Inclusion

For this challenge, I used Burp Suite to try to exploit a PHP file inclusion vulnerability. If we look around the website, on the flag page, we can see “The flag is just above this line (in the source code at least)!”. Thus, we can conclude that we need to leak some source code. Furthermore, from the name of this challenge, we can conclude that the source code contains a PHP file inclusion vulnerability. When looking at burp suite, we can also see that there is a “page=flag”. Include supports PHP stream filter URLs. Thus, we can change “page=flag” to “page=php://filter/convert.base64-encode/resource=flag” to get a base64 encoding of the flag. Then, once we decode the outputted string, we get the flag. Thus, the challenge is solved.

I edited the following request intercepted in burp suite to get the flag: