

Câu hỏi của tôi là: "Tại sao việc sử dụng Prepared Statement (như `prepare` và `execute` với dấu `?`) lại ngăn chặn được tấn công SQL Injection, trong khi việc cộng chuỗi trực tiếp (như `$sql = "INSERT... VALUES ('$ten')"`) lại không?"