TEH3261/ FTEH3261
ETHICAL HACKING AND SECURITY ASSESSMENT
PROJECT 2 – 10%

Lab Session : 1BV
Team Name : 3AM Hackers
Team Leader : 1191302861 Mayar Abdulmalik M Shenawi
Group Member 1 : 1181102166 Ahmed Aldughaither
Group Member 2 : 1191302763 Al Ghamdi Omar Saeed O
Group Member 3 : 1191201179 Rian Tiew Ming Sheen
Group Member 4 : 1171103833 Loo Wei Jun

Instructions:

1. Form a group of **3-5** students, remain in the same group for all projects and *Capture-the-Flag* (CTF) – lab tests.
2. Complete **ALL** the questions below by attaching a snapshot of your screen result as evidence.
3. Only **1 copy** to submit by Group Leader.
4. Submit latest by **4 March 2022, 5pm** to the MMLS Assignment Repository.

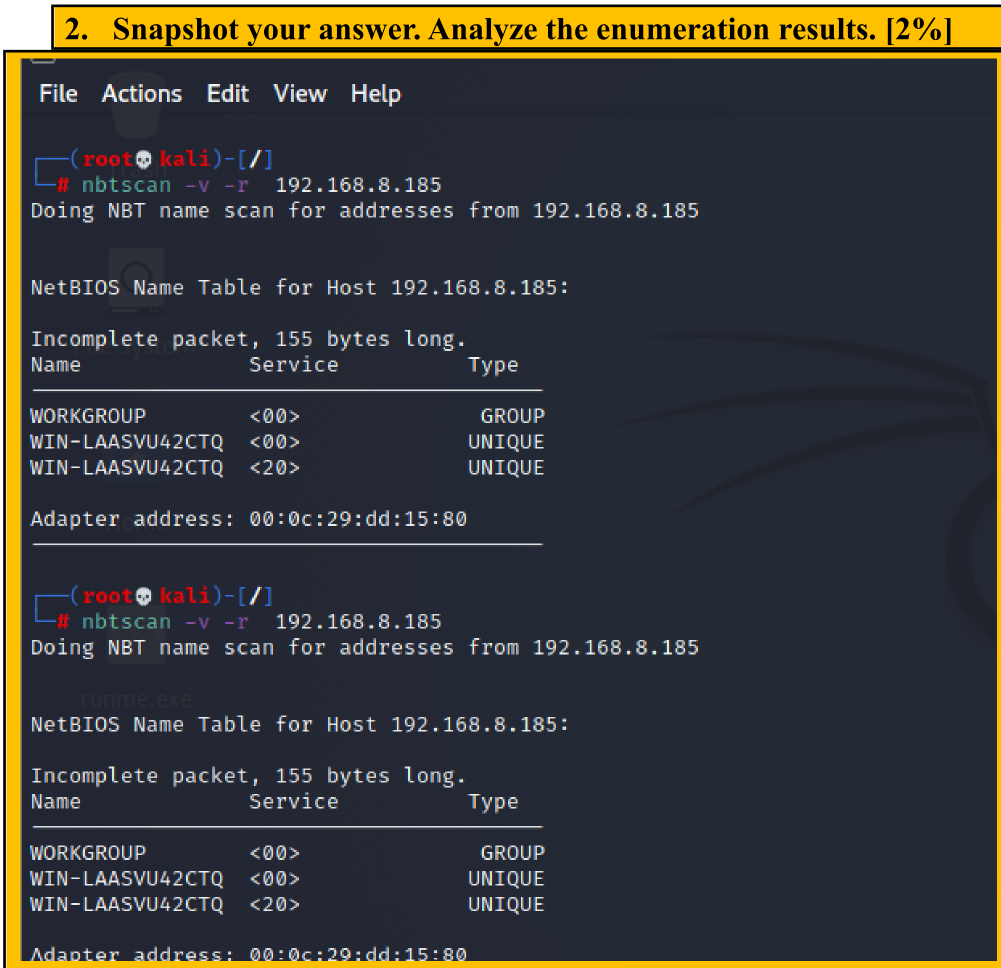
Netbios enumeration

Target: Windows Server 2016/2019

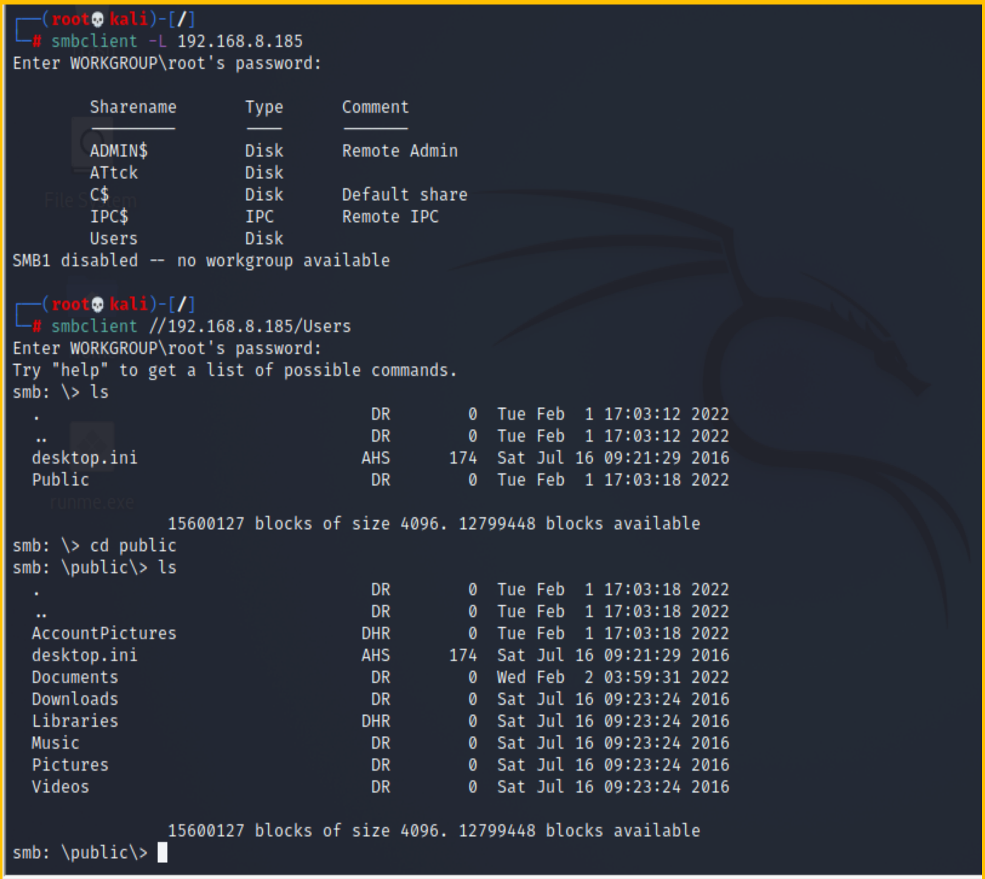
1. Recall from Lab Activity 1 in Lab 5, propose another Netbios Enumeration tool and try to enumerate Windows Server 2016 or 2019.

Prepared by: SY Ooi

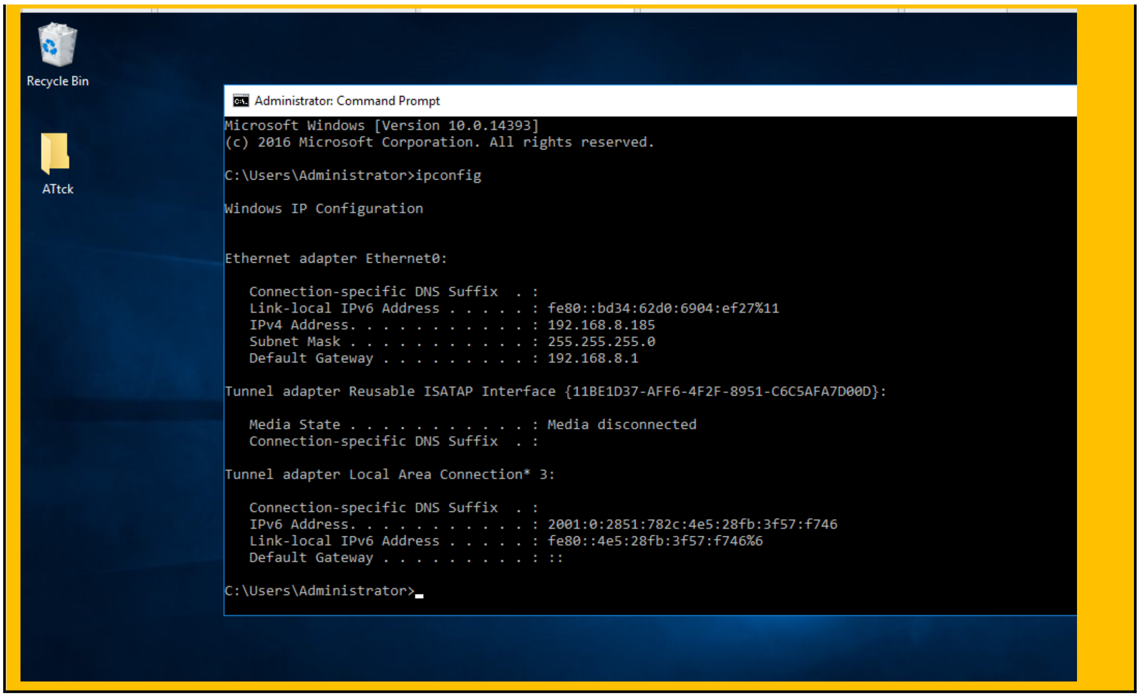
2. Snapshot your answer. Analyze the enumeration results. [2%]



```
┌──(root💀kali)-[/]
└─# nbtscan -v -r  192.168.8.185
Doing NBT name scan for addresses from 192.168.8.185


NetBIOS Name Table for Host 192.168.8.185:

Incomplete packet, 155 bytes long.
Name                Service             Type
----------------------------------------
WORKGROUP           <00>                 GROUP
WIN-LAASVU42CTQ     <00>                UNIQUE
WIN-LAASVU42CTQ     <20>                UNIQUE

Adapter address: 00:0c:29:dd:15:80
----------------------------------------

┌──(root💀kali)-[/]
└─# nbtscan -v -r  192.168.8.185
Doing NBT name scan for addresses from 192.168.8.185


NetBIOS Name Table for Host 192.168.8.185:

Incomplete packet, 155 bytes long.
Name                Service             Type
----------------------------------------
WORKGROUP           <00>                 GROUP
WIN-LAASVU42CTQ     <00>                UNIQUE
WIN-LAASVU42CTQ     <20>                UNIQUE

Adapter address: 00:0c:29:dd:15:80
```



```
┌──(root💀kali)-[/]
└─# smbclient -L 192.168.8.185
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        ATtck           Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
SMB1 disabled -- no workgroup available

┌──(root💀kali)-[/]
└─# smbclient //192.168.8.185/Users
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Tue Feb  1 17:03:12 2022
  ..                                 DR        0  Tue Feb  1 17:03:12 2022
  desktop.ini                       AHS      174  Sat Jul 16 09:21:29 2016
  Public                             DR        0  Tue Feb  1 17:03:18 2022

                15600127 blocks of size 4096. 12799448 blocks available
smb: \> cd public
smb: \public\> ls
  .                                  DR        0  Tue Feb  1 17:03:18 2022
  ..                                 DR        0  Tue Feb  1 17:03:18 2022
  AccountPictures                   DHR        0  Tue Feb  1 17:03:18 2022
  desktop.ini                       AHS      174  Sat Jul 16 09:21:29 2016
  Documents                          DR        0  Wed Feb  2 03:59:31 2022
  Downloads                          DR        0  Sat Jul 16 09:23:24 2016
  Libraries                         DHR        0  Sat Jul 16 09:23:24 2016
  Music                              DR        0  Sat Jul 16 09:23:24 2016
  Pictures                           DR        0  Sat Jul 16 09:23:24 2016
  Videos                             DR        0  Sat Jul 16 09:23:24 2016

                15600127 blocks of size 4096. 12799448 blocks available
smb: \public\> █
```



