Penetration Testing Report

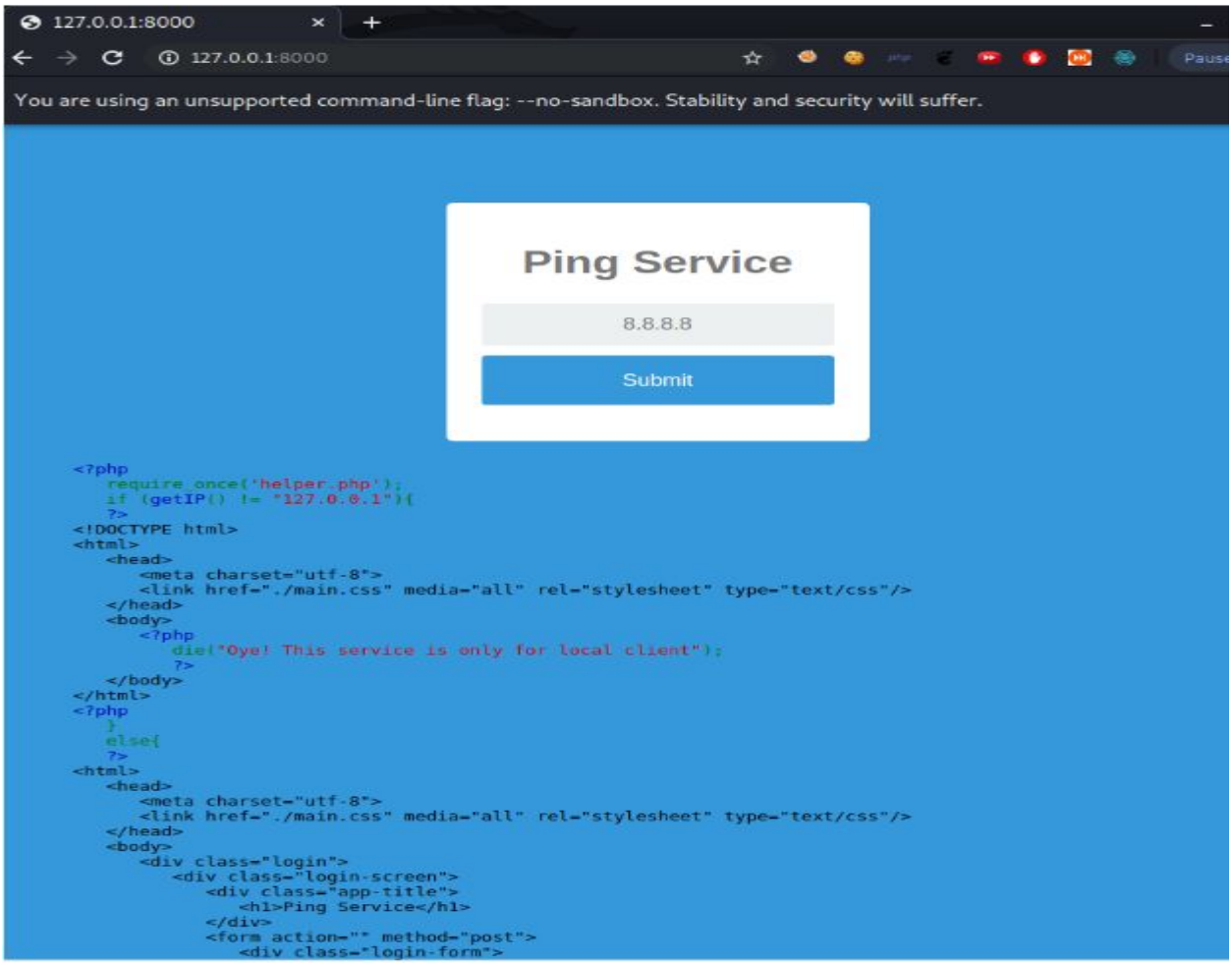
For

“Ping Services”

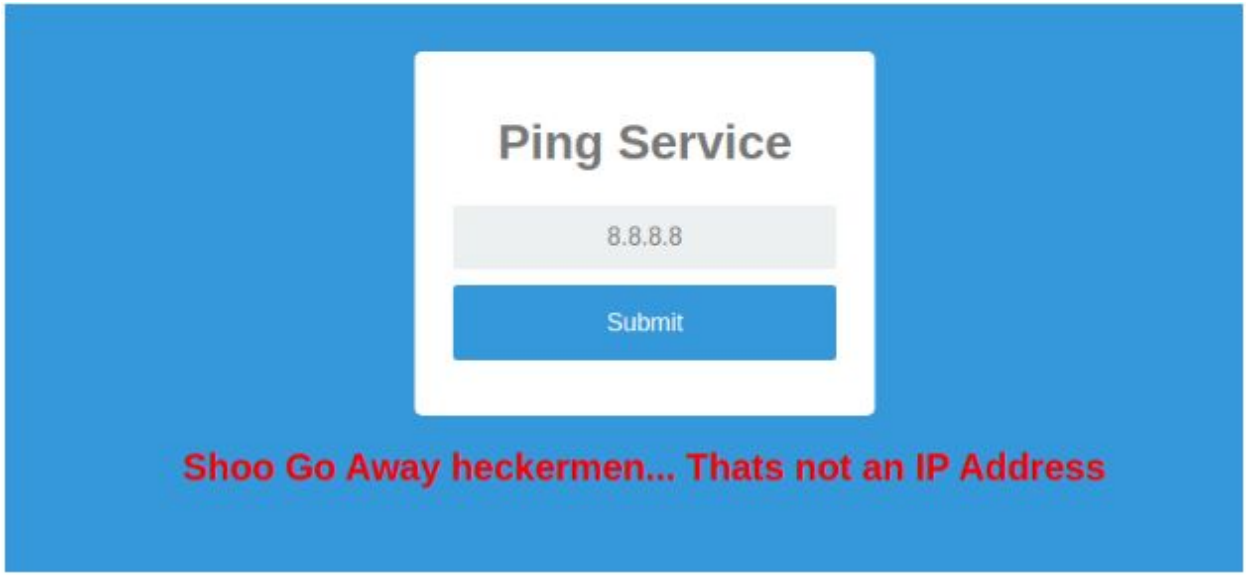
S.NO.	Title	#
1.	Challenge Category	Web Application
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. **When you click on given link you get a page saying this service is just for local client**
2. **So maybe we have to make sever think that you are a local client or this request is sent for a local client.**
3. **Add header => X-Forwarded-For: 127.0.0.1 to the request. (Using burp or maybe any extension)**

