Flag Validator (50)

Description

http://tenjin.compfest.web.id:10337

app.py:

```
import os
from flask import Flask, request, render_template_string

app = Flask(__name__)

@app.route('/', methods=['POST', 'GET'])
def index():
    template = None

    if request.method == 'GET':
        template = '''
        {% extends "index.html" %}
        {% block content %}
            <form method="post">
                <input type="text" name="flag" placeholder="COMPFEST9{...}">
                <button type="submit">Check</button>
            </form>
        {% endblock %}
        '''
    elif request.method == 'POST':
        data = request.form
        template = '''
        {{% extends "index.html" %}}
        {{% block content %}}
            <h3><code>{0}</code>
            {{% if "{0}" == env.FLAG %}}
                is the correct flag!
            {{% else %}}
                is not the correct flag.
            {{% endif %}}</h3>
        {{% endblock %}}
        '''.format(data['flag'])

    return render_template_string(template, env=os.environ)
```

Write up

- Opening the website gives us a form to validate our flag
- Try typing `asd` and check if it is the correct flag
- The website returns `asd is not the correct flag.`
- Well let's check for XSS, enter `<i>test</i>`
- (Not) surprisingly the website renders test in italic

- Since there is no way to get privileged user to visit our XSS'd page, we check for another vulnerabilities: XSS is a good sign for SSTI

> You can also see from `app.py` that it uses string formatting with `render_template_string` so we can inject anything and the server will render it for us (also see: Injecting Flask)

- Let's try entering `2`, it renders as `2`.
- The flag is in the environment variable, and it is provided in the `env` variable as you can see in the last line
- Entering `` will return all the environment variable:

```
environ({'HOSTNAME': '58ca4e79a8bf', 'SHLVL': '1', 'PYTHON_PIP_VERSION': '9.0.1', 'HOME': '/
```

- Thus the flag is `COMPFEST9{user_input_is_3v1L}`