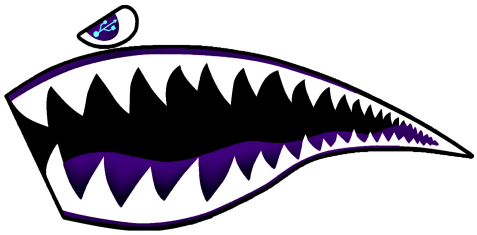
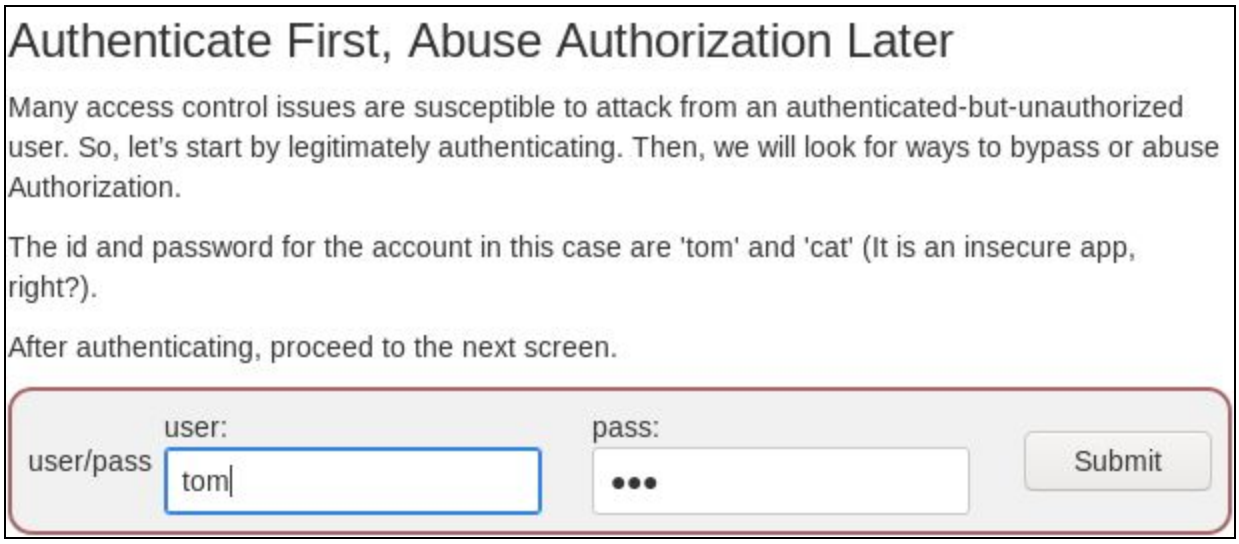


WebGoat Insecure Direct Object Reference

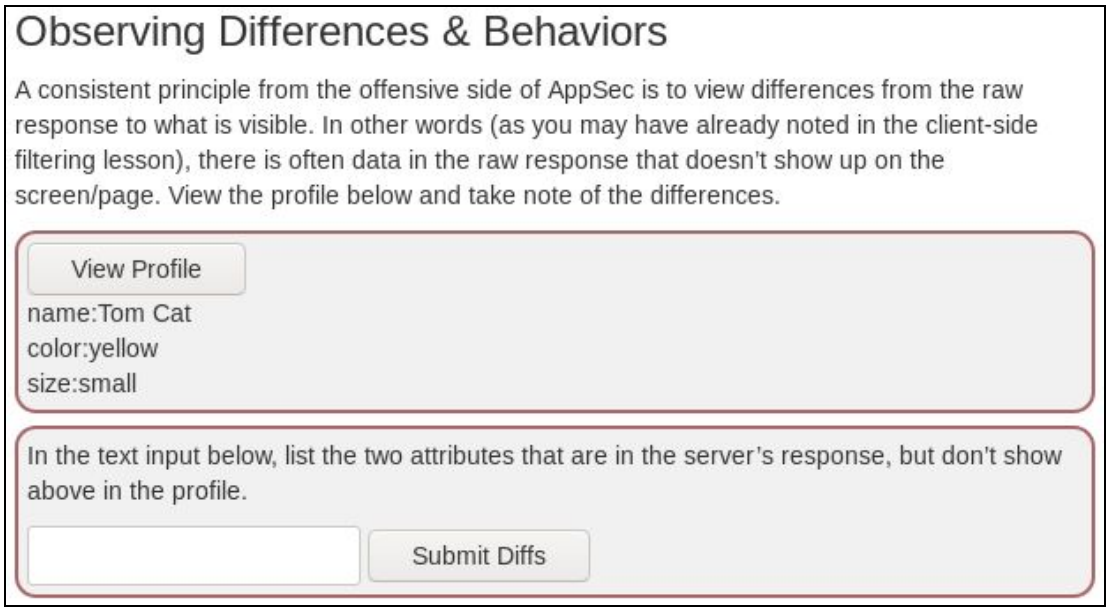
Twitter: @BlackSheepSpicy
Twitch: https://twitch.tv/BlackSheepSpicy

2. Not much to say here:

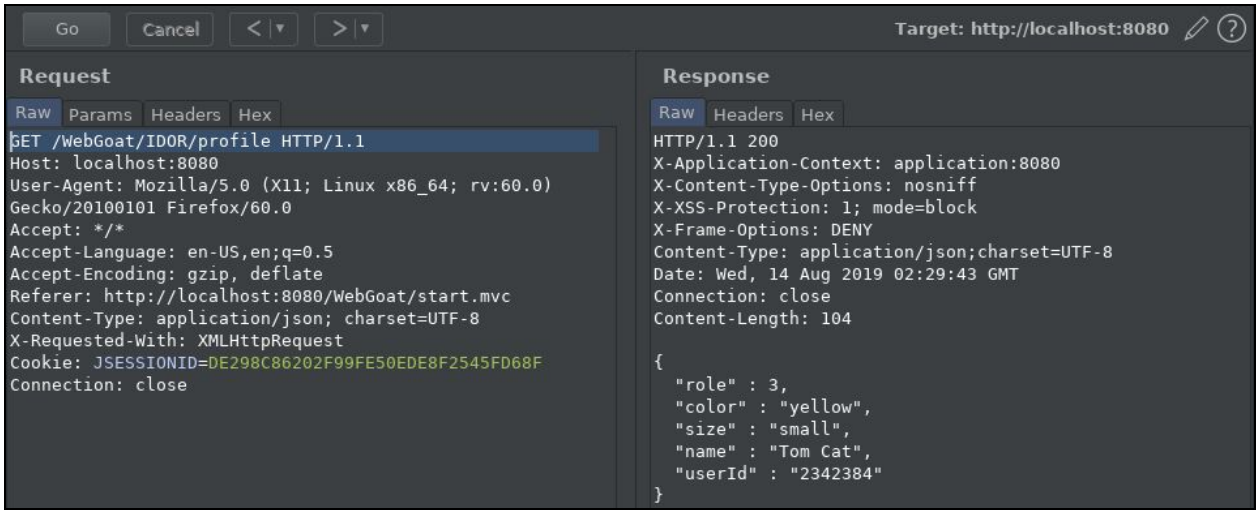


Don't ask me why I put this is, it's a formality thing

3. This next challenge is a bit more involved, but its relatively standard fare:



As stated in WebGoat, the information we need is located in the response from the server, so lets intercept the request from the “View Profile” button in burp and send it to repeater:

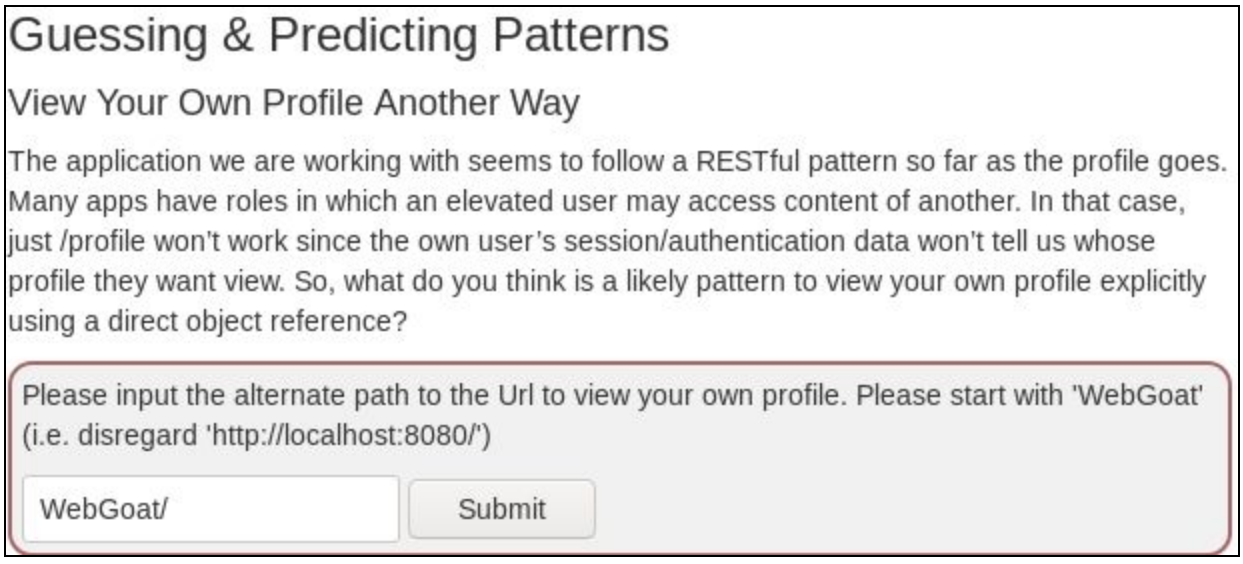


And then send it… got a bit excited sorry

Now from here we can see the two attributes that are not listed: **UserId** and **Role**

Keep in mind when submitting the attribute names to separate them with a comma. WebGoat likes to tell you that after you try submitting them, which is fun.

