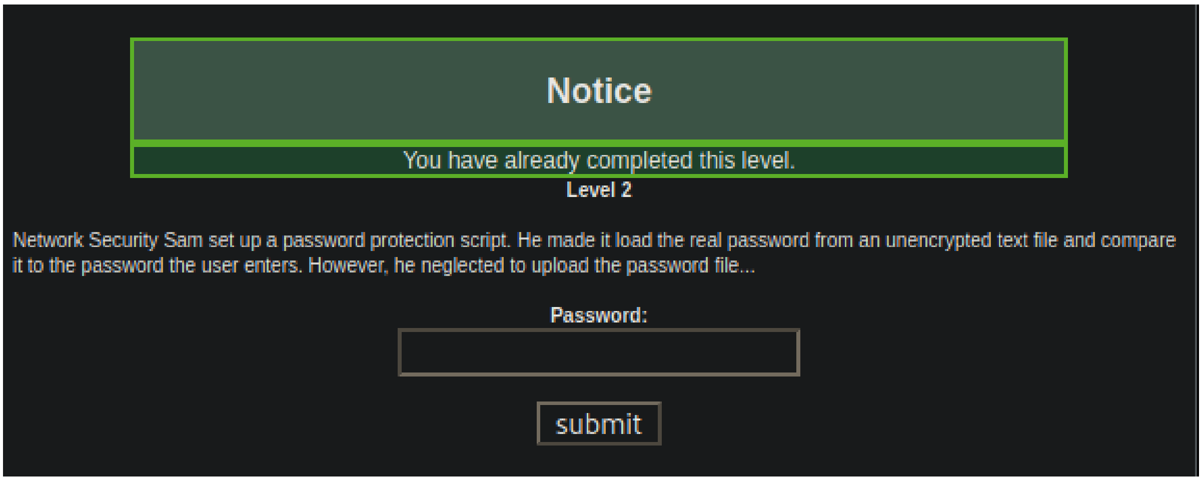
Hack This Site Basic 02

“Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...**”.**



Notice

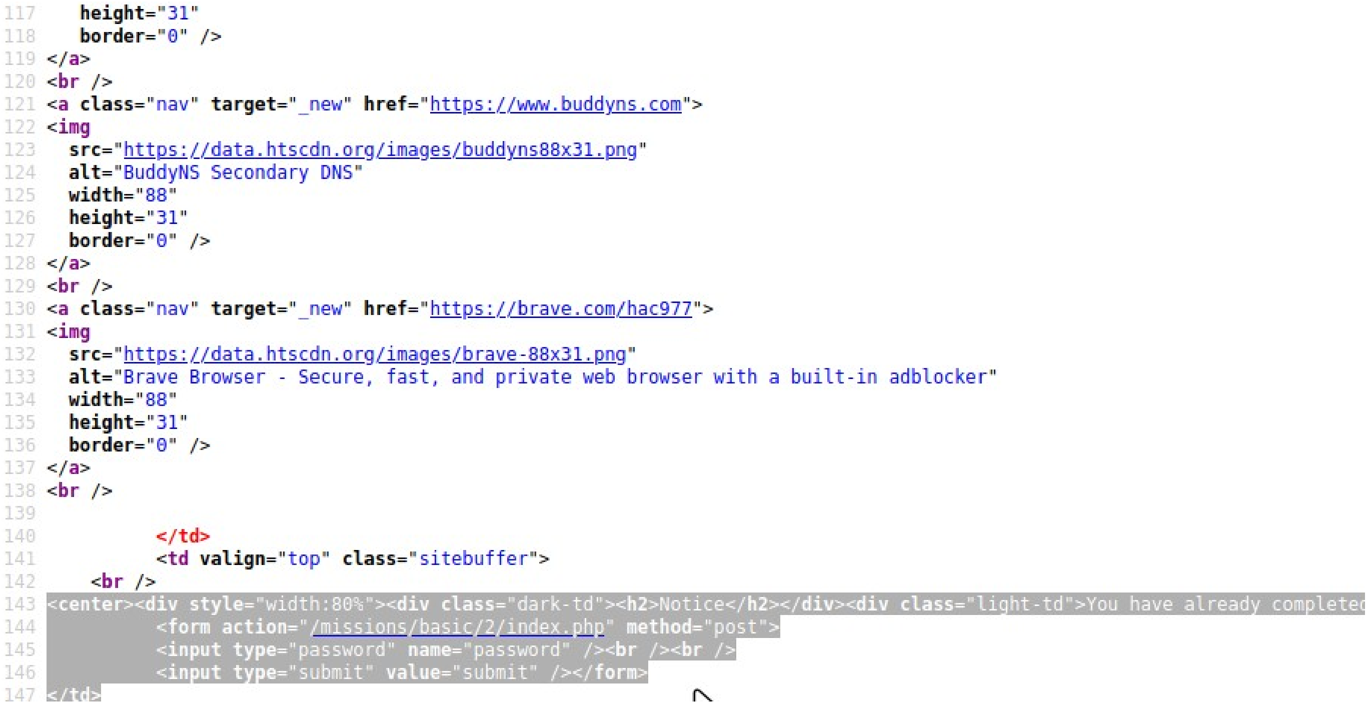
You have already completed this level.

Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

In basic mission 02, the message says that the sysadmin did not upload a password file to the login field, this means that there is no password authentication. So all you will need to do is click “Submit” and then you would have completed the challenge.

Vulnerability: No Password File.
Let’s begin with viewing the source of the webpage.

