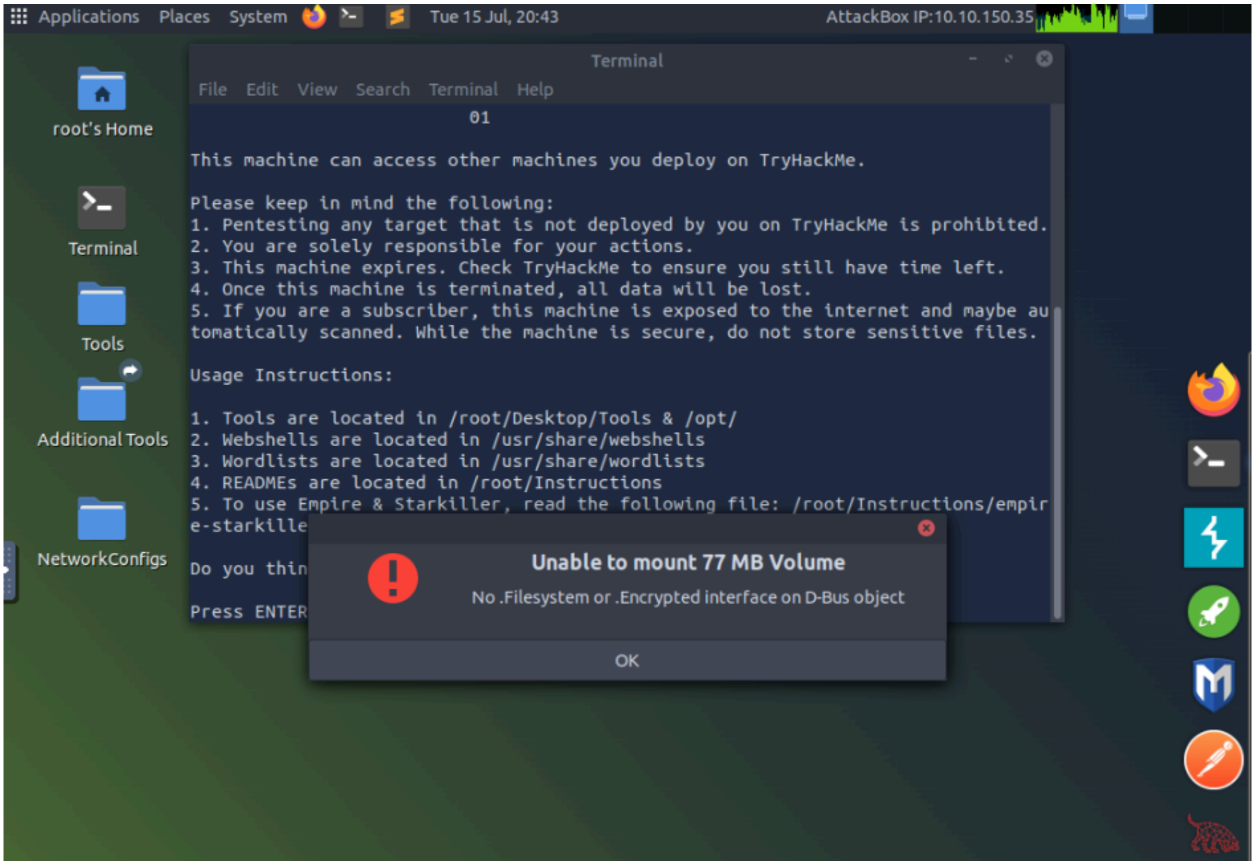
The idea with this scenario is we are given a public website and must view in “source” mode to find vulnerabilities.

So when the machine starts, we see this:



```
                      01

This machine can access other machines you deploy on TryHackMe.

Please keep in mind the following:
1. Pentesting any target that is not deployed by you on TryHackMe is prohibited.
2. You are solely responsible for your actions.
3. This machine expires. Check TryHackMe to ensure you still have time left.
4. Once this machine is terminated, all data will be lost.
5. If you are a subscriber, this machine is exposed to the internet and maybe au
tomatically scanned. While the machine is secure, do not store sensitive files.

Usage Instructions:

1. Tools are located in /root/Desktop/Tools & /opt/
2. Webshells are located in /usr/share/webshells
3. Wordlists are located in /usr/share/wordlists
4. READMEs are located in /root/Instructions
5. To use Empire & Starkiller, read the following file: /root/Instructions/empir
e-starkille

Do you thin

Press ENTER
```

Unable to mount 77 MB Volume

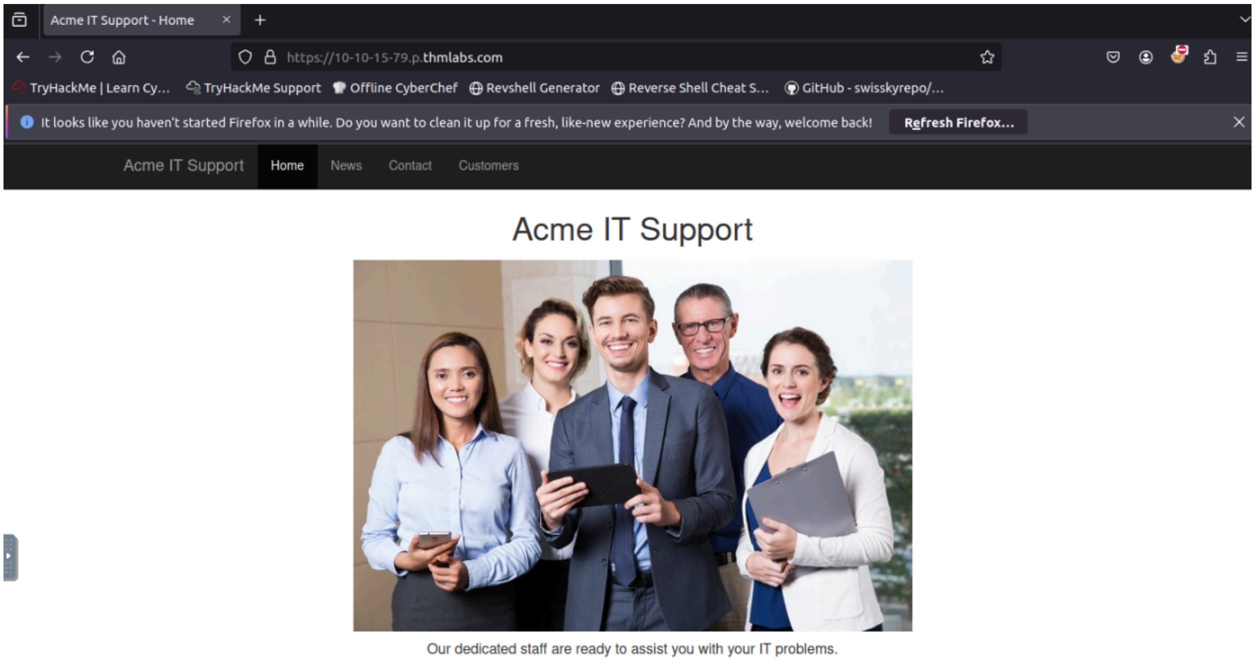
No .Filesystem or .Encrypted interface on D-Bus object

This is a remote desktop application where I can replicate real-world simulations in a sandbox area.

After waiting a few minutes, we finally have our objective,

https://10-10-15-79.p.thmlabs.com *(this URL will update 2 minutes from when you start the machine)*

We have the URL provided to us, which I will open firefox at the top of the screen and just paste the link, and see what happens!



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

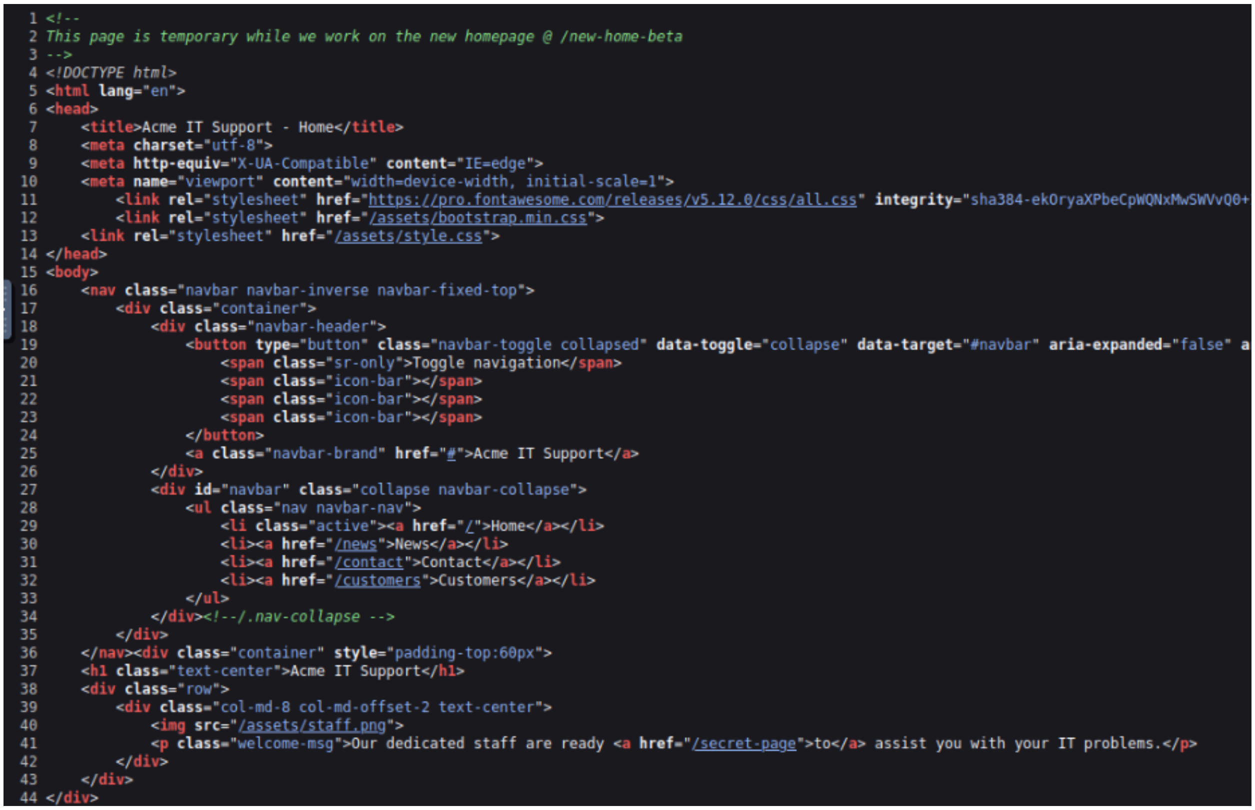
Acme IT Support

Our dedicated staff are ready to assist you with your IT problems.

To the eye initially, nothing seems out of the ordinary! As an ordinary user, we would think nothing of this, and in fact navigate it as usual.

But… We are no longer that “Ordinary user” so I right clicked the page and selected to “View page source” this now formatted the page into HTML (Hyper Text Markup Language).

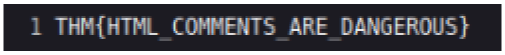
I will be honest, I have little to no experience with HTML, but I know the basics.



```html
<!--
This page is temporary while we work on the new homepage @ /new-home-beta
-->
<!DOCTYPE html>
<html lang="en">
<head>
    <title>Acme IT Support - Home</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="https://pro.fontawesome.com/releases/v5.12.0/css/all.css" integrity="sha384-ekOryaXPbeCpWQNxMwSWVvQ0+
        <link rel="stylesheet" href="/assets/bootstrap.min.css">
    <link rel="stylesheet" href="/assets/style.css">
</head>
<body>
    <nav class="navbar navbar-inverse navbar-fixed-top">
        <div class="container">
            <div class="navbar-header">
                <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-target="#navbar" aria-expanded="false" a
                    <span class="sr-only">Toggle navigation</span>
                    <span class="icon-bar"></span>
                    <span class="icon-bar"></span>
                    <span class="icon-bar"></span>
                </button>
                <a class="navbar-brand" href="#">Acme IT Support</a>
            </div>
            <div id="navbar" class="collapse navbar-collapse">
                <ul class="nav navbar-nav">
                    <li class="active"><a href="/">Home</a></li>
                    <li><a href="/news">News</a></li>
                    <li><a href="/contact">Contact</a></li>
                    <li><a href="/customers">Customers</a></li>
                </ul>
            </div><!--/.nav-collapse -->
        </div>
    </nav><div class="container" style="padding-top:60px">
    <h1 class="text-center">Acme IT Support</h1>
    <div class="row">
        <div class="col-md-8 col-md-offset-2 text-center">
            <img src="/assets/staff.png">
            <p class="welcome-msg">Our dedicated staff are ready <a href="/secret-page">to</a> assist you with your IT problems.</p>
        </div>
    </div>
</div>
```

So it looks quite complex! But, once we really skim through we notice it is organised, there are some patterns.

At the top however in green it says
<!--
This page is temporary while we work on the new homepage @ /new-home-beta
→
This is a comment! It is invisible on the actual web page, and is a very silly flaw that is easily overlooked by a developer.
The souce of the HTML in the URL is currently,
view-source:https://10-10-15-79.p.thmlabs.com/
Let's modify it! And on the end add the comment /new-home-beta (Which is the "Actual" web page the developer is working on)
view-source:https://10-10-15-79.p.thmlabs.com/new-home-beta



```
THM{HTML_COMMENTS_ARE_DANGEROUS}
```

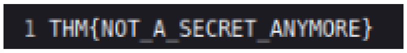
Absolutely right. Comments are indeed dangerous when they contain sensitive information such as "the real website". This is a vulnerability.

What is the flag from the HTML comment? Which was one of the questions asked, it is THM{HTML_COMMENTS_ARE_DANGEROUS}

What is the flag from the secret link? Which is the second question.

Line 41 in the code houses this string of text:
<p class="welcome-msg">Our dedicated staff are ready <a href="/secret-page">to</a> assist you with your IT problems.</p>

I simply clicked the secret link and…



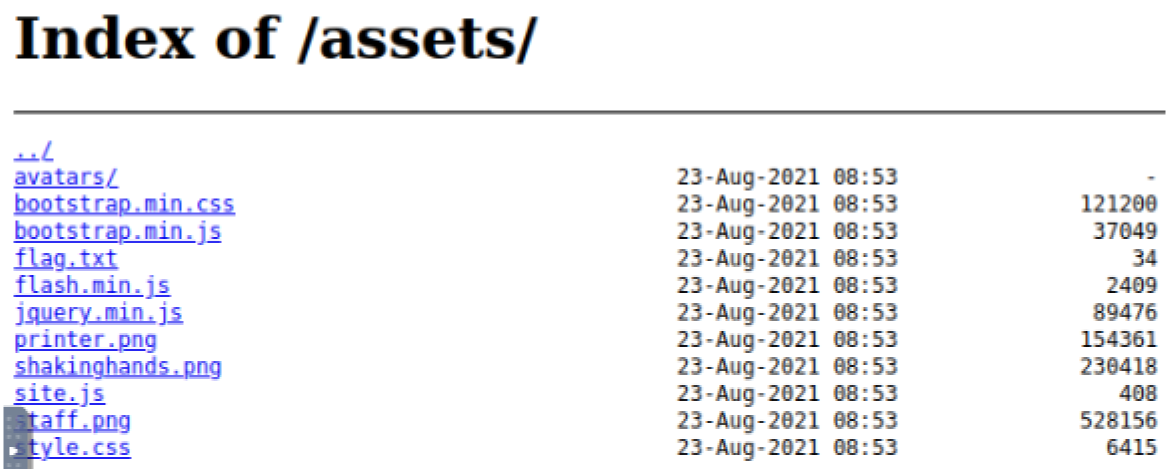
```
THM{NOT_A_SECRET_ANYMORE}
```

THM{NOT_A_SECRET_ANYMORE}... Haha. That flag is ours.

What is the directory listing flag?

Right! This took me a little while to figure out. Sometimes, especially in this case, different strings are assigned different values, and originate from a source file or link. In this case at the bottom especially src="/assets" was listed for a few items.
So assets.. Is mentioned a few times, it is a source file… So what else is in there!

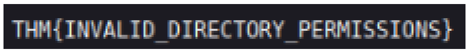
Let's modify the URL again and find out:
view-source:http://10-10-15-79.p.thmlabs.com/assets/
Same link as before just with "/assets" on the end.



Index of /assets/

```
../
avatars/                                 23-Aug-2021 08:53                   -
bootstrap.min.css                        23-Aug-2021 08:53              121200
bootstrap.min.js                         23-Aug-2021 08:53               37049
flag.txt                                 23-Aug-2021 08:53                  34
flash.min.js                             23-Aug-2021 08:53                2409
jquery.min.js                            23-Aug-2021 08:53               89476
printer.png                              23-Aug-2021 08:53              154361
shakinghands.png                         23-Aug-2021 08:53              230418
site.js                                  23-Aug-2021 08:53                 408
staff.png                                23-Aug-2021 08:53              528156
style.css                                23-Aug-2021 08:53                6415
```

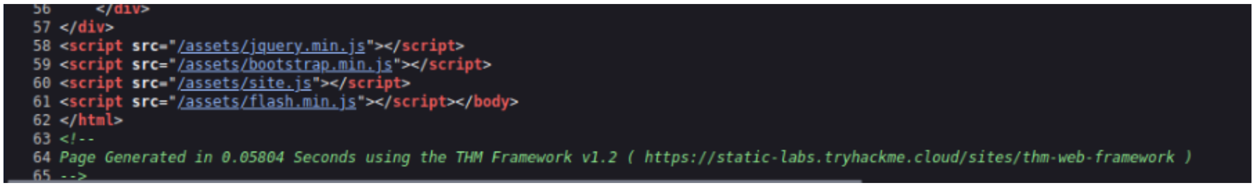
Boom! Flag.txt. That is exactly what we want.



```
THM{INVALID_DIRECTORY_PERMISSIONS}
```

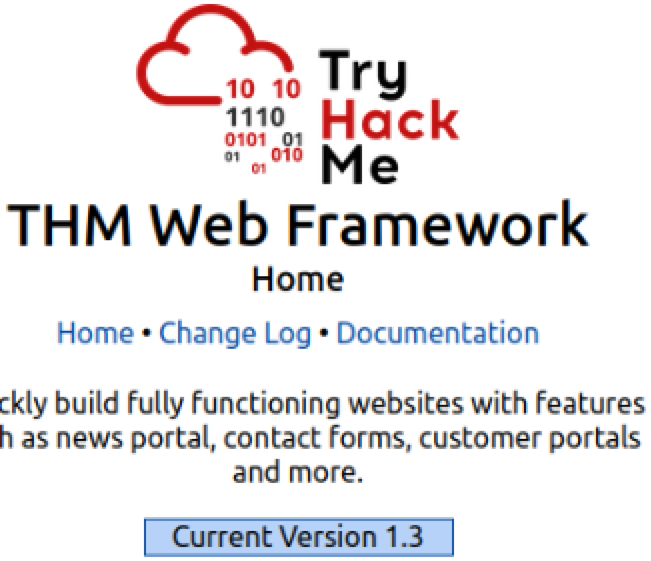
THM{INVALID_DIRECTORY_PERMISSIONS}

Finally, What is the framework flag?
Frame work flag? Ah yes! If we go to the original, all the way at the bottom is ANOTHER comment in green highlight.



```
    </div>
</div>
<script src="/assets/jquery.min.js"></script>
<script src="/assets/bootstrap.min.js"></script>
<script src="/assets/site.js"></script>
<script src="/assets/flash.min.js"></script></body>
</html>
<!--
Page Generated in 0.05804 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )
-->
```

<!--
Page Generated in 0.05804 Seconds using the THM Framework v1.2 (https://static-labs.tryhackme.cloud/sites/thm-web-framework)
-->
The developer was nice enough to give us the link already…
https://static-labs.tryhackme.cloud/sites/thm-web-framework

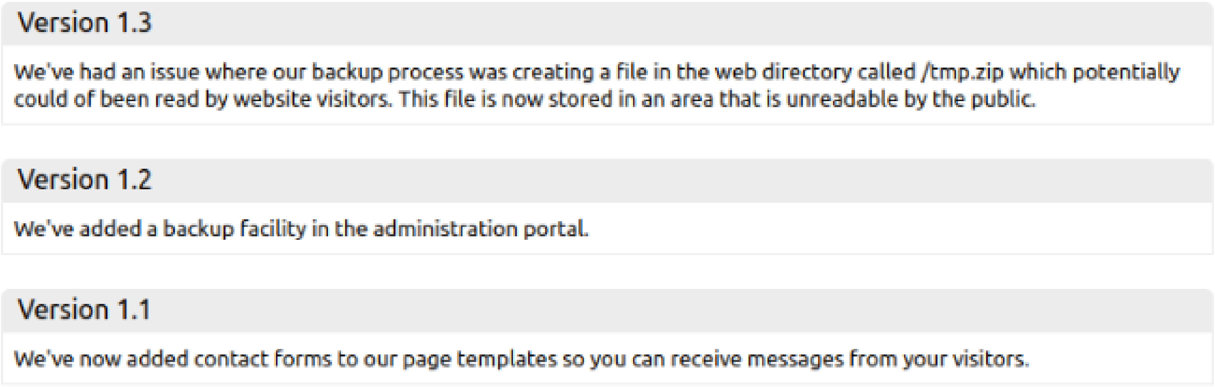


THM Web Framework

Home

Quickly build fully functioning websites with features such as news portal, contact forms, customer portals and more.

Hm… So this says “Current version 1.3” that.. IS not the one specified in the commend.
So let’s select “Change log”



Version 1.3

We've had an issue where our backup process was creating a file in the web directory called /tmp.zip which potentially could of been read by website visitors. This file is now stored in an area that is unreadable by the public.

Version 1.2

We've added a backup facility in the administration portal.

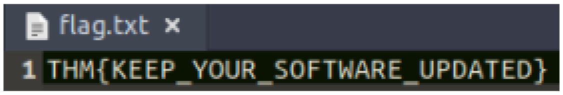
Version 1.1

We've now added contact forms to our page templates so you can receive messages from your visitors.

Version 1.3
We've had an issue where our backup process was creating a file in the web directory called /tmp.zip which potentially could of been read by website visitors. This file is now stored in an area that is unreadable by the public.

Naughty….
Let’s modify the original URL again…But it also says “The file is now stored in an area that is unreadable by the public… Perhaps hidden so that the public cannot easily access it, but we have all the information we need, a URL and the extension for the zip file.

http://10-10-15-79.p.thmlabs.com/tmp.zip - That downloaded a .zip file which contained our final flag.



```
THM{KEEP_YOUR_SOFTWARE_UPDATED}
```

THM{KEEP_YOUR_SOFTWARE_UPDATED}

Wow what a roller coaster!
But this goes to show how invisible things can be to a customer or client, and how visible and accessible it is to a hacker…