TOPIC Path Traversal

Challenge: 1 Guess a number between 1, and 1,000,000.. hmm, let's not, whilst keeping it civil and refrain from brute force.

"Little archaeologist, with no gifts you appear, Walking boldly where mortals should fear. To gain your freedom, you must find what exists in the etc folder, But remember, you are always 2 steps back, not any closer. The first test is simple, a number I hold, Guess it correctly, and secrets unfold. Between one and a million my number is found, Yet hidden like passwd in places profound. Step not once, but take two strides back, Lest you be trapped and lose the track. The sacrificial lamb may lead you astray, Unless you see through the dotted display."

Target: etc/passwd is what I got from the rhyme, and that I'm two 'stories' deep.. ../../etc/passwd

It finally came to me after testing different ways of traversing that I could use this ....//....//etc/passwd, in hindsight I guess it would have something to do with the dotted display, however I'm not sure what the lamb was about.

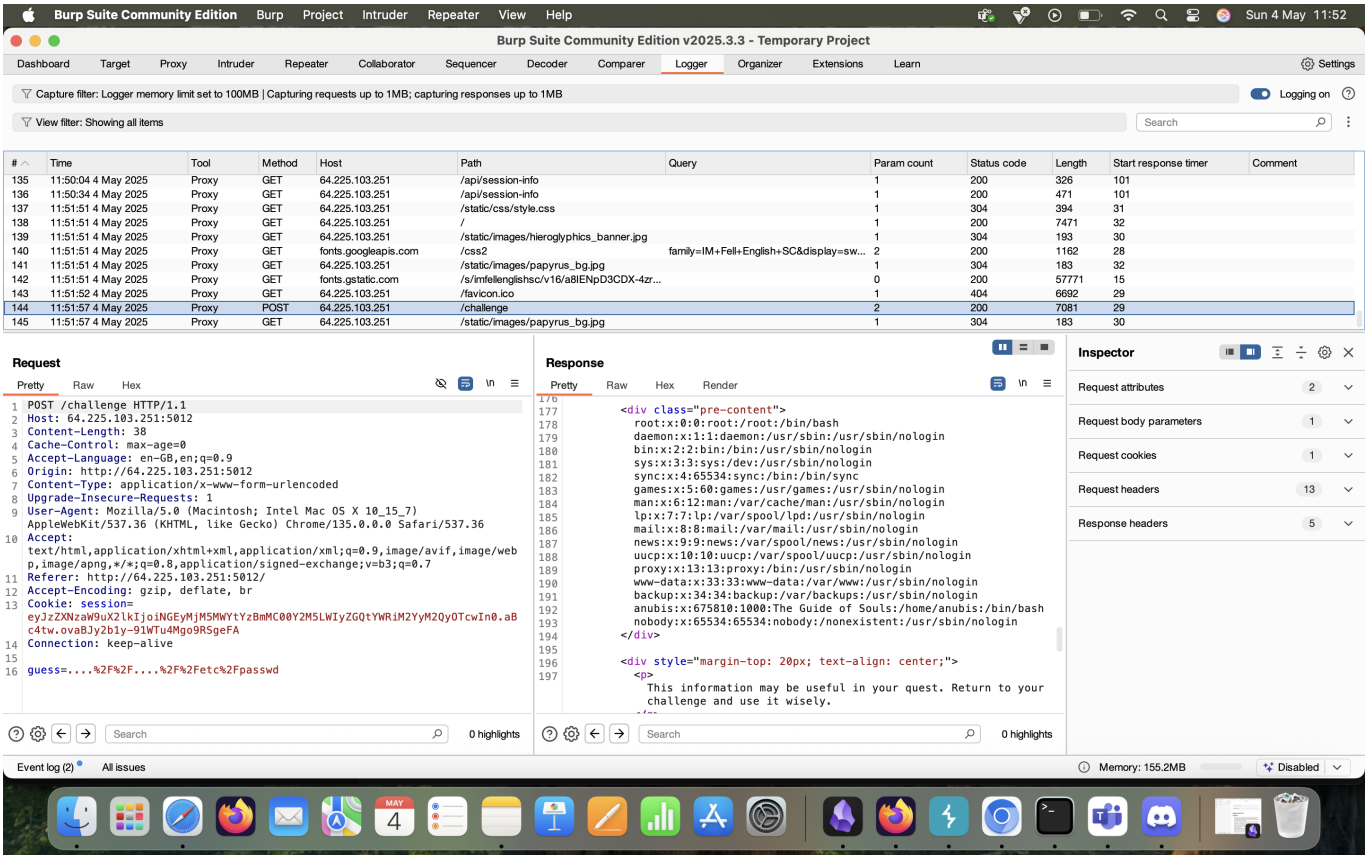


Image shows that anubis got an interesting UID, was the lamb..'nobody'?

Challenge: 2

"The first game was easy, that's of course true, But this one brings darkness, perhaps two. A game of chance where shadows grow deep, Where every resource needs a location unique. Look into the shadow realm, shrouded and veiled, The secrets within are carefully concealed. Three dice I shall throw with faces eighteen, Predict their sum total, and you'll be keen."

I have no idea how this rhyme translated to use %2f instead of slash and that's all you need for the payload to work, I tried TONS of variations but..this one did it;

