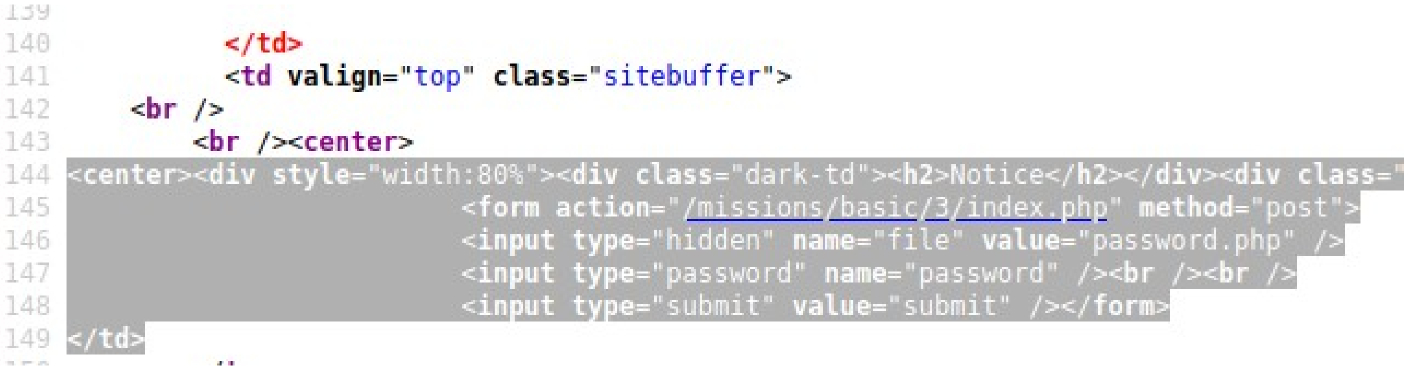
Hack This Site Basic 03

“**Level 3**

This time Network Security Sam remembered to upload the password file, but there were deeper problems than that.”

Basic Mission 03. In this mission, there is a warning that there might be a deeper issue. Sam remembered to upload the password file but no more clues from there. So let’s start by seeing what might be the issue.

First, let’s analyse the page source.



```
                </td>
                <td valign="top" class="sitebuffer">
        <br />
            <br /><center>
<center><div style="width:80%"><div class="dark-td"><h2>Notice</h2></div><div class="
                                <form action="/missions/basic/3/index.php" method="post">
                                <input type="hidden" name="file" value="password.php" />
                                <input type="password" name="password" /><br /><br />
                                <input type="submit" value="submit" /></form>
</td>
```

As we are trying to login we have to look at the page source to see what clues could be evident to us. I scroll down to where the login form is, I see that “hidden”, “password” and “submit” are three different types of input fields. “Password” and “Submit” is what we can see on the page as that is where we enter our password and click submit to enter the password, however, the line I care about is the “hidden” line, first of all, because it is hidden and also because it contains a “password.php” file which is the password we are looking for, however, it is not downloadable and is .php file.

Thinking about path traversal attacks I think to go to the URL of the page and append “password.php” to the end of the URL to see if the webserver is storing a file called password.php, if it does then it should show me the contents, being the password in this case.

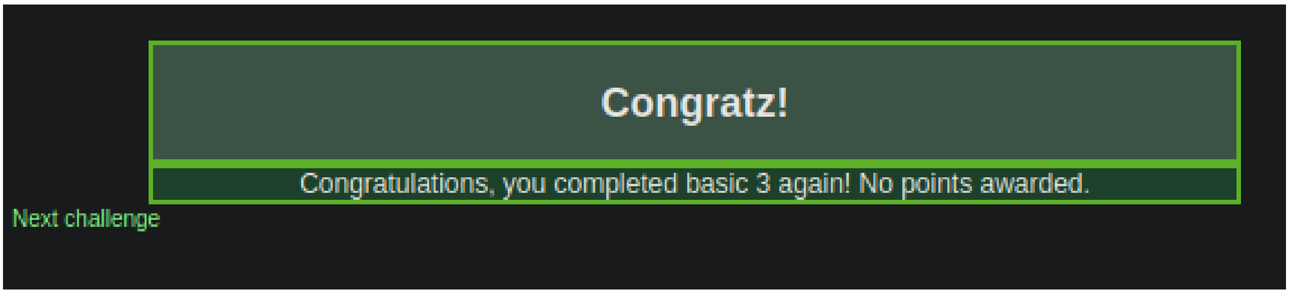
Link [https://www.hackthissite.org/missions/basic/3/password.php]
Result: e7d53814

I was correct, the webserver is storing a file called password.php and it displays the password needed for the challenge. This becomes obvious as password.php is a file type. Lets’s dissect the line of code.

```
<input type="hidden" name="file" value="password.php" />
```

Input type = hidden. Meaning hidden from the user. Name=file meaning that there is a file on the server, and value of the file is password.php, so this means that under file there is a file called password.php which in this case is the password file for the login form.

As it’s the login form we care about, you should instinctively navigate straight to the code in the source to look for any clues that could yield an answer, in this case, we saw that there is a PHP file funny enough called password.php. So this is the password file that is being used to store the password. All you have to do is append “password.php” to end of the URL to go to that directory on the server and see the contents of that file which intern is the password.



Congratz!

Congratulations, you completed basic 3 again! No points awarded.