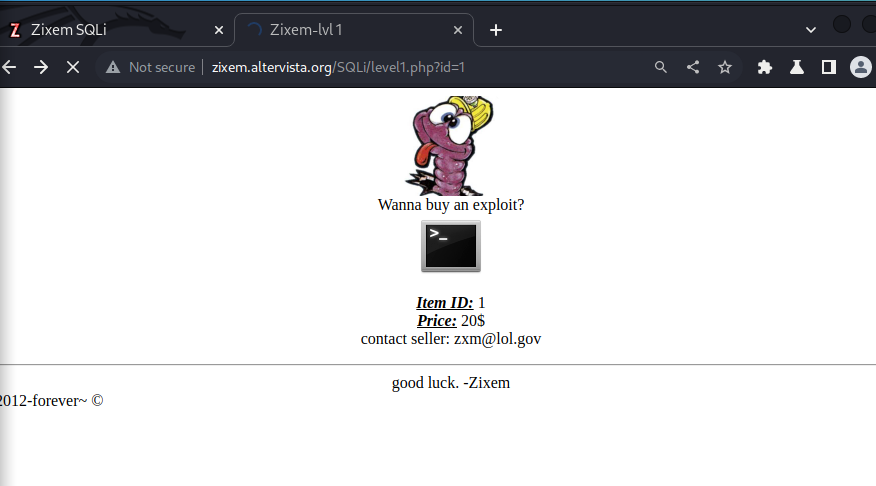
# SQLi

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Đề yêu cầu ta tìm version và user
* Level 1



* Đầu tiên truy cập vào challenge level 1
* Ta muốn kiểm tra xem trang web có bị lỗi sql injection hay không ta thêm 1 ký tự đặc biệt vào

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thêm vào ký tự ‘ để kiểm tra sau đó forward gói tin đi

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta thấy trang web trả về lỗi như trên
* Vậy trang web có bị lỗi SQL injection

Ảnh có chứa văn bản

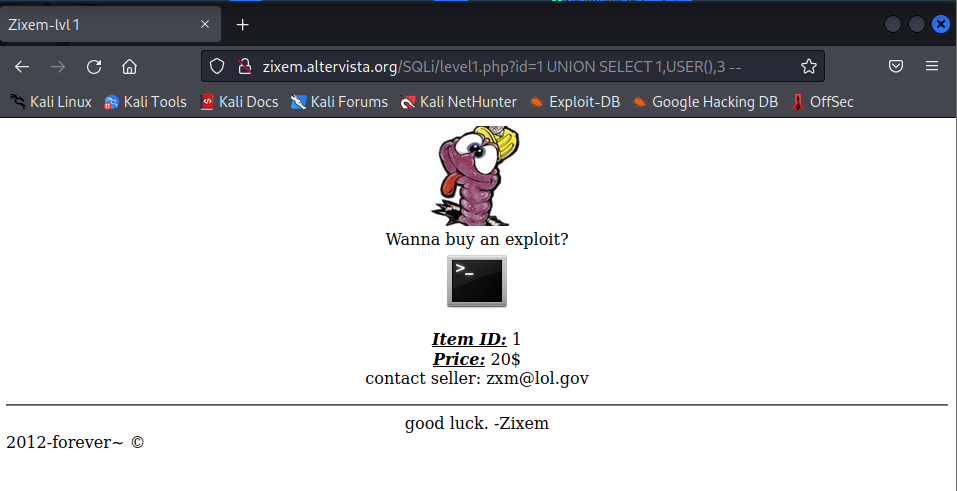
Mô tả được tạo tự động

* Ta tìm thử số cột của bảng bằng cách dùng lệnh ORDER BY n với n tăng dần từ \*2. Sau khi thử số 4 thì trang web xuất hiện lỗi

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bảng có 3 cột

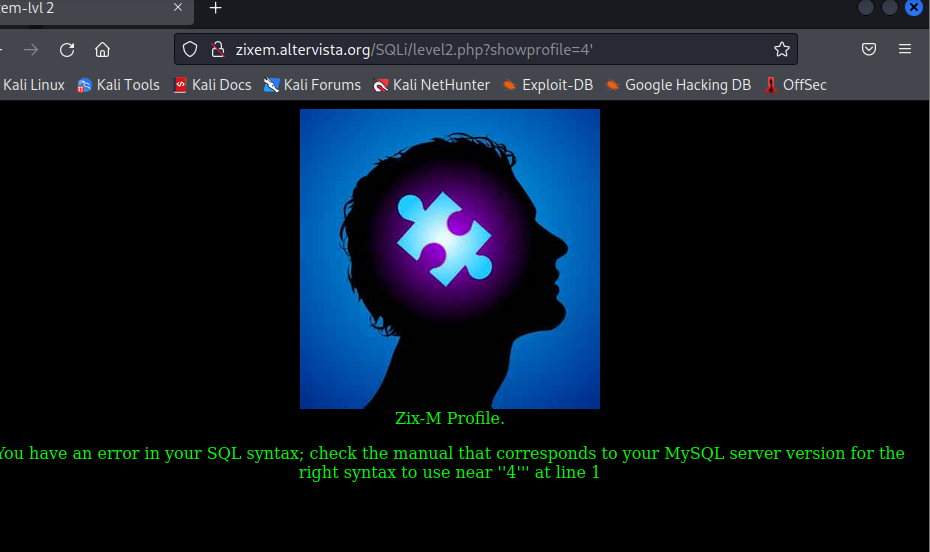


* Ta thử dùng câu lệnh để xem các giá trị trong bảng nhưng không có điều gì xảy ra. Để đảm bảo câu lệnh SQL của ta sẽ được trả về thì ta cần vô hiệu hóa câu lệnh SQL ban đầu bằng 1 điều kiện sai
* Khi đó câu lệnh của ta sẽ được thực thi
* **Câu lệnh SQL sẽ là: AND 1=2 UNION SELECT version(),USER(),3 - -**

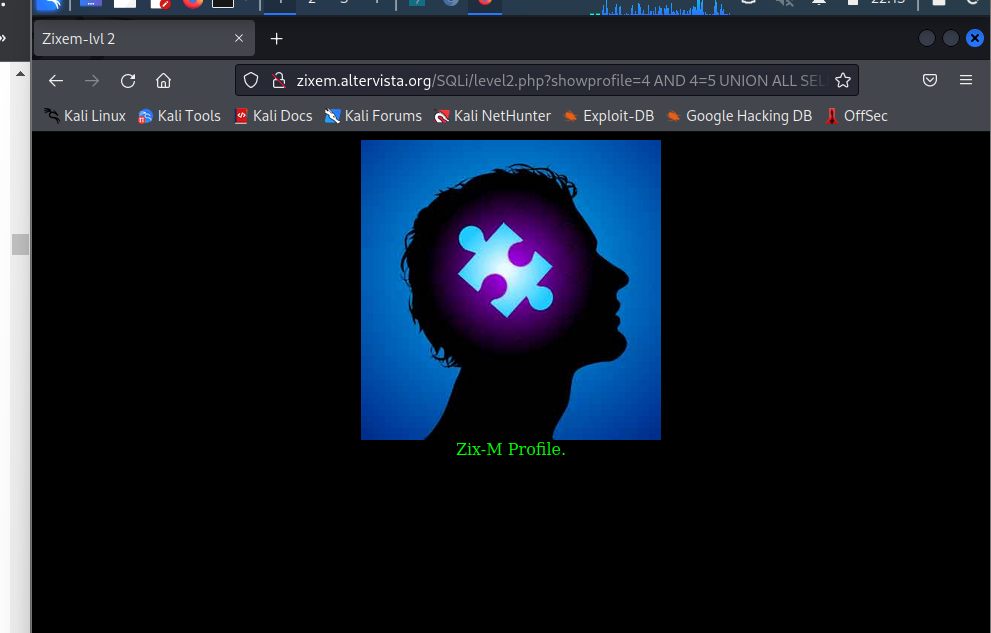
Ảnh có chứa văn bản

Mô tả được tạo tự động

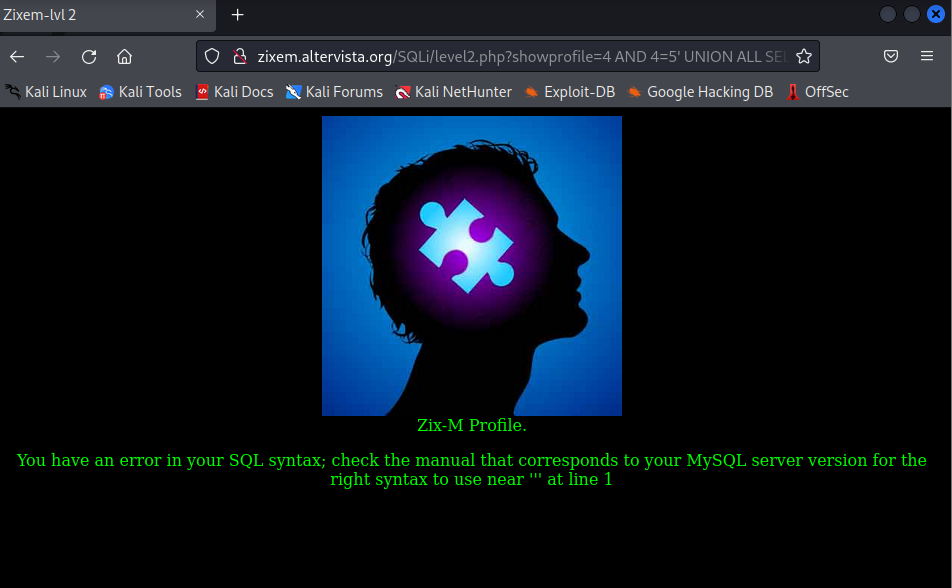
* Ta đã thấy được thông tin version và user
* Level 2