..%2f..%2fetc%2fshadow

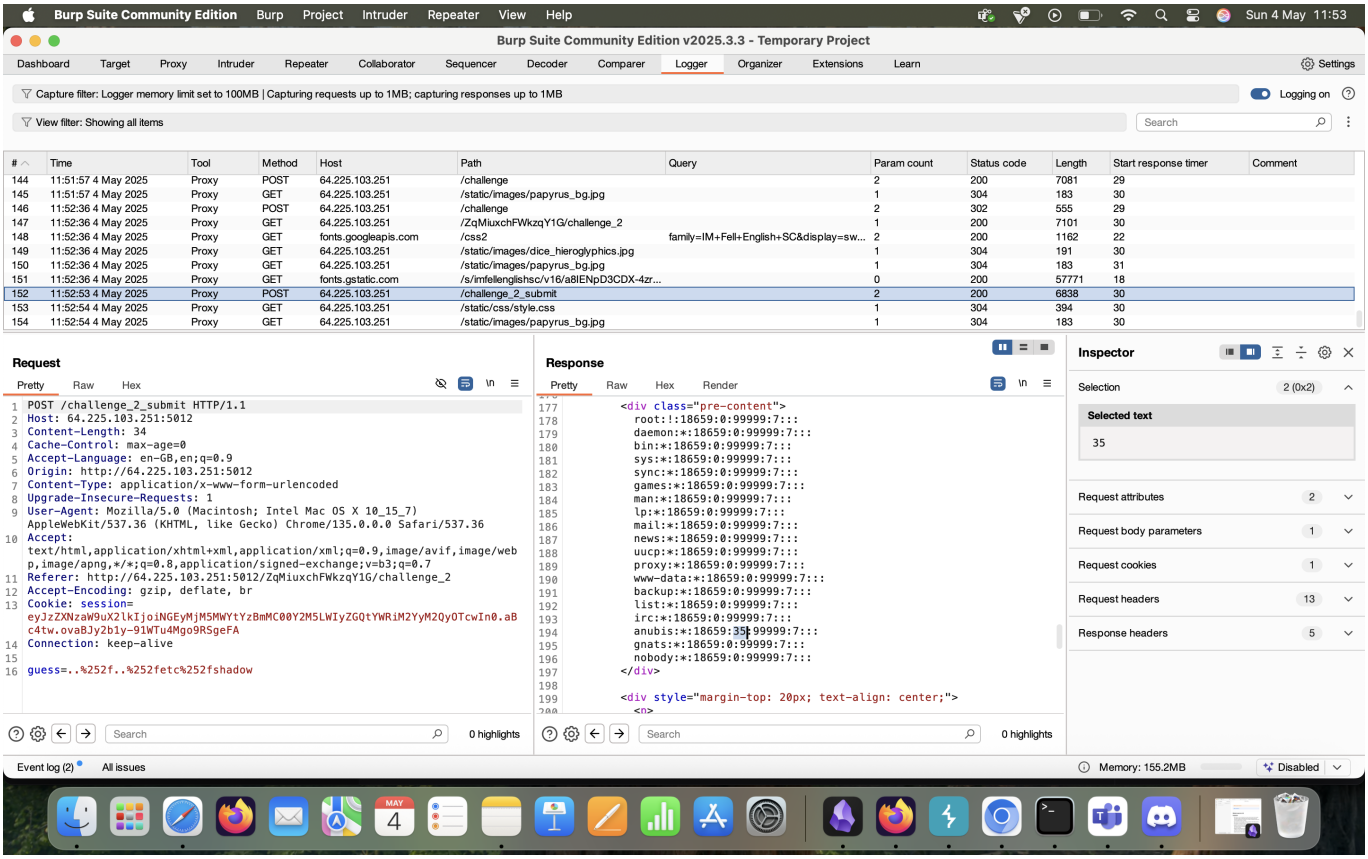
