Source Code of the php html file <http://pastebin.com/Dv6g68kj>

Html File Refrencing <http://www.ehow.com/how_8365119_reference-file-html.html>

Looking at the source code, you can tell it’s in HTML format and closely resembles the actual webpage.

But the php code is missing in the actual webpage so you will use that for referencing.

As what the hint said, the images are loaded weirdly.

Their URL is **http://web2014.picoctf.com/potentially-hidden-password-3878213/file\_loader.php?file=zone[#1-6].jpg**

The main part of the URL you want to focus on is **file\_loader.php?file=**

If you type in a non-existing file such as <http://web2014.picoctf.com/potentially-hidden-password-3878213/file_loader.php?file=test.txt>

It will return

**No such file: /resources/files/test.txt**

By looking at the error, you can see that file\_loader.php is starting in the directory

**/resources/files/**

Now, if you look back at the source code provided, you’ll see this line inside the php code:

**$config\_file = fopen("/resources/config/admin\_mode.config", "r");**

You can see that there’s a file called “admin\_mode.config” inside /resources/config/

Currently you’re at **/resources/files** and you want to get into **/resources/config**.

To access that directory, you’ll have to move up 1 directory.

To go up a directory, you use 2 periods and a forward slash (../).

In the URL, you will replace the current fileloader path with this:

**file\_loader.php?file=../config/admin\_mode.config**

This moves you up one directory, then into “config” directory and opens up admin\_mode.config.

What you’ll see is just a blank page with the word: **false**

This means admin\_mode is false and in the source code, you’ll see that if it was set to true, it’ll go into

**/resources/secrets/flag**

Since it gave you the pathway, you can manually go into the directory.

The “secrets” directory is also in the same directory as “files” and “config” so you just practically type the same thing as before.

The file pathway will be:

**file\_loader.php?file=../secrets/flag**

and tada, there’s the password.

And yes, you could’ve just skipped the whole part about admin\_mode.config.

Here’s a diagram of all the directories mentioned:

