lukeflima / **CTF-Writeups**

Branch: **master** ▾ **CTF-Writeups** / 35c3 Junior / **flags** /

Create new file | Upload files | Find file | History

lukeflima README Update Latest commit `b2ee250` on Dec 30, 2018

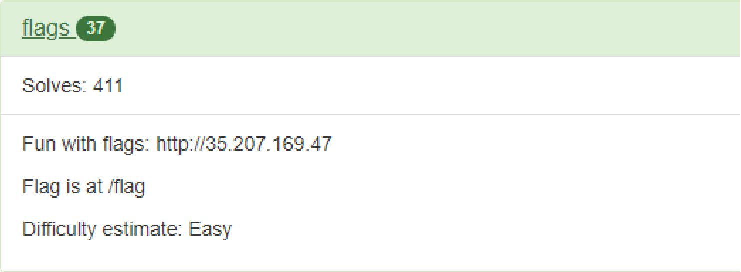
..

README.md	README Update	a month ago
flags.py	commit flags	a month ago

README.md

flags

The challange was:



flags 37

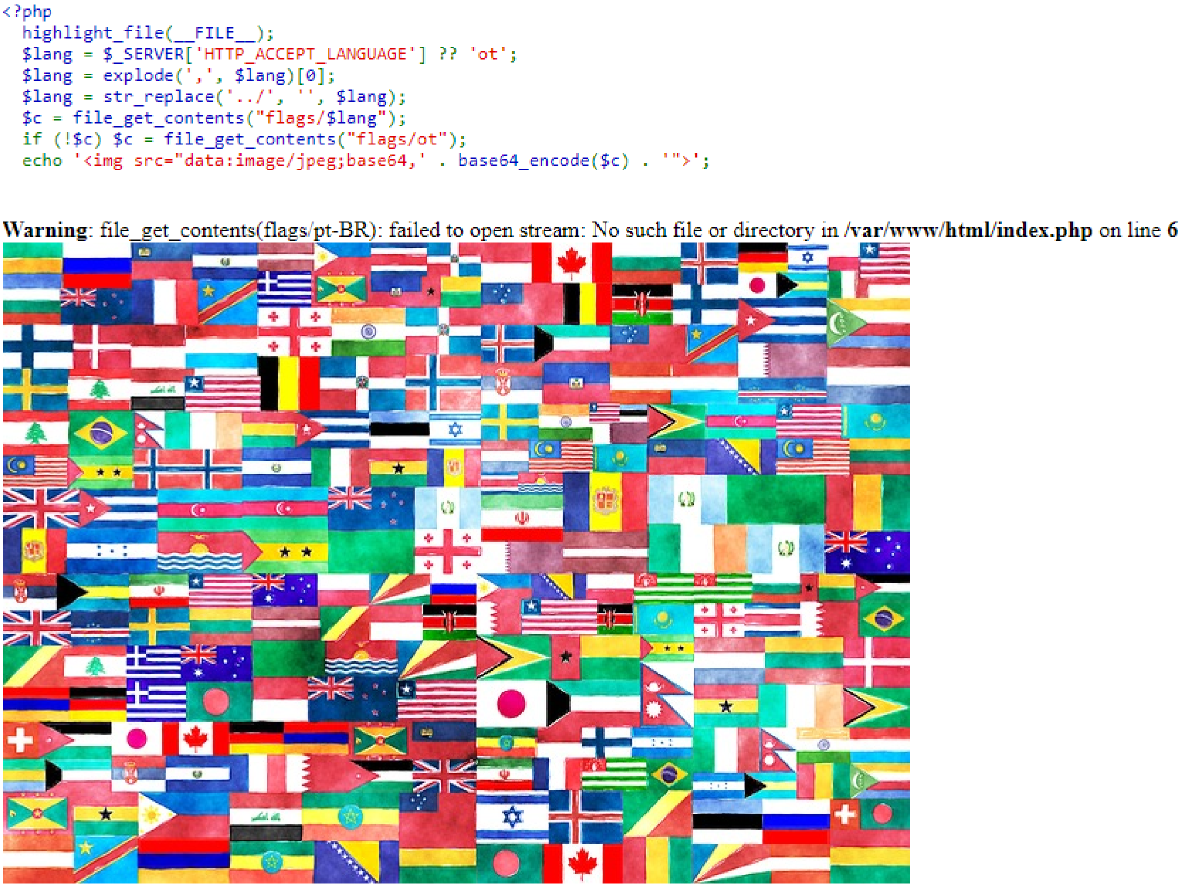
Solves: 411

Fun with flags: http://35.207.169.47

Flag is at /flag

Difficulty estimate: Easy

When you open the link this shows up.



```
<?php
  highlight_file(__FILE__);
  $lang = $_SERVER['HTTP_ACCEPT_LANGUAGE'] ?? 'ot';
  $lang = explode(',', $lang)[0];
  $lang = str_replace('../', '', $lang);
  $c = file_get_contents("flags/$lang");
  if (!$c) $c = file_get_contents("flags/ot");
  echo '<img src="data:image/jpeg;base64,' . base64_encode($c) . '">';
```

Warning: file_get_contents(flags/pt-BR): failed to open stream: No such file or directory in **/var/www/html/index.php** on line **6**

It shows the php code of the server, an warning and an image of flags.

It can be observed that it takes the Accept-Language fild of the http header and it uses to open a file in the dir `flags/`. So it seems simple, just traverse back to `/` and get the flag.
The only hicup is the str_replace function removes `../` from the string. To bypass that we use the string `....//` that when passed onto the replace func it retruns `../`

With that I created a script that changed the Accept-Language fild of th http request's header to `....//....//....//....//flag` and then get the base64 file and decode it.
In the end the flag is outputed `35c3_this_flag_is_the_be5t_fl4g`