4. Next challenge:



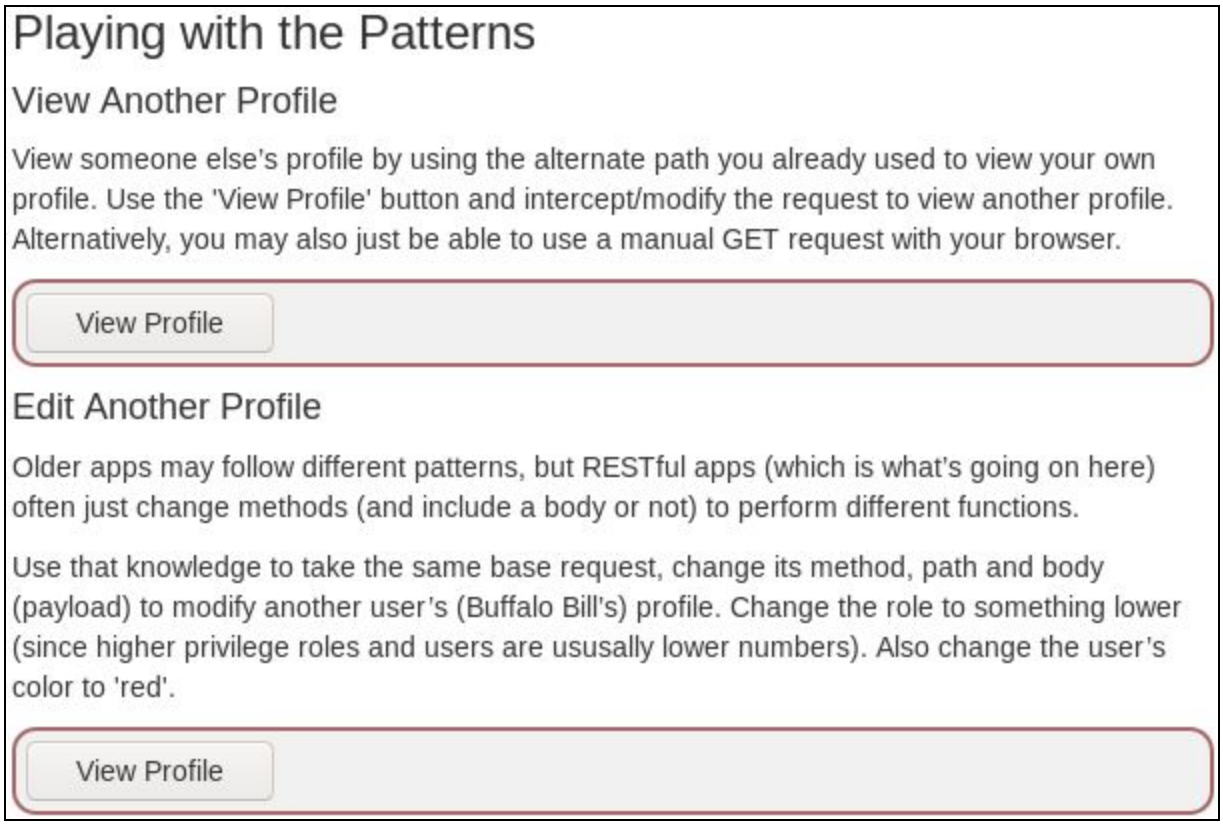
Completing this challenge requires two bits of information you actually saw in the previous challenge:

```
"userId" : "2342384"
```

