Jr PenTester-1--Walking_a_WebApp

What I learned:

- element inpector is for troubleshooting web apps but they can also be used to find exploits, too
- you can check the html code for any dir that may be accessible
- check framework to make sure its updated
- some of the web page can be manipulated and viewed, like with the styles tab
- what 'pretty print' and 'breakpoints' are
- some responses can be viewed in the element inspection

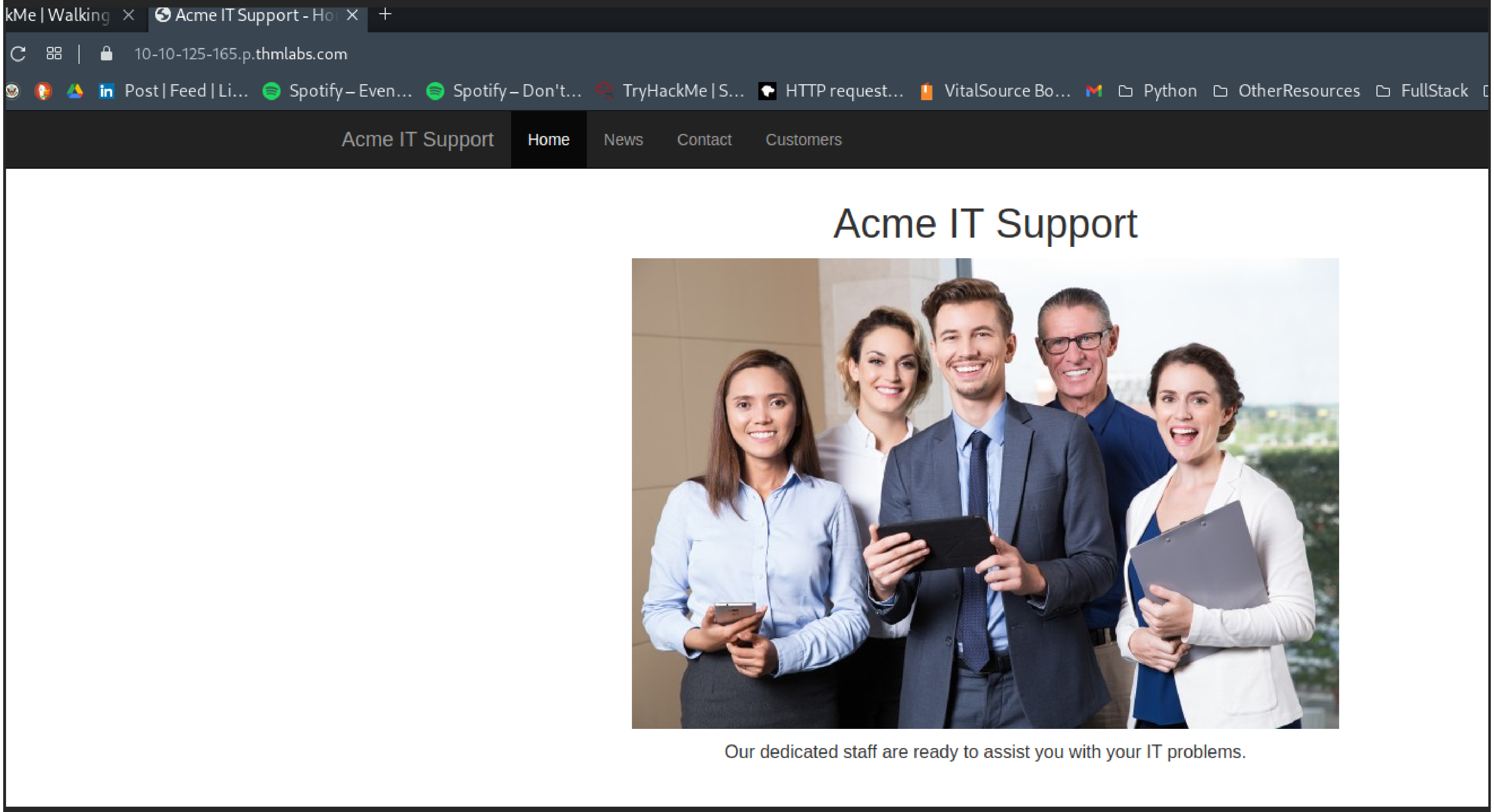
Here is a short breakdown of the in-built browser tools you will use throughout this room:

- **View Source** - Use your browser to view the human-readable source code of a website.
- **Inspector** - Learn how to inspect page elements and make changes to view usually blocked content.
- **Debugger** - Inspect and control the flow of a page's JavaScript
- **Network** - See all the network requests a page makes.

