

<div> <div><</div> <div>Menu</div> </div>	SQL injection	
	<div> <div>LAB</div> <div>APPRENTICE</div> </div>	SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →
	<div> <div>LAB</div> <div>APPRENTICE</div> </div>	SQL injection vulnerability allowing login bypass →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection attack, querying the database type and version on Oracle →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection attack, querying the database type and version on MySQL and Microsoft →
<div> <div><</div> <div>Menu</div> </div>	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection attack, listing the database contents on non-Oracle databases →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection attack, listing the database contents on Oracle →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection UNION attack, determining the number of columns returned by the query →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection UNION attack, finding a column containing text →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection UNION attack, retrieving data from other tables →
<div> <div><</div> <div>Menu</div> </div>	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	SQL injection UNION attack, retrieving multiple values in a single column →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	Blind SQL injection with conditional responses →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	Blind SQL injection with conditional errors →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	Visible error-based SQL injection →
	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	Blind SQL injection with time delays →
<div> <div><</div> <div>Menu</div> </div>	<div> <div>LAB</div> <div>PRACTITIONER</div> </div>	

< Menu

Blind SQL injection with time delays →

LAB

PRACTITIONER

Blind SQL injection with time delays and information retrieval →

Solved

LAB

PRACTITIONER

Blind SQL injection with out-of-band interaction →

Solved

LAB

PRACTITIONER

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

Solved

LAB

PRACTITIONER

SQL injection with filter bypass via XML encoding →

Solved

Cross-site scripting

LAB

APPRENTICE

Reflected XSS into HTML context with nothing encoded →

Not solved