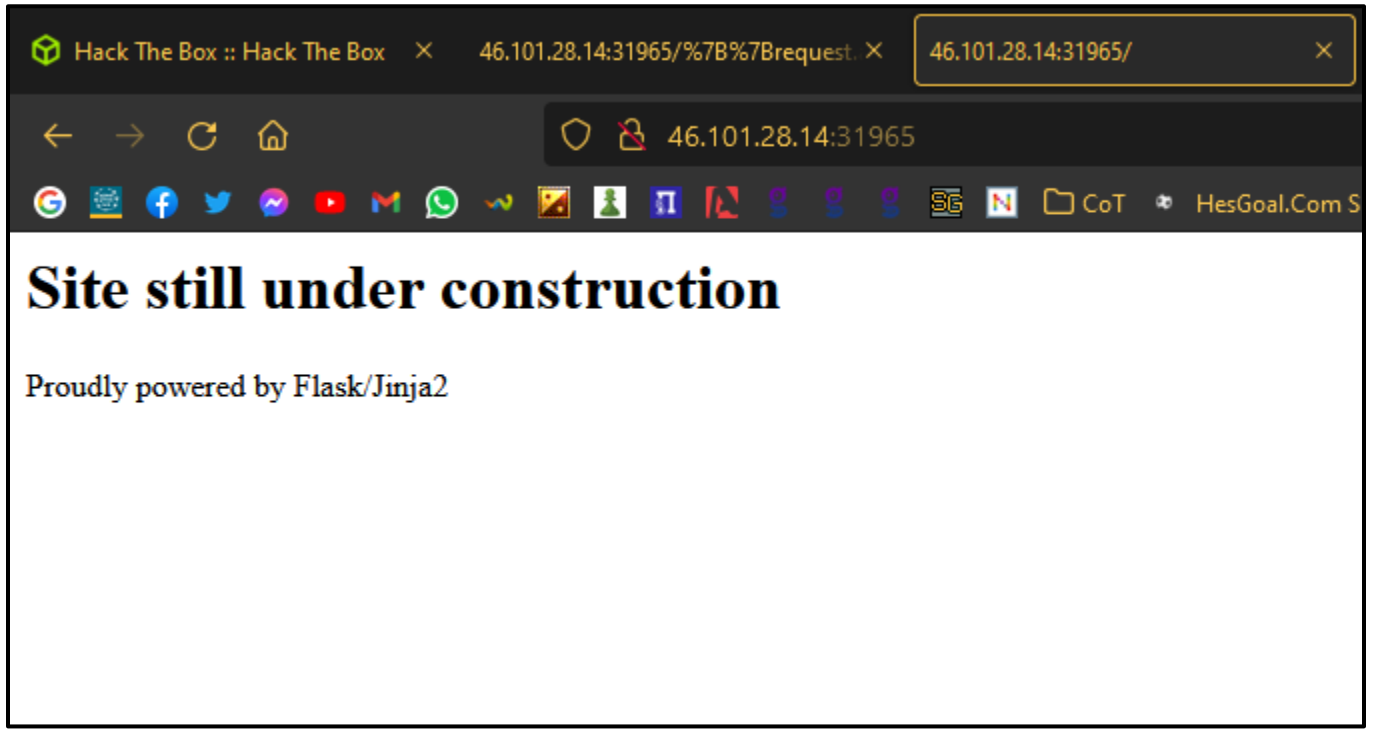
Templated

Write-Up

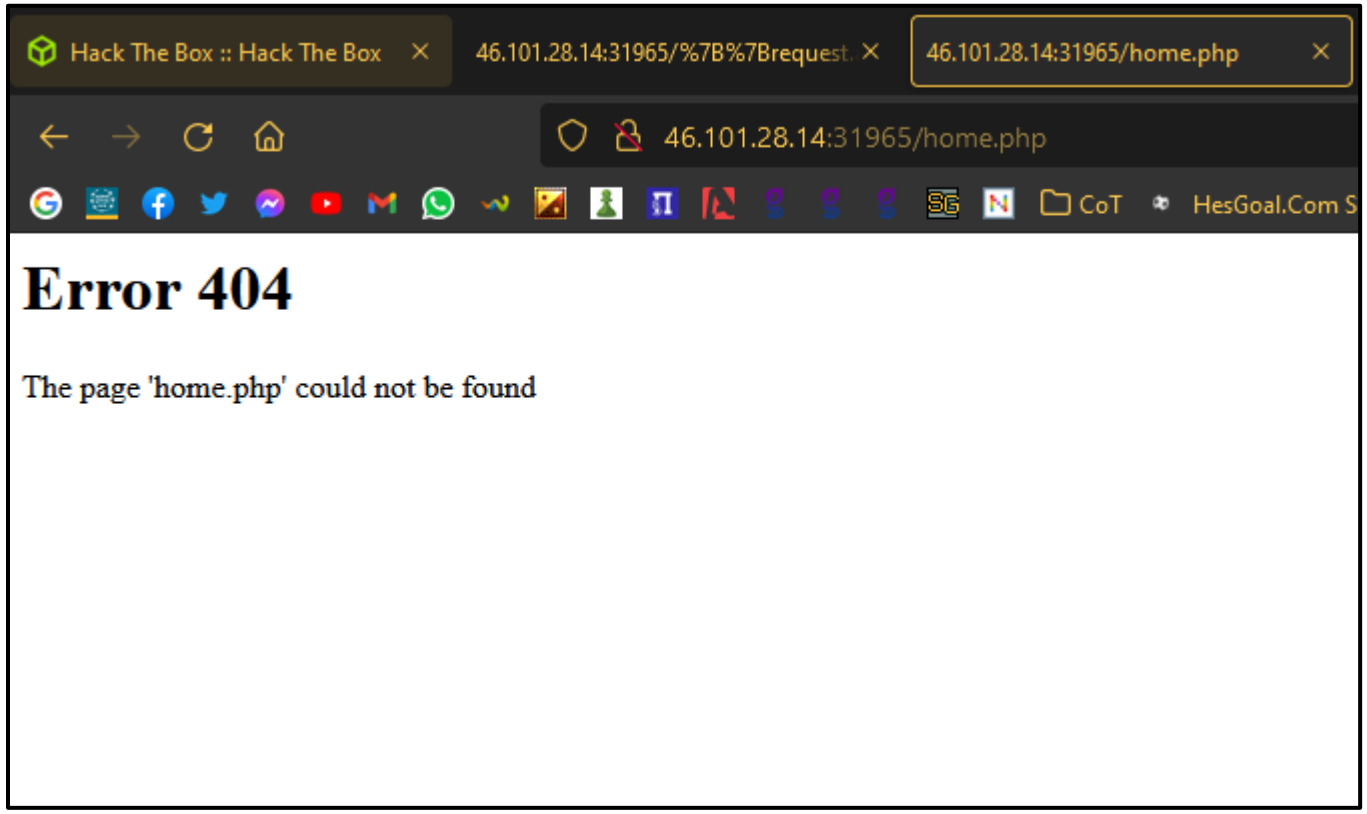
Homepage

- In homepage, there is nothing much.
- Neither the source code reveals anything juicy.



Reconnaissance

- When trying to search for any other page we get an error message that the page does not exist.

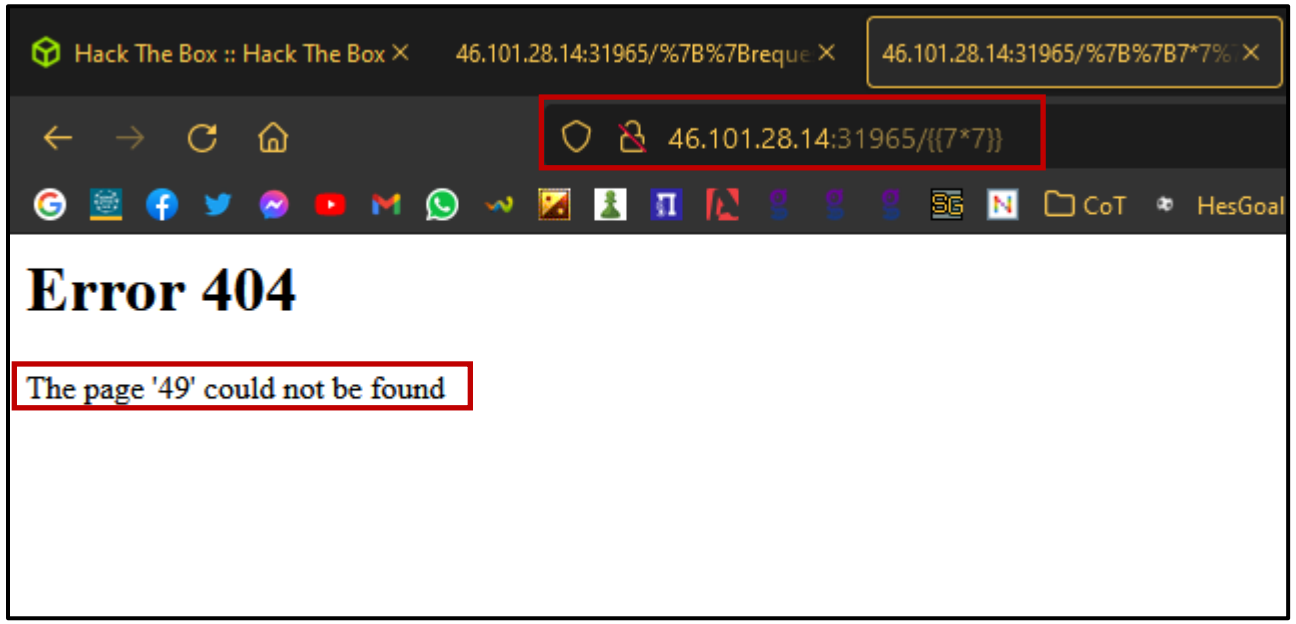


SSTI

- When trying a few things, I managed to do a Server-Side Template Injection (SSTI).
- Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side
- Template engines are designed to generate web pages by combining fixed templates with volatile data. Server-side template injection attacks can occur when user input is concatenated directly into a template, rather than passed in as data. This allows attackers to inject arbitrary template directives in order to manipulate the template engine, often enabling them to take complete control of the server. As the name suggests, server-side template injection payloads are delivered and evaluated server-side, potentially making them much more dangerous than a typical client-side template injection.

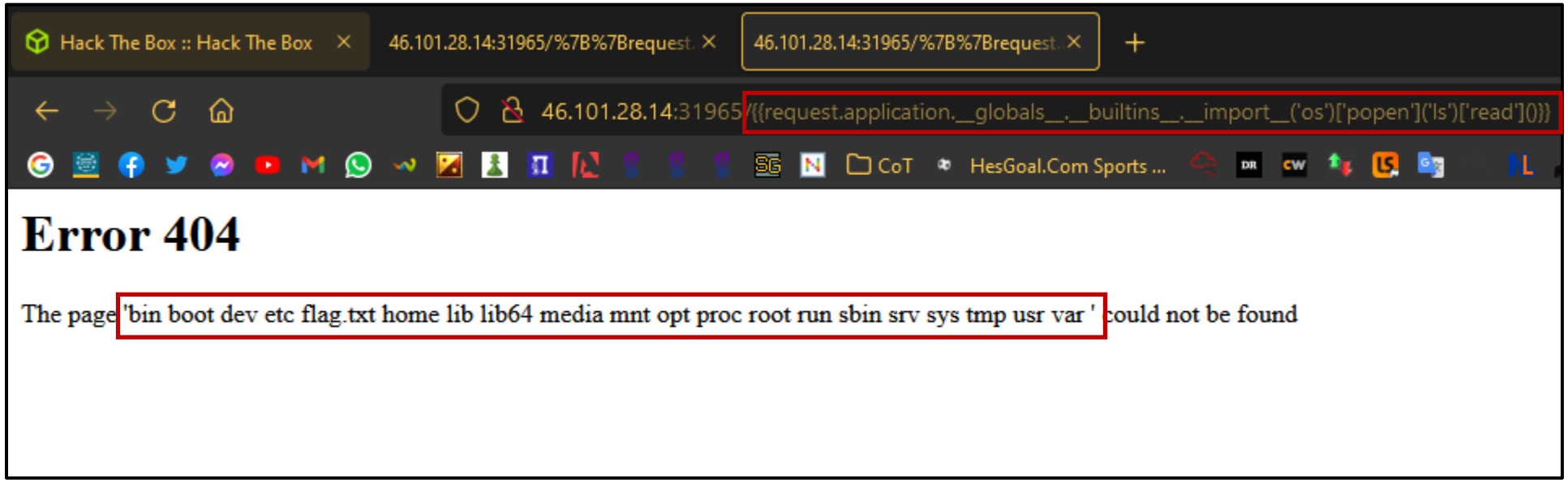
SSTI in Templated

- The following screenshot illustrates the vulnerable website.
  - When passing {{7*7}} as a page, the return shows the result of the quation (7*7=49)



Reading the files on the system

- Exploring online, I found the exploit to read the system files
  - `{{request.application.__globals__.__builtins__.__import__('os')['popen']('ls')['read']()}}`



Grabbing the flag

- Having already exploited the vulnerability and we read the files, now we need to read the flag to finish the challenge.
  - The only change we need to do is to include the “cat flag.txt” command in the payload and grab the flag.