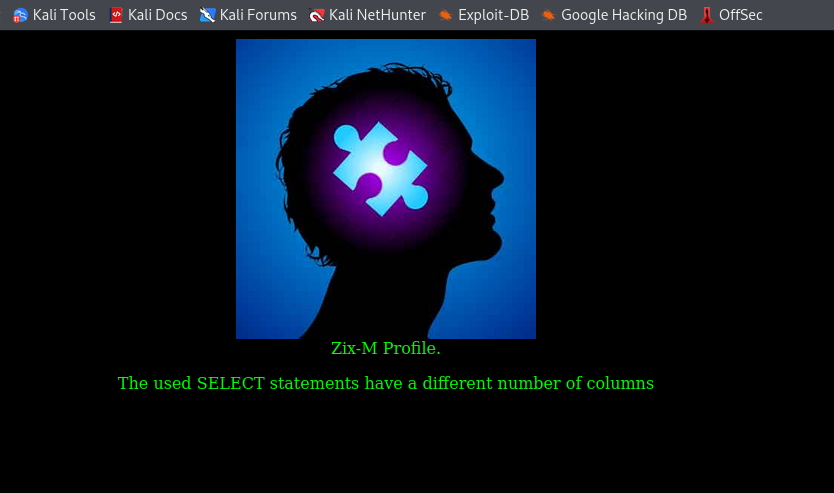
* Ta thực hiện kiểm tra và thấy trang web có bị lỗi SQL injection
* Nhưng khi thực hiện câu lệnh ORDER BY để kiểm tra số cột thì nó không trả về gì dù đã thay đổi số lượng



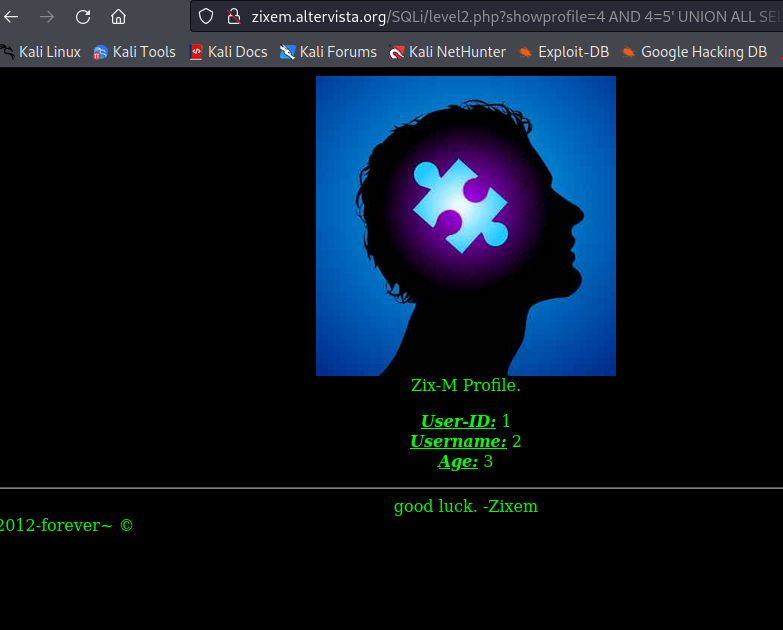
* Thực hiện câu truy vấn nhưng không có gì xảy ra
* Có thể do trang web này đang lấy ID dưới dạng 1 chuỗi, thay vì số nguyên



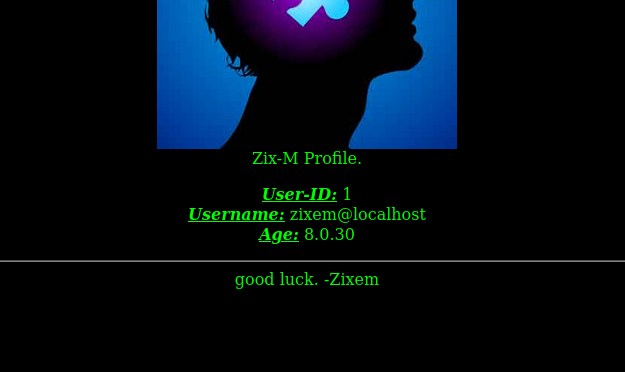
* Và để khai thác được lỗi này thì ta thêm vào ký tự ‘ để kết thúc chuỗi truy vấn ban đầu
* Và lỗi trên nói rằng chúng ta quên đóng dấu ‘ và
* Câu truy vấn AND 4=5' UNION ALL SELECT 1,2,3 --'



* Kết quả khi thực hiện câu truy vấn trên
* Lỗi này cho thấy là câu lệnh SELECT có só cột khác vậy thì ta sẽ thử tăng hoặc giảm số cột



* Sau khi tăng số cột lên 4 thì ta thấy được trang web đã trả về kết quả
* Giờ ta chỉ cần thay các cột bằng user và version là được



* **Câu lệnh : showprofile=4 AND 4=5' UNION ALL SELECT 1 ,USER(),VERSION(),4--'**
* Level 3

