



# Universidad del Caribe

2000

CANCUN, QUINTANA ROO, MÉXICO

CONOCIMIENTO Y CULTURA PARA EL DESARROLLO HUMANO

## SQL injection

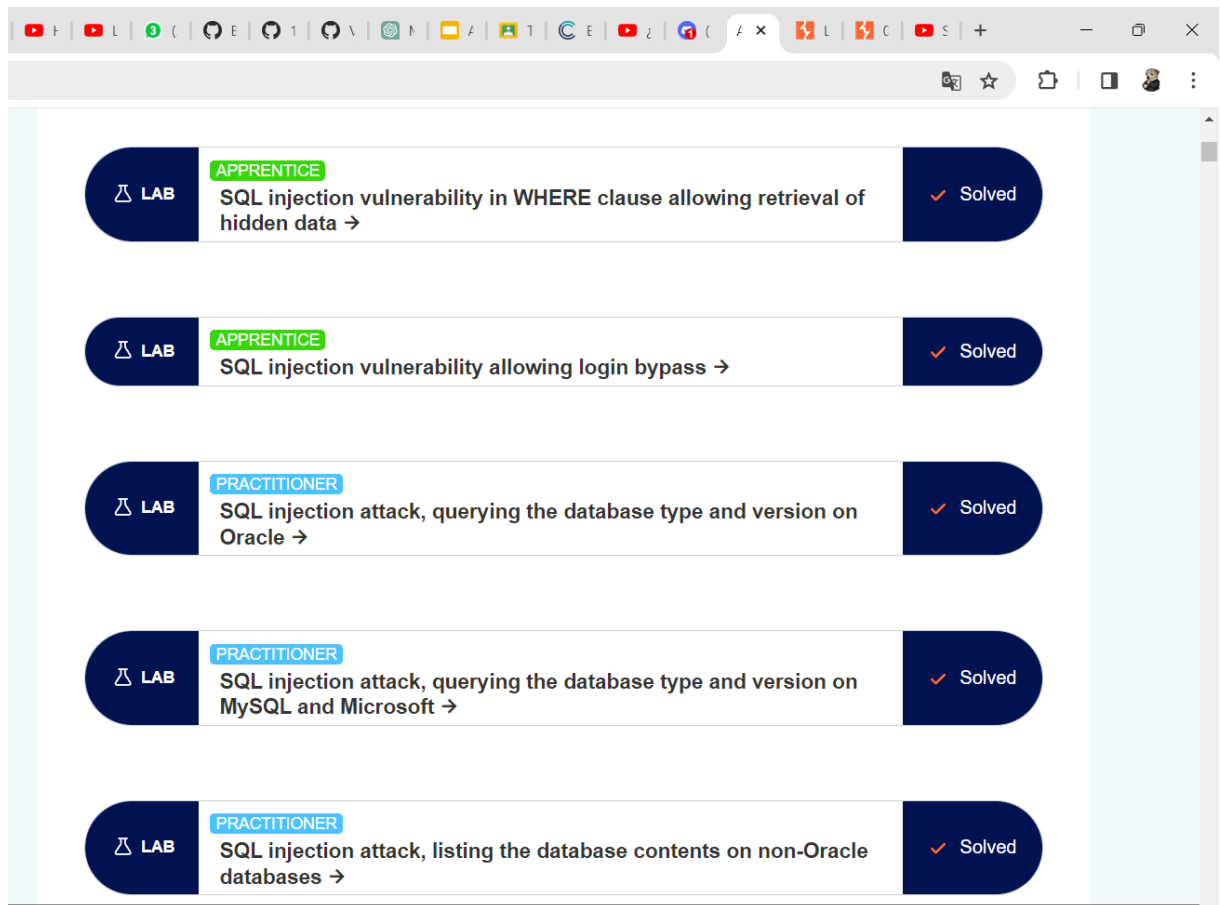
# A

Alumno: yam Segovia fernando

Matricula: 180300380

Maestro: Ismael Jiménez (tuxtter)










# Ejercicios SQL injectio resueltos



A screenshot of a web browser displaying a list of solved SQL injection exercises. The browser's address bar shows a URL with various icons. The exercises are listed in a table-like format with columns for a flag icon, a difficulty level, a description, and a status.

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 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
LAB	PRACTITIONER	SQL injection UNION attack, retrieving multiple values in a single column →	✓ Solved

 LAB	<b>PRACTITIONER</b> SQL injection UNION attack, retrieving multiple values in a single column →	✓ Solved
 LAB	<b>PRACTITIONER</b> Blind SQL injection with conditional responses →	✓ Solved
 LAB	<b>PRACTITIONER</b> Blind SQL injection with conditional errors →	✓ Solved
 LAB	<b>PRACTITIONER</b> Visible error-based SQL injection →	✓ Solved
 LAB	<b>PRACTITIONER</b> Blind SQL injection with time delays →	✓ Solved
<hr/>		
 LAB	<b>PRACTITIONER</b> Blind SQL injection with time delays and information retrieval →	✓ Solved
 LAB	<b>PRACTITIONER</b> Blind SQL injection with out-of-band interaction →	Not solved
 LAB	<b>PRACTITIONER</b> Blind SQL injection with out-of-band data exfiltration →	Not solved
 LAB	<b>PRACTITIONER</b> SQL injection with filter bypass via XML encoding →	✓ Solved
<hr/>		
<b>Cross site scripting</b>		

Los ejercicios que están ahí como no resueltos solo se pueden hacer con una edición de pago, no se pueden realizar ya que necesita un apartado que solo tiene la versión donde se paga

