1. Truy xuất dữ liệu ẩn: là nơi chúng ta có thể truy vấn SQL để trả về kết quả như mong muốn chẳng hạn như trên thanh URL của trình duyệt website.

* VD: Chúng ta có URL như sau: https://example.com/products?category=Gifts
  + Câu truy vấn SQL như sau: SELECT \* FROM products WHERE category = 'Gifts' AND released =1. Với câu SQL này kết quả sẽ trả về chi tiết các sản phẩm trong category từ bảng products nơi có category là ‘Gifts’ và giá trị của released là 1 còn giá trị 0 sẽ không hiển thị.
  + Bây giờ chúng ta sẽ thêm 2 kí tự gạch ngang của URL trên. https:///example.com/products?category=Gifts'--. Và câu SQL của chúng ta lúc này sẽ như thế này: SELECT \* FROM products WHERE category = 'Gifts'--' AND released = 1 . Vì trong SQL, dấu "--" là comment nên kết quả trả về sẽ là những sản phẩm chỉ cần có category='Gifts'.

1. Chuyển logic ứng dụng: được thể hiện qua việc xác thực đăng nhập của một người dụng đối với website ứng dụng.
2. Tấn công UNION: sử dụng toán tử UNION trong ngôn ngữ SQL cho phép tổng hợp kết quả của 2 hay nhiều câu truy vấn SELECTION trong cùng 1 kết quả và được trả về như một phần của HTTP response

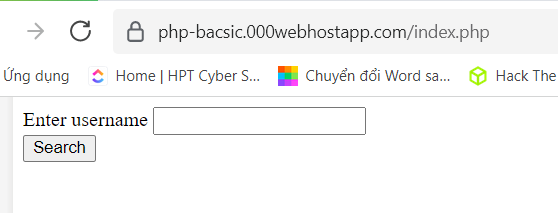
* VD: cũng dùng web trên và thêm vào sau "' UNION SELECT username, password FROM users--"

1. Blind SQLi: các phản hồi HTTP của nó không chứa kết quả của truy vấn SQL có liên quan hoặc chi tiết về bất kỳ lỗi cơ sở dữ liệu nào. Loại tấn công này chủ yếu sẽ dựa vào các boolean trả về.
2. Stored-procedures: tấn công này chủ yếu nhắm vào các tài khoản quản trị (như tài khoản 'root' Mysql hoặc 'sa' MS Server) để hacker có thể điều khiển và làm rối loạn hệ thống.
3. Error-base: Là một kỹ thuật tấn công SQL Injection dựa vào thông báo lỗi được trả về từ Database Server có chứa thông tin về cấu trúc của cơ sở dữ liệu.

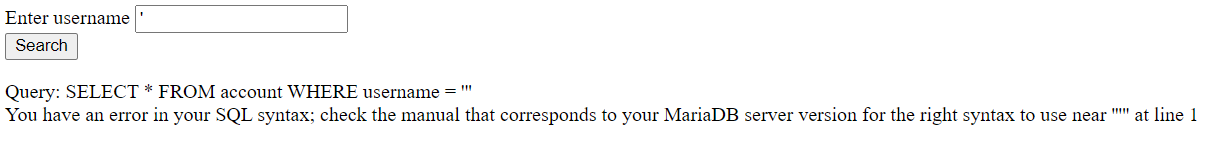
* VD:
  + Database chỉ có 1 bảng account với dữ liệu là 3 account đã thêm vào trước đó.



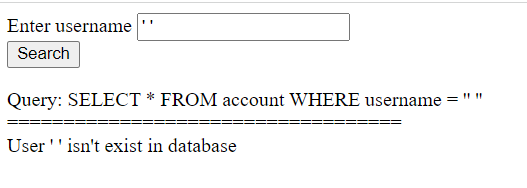
* + Bây giờ, ta vào web này để làm: https://php-bacsic.000webhostapp.com/index.php



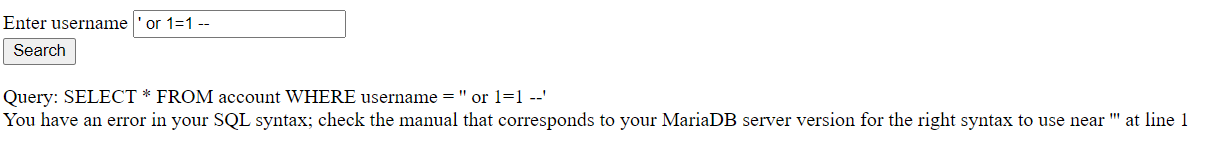
* + Bây giờ, chúng ta thử thêm dấu nháy đơn “ ‘ ” vào thanh search và search thử.



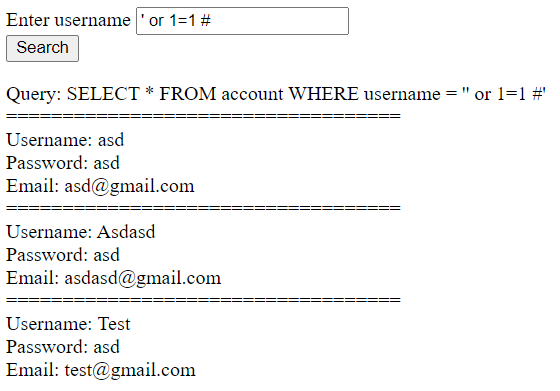
* + Ta có thể thấy, khi nhập vào input dấu nháy đơn “ ‘ ” thì gây ra lỗi – đây là error base SQLi. Như ta thấy lỗi ở trên chính là 1 lỗi của sqli. Và nó cũng cho chúng ta biết lỗi là thừa 1 dấu nháy đơn. Bây giờ, ta hãy thử thêm 1 dấu nháy đơn vào thanh search.



* + Điều này chứng tỏ, chúng ta đã nhập vào user là “ ‘ ‘ “ nhưng tìm trong DB không có username nào như vậy cả.
  + Giờ chúng ta sẽ thử qua truy vấn logic và nhập giá trị ' or 1=1 --. Ở đây dấu “--” này là comment của SQL server.



* + Giờ hãy thử thay dấu “--” bằng dấu “#” – là dấu để comment của mysql. Như đã thấy ở dưới chúng ta đã lấy hết được các user.



* + Tôi sẽ thử thêm 1 query UNION nữa. Kết quả, chúng ta vẫn lấy được tất cả user có trong DB.