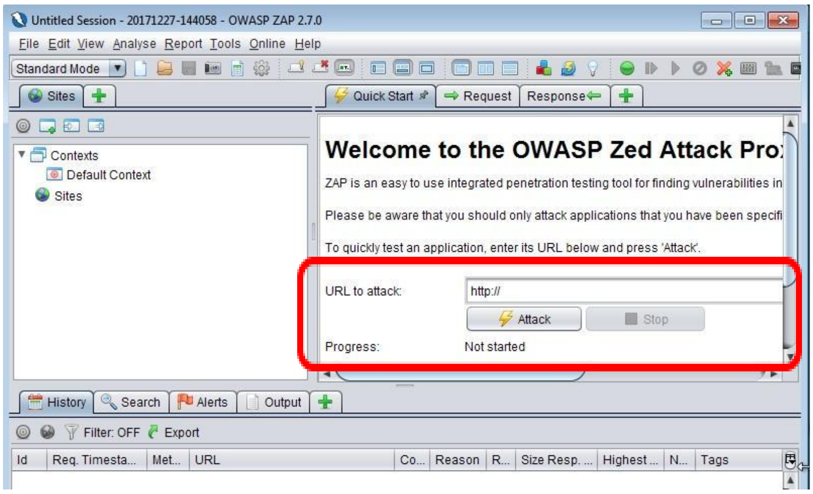
```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bd34:62d0:6904:ef27%11
   IPv4 Address. . . . . . . . . . . : 192.168.8.185
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.1

Tunnel adapter Reusable ISATAP Interface {11BE1D37-AFF6-4F2F-8951-C6C5AFA7D00D}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:4e5:28fb:3f57:f746
   Link-local IPv6 Address . . . . . : fe80::4e5:28fb:3f57:f746%6
   Default Gateway . . . . . . . . . : ::

C:\Users\Administrator>_
```

Vulnerability scanner

Host: Kali (VM)
Tool: OWASP Zed Attack Proxy (ZAP)
Target: Select 1 MMU Web Server IP (in this lab, please try on mmu.edu.my, mmls2.mmu.edu.my, and any other MMU web server)

1. Look for OWASP Zed Attack Proxy (ZAP) from Applications 3. Web Application Analysis owasp zap / ZAP.

2. Insert the target URL accordingly press ATTACK and observed the results.



Welcome to the OWASP Zed Attack Pro

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in

Please be aware that you should only attack applications that you have been specifi

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://

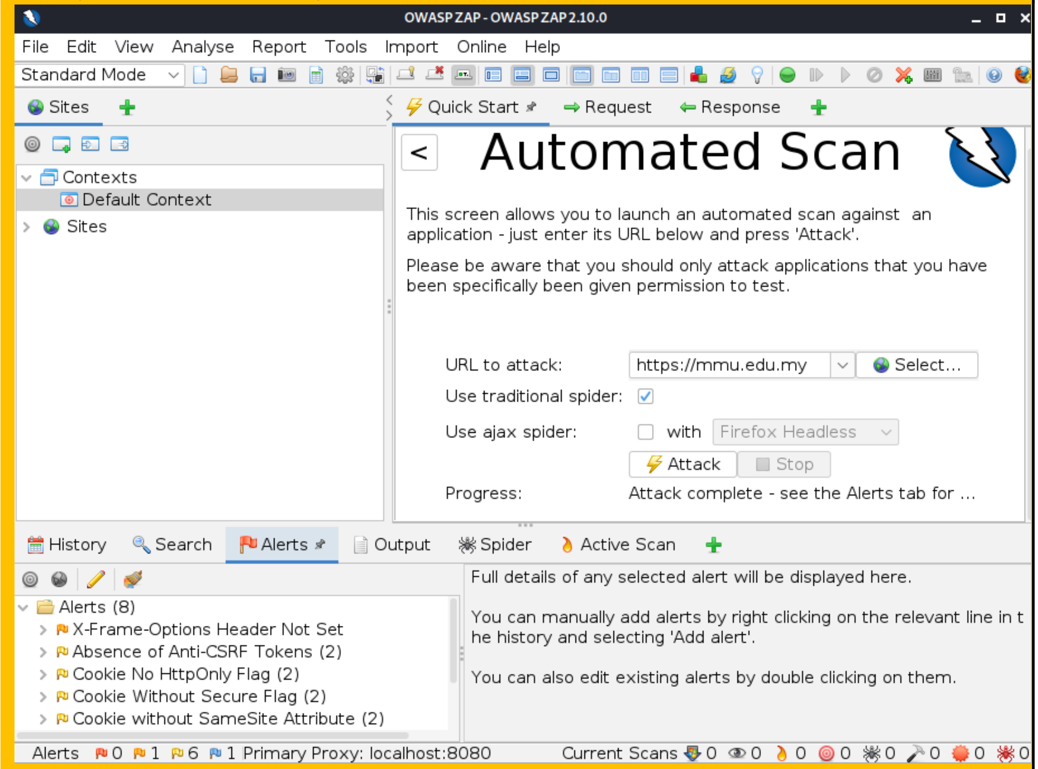
Attack   Stop

Progress: Not started

Prepared by: SY Ooi

3. Any vulnerability found?

Analyze and show me your result. [2%]



OWASP ZAP - OWASP ZAP 2.10.0

File Edit View Analyse Report Tools Import Online Help

Standard Mode

Sites

- Contexts
  - Default Context
- Sites

Quick Start Request Response

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://mmu.edu.my Select...

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Attack Stop

Progress: Attack complete - see the Alerts tab for ...

History Search Alerts Output Spider Active Scan

- Alerts (8)
  - X-Frame-Options Header Not Set
  - Absence of Anti-CSRF Tokens (2)
  - Cookie No HttpOnly Flag (2)
  - Cookie Without Secure Flag (2)
  - Cookie without SameSite Attribute (2)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

Alerts 0 1 6 1 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

There are multiple alerts, one of them is cookie without a secure flag which means that the cookie can be accessed via unencrypted connections.

Cookie no httponly flag: A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

x-frame options header is not set. : X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks

Zap also gives you how to fix the alerts with solutions.

Patch the vulnerable C program

Recall the **hello2.c** from Lab 7.

We need to patch hello2.c code. You can make in a new version, naming as hello3:

```
cp hello2.c hello2_fixed.c
```

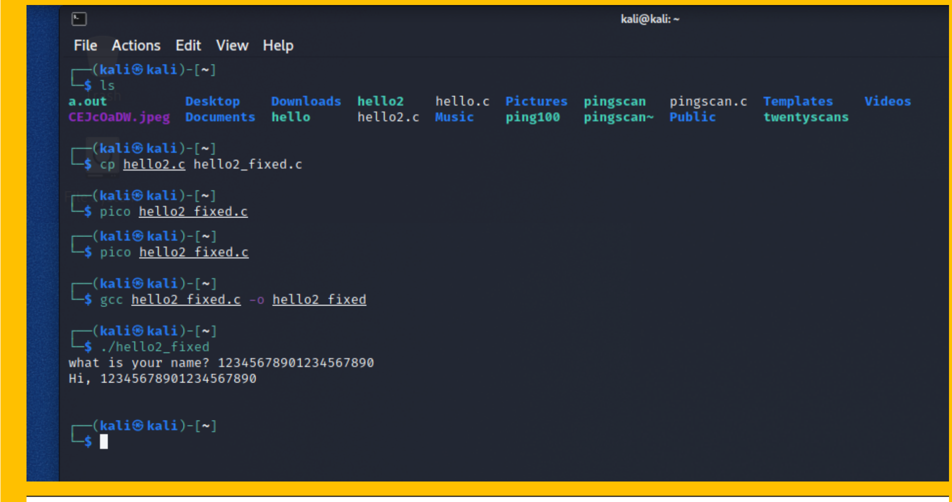
This makes a copy of **hello2.c** named **hello2_fixed.c**.

In the Kali Terminal window, enter this command, then press the Enter key:

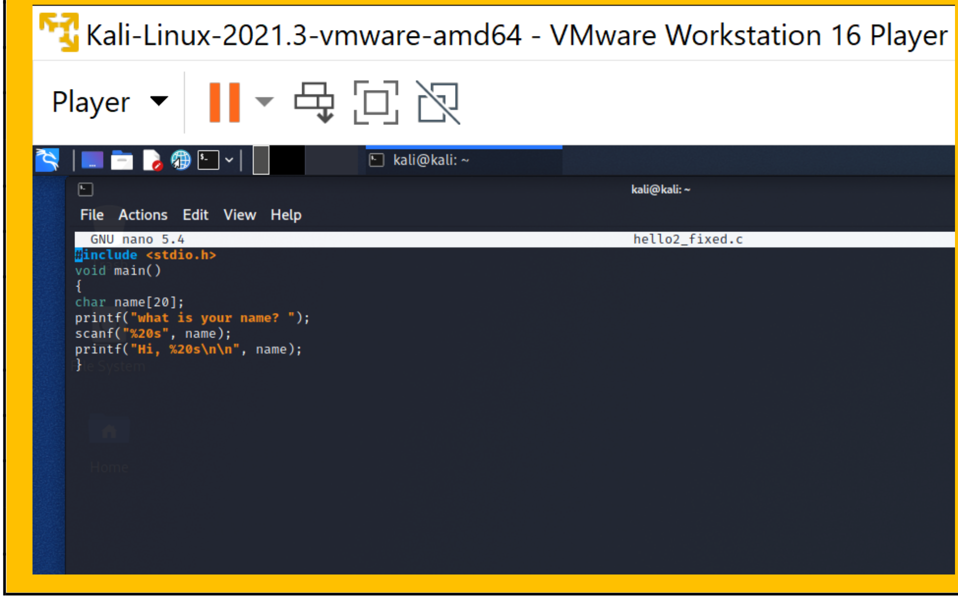
```
pico hello2_fixed.c
```

The pico editor opens.