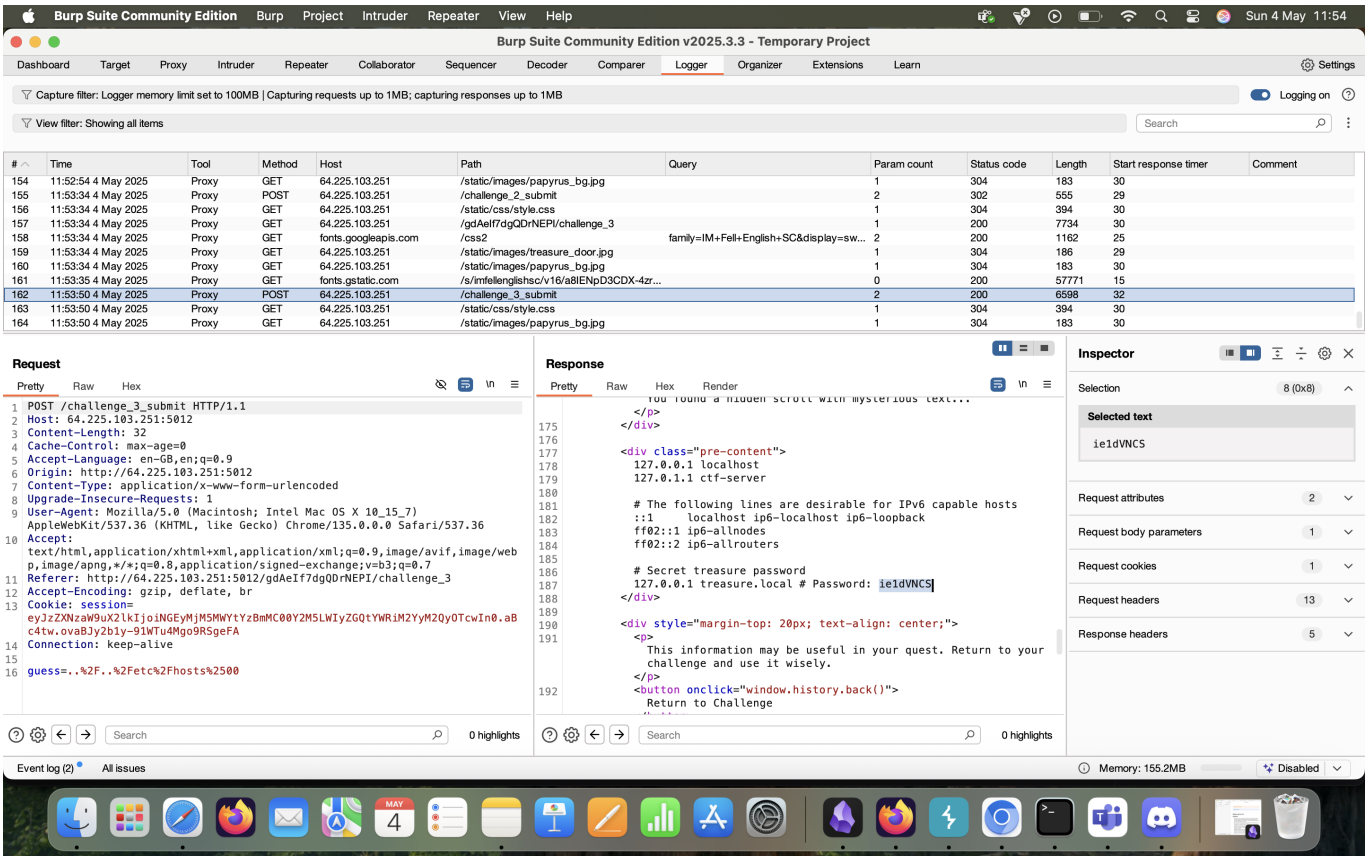


