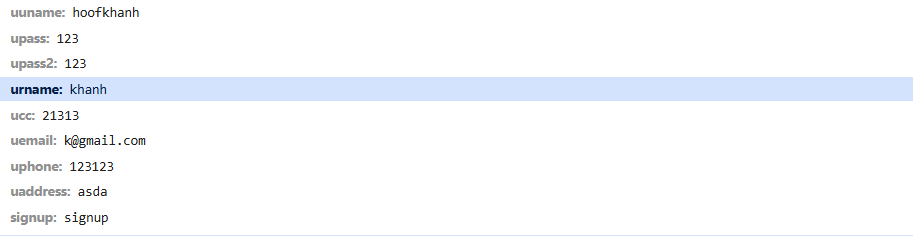
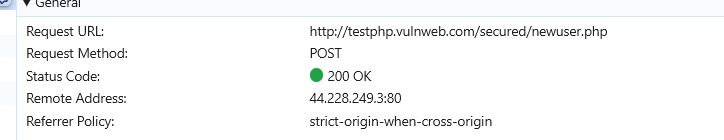


1.

**Các tham số đầu vào**: uname, upass, upass2, email, name, phone, address, signup

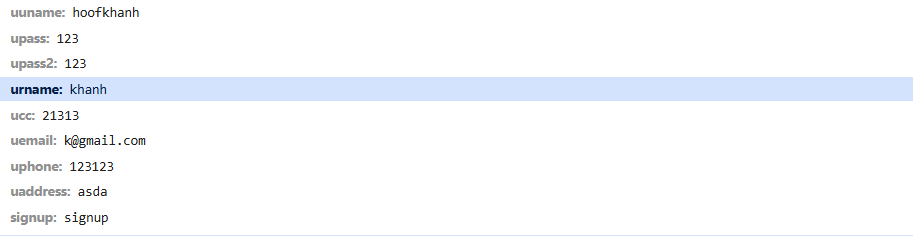


**Gửi bằng** post method



**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 users (...) VALUES (...)

**Xác định mức độ ảnh hưởng: trung bình đến nghiêm trọng**

 Mục tiêu: Kiểm tra khả năng chèn mã độc SQL vào các trường nhập

 Ví dụ payload:

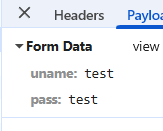
* uname = admin', '123', 'admin@example.com', 'Admin', '1234567890', 'Address'); --
* uname = test' OR 1=1 --

 Mức độ ảnh hưởng:

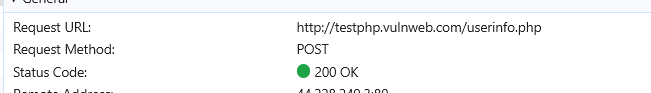
* Có thể **thêm user trái phép**
* Có thể gây **sai lệch dữ liệu**
* → **Mức độ: Trung bình đến nghiêm trọng**

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

 Mục tiêu: **Bypass đăng nhập**

 Payload kiểm thử:

* uname = ' OR '1'='1
* upass = ' OR '1'='1
* ' UNION SELECT null, version(), null --

 Kết quả:

* Bỏ qua kiểm tra mật khẩu
* Lấy thông tin hệ thống
* Truy cập trái phép với quyền admin
* → **Mức độ: Rất nghiêm trọng**

3.

**Tham số và cách gửi**:

* Tham số: id (truyền qua URL, GET method)
* Ví dụ URL: index.php?id=1

2. **Vị trí trong truy vấn:**

* Truy vấn kiểu: SELECT \* FROM products WHERE id = '...'
* id được đưa trực tiếp vào WHERE

3. **Kiểm thử SQLi & mức độ ảnh hưởng:**

* Payload:
  + id=1 OR 1=1
  + id=1 UNION SELECT null, version(), null --
  + id=-1 OR 1=1 --
* Mục tiêu:
  + Xem toàn bộ sản phẩm
  + Lấy thông tin hệ thống
  + Khai thác dữ liệu ẩn
  + → **Mức độ:** Cao