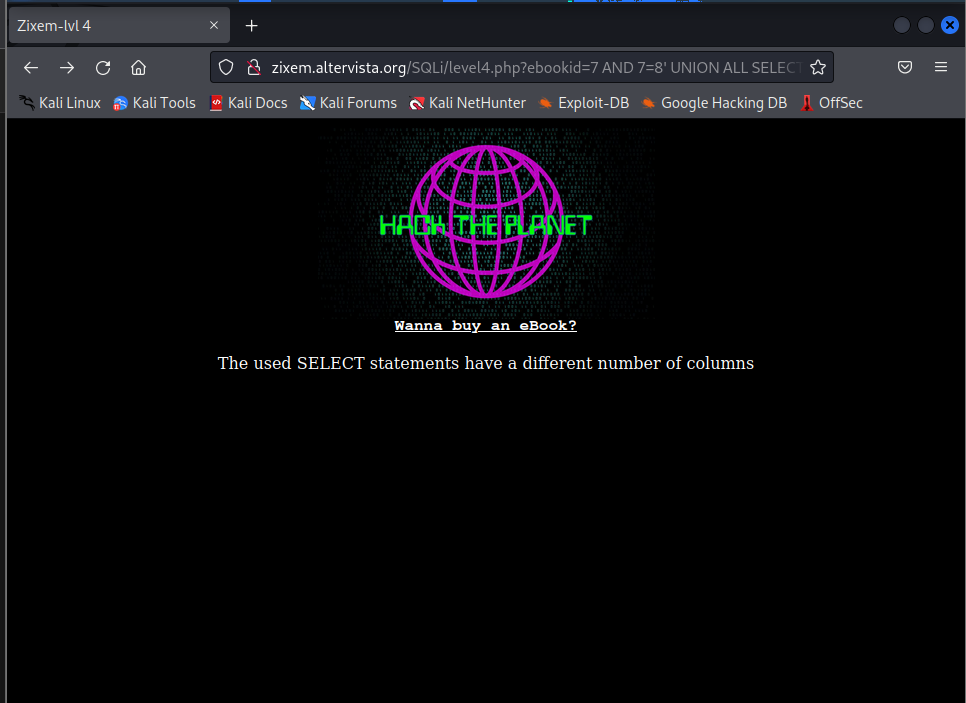
****

* Ta thử dùng lại câu lệnh ở level trước và nó trả về lỗi như trên
* Ta thấy là trong câu lệnh ta nhập là UNION nhưng nó lại thông báo là lỗi UNI. Vậy có nghĩa là trong câu lệnh này từ ON có vẻ như được lọc để tránh khai thác lỗi SQL Injection bằng câu lệnh UNION
* Để có thể bypass thì ta có thể sử dụng ON 2 lần nếu nó được lọc 1 lần thì vẫn có thể được truy vấn

Ảnh có chứa biểu đồ

Mô tả được tạo tự động

* **Câu lệnh: AND 3=4' UNIONON ALL SELECT 1 ,USER(),VERSION(),4--'**
* Level 4

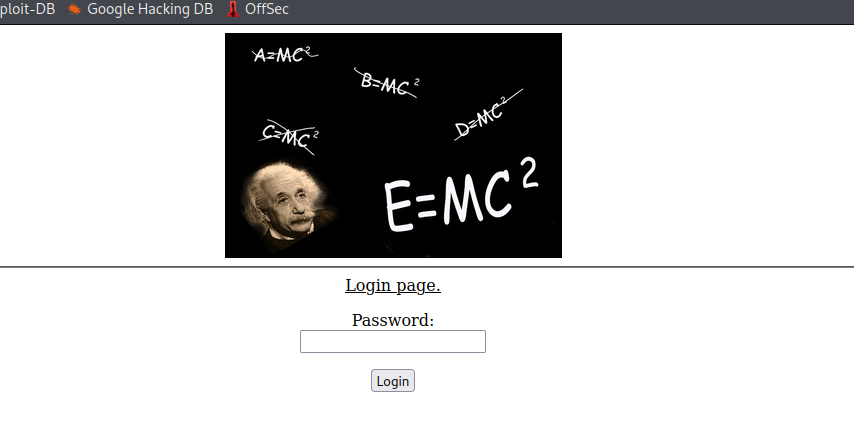


* Ta sử dụng câu lệnh như ở Level 3 để khai thác và thấy trang web trả về có số cột khác nhau
* Ta thử tăng hoặc giảm số cột để xem kết quả

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, bình phong

Mô tả được tạo tự động

* Khi tăng lên 5 thì ta có được kết quả của version(), và user()
* **Câu lệnh SQL: AND 7=8' UNION ALL SELECT 1 ,USER(),VERSION(),4,5--'**
* Level 5

****

* Ta được 1 trang web yêu cầu mật khẩu để đăng nhập

Ảnh có chứa văn bản, bức thư

Mô tả được tạo tự động

* Khi xem source trang ta được hướng dẫn như trên
* Ta làm theo hướng dẫn

Ảnh có chứa văn bản

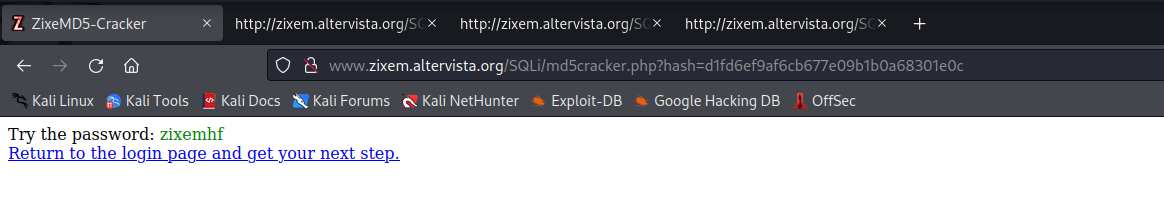
Mô tả được tạo tự động

* Sau khi nhập mật khẩu thì ta được đường dẫn như trên
* Sau đó ta truy cập vào đường dẫn /SQLi/md5cracker.php

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta được 1 trang web như trên để giúp ta giải mã hash



* Ta có được password

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Nhưng khi nhập vào thì có được thêm 1 hint để có thể brute force

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta viết code để có thể gửi reqest đến trang web sau đó sẽ đưa chuỗi pass word vào để brute force

Ảnh có chứa bàn

Mô tả được tạo tự động

* Kết quả Pass là “1337”

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Level 6:

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Nhiệm vụ của ta là tìm detail của teacher có id hoặc serial number là 11

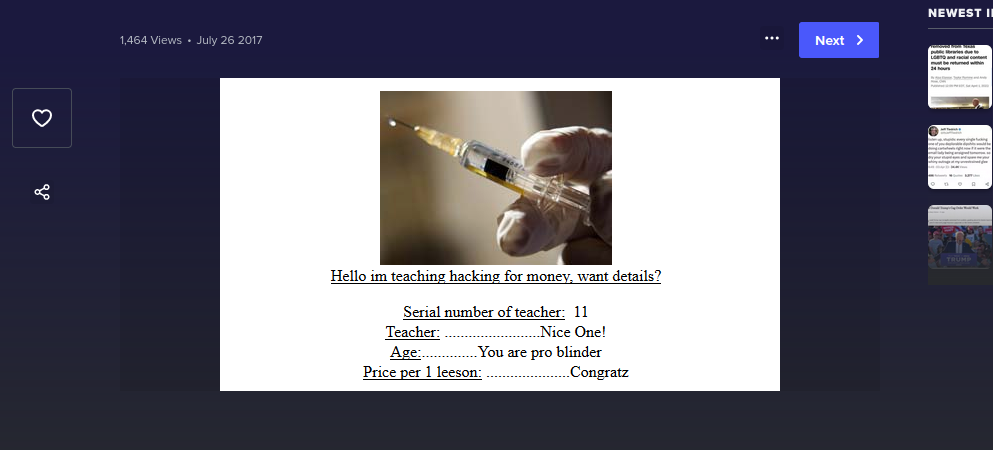
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Sử dụng câu truy vấn như ở các challenge trên AND 10=11 UNION ALL SELECT 1 ,2,3,4—ta được kết quả như trên

Ảnh có chứa văn bản

Mô tả được tạo tự động



* Đề cho ta 2 bức ảnh để có thể đoán được các cột ở trong bảng
* Ta sẽ có các cột như là ID/Serial No, teacher, teacherage/age/tacher\_age,price
* Thử các giá trị cột trên vào câu truy vấn

Ảnh có chứa văn bản

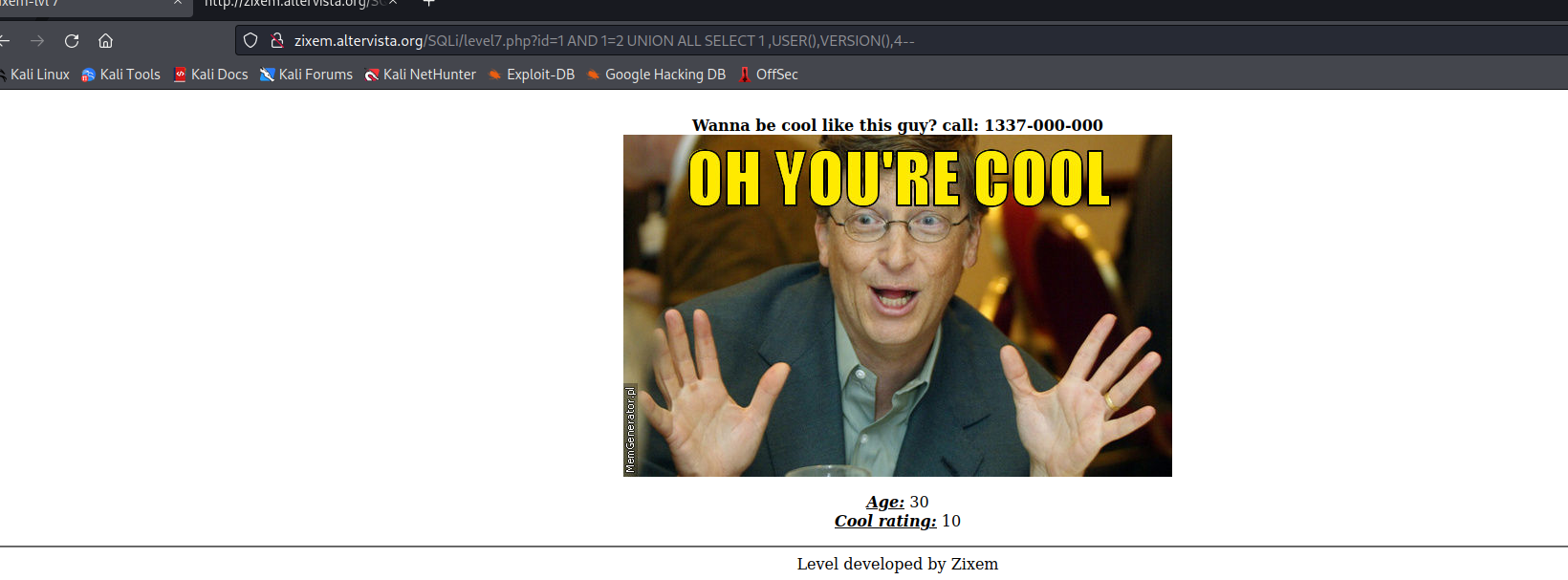
Mô tả được tạo tự động

* Có vẻ như câu truy vấn đã đúng và nó trả về các kết quả của ta
* **Câu truy vấn: AND 10=11 UNION ALL SELECT id,teacher,teacher\_age,price FROM teachers**
* Nhưng kết quả lại không giống với ảnh mà người ta cung cấp
* Ở đây người ta yêu cầu mình tìm thông tin của người có ID=11 vậy thì ta thêm điều kiện là ID=11 vào câu truy vấn

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta đã lấy được thông tin
* **Câu truy vấn: AND 10=11 UNION ALL SELECT id,teacher,teacher\_age,price FROM teachers WHERE ID=11**
* Level 7

****

* Ta thử truy vấn như ở những level đầu thì không có gì xảy ra
* Ta xem thử source trang xem sao

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Đây là source trang trước khi thực hiện attack

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Đây là source trang sau khi thực hiện
* Thì ta thấy value đã thay đổi thành error vậy nghĩa là các câu truy vấn của ta sẽ thay đổi ở đây

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Khi ta sử dụng câu lệnh ORDER BY 4 thì giá trị value là error
* Có 3 cột

Ảnh có chứa văn bản

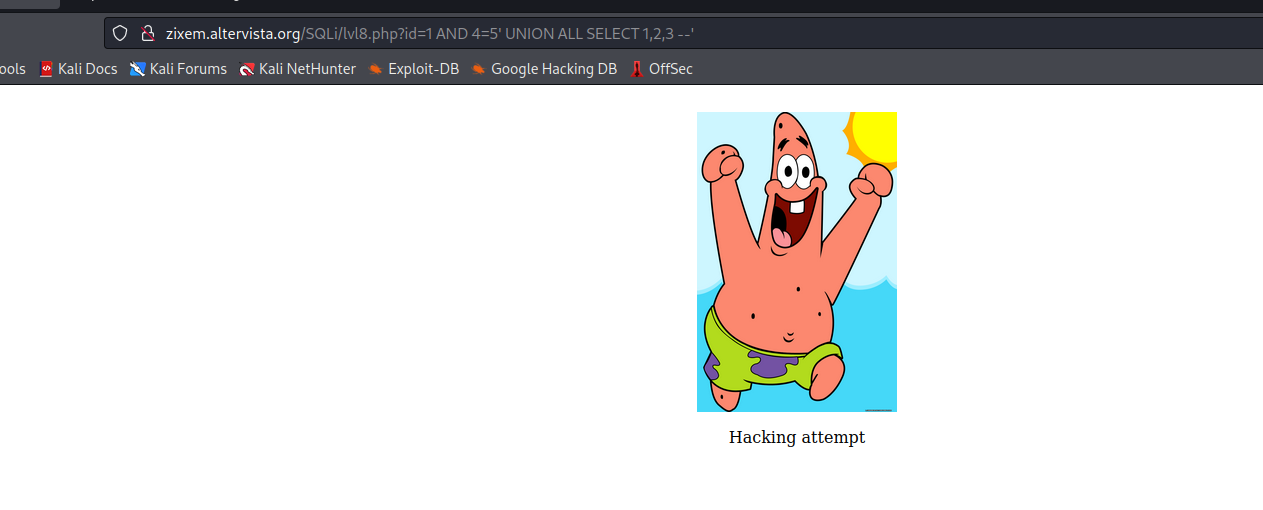
Mô tả được tạo tự động

* Ta thực hiện các câu lệnh như ở level trước thì lấy được thông tin User ở trong toán tử thứ 2 trong câu lệnh SELECT của ta
* Vậy value sẽ là cột thứ 2 trong bảng

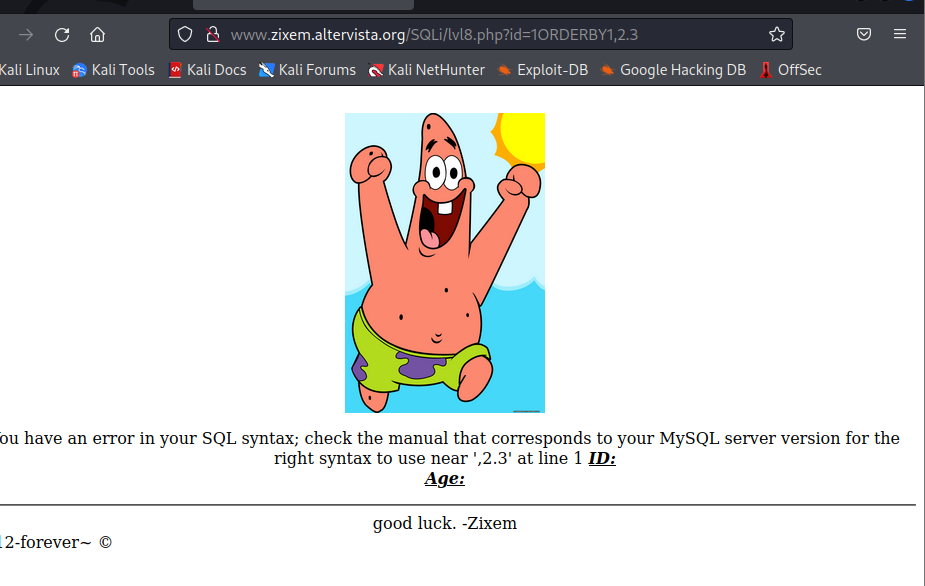
Ảnh có chứa văn bản

Mô tả được tạo tự động

* Đây là thông tin version
* Level 8



* Khi ta thử dùng những câu truy vấn như ở những level trên thì nó hiện cho ta dòng chữ “Hacking attempt”
* Từ đây ta có thể đoán là trang web đang được lọc hoặc filter gì đó để có thể tránh SQL Injection
* Sau khi tìm hiểu thì biết trang web này có cài đặt WAF để filter các chuỗi câu lệnh SQL



