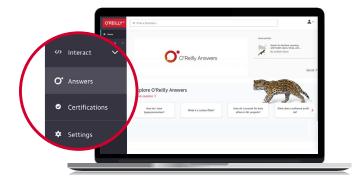


How to use O'Reilly Answers

O'Reilly Answers is an advanced natural language processing engine that finds quick solutions to challenging technical questions. Just ask a question and O'Reilly Answers leverages machine learning techniques to scan expert content across thousands of O'Reilly titles to deliver highly relevant content snippets to further explore. It's even easier to use than it sounds.

1. Find Answers

Once you've logged on to O'Reilly online learning, click "Answers" on the left-side navigation bar.



3. See results

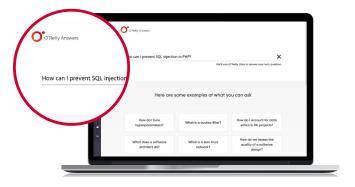
O'Reilly Answers finds and highlights the content that best answers your question. Click the arrows to get to additional answers.



For questions please contact customercare@oreiilly.com.

2. Ask questions

Just type in any question you might have, from something as general as "What is ACID?" to a more specific "How can I prevent SQL injection in PHP?"



4. Know more

You can scroll to see more information to better understand the context of your highlighted answer. Or click "Read more" on any selection for even more information.

× How can I prevent SQL inject	tion in PHP? Flid Answers
8 Answers to: How can I preve	nt SQL injection in PHP?
Programming PHP, 4th E By Kevin Tatroe and Peter A	
However, this only ensures	that the data you escape is interpreted as data. You still need to filter data
The best protection against	50L injection is the use of bound parameters. The following example
< Smgl = \$db -> preps	h be considered anyth
	d is necessary.
	ensure that the data never enters a context where it can be considered anyon interpreted), no escaping of the username and password is necessary.
>	Read more