Patch the code to avoid the buffer overflow. Snapshot your screen to prove that the buffer overflow will not occur again with this patched code. [2%]



```
┌──(kali㉿kali)-[~]
└─$ ls
a.out            Desktop    Downloads  hello2    hello.c  Pictures  pingscan   pingscan.c  Templates    Videos
CEJcOaDW.jpeg    Documents  hello      hello2.c  Music    ping100   pingscan~  Public      twentyscans

┌──(kali㉿kali)-[~]
└─$ cp hello2.c hello2_fixed.c

┌──(kali㉿kali)-[~]
└─$ pico hello2_fixed.c

┌──(kali㉿kali)-[~]
└─$ pico hello2_fixed.c

┌──(kali㉿kali)-[~]
└─$ gcc hello2_fixed.c -o hello2_fixed

┌──(kali㉿kali)-[~]
└─$ ./hello2_fixed
what is your name? 12345678901234567890
Hi, 12345678901234567890


┌──(kali㉿kali)-[~]
└─$ 
```


Kali-Linux-2021.3-vmware-amd64 - VMware Workstation 16 Player
Player
kali@kali: ~
kali@kali: ~
File Actions Edit View Help

```
  GNU nano 5.4                                                  hello2_fixed.c
#include <stdio.h>
void main()
{
char name[20];
printf("what is your name? ");
scanf("%20s", name);
printf("Hi, %20s\n\n", name);
}
```

Recalling the hello2.c from Lab 7. First, creating a copy of hello2.c named hello2_fixed.c. So that we can fix the hello2 program to avoid the machine being exposed by hackers. The problem is that it takes the name from typed input and puts it in the name string, but the names longer than 10 characters will cause user-input data to overwrite parts of memory that were not intended to store data, making the program crash. This is a Buffer Overflow. When users type in the prompt “12345678901234567890” , It will show an error message. *** stack smashing detected *** OR *** Segmentation fault ***

Therefore, to fix this buffer overflow, in the pico editor, the string size limit needs to be changed from **“%s”** to **“%20s”.** This is because the name string has a size limit; it only has enough room for 10 characters only.

Familiarize with *Capture-the-Flag (CTF)*

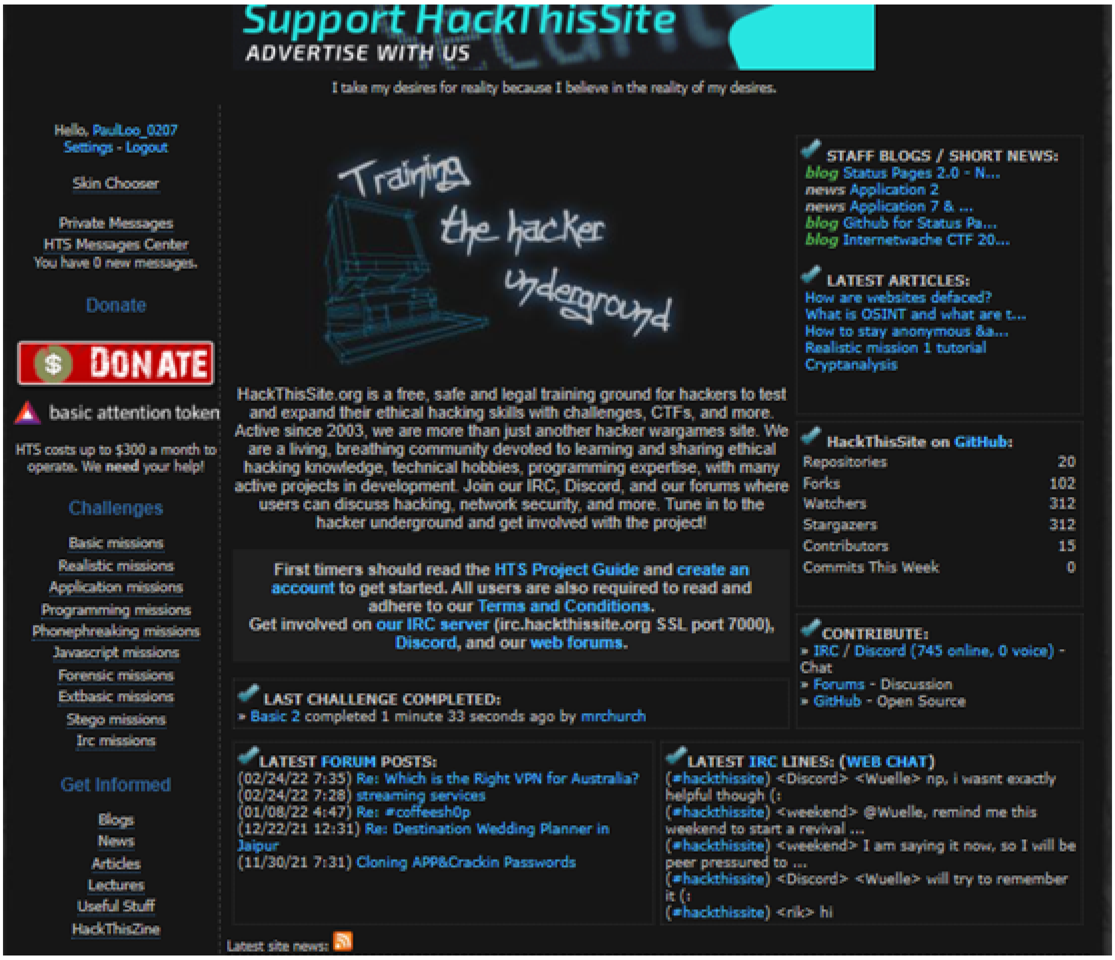
Platform: Hack This Site (https://hackthissite.org/)

1. Be warned: in this project, you will be learning real criminal techniques from real criminals. Do not reveal your real name or address or trust these people.

2. Open a browser and go to **hackthissite.org**

3. In the upper left, click on the word **register**.

4. Fill out the form to create an account. Do **NOT** give these people your real name or any correct information, not even a real email address (you may create another new email, mainly for this game).



I take my desires for reality because I believe in the reality of my desires.

HackThisSite.org is a free, safe and legal training ground for hackers to test and expand their ethical hacking skills with challenges, CTFs, and more. Active since 2003, we are more than just another hacker wargames site. We are a living, breathing community devoted to learning and sharing ethical hacking knowledge, technical hobbies, programming expertise, with many active projects in development. Join our IRC, Discord, and our forums where users can discuss hacking, network security, and more. Tune in to the hacker underground and get involved with the project!

First timers should read the HTS Project Guide and create an account to get started. All users are also required to read and adhere to our Terms and Conditions.
Get involved on our IRC server (irc.hackthissite.org SSL port 7000), Discord, and our web forums.

LAST CHALLENGE COMPLETED:
» Basic 2 completed 1 minute 33 seconds ago by mrchurch

STAFF BLOGS / SHORT NEWS:
blog Status Pages 2.0 - N...
news Application 2
news Application 7 & ...
blog Github for Status Pa...
blog Internetwache CTF 20...

LATEST ARTICLES:
How are websites defaced?
What is OSINT and what are t...
How to stay anonymous &a...
Realistic mission 1 tutorial
Cryptanalysis

HackThisSite on GitHub:

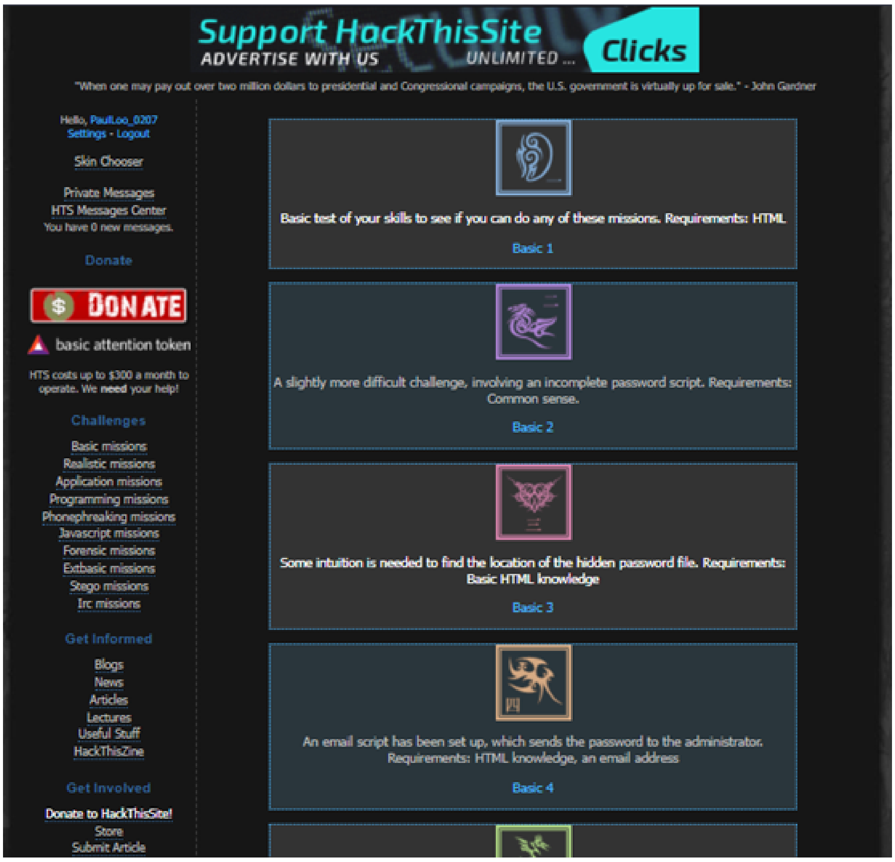
Repositories	20
Forks	102
Watchers	312
Stargazers	312
Contributors	15
Commits This Week	0

CONTRIBUTE:
» IRC / Discord (745 online, 0 voice) - Chat
» Forums - Discussion
» GitHub - Open Source

LATEST FORUM POSTS:
(02/24/22 7:35) Re: Which is the Right VPN for Australia?
(02/24/22 7:28) streaming services
(01/08/22 4:47) Re: #coffeesh0p
(12/22/21 12:31) Re: Destination Wedding Planner in Jaipur
(11/30/21 7:31) Cloning APP&Crackin Passwords

LATEST IRC LINES: (WEB CHAT)
(#hackthissite) <Discord> <Wuelle> np, i wasnt exactly helpful though (:
(#hackthissite) <weekend> @Wuelle, remind me this weekend to start a revival ...
(#hackthissite) <weekend> I am saying it now, so I will be peer pressured to ...
(#hackthissite) <Discord> <Wuelle> will try to remember it (:
(#hackthissite) <rik> hi

5. After creating your account, log in. Then, on the left tab of the main page, in the **challenges** section, click "**Basic Missions**"



"When one may pay out over two million dollars to presidential and Congressional campaigns, the U.S. government is virtually up for sale." - John Gardner

You have 0 new messages.

HTS costs up to $300 a month to operate. We **need** your help!

Basic test of your skills to see if you can do any of these missions. Requirements: HTML

Basic 1

A slightly more difficult challenge, involving an incomplete password script. Requirements: Common sense.