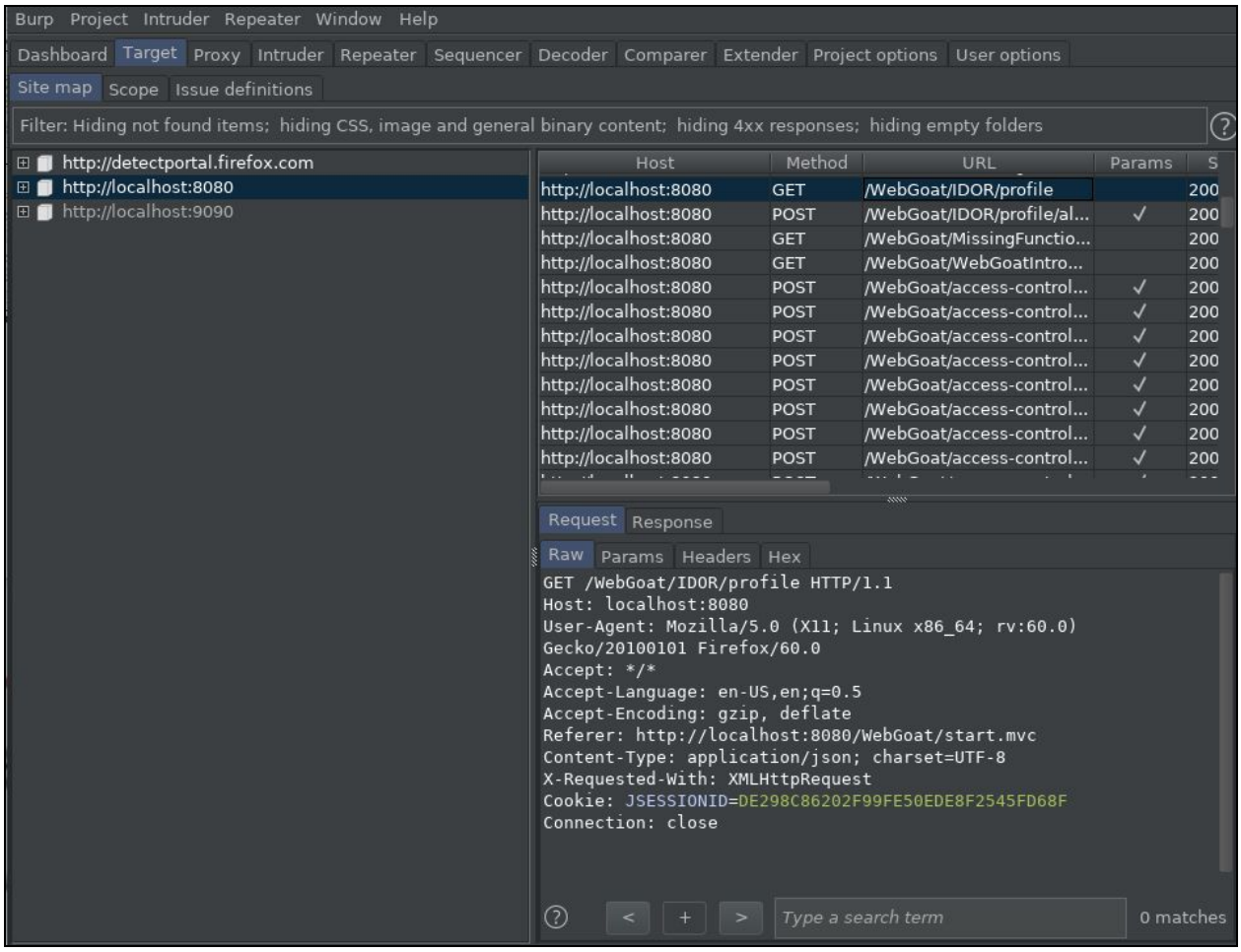
```
/WebGoat/IDOR/profile
```

Slap them bad boys together and we got that alternative path to the profile:

5. Last challenge, let's get into it:

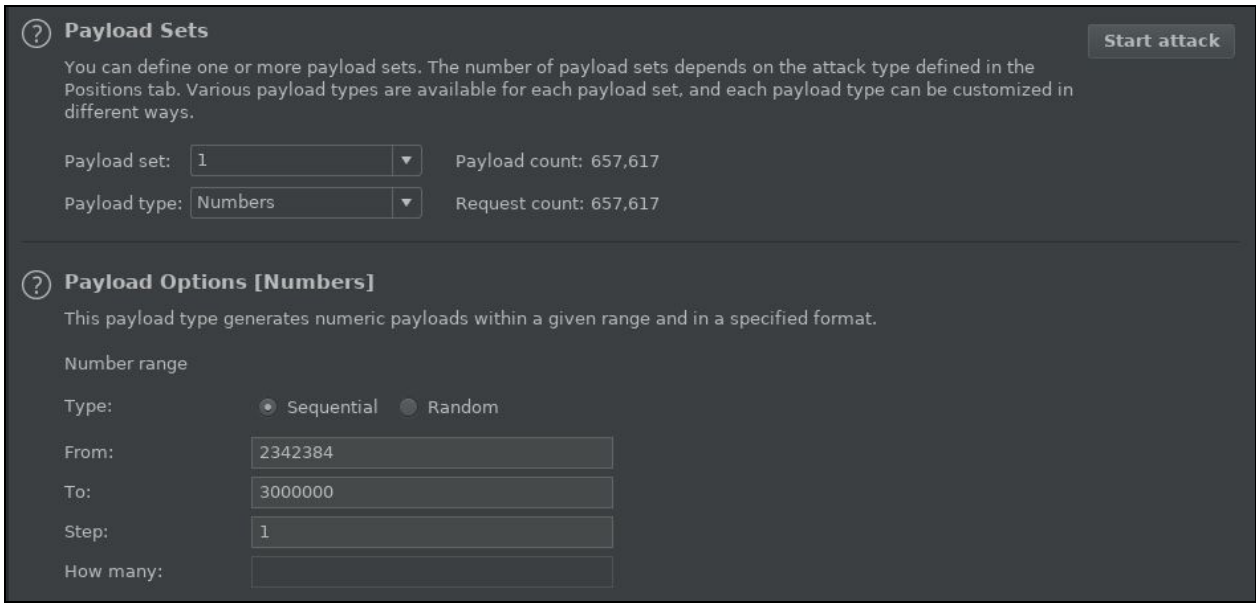


Remember that packet to find the hidden attributes? Yeah we need it again here. If you don't have it right off it might be in your burp target history:

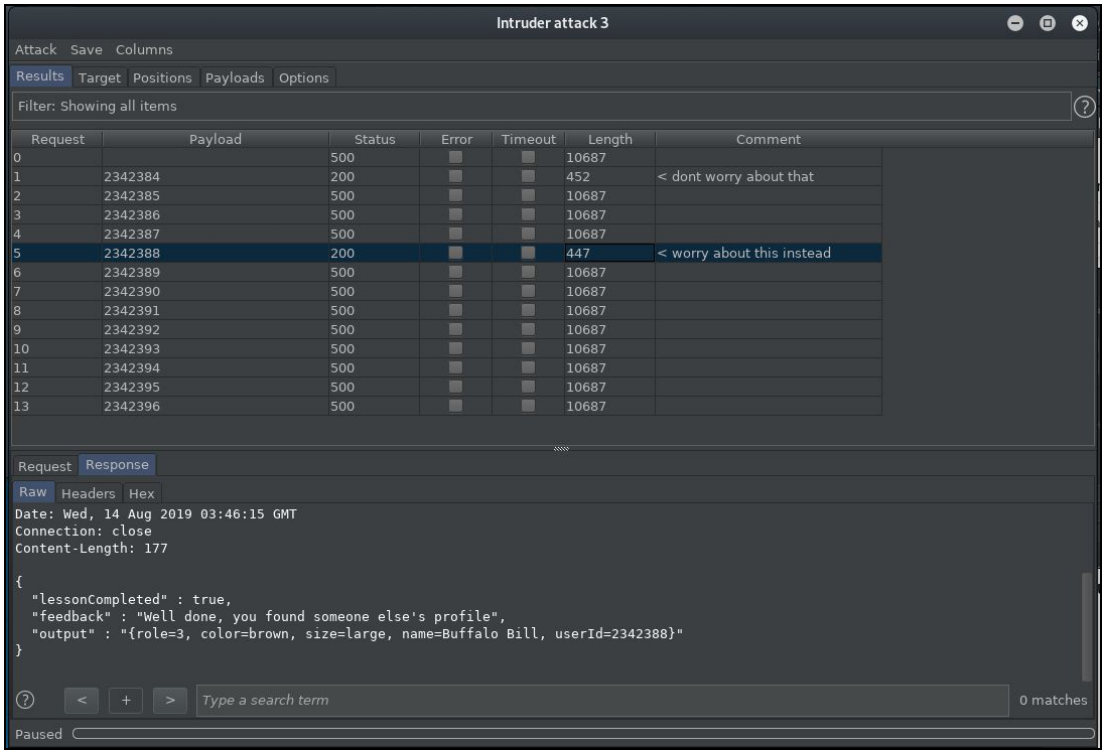


Go ahead and send this over to intruder and we'll set up a brute force using that alternative path we found earlier:

For our payload we're going to use the **numbers** type with our original userid being the starting point and whatever the fuck being our endpoint (I used the number 3 and however many zeros after it so its a bigger number, this is not an exact science):



So now we launch our attack and wait for something good to happen:



Hope you enjoyed this Writeup and if you want to see me attempt these challenges live be sure to drop by my Twitch when I’m live and also follow my Twitter for some quality shitposting!