hackerearth

Penetration Testing Report

For

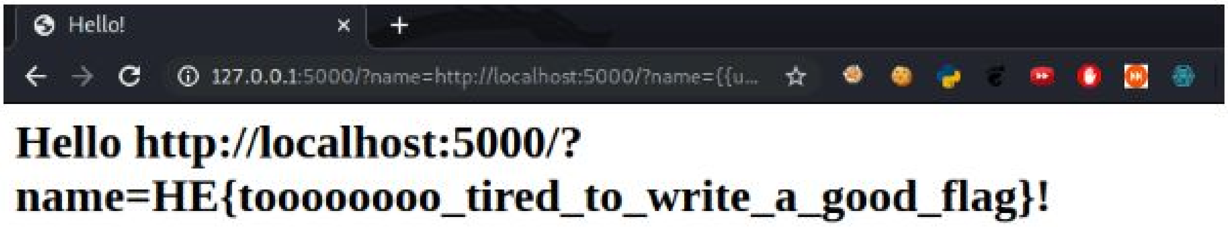
“Another EL Clasico”

S.NO.	Title	#
1.	Challenge Category	Web Application
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. **After clicking on the link we get a page where we are asked to give input and it's reflected on the page.**
2. **Trying different payloads we get that it might be SSTI.**
3. **So for checking what template its using we put {{7*’7’}}.**
4. **It prints Hello 7777777! Based on that we get to know its jinja2.**
5. **Port Swigger has a nice article on how to exploit this properly.**
6. **Final payload   :** http://localhost:5000/?name={{url_for.__globals__.__builtins__.open(%27/flag.txt%27).read()}}

7. **After some tinkering we get final payload to inject**



Hello http://localhost:5000/?name=HE{toooooooo_tired_to_write_a_good_flag}!

Flags:

S.No.	**Flag - No.**	**Flag**
1.	Flag 1	HE{toooooooo_tired_to_write_a_good_flag}