**ctf.wargame.vn 2013 Web200 writeup – Kyuubi Kurama**

“Mario đang trên đường đi cứu công chúa thì xe anh đã hết xăng :(. Nhưng trong túi anh chỉ có 50.000 VNĐ làm sao mua đủ xăng để tiếp tục hành trình đây, hãy giúp Mario với :(.”

Link: <http://challenges.wargame.vn:1337/web200_3b3b44938292fda6efa33655c0954123/>

Nào, hào hứng cùng Mario vào cây xăng để mua xăng đi cứu công chúa thì ôi thôi 50000 VND chỉ mua được khoảng 2 lít xăng @\_@.

View Page Source xuống phía cuối đoạn HTML thì thấy hint này:

“<!-- if($fuel >= 13.37) { show\_flag(); reset(); }-->”

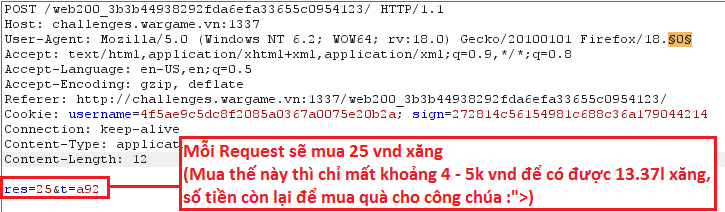
Vậy là với ít nhất 13.37 lít xăng là Mario của chúng ta có thể đi cứu công chúa rồi :”>

Cũng có nghĩa là phải có khoảng 334250 vnd mới đủ điều kiện đi tiếp :( (Chưa kể gặp phải mấy cây xăng móc túi khách hàng thì còn tốn nữa nhé)

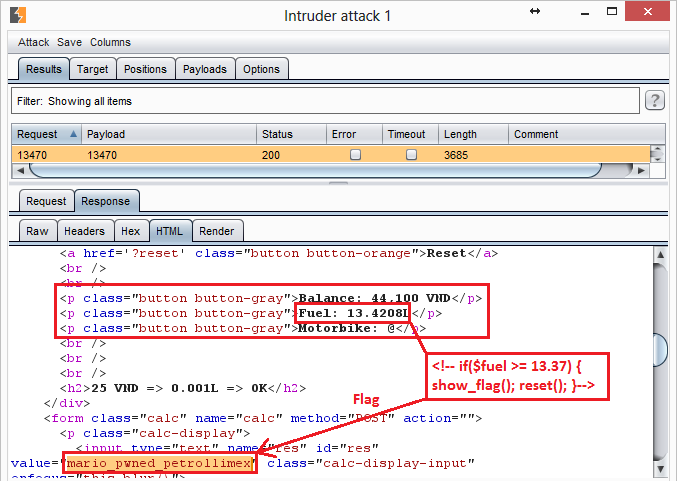
Đến đây thì nghĩ ngay đến Race\_condition, lần trước có 1 lần được nhìn anh Gamma95 biểu diễn demo khai thác lỗi này :D

Link tham khảo: http://antoanthongtin.vn/Portals/0/UploadImages/kiennt2/KyYeu/DuLieuTrongNuoc/Dulieu/KyYeu/07.race-condition-attacks-in-the-web.pdf

Mở Burpsuite ra, vào Burpintruder gửi khoảng 50000 request với nội dung mua 25 vnd xăng (sẽ mua được 0.001 lít). Mình sử dụng 100 Threads trong 1 thời điểm ^^



Sau 13470 request thì mua được 13.4208L ( >13.37 rồi).



Tada… Flag hiện ra rồi nè: **mario\_pwned\_petrollimex**

Vẫn còn dư 44,100 VND nhé, số tiền còn lại này Mario sẽ mua quà cho công chúa :”>