Image shows that yet again anubis is a suspect, since 35 surely fits the box 3-54 (min and max value of the described dice toss)

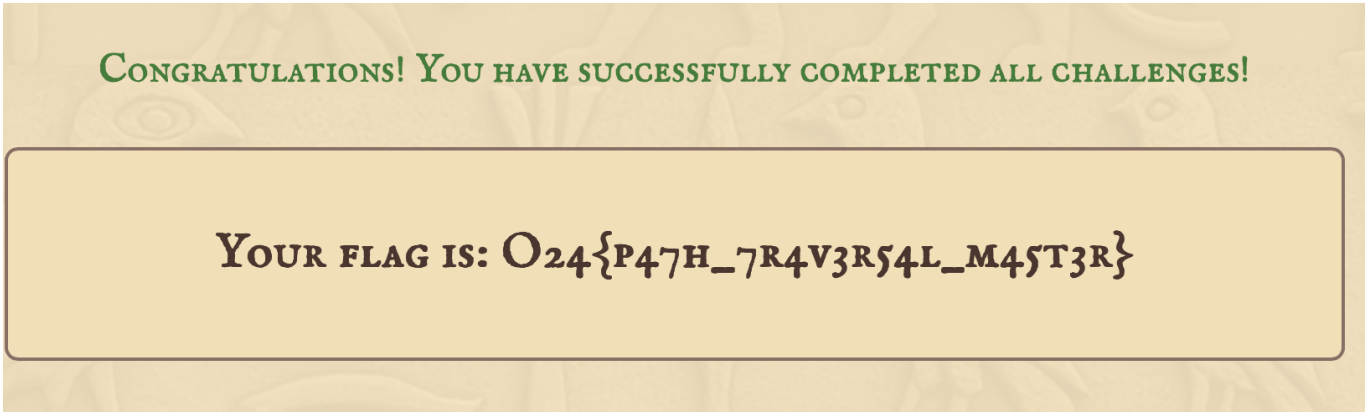
"Explore the path to my dwelling place divine, Travel back where connections and names align. Carefully through passages, take two steps behind, Hidden origins of digital homes you'll find. Observe how scripts twist what you compose, Subtle deceptions veil paths in strange clothes. The zero offering, subtle and keen, Solutions will surface, where clues are seen."

So that looks to be pointing towards etc/hosts to me, and 'zero offering' zero, nothing, nil, null, %00?

../../etc/hosts%00



And there's the password, and the flag is in reach..



Another flag in the bag!

NOTE: I did it through the browser hence why the payload in burp logger looks different, because it's double URL encoded.