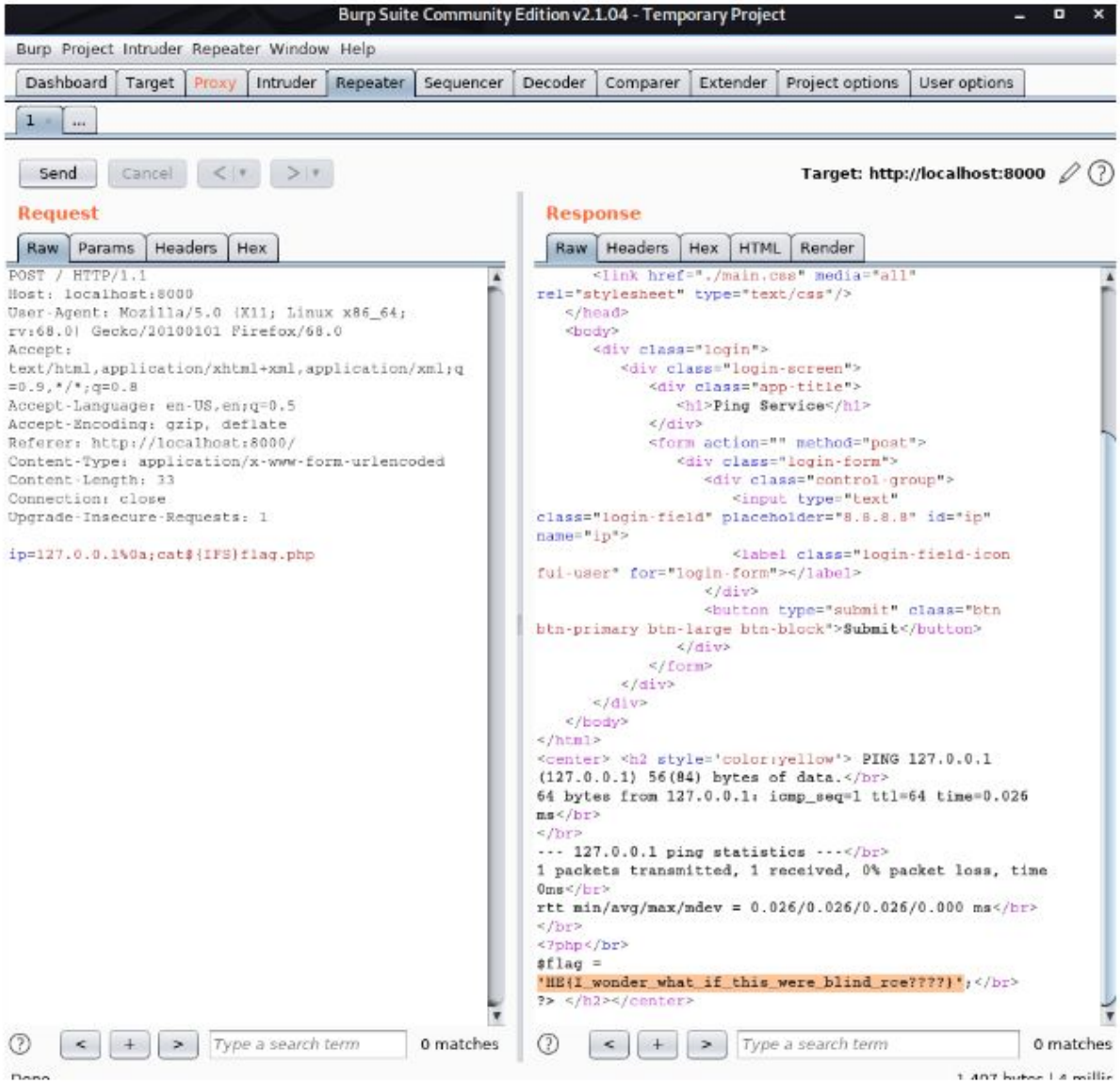


4. **Now you are greeted with a page which asks for an IP to ping**
5. **Try different payloads it just use a blacklists of char to bypass any hacking attempt**



6. **Do a Little bit of research and testing**
7. **After then you get to know that linebreak can bypass the check.**
8. **After that even " " space is also removed from payload so we use ${IFS} of shell instead of space**
9. **Use burp for payload testing to make things easy.**

10. **Build the final payload for post request and get the flag.**
    ip=127.0.0.1%0a;cat${IFS}flag.php



Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{I_wonder_what_if_this_were_blind_rce????}