Arnabi Dutta

24/A02/017

Ext Writeup

September 04, 20XX

First Impression/Thoughts:

The first thing I see is a simple webpage with an upload functionality. After a couple of tries of uploading random file types, I stumbled upon hint1.

Hint 1: .phtml

I saw the hint ".phtml" which hinted towards uploading a .phtml file.

What's .phtml?

A `.phtml` file is a type of file that contains PHP code and is used as a script in web development. The `.phtml` extension stands for "PHP HTML" and is typically used to indicate that the file contains a mix of PHP and HTML code. : When a web server processes a `.phtml` file, it interprets the PHP code on the server before sending the resulting HTML to the client's browser. This means that PHP code is not visible in the client's browser; only the resulting HTML is displayed.

Sources: Google Search

This gave me the idea to upload an .phtml file.

Format of .phtml file

I looked up the format of a .phtml file and made a simple file named JG.phtml.

"Success! Be sure that you have uploaded a file with unique name"

Hint 2: /uploads/

The 2nd hint given was /uploads/ which made me think if I could access the uploads directory.

“Forbidden You don't have permission to access this resource.”

So I tried accessing my uploaded file JG.phtml in the uploads directory.

http://98.70.76.80:8002/uploads/JG.phtml

When I visit this URL, if the `.phtml` file was uploaded correctly and the server is configured to execute `.phtml` files, I should see the output of the PHP code that I wrote.

Hint 3: RCE

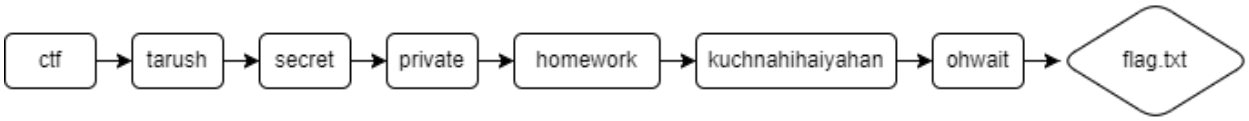
With my file uploaded, I could now execute shell commands. To test, i accessed:

http://98.70.76.80:8002/uploads/JG.phtml?cmd=ls

This listed all files in the current directory.

cd

Using the cd (change directory command) I eventually found ctf. It led me to http://98.70.76.80:8002/uploads/RCEJG.phtml?cmd=cd%20/ctf/tarush/secret/private/homework/kuchnahihaiyahan/ohwait/flag.txt



cat

Now to display the contents of flag.txt i used cat (concatenate cmd).
http://98.70.76.80:8002/uploads/RCEJG.phtml?cmd=cat%20/ctf/tarush/secret/private/homework/kuchnahihaiyahan/ohwait/flag.txt;

Finally found the flag ehax{first_year_ka_homework_bhejdo}

Essential Linux Commands: ls, pwd, mkdir, cd, touch, vim, cat

This basic video helped me with cd and cat commands.