Basic 2

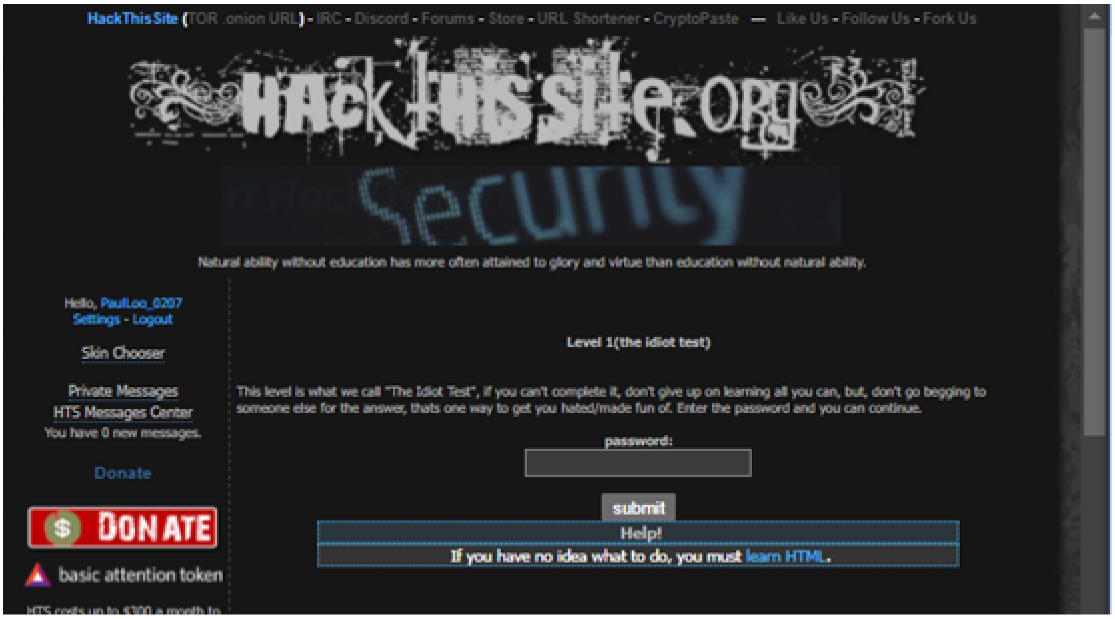
Some intuition is needed to find the location of the hidden password file. Requirements: Basic HTML knowledge

Basic 3

An email script has been set up, which sends the password to the administrator. Requirements: HTML knowledge, an email address

Basic 4

6. There is a Help! Link at the bottom which can help you.



Natural ability without education has more often attained to glory and virtue than education without natural ability.

You have 0 new messages.

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:

Help!

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

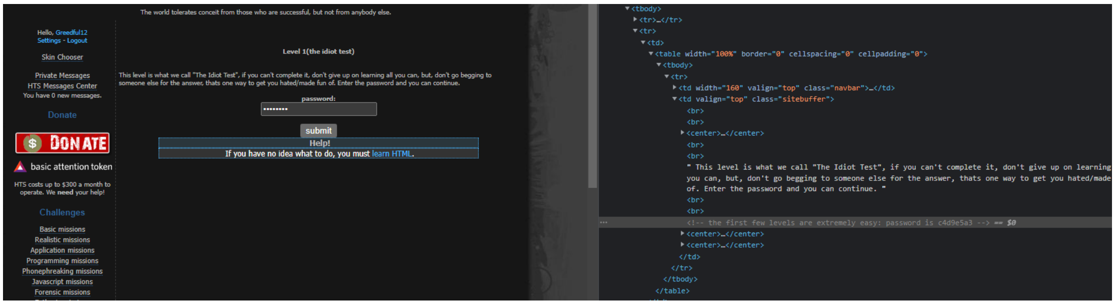
HTS costs up to $300 a month to

Prepared by: SY Ooi

7. The Web hacking challenges includes **eleven** Basic Web Challenges. Solve at least **eight (8)** puzzles. You get **0.5 point** per level completed.

Show your steps on how you solved the challenge. [4%]
Notes: your account name must be shown when you snapshot your answer – to prove that you attempted the challenges/ puzzles by using your account.

Challenge 1 > Right click inspect and you find the password which is c4d9e5a3



The world tolerates conceit from those who are successful, but not from anybody else.

Level 1(the idiot test)

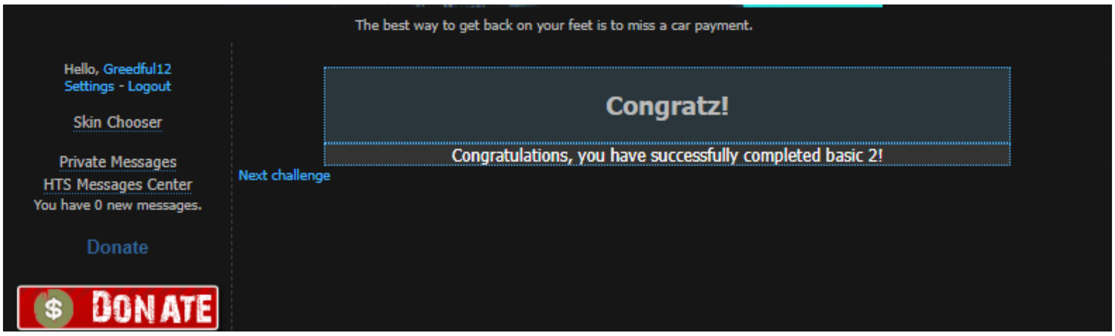
This level is what we call "The Idiot Test", if you can't complete it, don't give up on learning all you can, but, don't go begging to someone else for the answer, thats one way to get you hated/made fun of. Enter the password and you can continue.

password: ••••••••

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

```
▼<tbody>
  ▶<tr>…</tr>
  ▼<tr>
    ▼<td>
      ▼<table width="100%" border="0" cellspacing="0" cellpadding="0">
        ▼<tbody>
          ▼<tr>
            ▶<td width="160" valign="top" class="navbar">…</td>
            ▼<td valign="top" class="sitebuffer">
              <br>
              <br>
             ▶<center>…</center>
              <br>
              <br>
              " This level is what we call "The Idiot Test", if you can't complete it, don't give up on learning
              you can, but, don't go begging to someone else for the answer, thats one way to get you hated/made
              of. Enter the password and you can continue. "
              <br>
              <br>
...           <!-- the first few levels are extremely easy: password is c4d9e5a3 --> == $0
             ▶<center>…</center>
             ▶<center>…</center>
            </td>
          </tr>
        </tbody>
      </table>
```

Challenge 2 > Since he neglected to upload the file, you can login with an empty password

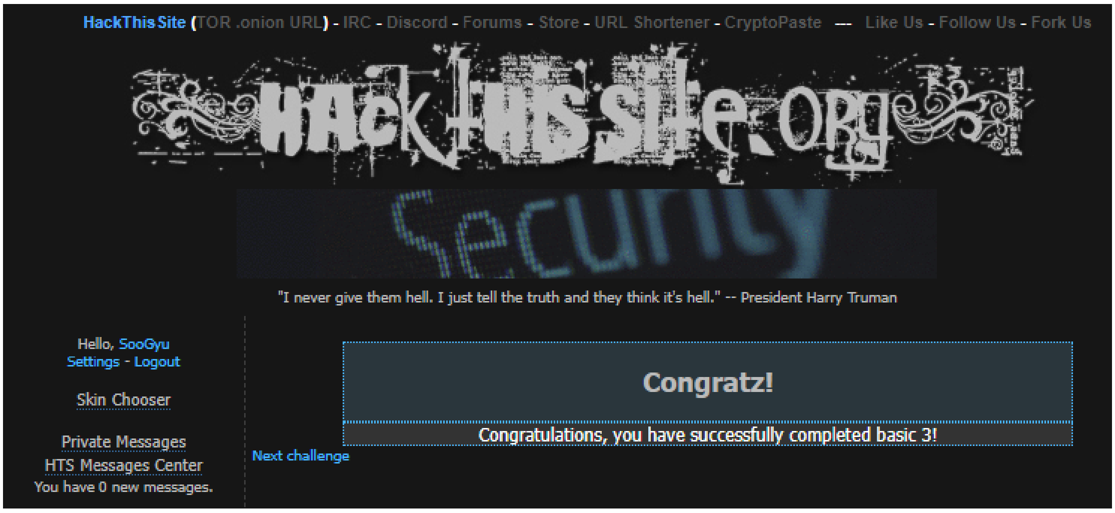


The best way to get back on your feet is to miss a car payment.

Congratz!

Congratulations, you have successfully completed basic 2!

Challenge 3 >



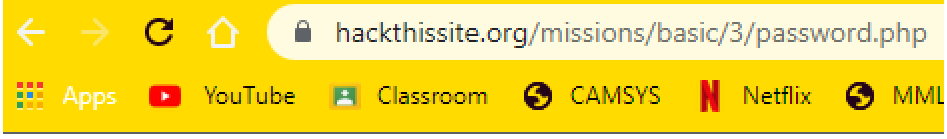
"I never give them hell. I just tell the truth and they think it's hell." -- President Harry Truman

Congratz!

Congratulations, you have successfully completed basic 3!

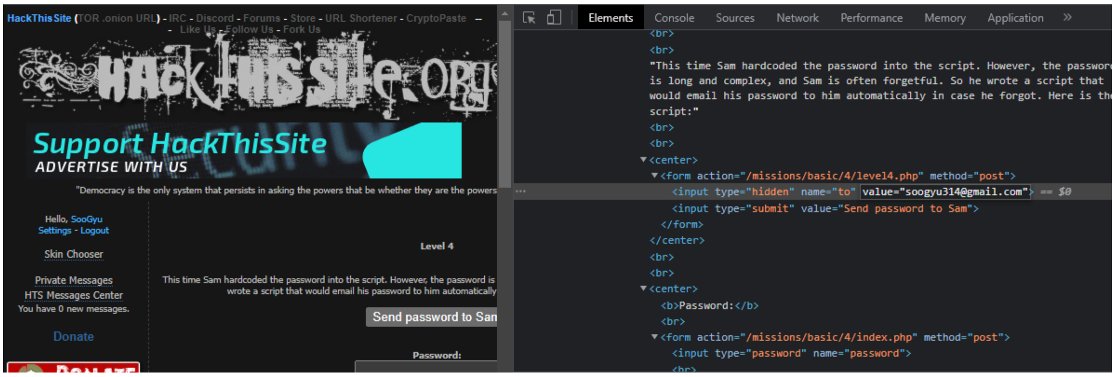
Solution 3 >

password.php added at the end of the url


hackthissite.org/missions/basic/3/password.php

```
36511067
```

Challenge 4 >



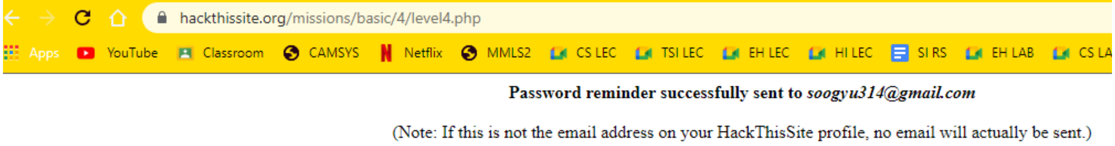
"Democracy is the only system that persists in asking the powers that be whether they are the powers

Level 4

This time Sam hardcoded the password into the script. However, the password is
wrote a script that would email his password to him automatically