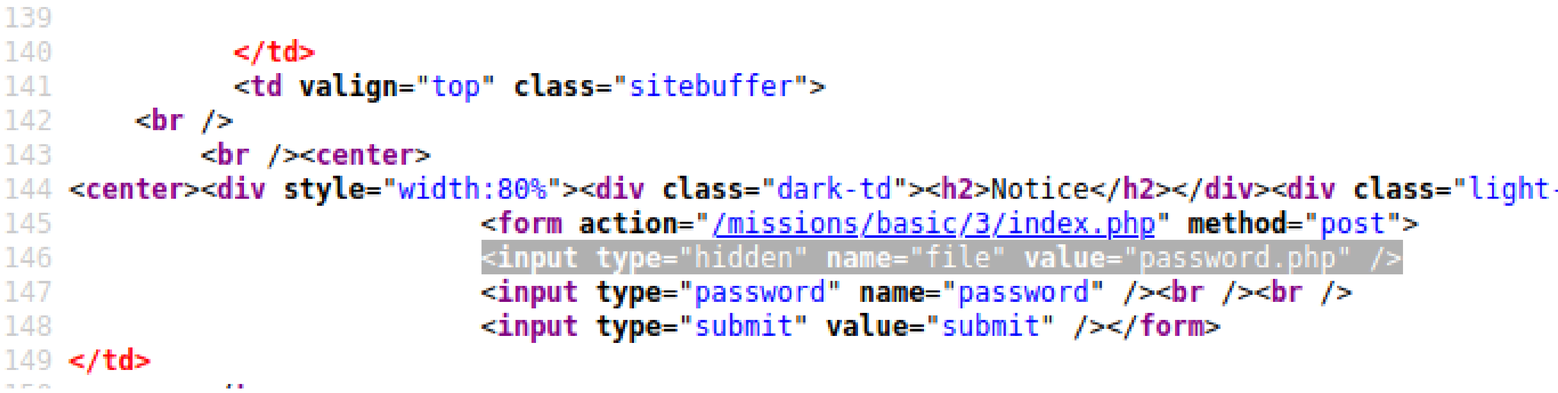


```
   height="31"
   border="0" />
</a>
<br />
<a class="nav" target="_new" href="https://www.buddyns.com">
<img
  src="https://data.htscdn.org/images/buddyns88x31.png"
  alt="BuddyNS Secondary DNS"
  width="88"
  height="31"
  border="0" />
</a>
<br />
<a class="nav" target="_new" href="https://brave.com/hac977">
<img
  src="https://data.htscdn.org/images/brave-88x31.png"
  alt="Brave Browser - Secure, fast, and private web browser with a built-in adblocker"
  width="88"
  height="31"
  border="0" />
</a>
<br />

          </td>
          <td valign="top" class="sitebuffer">
    <br />
<center><div style="width:80%"><div class="dark-td"><h2>Notice</h2></div><div class="light-td">You have already completed
          <form action="/missions/basic/2/index.php" method="post">
          <input type="password" name="password" /><br /><br />
          <input type="submit" value="submit" /></form>
</td>
```

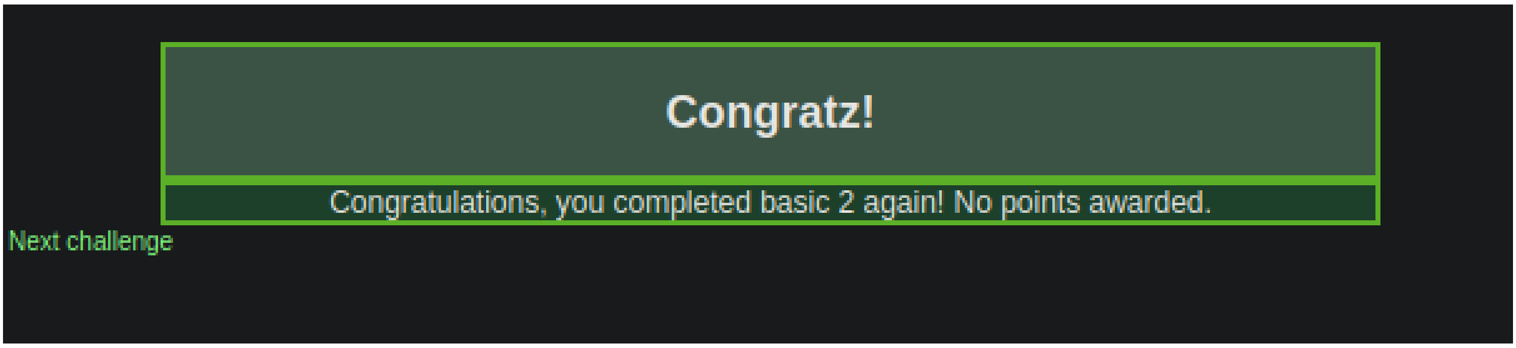
As you can see that in the code above there is no file within the login form. Compared to the source beneath where there is (<input type=hidden” name-”file”= value=”password.php” />). Password.php is a password file however this line of code does not exist on challenge 02 source meaning there is not a password file so the user can just click submit and move on.

Some sites such as verifications.io have fallen prey to this attack. They had a MongoDB publicly facing with no password protection so the hackers could just login without a password and they stole 761million emails and passwords.



```

          </td>
          <td valign="top" class="sitebuffer">
     <br />
         <br /><center>
<center><div style="width:80%"><div class="dark-td"><h2>Notice</h2></div><div class="light-
                         <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>
```



Congratz!

Congratulations, you completed basic 2 again! No points awarded.