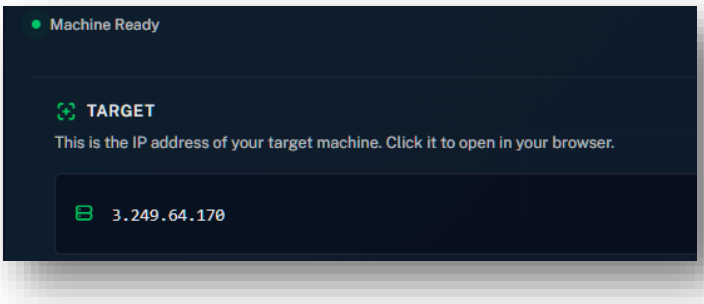
Spoof!

https://hackerdna.com/labs/spoof/flags

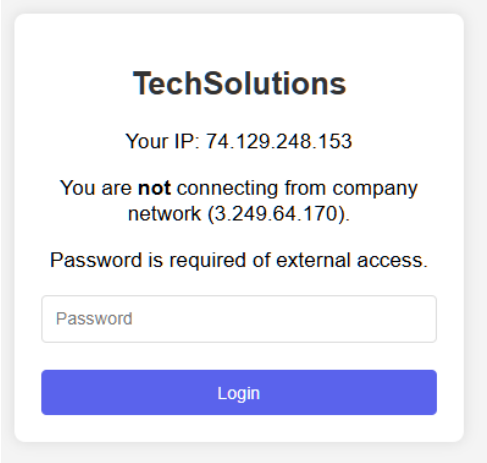
Author: Dorothy Spencer
Date: 02/16/2026
Platform: HackerDNA
Difficulty: Easy Level
Flag Points: 10 (1 flag worth +5 pts)
**Additional points can be earned by doing a community Writeup*
Objective: This lab is designed to manipulate or spoof client-side inputs to bypass the intended authentication or validation checks, gain access to the protected page, and retrieve the lab flag. The server only allowed "internal" company users to access the administrative area without a password.
Tools that will be used:
cURL or cURL via powershell (which worked for me in this lab)
Vulnerability Description:
The application suffers from **Broken Access Control** due to insecure trust in user-supplied HTTP headers. Specifically, the server relies on the ***X-Forwarded-For*** header to determine the client's geographic or network location. Because this header can be manually set by any user, it cannot be trusted for security decisions.

Target Example: https://hackerdna.com/labs/spoof/flags
Start the Machine: Once the machine is ready, click the provided target URL in your Lab.
Example Below.



Inspect the Page:
The whole point of the Spoof! lab is that the page is doing client-side validation, meaning the browser is checking something before allowing access.

Navigating to the target IP revealed a login page stating: ***"You are not connecting from company network*** *Example: (108.130.178.159)."* This provided the specific "trusted" IP needed for the exploit.



NOTE: This lab is NOT about a login script.

It's about ***spoofing*** your IP address check, which is happening client-side.

The page is literally telling you:

- "Your IP: 74.xxx.xxx.xxx"
- "You are not connecting from company network, Example Address: (34.242.140.102)."
- "Password is required for external access."

That is the giveaway.

This lab is about bypassing the IP check, not guessing **a password.**

The entire challenge is:

- **The page checking your IP**
- **You overriding the IP value using a client-controlled header**
- **Accessing the internal-only page**

If you are not able to get to the source js you are looking for, you may need to disable the **IETab extension. I had to for this lab.*

Command Prompt to use curl: In my lab, I used powershell to get what I was after.

Open CMD and run a curl command much like the one listed below.

curl.exe -L -H "X-Forwarded-For: 108.130.178.159" [**http://108.130.178.159**](http://108.130.178.159)

Retrieve the Flag

Depending on the lab version:

- The flag may appear directly on the page after login.
- Or you may need to open the referenced file in the browser: Example: https://lab.hdna.me/.../flag.txt

Copy the flag exactly as shown in screen shot below.

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> curl.exe -L -H "X-Forwarded-For: 108.130.178.159" http://108.130.178.159
5 *******-****-****-********** d
PS C:\WINDOWS\system32>
```

Submit the Flag

- Return to the HackerDNA lab interface.
- Paste the flag into the submission box.
- Click **Submit** to complete the lab.

Copy this code as it appears and paste in the designated field in the lab.