* Sau khi thử các câu lệnh ORDER BY để tìm số lượng cột nhưng không được
* Ta nghĩ đến việc có thể trang web đã chặn khoảng trắng để ngăn ta SQL Injection nên trong câu lệnh ta bỏ khoảng trắng thì được kết quả như trên

Ảnh có chứa văn bản

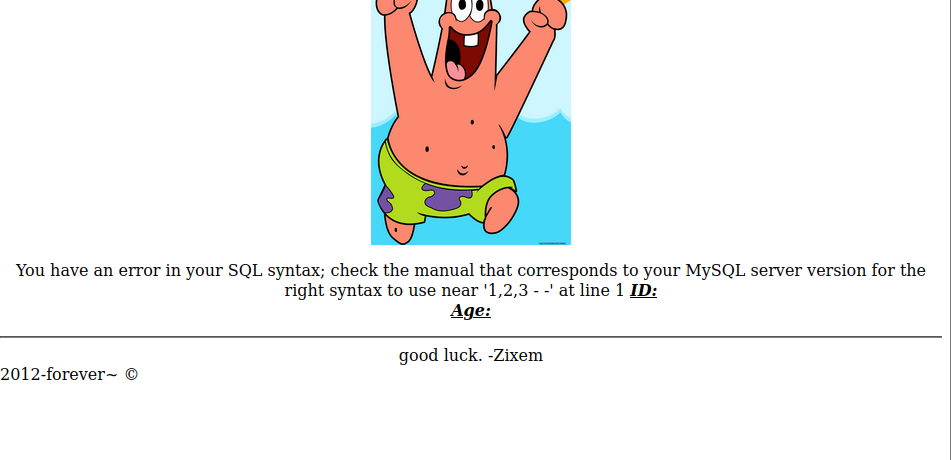
Mô tả được tạo tự động

* Sau khi tìm hiểu cách để có thể bypass khoảng trắng trên google thì được kết quả như trên
* Ta có thể thay khoảng trắng bằng “%0b” để có thể khai thác

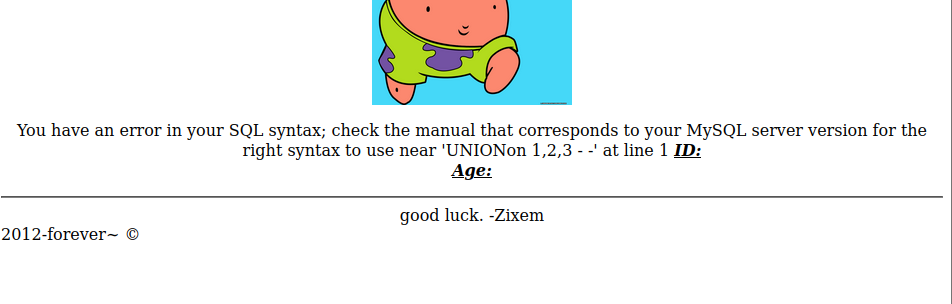
Ảnh có chứa Website

Mô tả được tạo tự động

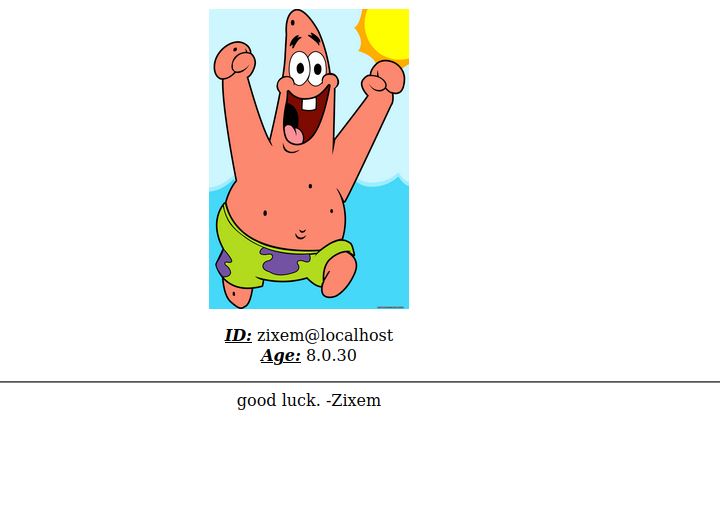
* Sau khi thay khoảng trắng trong câu lệnh ORDER BY để tìm số cột thì ta biết được có 3 cột
* Ta thực hiện tiếp câu lệnh
* **%0BUNION%0BSELECT%0B1,2,3%0B-%0B-**



* Nó trả về kết quả như trên. Nghĩa là server không hiểu 1,2,3 là gì
* Nghĩa là lỗi xảy ra ở select hoặc union
* Ta thử câu lệnh SELselectECT hoặc là UNIONon



* Thử UNIONon không được vậy là UNION bị lọc còn SELECT không bị lọc



* **Câu lệnh SQL: %0DAND%0D1=2%0DUNION%0DSELselectECT%0DVERSION(),USER(),3- -**
* Level 9

**Ảnh có chứa biểu đồ, văn bản

Mô tả được tạo tự động**

* Yêu cầu thử thách này là ta tìm thử pass ở trong đường dẫn /etc/passwd
* Ta truy cập thử đường dẫn

Ảnh có chứa biểu đồ

Mô tả được tạo tự động

* Nó hiện ra lỗi như trên

Ảnh có chứa biểu đồ

Mô tả được tạo tự động

* Sau khi thử dùng câu truy vấn của Level 2 là nó so sánh chuỗi thì ta được kết quả trên
* Vậy suy ra là bảng có 2 cột

Ảnh có chứa biểu đồ

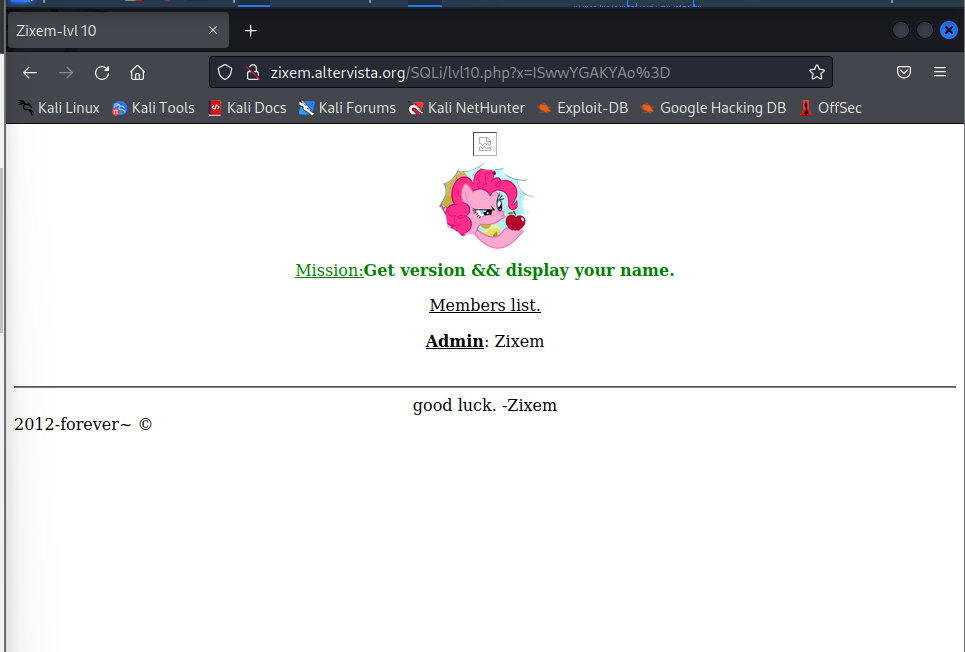
Mô tả được tạo tự động

* Ta truy xuất thử 2 cột thì nó xảy ra lỗi như trên
* Lỗi cho ta biết đại chỉ đường dẫn là /membri/zixem/SQLi/lv9.php
* Thay ở 1 bằng đường dẫn /etc/passwd

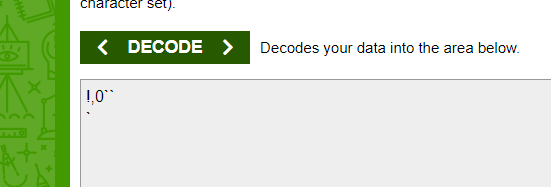
Ảnh có chứa văn bản

Mô tả được tạo tự động

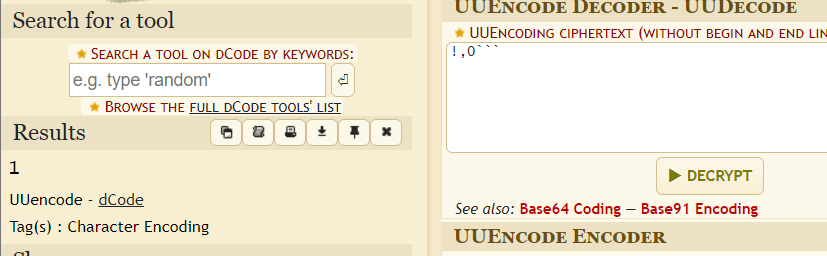
* **Câu lệnh SQL: AND 1=2' UNION ALL SELECT '../etc/passwd',2' –**
* Level 10

****

* Truy cập vào challenge thì ta thấy có đường dẫn khác so với những level khác
* Nó là base64 encode vậy ta dùng tool để giải mã xem sao



* Nó ra 1 chuỗi ký tự khá lạ
* Sau khi tìm hiểu thì đây là 1 loại cipher gọi là Uuencode



* Sau khi giải mã thì nó lại giống như ở những level trước
* Để làm được loại này ta chỉ cần thực hiện mã hóa câu SQL của ta bằng Uuencode sau đó bằng base64 rồi đưa vào lại URL là được

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Dùng ORDER BY để biết số cột thì ta biết có 2 cột

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Ta dùng lệnh CONCAT() để nối chuỗi tên của ta và version() lại vì bảng chỉ có 2 cột
* **Câu truy vấn SQL: 1 AND 1=2 UNION ALL SELECT 1,CONCAT("Thiet Vu",version()) --**