

Connect to 144.126.196.214:32329



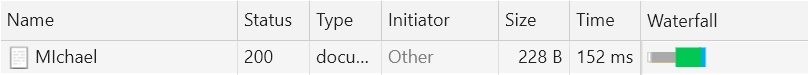
While monitoring the network simultaneously there is nothing there.

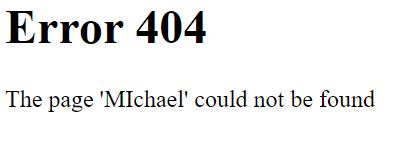
Trying to search /robots.txt – Nope

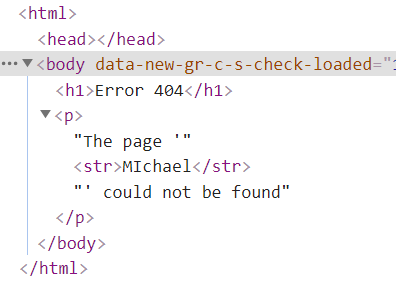
What about Flask/Jinja2? What it is?

Server side is actually built from python library with special looking for variables: {{user.name}} , etc..

When I inject some string like "Michael" I saw:



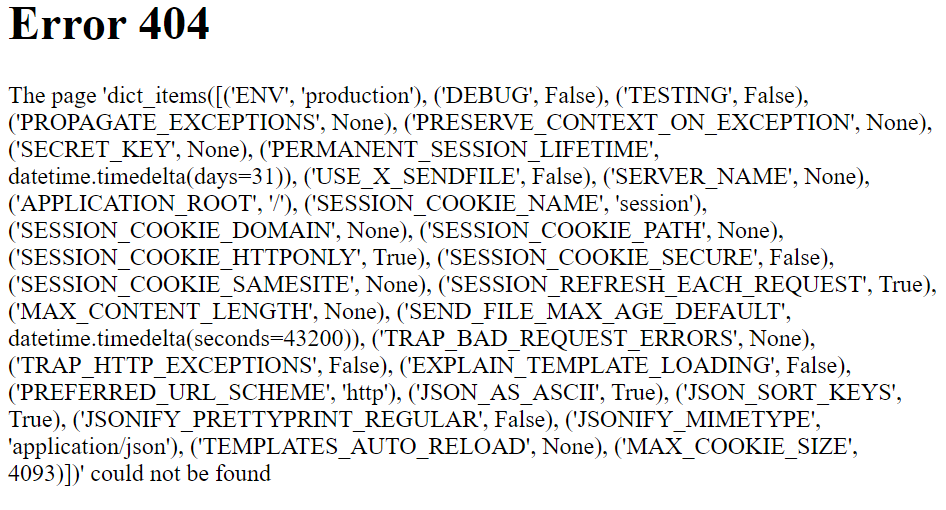




So this is server side injection but we need to figure it out which code to inject…

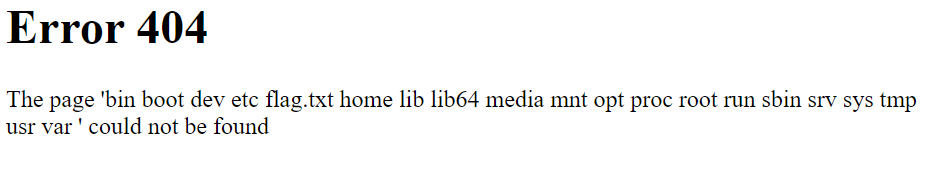
After some search in <https://github.com/payloadbox/ssti-payloads>

I injected to the path: "{{config.items()}}" the results:

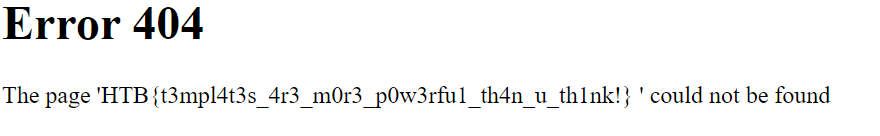


I saw that the server leak data like I wanted…

I played with around and get: {{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_['os'].popen('ls').read()}}



So I injected: {{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_['os'].popen('cat flag.txt').read()}}



Flag: HTB{t3mpl4t3s\_4r3\_m0r3\_p0w3rfu1\_th4n\_u\_th1nk!}