**Bài 1: Low-level logic flaw**

Bài này không xác thực đầu vào của người dùng đầy đủ. Bạn có thể khai thác lỗi logic để mua hàng với giá không mong muốn. Để giải được bài này, bạn phải mua được “Lightweight I33t leather jacket”

Đầu tiên mình đăng nhập tài khoản wiener:peter thì trong tài khoản có 100$. Nhưng áo khoác mình muốn mua có giá 1337$.

Lần này, mình không thể chỉnh số lượng là âm nên cách khai thác sẽ không giống như bài trước. Nó cho số lượng sản phẩm giới hạn từ 0 đến 99.

Cách khai thác bài này là mình sẽ làm cho tổng tiền vượt qua giá trị tối đa của số nguyên là 2.147.483.647 hay còn gọi là integer overflow. Do đó, giá trị sẽ trở về giá trị tối thiểu là -2.147.483.647

Ta sẽ mua áo leather jacket với số lượng là 99 . Gửi yêu cầu đến burp intruder, chọn payload là null 🡪 continue indefinitely 🡪 brute force đến 1 giá trị chúng ta mong muốn (trong phạm vi thanh toán) 🡪 Đặt hàng

**Bài 2: Inconsistent handling of exceptional input**

Bài này không xác thực đầu vào của người dùng đầy đủ. Bạn có thể khai thác lỗi logic trong quá trình đăng kí người dùng để giành quyền truy cập chức năng quản trị viên. Để giải được bài này, truy cập admin panel và xóa người dùng carlos.

Bài cung cấp cho chúng ta 1 máy chủ email riêng. Nó dùng để nhận và gửi tin nhắn. Còn email client giúp hiển thị tất cả tin nhắn được gửi đến máy chủ. Tên email có định dạng sau: @exploit-0a27005a04f550f3826c3e4301910089.exploit-server.net và các tên miền con của nó.

Vào mục đăng kí, username là admin, password là admin, email nếu bạn để là admin@exploit-0a27005a04f550f3826c3e4301910089.exploit-server.net hay admin@subdomain.exploit-0a27005a04f550f3826c3e4301910089.exploit-server.net cũng đều nhận được email xác nhận đăng kí.

Bài toán nó gợi ý: Nếu bạn làm việc cho DontWannaCry, phải dùng địa chỉ email @dontwannacry.

Mình thử để email là admin@dontwannacry.exploit-0a27005a04f550f3826c3e4301910089.exploit-server.net cũng nhận được email xác nhận đăng kí. Mình để đúng địa chỉ email rồi, mình nghĩ mình sẽ nhận được 1 tin nhắn nữa là gợi ý để giải bài toán. Nhưng đợi mãi nó không có.

Mình tự hỏi, chức năng đăng kí làm sao lấy được tài khoản của admin??

Mình truy cập thử url /admin, nó báo:

Admin interface only available if logged in as a DontWannaCry user

Rõ ràng mình đã là DontWannaCry user nhưng vẫn không truy cập được giao diện admin, chứng tỏ email phải là @dontwannacry thôi.

Cách làm là truncation. Nếu bạn để 1 email rất dài lớn hơn 255 kí tự, nếu ứng dụng không lọc dữ liệu cẩn thận thì email chỉ còn 255 kí tự.

Đến đăng kí lại 1 tài khoản, phải điều chỉnh sao cho email rút ngắn chỉ còn admin....@dontwannacry.com (255 kí tự) nhưng vẫn nhận được thông báo xác nhận đăng kí nha.

Vậy là bạn có thể truy cập được giao diện của admin và xóa người dùng carlos.

Tại sao bài toán lại có tên: xử lí đầu vào bất thường không đồng nhất?

Phần đăng kí nó chấp nhận email lớn hơn 255 kí tự nhưng khi đăng kí thành công, đăng nhập nó chỉ hiển thị 1 email có 255 kí tự. Miễn là đuôi @dontwannacry.com là bạn có thể truy cập được admin. Nên nó mới sinh ra lỗi như vậy.