and community solutions.
6) Proceed with the lab as the problem statement
7) Complete the labs.

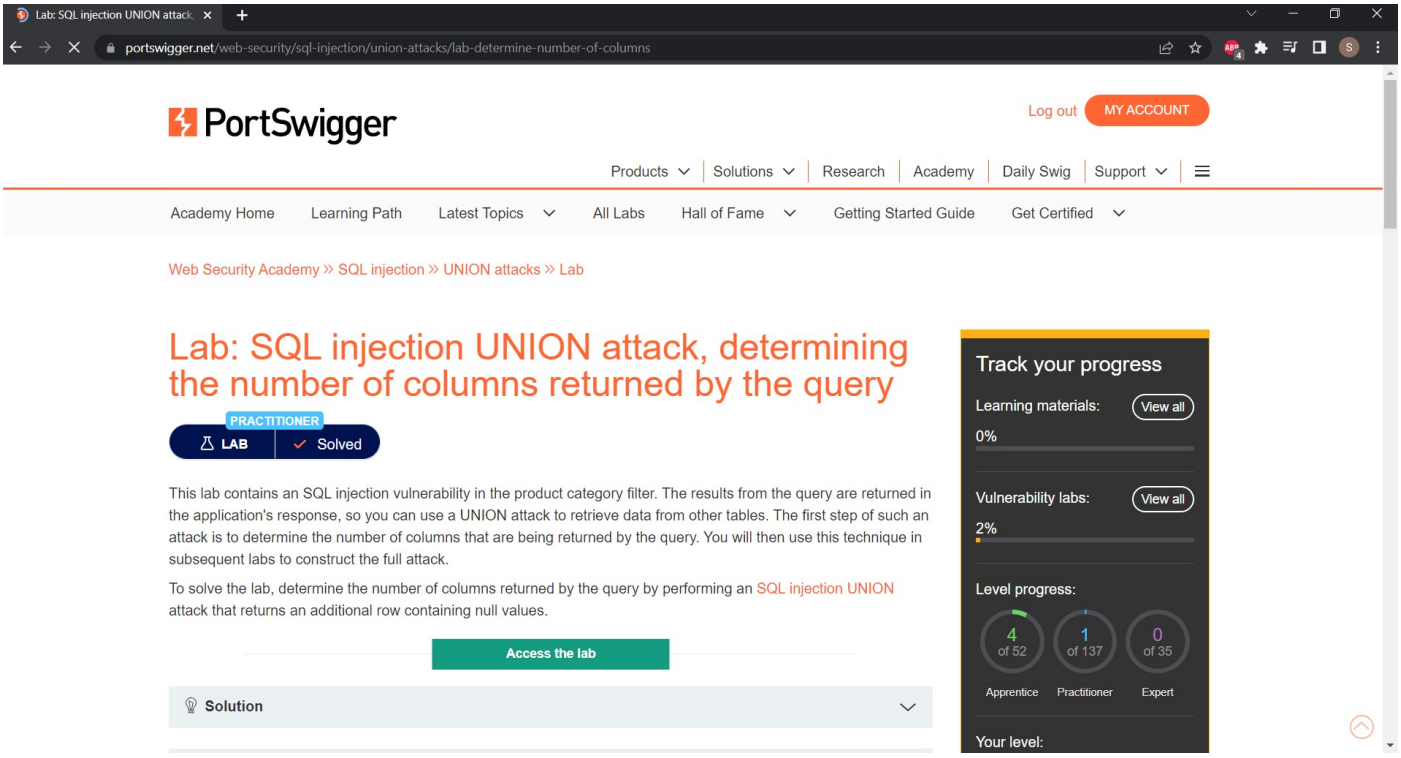
Screenshots of Portswigger labs:




portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » SQL injection » Lab
Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
APPRENTICE
LAB
Solved
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.
Access the lab
Solution
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
1%
Level progress:
3 of 52
Apprentice
0 of 137
Practitioner
0 of 35
Expert
Your level:
Ne
NEWBIE
Solve 49 more labs to become an apprentice.
https://portswigger.net/web-security/getting-started/index.html


portswigger.net/web-security/sql-injection/lab-login-bypass
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
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
Community solutions
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
1%
Level progress:
4 of 52
Apprentice
0 of 137
Practitioner
0 of 35
Expert
Your level:


portswigger.net/web-security/cross-site-scripting/dom-based/lab-document-write-sink
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
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
2%
Level progress:
5 of 52
1 of 137
0 of 35
Apprentice
Practitioner
Expert
Your level:


Lab: SQL injection UNION attack
portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » SQL injection » UNION attacks » Lab
Lab: SQL injection UNION attack, determining the number of columns returned by the query
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 first step of such an attack is to determine the number of columns that are being returned by the query. You will then use this technique in subsequent labs to construct the full attack.
To solve the lab, determine the number of columns returned by the query by performing an SQL injection UNION attack that returns an additional row containing null values.
Access the lab
Solution
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
2%
Level progress:
4 of 52
1 of 137
0 of 35
Apprentice
Practitioner
Expert
Your level:

Task-2

Please click on the link to see the ppts and report
https://docs.google.com/presentation/d/1oko448nprOUufGarGqSXIFSPdUk4apvZKxbZAWIJpYQ/edit?usp=sharing

Task-3

Please click on the link to see the ppts and POC

https://docs.google.com/presentation/d/1EcbHk1CUwVK21qA-SwEwjw6B0FVPIrDKT1oxndZxngo/edit?usp=sharing

Y. Subbaramireddy