# Intro to Hacking

### Basic Hacking

We will be using a hacking site for these activities. It can be found here:

[www.hackthissite.org](http://www.hackthissite.org)

Login credentials are as below:

|  |  |
| --- | --- |
| Username: | stephen-jay |
| Password: | techCamp1234RRC |

Once logged in, you should be able to begin the basic activities. Be advised if you wish to do this outside of RRC, you should likely create your own account, as a couple of the activities require email.

# Hacking

Steps to hacking a site

1. Get Permission!
2. Review Source Code
3. Submit empty form
4. Submit form with bad data
5. Attempt data injections

### Mission 1:

Very basic, you need only look at the source code for the page. Right click on any text on the page, and select “View Page Source”, and scroll about 1/2 way down you should see something like:

<!-- the first few levels are extremely easy: password is 00cc5ef1 -->

### Mission 2:

As the mission states, Network Security Sam neglected to upload the password file, so you should try and submit an empty form

### Mission 3:

You can try entering bad data, as the steps indicate, however, in this case, a review of the source code is the key. By checking the source, we see the following:

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

If we add the above to our browser’s link, we get the following link:

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

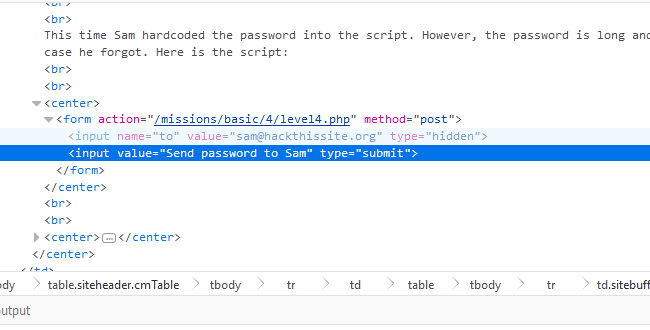
This gives us our password we can enter - 97901bf5

### Mission 4:

Again, we don’t have any value in entering dummy data. If we do check the page source again, we see the following:

<input type="hidden" name="to" value="sam@hackthissite.org" />

We need to modify this using Firefox’s DOM tool. Right click near the “Send password to Sam” button, and select Inspect Element (Q). You will see there is a hidden field called “to” You will need to change this to your email, or the email assigned to this course, which is [sjay@mts.net](mailto:sjay@mts.net)



You can also create a local copy of the form above, change the “to” value to your email address, and the action to: <https://www.hackthissite.org/missions/basic/4/level4.php>. Either works here. If you choose to make a form, it should look like the following, and stored locally (I called mine mission4.html)

<form action="https://www.hackthissite.org/missions/basic/4/level4.php"

method="post">

<input type="hidden" name="to" value="sjay@mts.net" />

<input type="submit" value="Send password to Sam" /></form>

This will generate a password reminder, that being the following email:

Sam,  
Here is the password: '793cfae5'.

Simply go back to the Misssion 4 page, and enter 793cfae5 for the password to move to the next mission!

### Mission 5:

Mission 5 is basically the same as Mission 4, except it only allows the DOM manipulation. Simply repeat the DOM example above, and you get the following email:

Sam,  
Here is the password: '9b38150c'.

### Mission 6:

With Mission 6, we get into basic encryption. Encryption is using a modification process to take a string of characters, convert it to something less understandable, and back again.

In this case, it is simply modifying the next letter offsetting it by one. Fortunately the mission has an encryption tool. If you enter aaaaaaaa to be encrypted, it comes back abcdefgh. Knowing this, we can then take **093ehh=>** and decrypt it backwards:

0  
8 (9-1)  
1 (3-2)  
 b (e-3)   
d (h-4)  
c (h-5)  
7 (=-6)  
7 (>-7)

Therefore, our password is 081bdc77. We can test this using the encryption tool.

We need to use an ASCII table to get the last 2 characters. It can be found at the end of this document.

### Mission 7

Mission 7 requires an understanding of file systems, and some UNIX command experience. It uses the basic UNIX command cal. If you enter 5 2014 into the form, it gives you the calendar for May 2014.

With UNIX, however, you can add one command after another using the semicolon, as below:

cal; ls

The above will allow you to do the cal command and the ls command . ls allows you to do a directory listing. When we add ls to the end of our cal command, as below, we get an interesting output.

First type in the following in the form:

5 2014; ls

We then get:

May 2014

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

.

..

cal.pl

index.php

k1kh31b1n55h.php

level7.php

This now shows us the file k1kh31b1n55h.php in the same directory as we are in. When we open this page, we see the following:

b00d54b9

This then is our password for Mission 7.

### Mission 8

This mission requires an understanding of a feature in web sites called Server Side Includes. With SSI, you can embed little files within a web page for items such as navigation, page headers and footers, and copyright info. With SSI, you can also execute some basic UNIX commands.

Mission 8 asks us for our name. When we enter our name, it adds it to a document. If we use SSI, we can also get a directory listing (ls).

First, test the script by putting your name in it.

Next, enter the following

<!--#exec cmd="ls" -->

Space is very important. It gives us a listing of the files in this directory. To do a listing of the parent directory, we merely modify the above

<!--#exec cmd="ls .." -->

This gives us a listing of the parent, and we now see the password file au12ha39vc.php. We can then open this with the link https://www.hackthissite.org/missions/basic/8/au12ha39vc.php, giving us the password 16de7170.

### Mission 9

Mission 9 is very similar, and uses, mission 8. To get this password, we simply need to use the ls command SSI injection from mission 8 to go to the directory for mission 9. Simply go back to basic missions, select mission 8, and enter the following in the name field:

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

This gives us the ability to go up to the directory for 8, the directory above 8 called basic, and into the directory for 9. It gives us the following listing:

Hi, index.php p91e283zc3.php!

Your name contains 24 characters.

You can then use p91e283zc3.php to open up the password file. It gives us the link:  
https://www.hackthissite.org/missions/basic/9/p91e283zc3.php

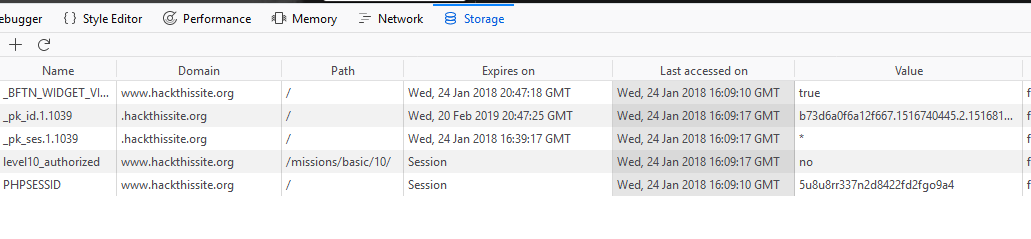
The file contains the following password:

026cc3d7

### Mission 10

Mission 10 uses javascript and cookies for loggin in. It is simply a case of modifying your login session to yes.

This time we are going to use the Firefox built in Web development tools, but we are going to use the Storage tab. Best achieved by hitting Shift + F9 on your key board, and look for a cookie named “level10\_authorized” as below:



One of the values is the cookie, and for the cookie, one of the entries is level10\_authorized. It is set to no, double click on the word “no” and set it to yes, click away, and click Submit on the form

### Mission 11

Mission 11 is just dumb. Don’t bother.

## Get PERMISSION

**As you can see, these are real tools and tactics. Get permission before using these on systems!**

More info, including how to set up your own pentest environment can be found on my git repository: <https://github.com/stephenmjay/pentest>

ASCII Table used for mission 6:

