Burp Suite 2

Please refer to binder: Burp Suite for more information on settings etc. Used in conjunction with firefox and the foxyproxy extension.

Welcome back to another challenge, this time we have our orders.

To begin, make sure intercept is disabled in your Proxy module and navigate to `http://10.10.178.92/products/`. Next, try clicking on some of the **See More** links.

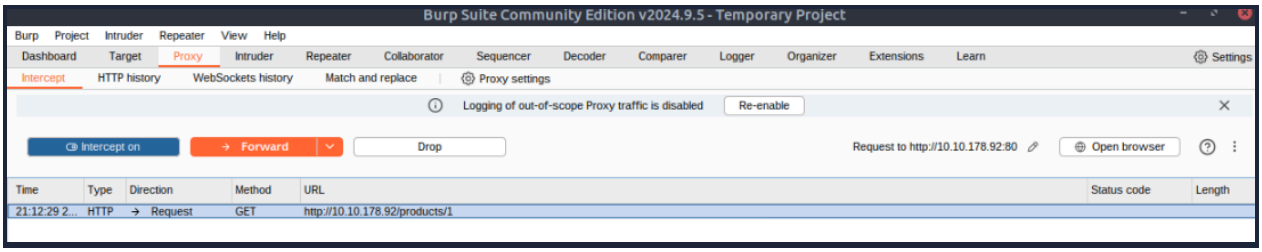
Observe that you are redirected to a numeric endpoint (e.g., /products/3).

The objective is to validate the endpoint, confirming the existence of the number you wish to navigate to and ensuring it is a valid integer. However, consider what might occur if this endpoint is not adequately validated.

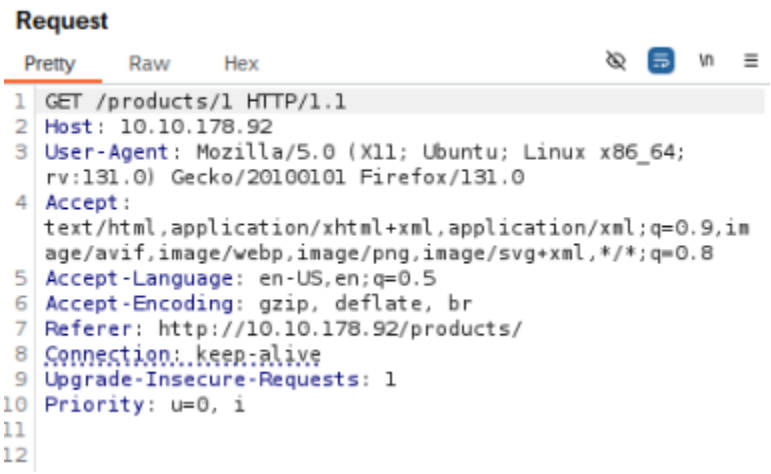
The target is /products/3 we need to validate the endpoint. Already at this point have taken initiative to prepare my burp console to scope the IP: `http://10.10.178.92` only.

So it is the same website as before, the bastion one, but I mapped the whole site first just to be sure nothing changed. I did find some useful info, such as another provided url… But alas that is not our task for today.

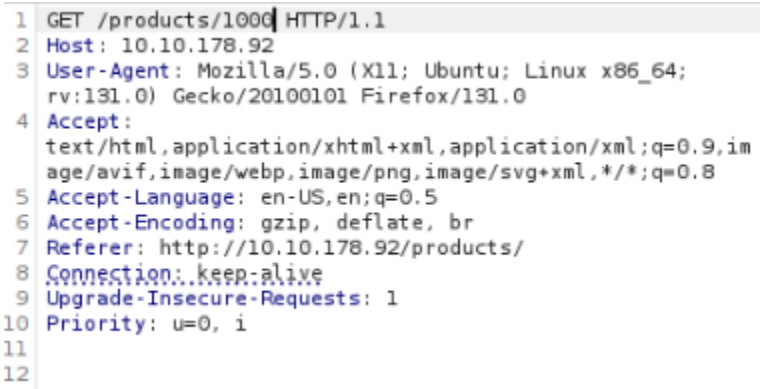
So firstly,
Enable intercept again and capture a request to one of the numeric products endpoints in the Proxy module, then forward it to Repeater.



So here we are, I went into the products section and ran the request… We are in. I right click the request and send to repeater.

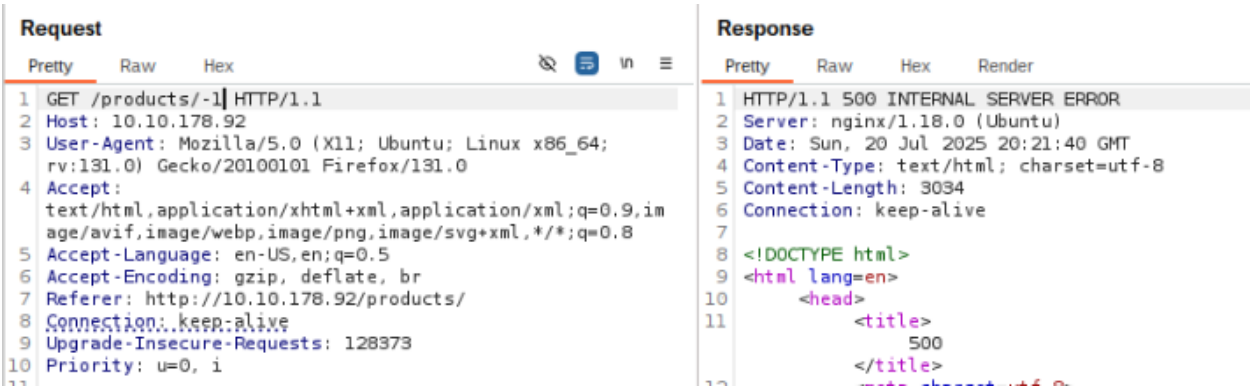


So the product code is seen at the top in the get request, took me a minute to find it I will not lie. /products/1 and we can change that number to… 1000?



Click send and see what happens.

404 not found… NOT good enough. So I need to experiment a bit. Why not try a negative value, like the reversal of the original value? Eg. -1 instead.



Success!!! It works. We created a 500 internal server error.
Notice I also changed the Upgrade-Insecure-Requests too just because I could? But it's all about trial and error and just messing around with things.. I will put that back to the original though now I have found what I wanted.

```
            </div>
        </div>
    </nav>
    <section class="py-5" id="features">
        <div class="container px-5 my-5">
            <div class="text-center mb-5">
                <h1 class="jumbotron">
                    500
                </h1>
                <h2>
                    <code>
                        THM{N2MzMzFhMTA1MmZiYj
                        A2YWQ4M2ZmMzhl}
                    </code>
                </h2>
            </div>
        </div>
    </section>
```

The sweet, sweet flag hiding amongst the code! We did it!

Conclusion:

I am really starting to appreciate the ease of use with Burp (foxyproxy) because it allows us to identify bits of information with ease and is very simple to use. Not only that but the modification and filtering we can use in order to achieve a more customisable UI is impressive and after configuring my panel to my own preference I can increase the efficiency at which I obtain the information!