Password:

```
<br>
<br>
"This time Sam hardcoded the password into the script. However, the passwor
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 th
script:"
<br>
<br>
▼<center>
  ▼<form action="/missions/basic/4/level4.php" method="post">
      <input type="hidden" name="to" value="soogyu314@gmail.com"> == $0
      <input type="submit" value="Send password to Sam">
    </form>
  </center>
  <br>
  <br>
▼<center>
    <b>Password:</b>
    <br>
  ▼<form action="/missions/basic/4/index.php" method="post">
      <input type="password" name="password">
      <br>
```

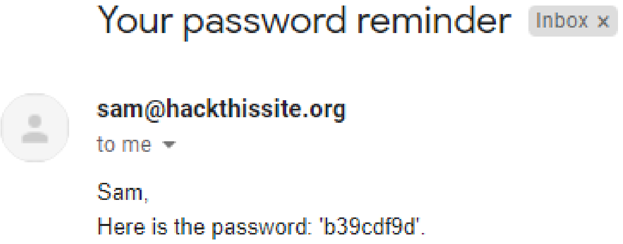

hackthissite.org/missions/basic/4/level4.php

Password reminder successfully sent to ***soogyu314@gmail.com***

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

Solution 4 >

personal email is edited into the source code for the email to be sent

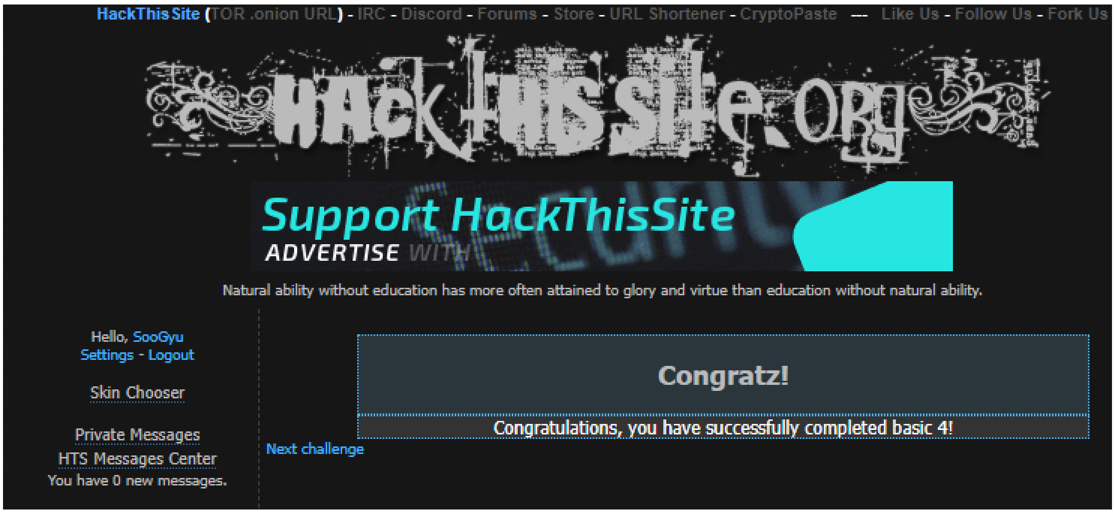

Your password reminder

sam@hackthissite.org

to me

Sam,

Here is the password: 'b39cdf9d'.



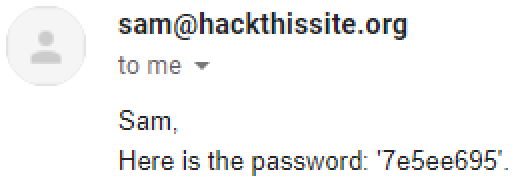
Natural ability without education has more often attained to glory and virtue than education without natural ability.

Congratz!

Congratulations, you have successfully completed basic 4!

Prepared by: SY Ooi

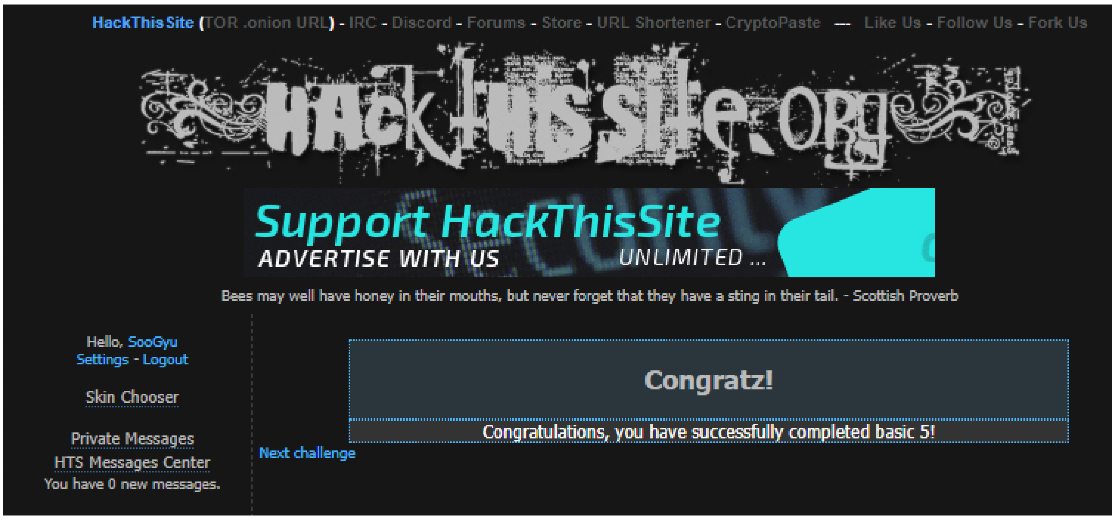
Challenge 5 is equivalent to Challenge 4


sam@hackthissite.org

to me

Sam,

Here is the password: '7e5ee695'.



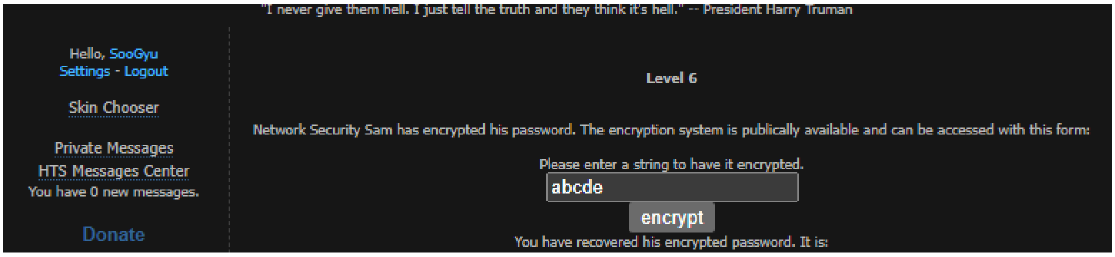
Bees may well have honey in their mouths, but never forget that they have a sting in their tail. - Scottish Proverb

You have 0 new messages.

Congratz!

Congratulations, you have successfully completed basic 5!

Challenge 6 >



"I never give them hell. I just tell the truth and they think it's hell." -- President Harry Truman

You have 0 new messages.

Level 6

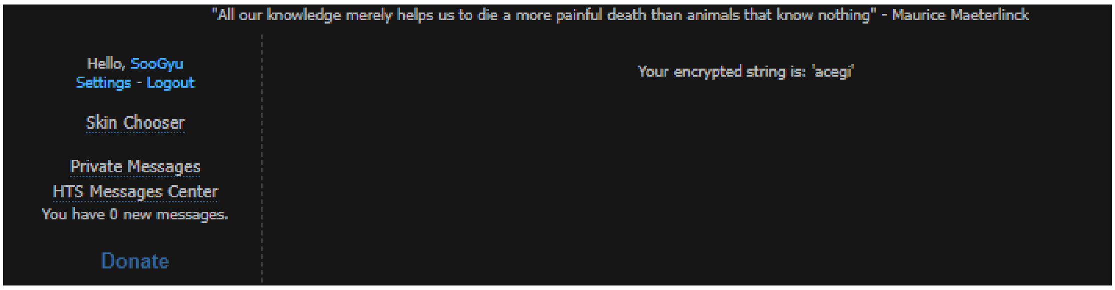
Network Security Sam has encrypted his password. The encryption system is publically available and can be accessed with this form:

Please enter a string to have it encrypted.

abcde

You have recovered his encrypted password. It is:

Solution 6 > Assuming the password we have is "abcde", and we click on the encrypt button



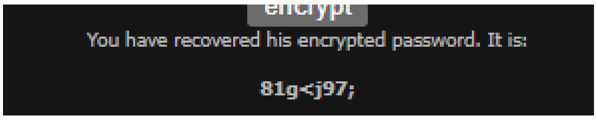
"All our knowledge merely helps us to die a more painful death than animals that know nothing" - Maurice Maeterlinck

You have 0 new messages.

Your encrypted string is: 'acegi'

As we can see that there is a pattern of increment in string value (ASCII) where the string value is increased in a pattern of string position. For example, 'a' is in the position of 0 in computer language. Therefore, 'a' + 0 in (ASCII) is equalled to 'a', whereas 'b' + (position of 1) = 'c', thus, so forth. That is how we obtained the encrypted string equal to 'acegi'.

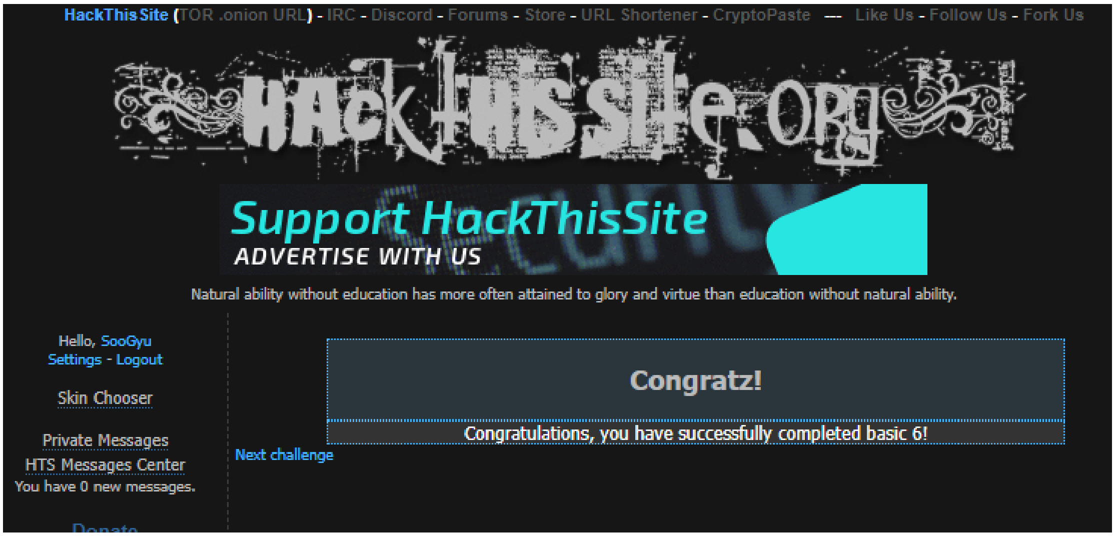
Prepared by: SY Ooi



You have recovered his encrypted password. It is:

81g<j97;

Since we have this pattern of encryption, we can decrypt the encrypted password as simply as subtracting the position value. For example, 8 is at the position of zero, so we subtract 8 with 0 which equals to 8; 1 is at position 1 so 1-1 = 0; ‘g’ is at the position of 2 so ‘g’ reverse sequence by 2 is ‘e’; ‘<’ requires reference of ASCII table, (https://www.asciitable.com/) we may see that ‘<’ has the decimal value of 60. By subtracting 60 - 3, we get value 57, which refers to ‘9’ in the ASCII table.
As per reference, the decrypted message will be, **80e9f414**



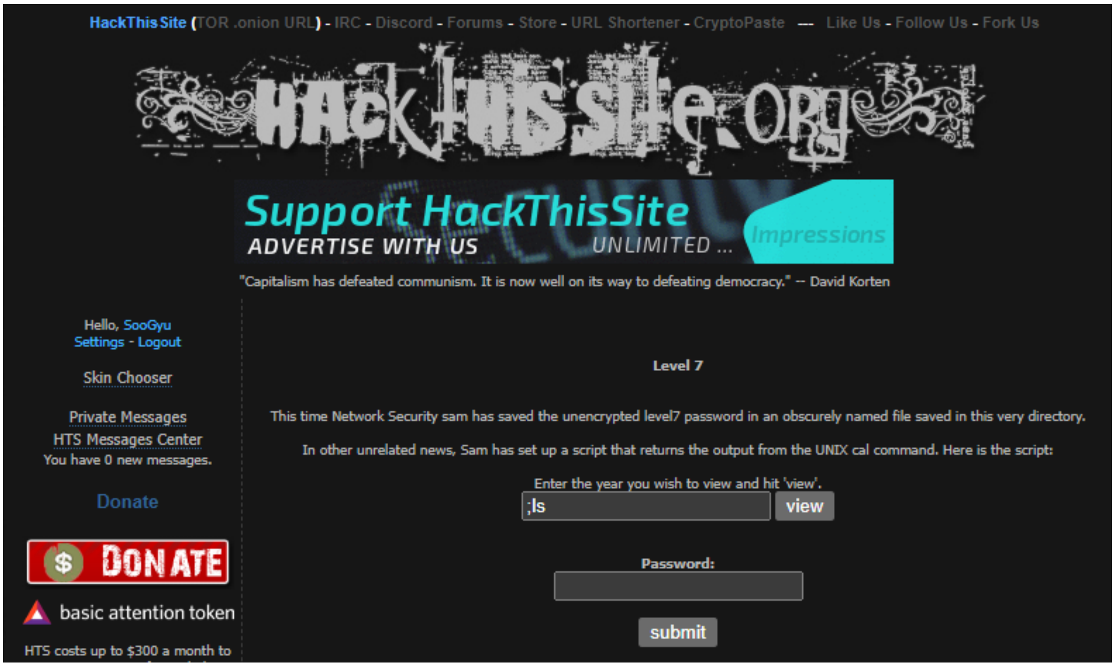
Natural ability without education has more often attained to glory and virtue than education without natural ability.

You have 0 new messages.

Congratz!

Congratulations, you have successfully completed basic 6!

Challenge 7 >



"Capitalism has defeated communism. It is now well on its way to defeating democracy." -- David Korten

You have 0 new messages.

HTS costs up to $300 a month to

Level 7

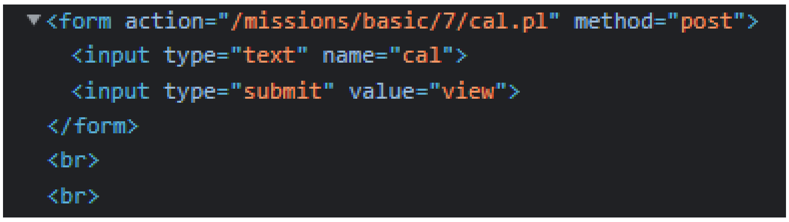
This time Network Security sam has saved the unencrypted level7 password in an obscurely named file saved in this very directory.

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'.

;ls

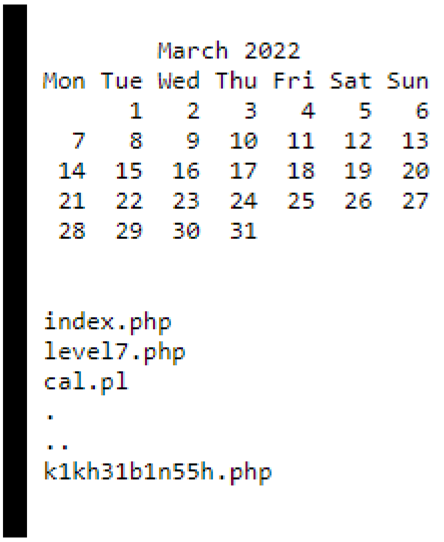
Password:



```
▼<form action="/missions/basic/7/cal.pl" method="post">
   <input type="text" name="cal">
   <input type="submit" value="view">
 </form>
 <br>
 <br>
```

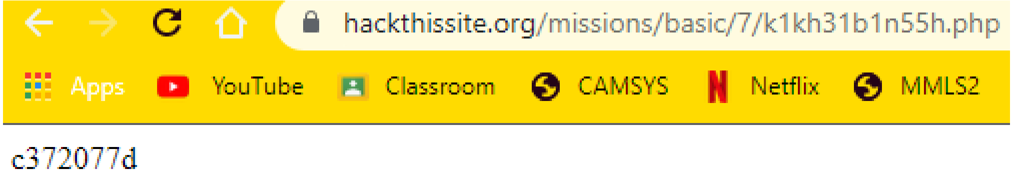
Since the form did not specify the input type , any special characters can be input even command characters. Thus, we can insert commands to retrieve and trigger information from the site. This is a best example of an injection attack.

Since there is a hint that the system is using Unix command, therefore we can input ‘;ls’ to list the files within this site.



```
        March 2022
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
```

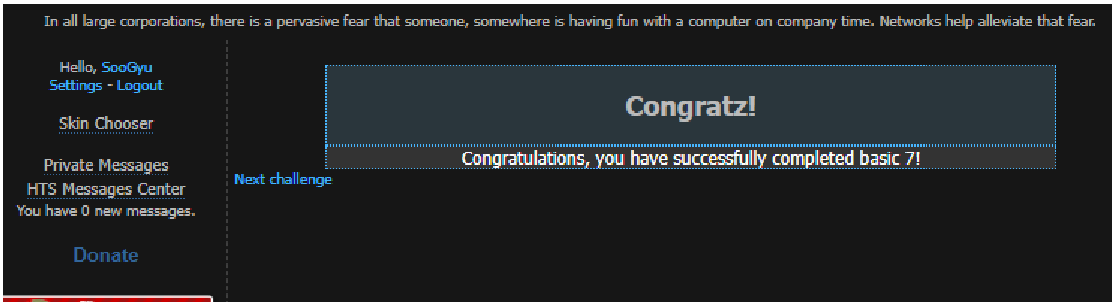
As shown, there is an obscurely named file at the bottom section.



hackthissite.org/missions/basic/7/k1kh31b1n55h.php

c372077d

After inserting the weird php into the url, the password is shown.



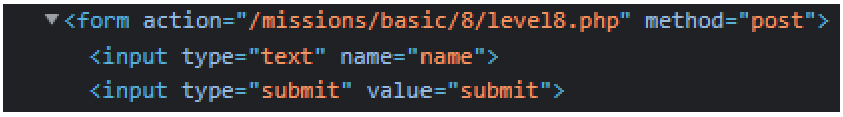
In all large corporations, there is a pervasive fear that someone, somewhere is having fun with a computer on company time. Networks help alleviate that fear.

Congratz!

Congratulations, you have successfully completed basic 7!

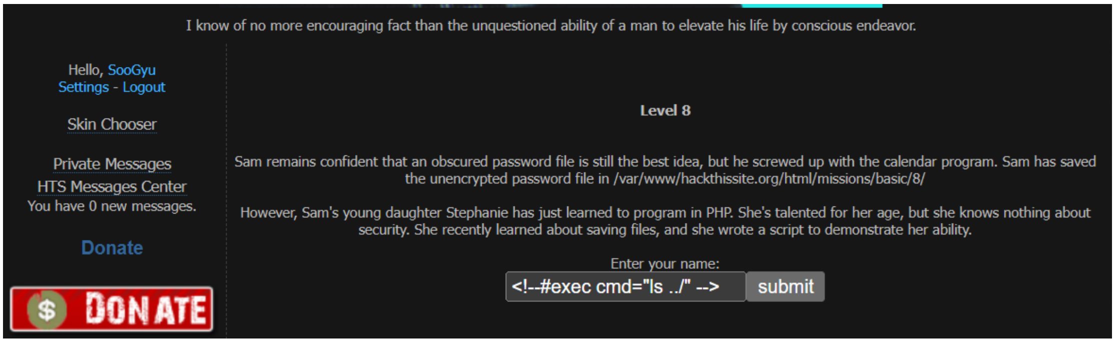
Prepared by: SY Ooi

Challenge 8 >



```
▼<form action="/missions/basic/8/level8.php" method="post">
    <input type="text" name="name">
    <input type="submit" value="submit">
```

Based on this screenshot of codes, we can see that the developer hasn't restricted special character inputs. Therefore, we can perform SSI injection attack.



I know of no more encouraging fact than the unquestioned ability of a man to elevate his life by conscious endeavor.

Hello, SooGyu
Settings - Logout

Skin Chooser

Private Messages
HTS Messages Center
You have 0 new messages.

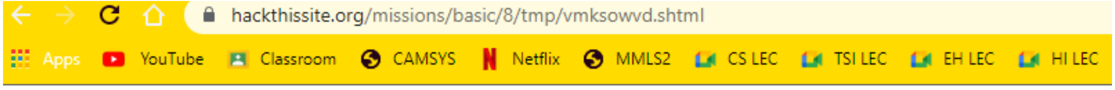
Donate

Level 8

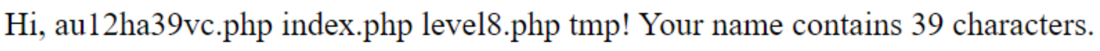
Sam remains confident that an obscured password file is still the best idea, but he screwed up with the calendar program. Sam has saved the unencrypted password file in /var/www/hackthissite.org/html/missions/basic/8/

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.

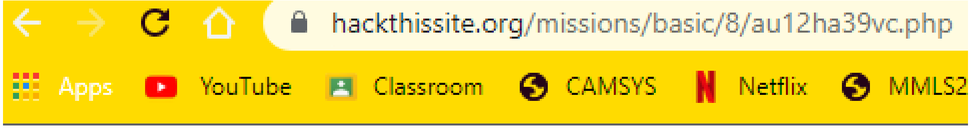
Enter your name: <!--#exec cmd="ls ../" -->



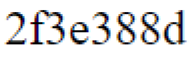
hackthissite.org/missions/basic/8/tmp/vmksowvd.shtml



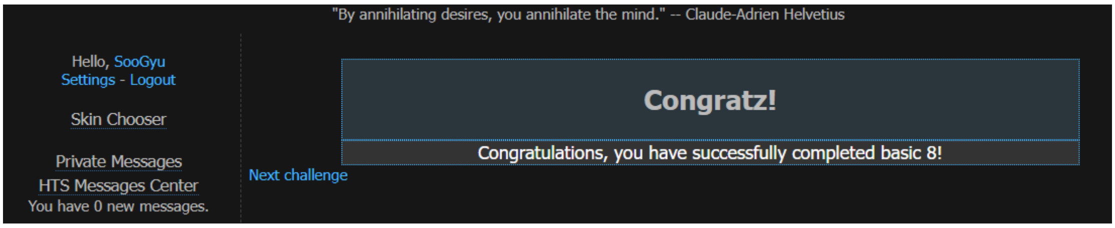
Hi, au12ha39vc.php index.php level8.php tmp! Your name contains 39 characters.



hackthissite.org/missions/basic/8/au12ha39vc.php



2f3e388d



"By annihilating desires, you annihilate the mind." -- Claude-Adrien Helvetius

Hello, SooGyu
Settings - Logout

Skin Chooser

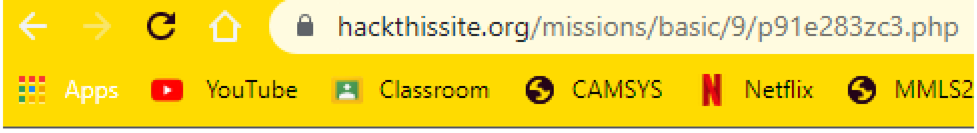
Private Messages
HTS Messages Center
You have 0 new messages.

Congratz!

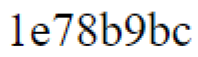
Congratulations, you have successfully completed basic 8!

Next challenge

Challenge 9 >

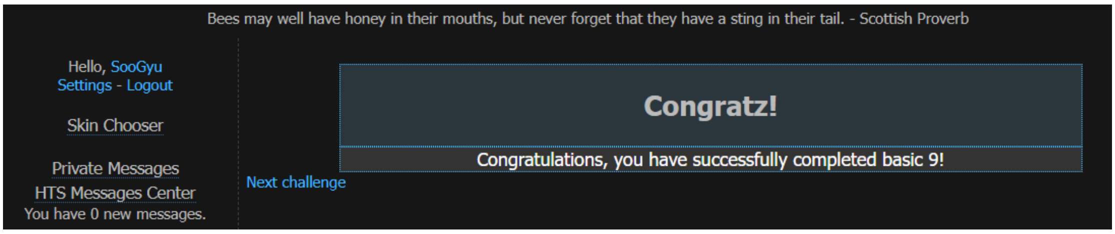


hackthissite.org/missions/basic/9/p91e283zc3.php



1e78b9bc

In this mission, there is no input box in the site, therefore, we went back to mission 8's input box to paste the command "**<!--#exec cmd="ls ../../9" -->**".
../../9 stands for website name/ sub file/ subfile/9



Bees may well have honey in their mouths, but never forget that they have a sting in their tail. - Scottish Proverb

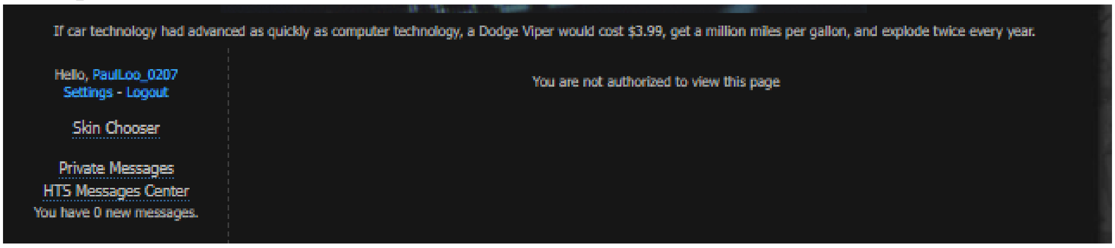
Hello, SooGyu

Congratz!

Congratulations, you have successfully completed basic 9!

Challenge 10 >

Enter password

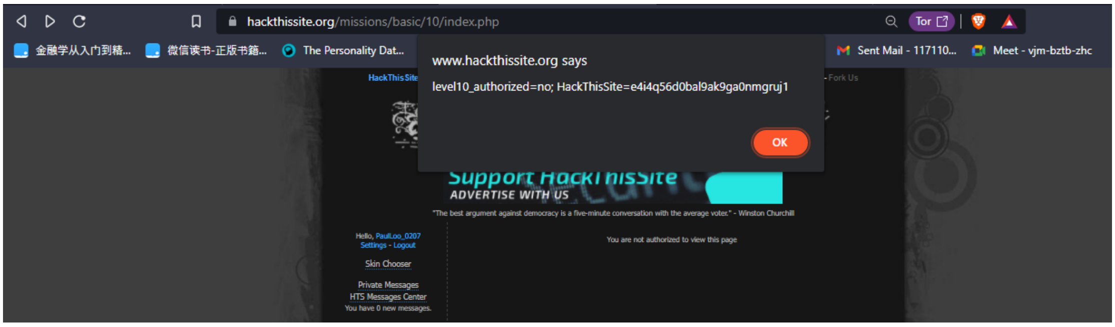


If car technology had advanced as quickly as computer technology, a Dodge Viper would cost $3.99, get a million miles per gallon, and explode twice every year.

Hello, PaulLoo_0207

You are not authorized to view this page

Enter javascript:alert(document.cookie);



hackthissite.org/missions/basic/10/index.php

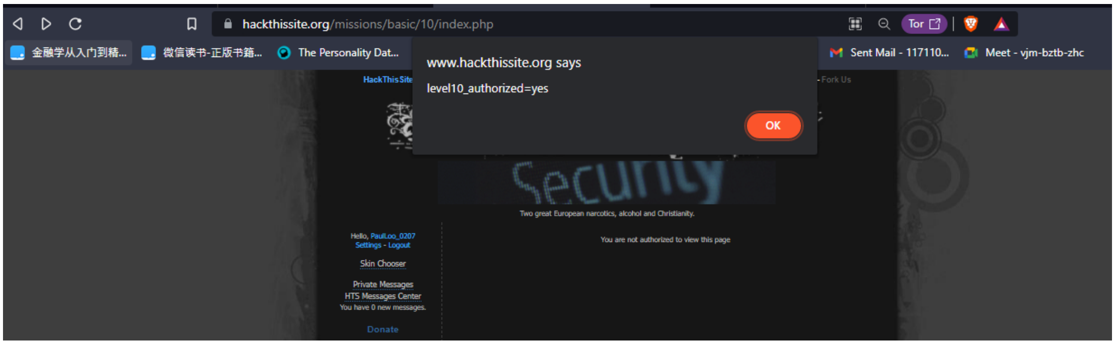
www.hackthissite.org says

level10_authorized=no; HackThisSite=e4i4q56d0bal9ak9ga0nmgruj1

"The best argument against democracy is a five-minute conversation with the average voter." - Winston Churchill

You are not authorized to view this page

Enter javascript:alert(document.cookie="level10_authorized=yes");



hackthissite.org/missions/basic/10/index.php

www.hackthissite.org says

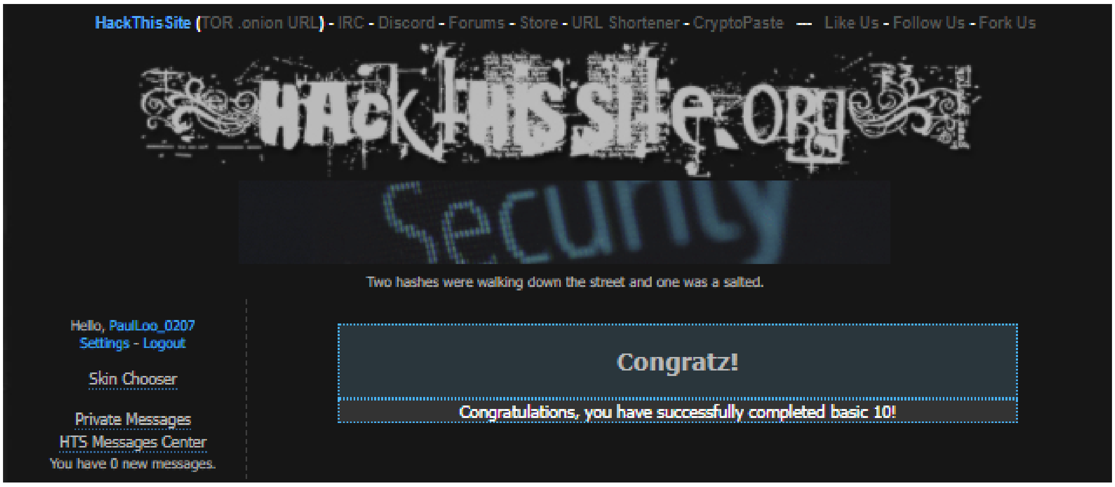
level10_authorized=yes

Two great European narcotics, alcohol and Christianity.

You are not authorized to view this page

Prepared by: SY Ooi

Reload and the it submitted successfully


HackThisSite (TOR .onion URL) - IRC - Discord - Forums - Store - URL Shortener - CryptoPaste — Like Us - Follow Us - Fork Us
HackThisSite.org
Security

Two hashes were walking down the street and one was a salted.

Hello, PaulLoo_0207
Settings - Logout

Skin Chooser

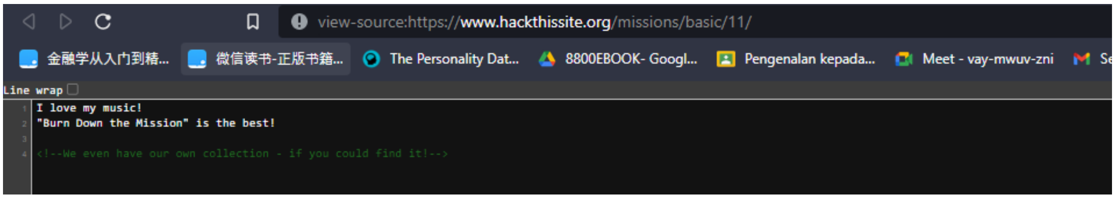
Private Messages
HTS Messages Center
You have 0 new messages.

Congratz!

Congratulations, you have successfully completed basic 10!

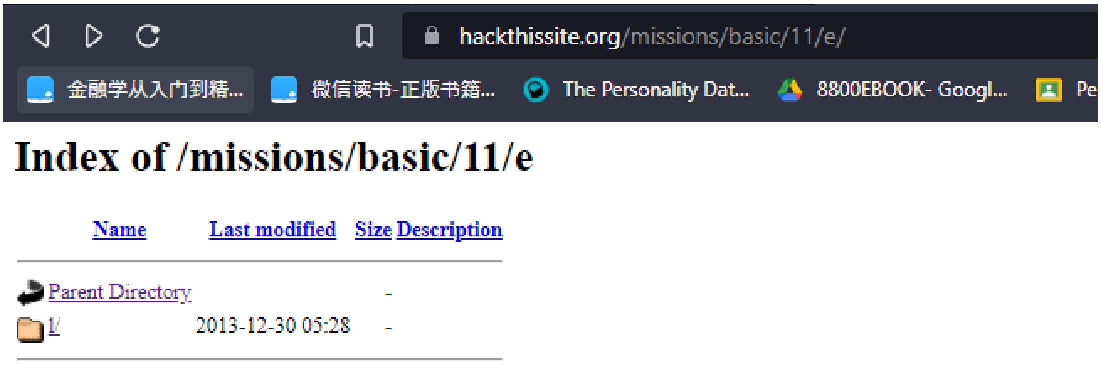
Challenge 11 >

View page source


view-source:https://www.hackthissite.org/missions/basic/11/
金融学从入门到精... 微信读书-正版书籍... The Personality Dat... 8800EBOOK- Googl... Pengenalan kepada... Meet - vay-mwuv-zni Se
Line wrap □

```
I love my music!
"Burn Down the Mission" is the best!

<!--We even have our own collection - if you could find it!-->
```

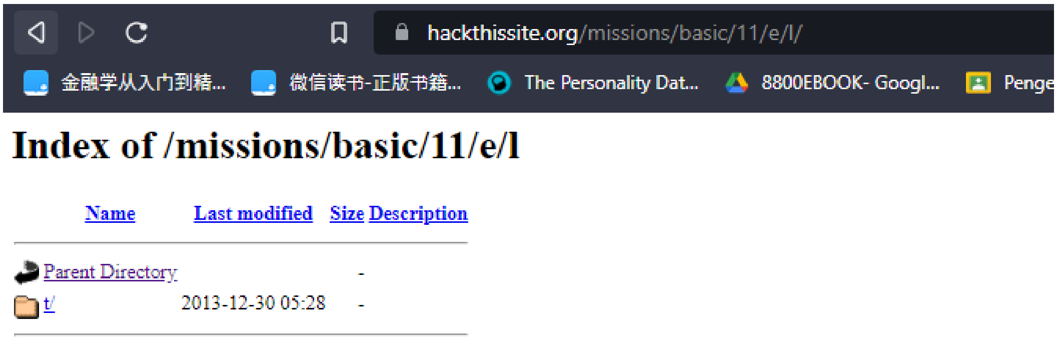
put e in the end


hackthissite.org/missions/basic/11/e/
金融学从入门到精... 微信读书-正版书籍... The Personality Dat... 8800EBOOK- Googl... Pe

Index of /missions/basic/11/e

Name	Last modified	Size	Description
Parent Directory		-	
l/	2013-12-30 05:28	-	

go with l

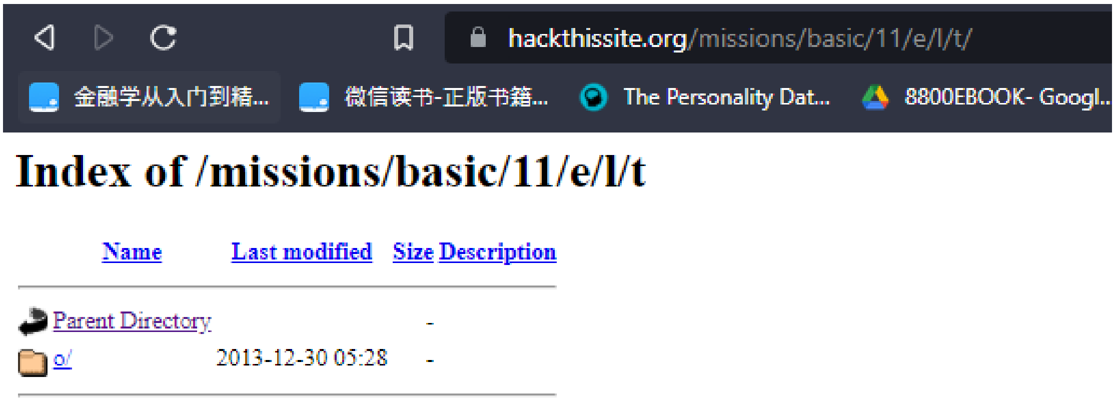

hackthissite.org/missions/basic/11/e/l/
金融学从入门到精... 微信读书-正版书籍... The Personality Dat... 8800EBOOK- Googl... Penge

Index of /missions/basic/11/e/l

Name	Last modified	Size	Description
Parent Directory		-	
t/	2013-12-30 05:28	-	

Prepared by: SY Ooi

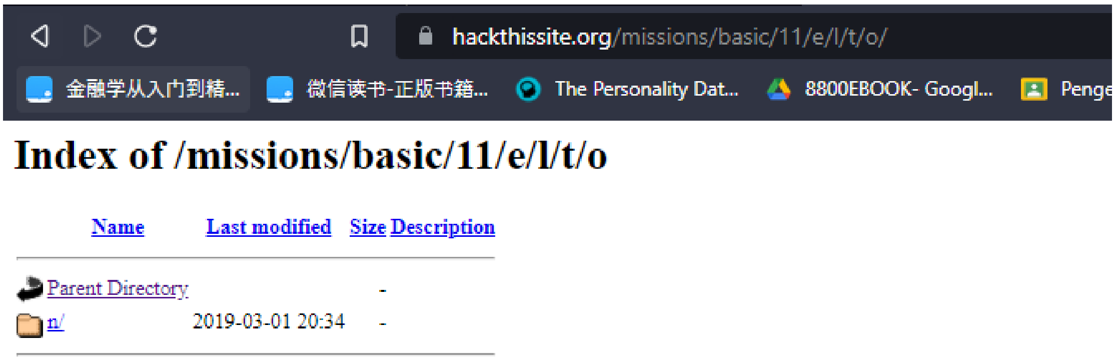
go with t



Index of /missions/basic/11/e/l/t

Name	Last modified	Size	Description
Parent Directory		-	
o/	2013-12-30 05:28	-	

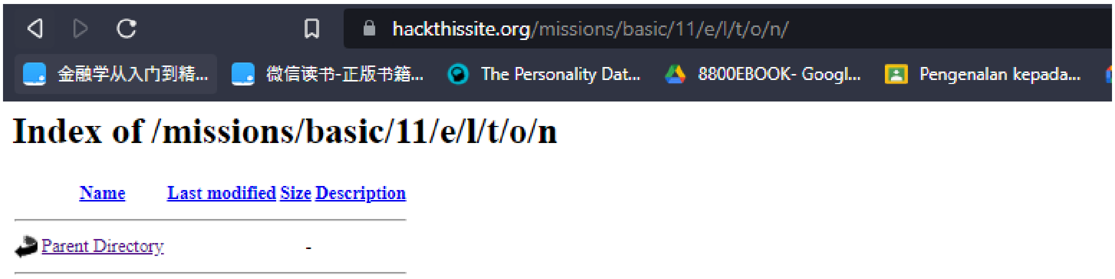
go with o



Index of /missions/basic/11/e/l/t/o

Name	Last modified	Size	Description
Parent Directory		-	
n/	2019-03-01 20:34	-	

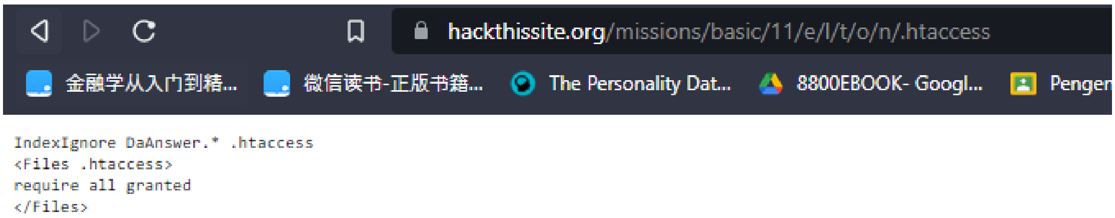
go with n



Index of /missions/basic/11/e/l/t/o/n

Name	Last modified	Size	Description
Parent Directory		-	

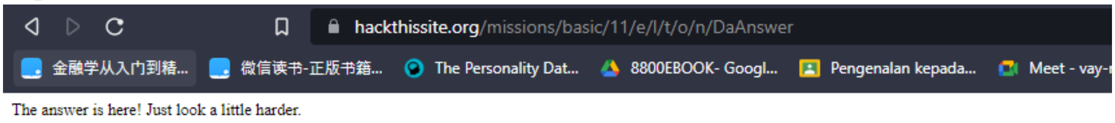
Put .htaccess in the end



```
IndexIgnore DaAnswer.* .htaccess
<Files .htaccess>
require all granted
</Files>
```

Prepared by: SY Ooi

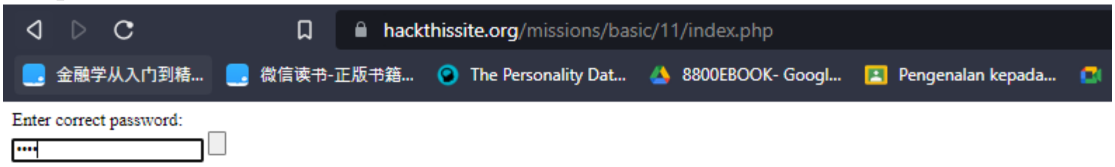
Replace .htaccess with DaAnswer



hackthissite.org/missions/basic/11/e/l/t/o/n/DaAnswer

The answer is here! Just look a little harder.

The password is “here”

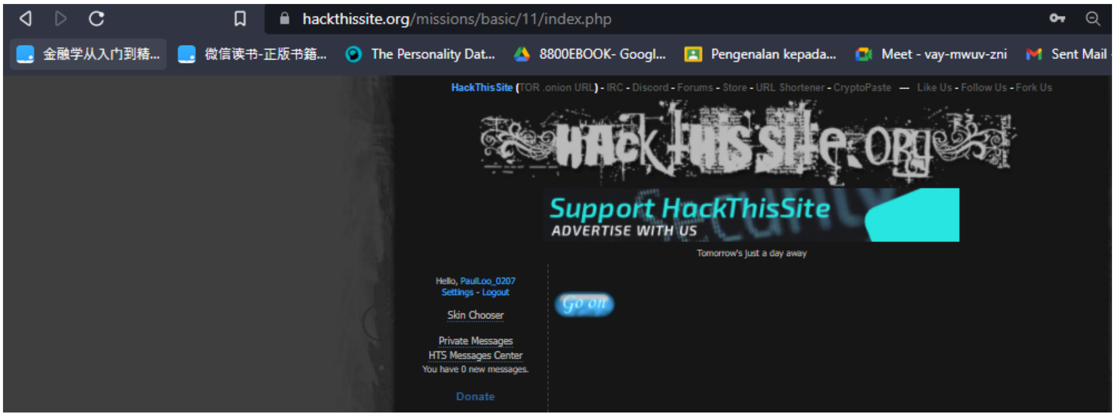


hackthissite.org/missions/basic/11/index.php

Enter correct password:

••••

All the basic exercises are completed



hackthissite.org/missions/basic/11/index.php

Hello, PaulLoo_0207

Settings - Logout

You have 0 new messages.

Prepared by: SY Ooi