How do I view the Page Source?

1. While viewing a website, you can right-click on the page, and you'll see an option on the menu that says View Page Source.
2. Most browsers support putting view-source: in front of the URL for example, **view-source:**https://www.google.com/
3. In your browser menu, you'll find an option to view the page source. This option can sometimes be in submenus such as developer tools or more tools.

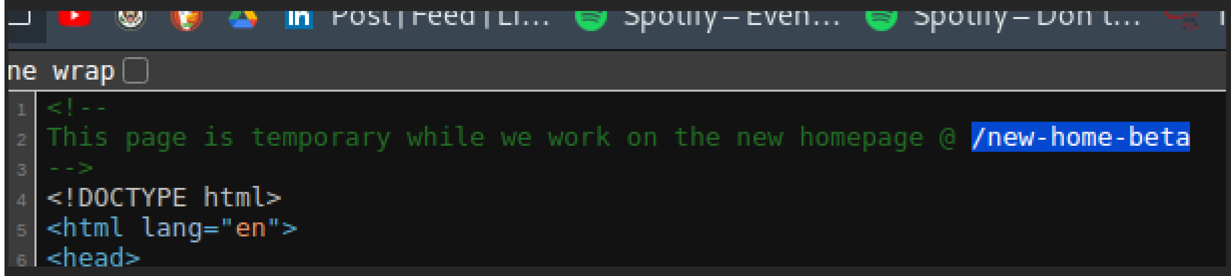
Task 3 Viewing The Page Source



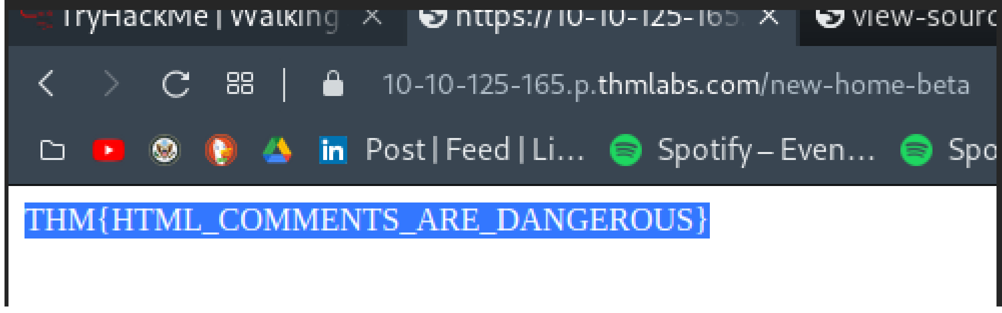
Acme IT Support

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

What is the flag from the HTML comment?

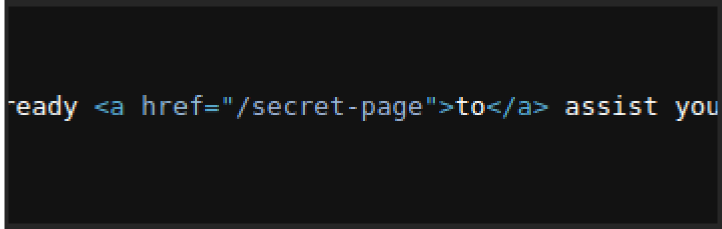


```
<!--
This page is temporary while we work on the new homepage @ /new-home-beta
-->
<!DOCTYPE html>
<html lang="en">
<head>
```

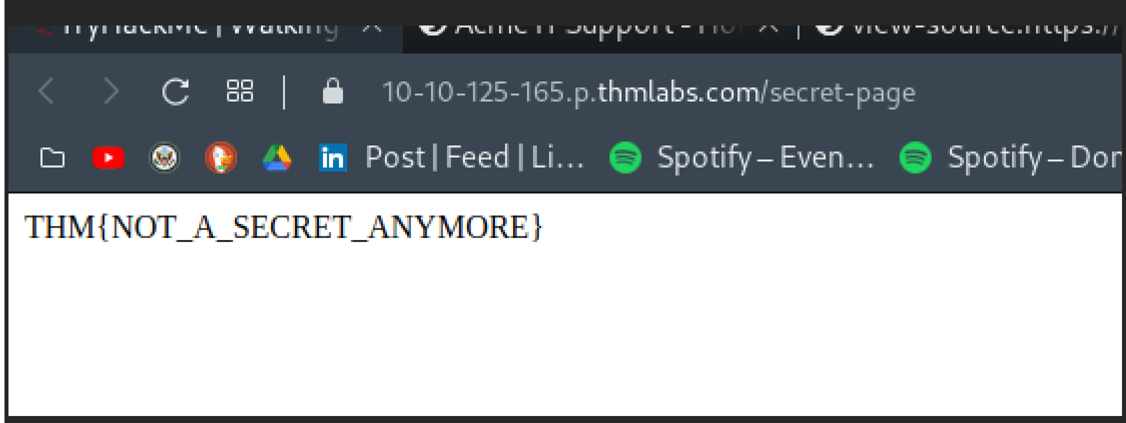


THM{HTML_COMMENTS_ARE_DANGEROUS}

What is the flag from the secret link?

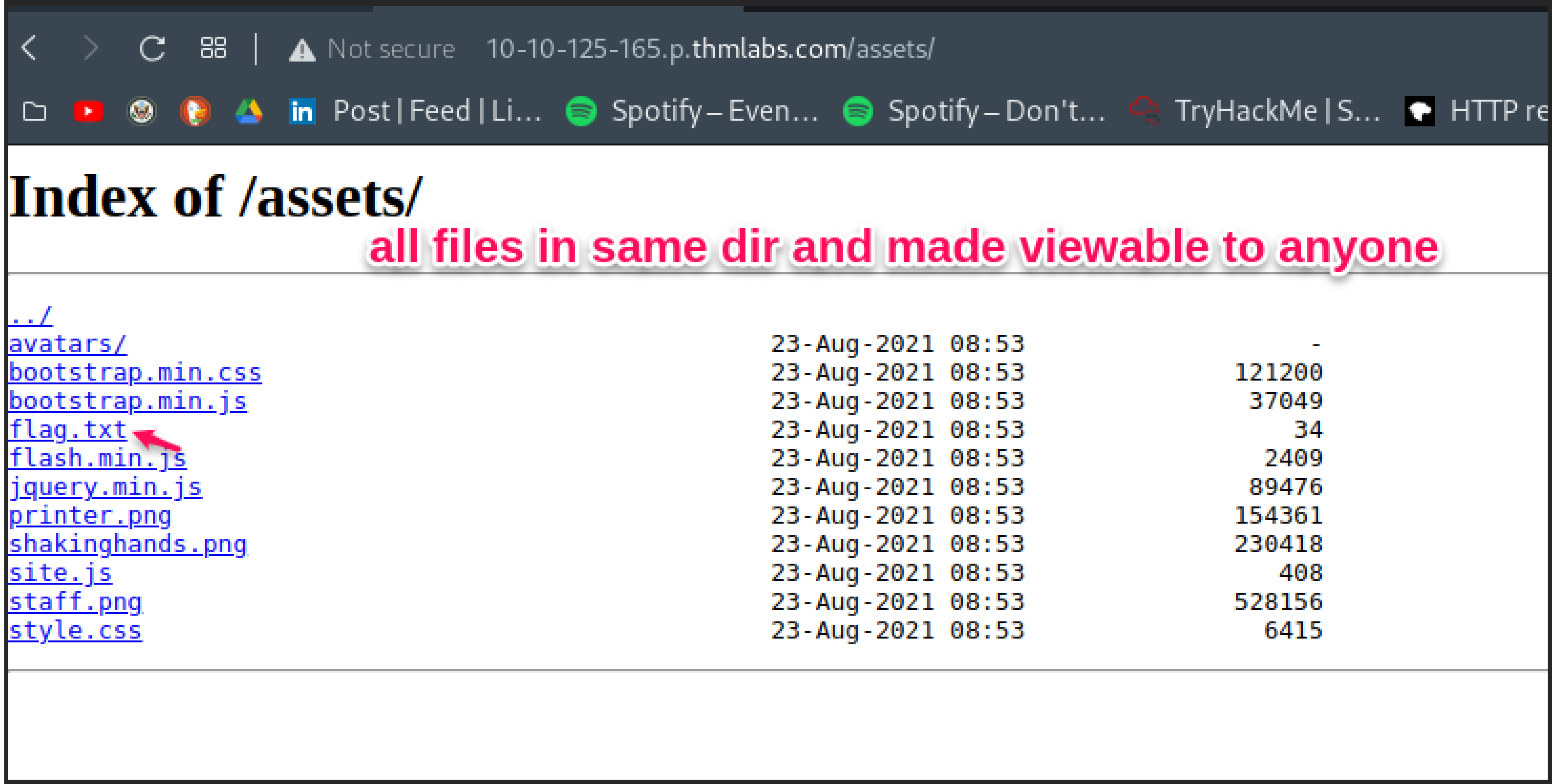


```
ready <a href="/secret-page">to</a> assist you
```



THM{NOT_A_SECRET_ANYMORE}

What is the directory listing flag?



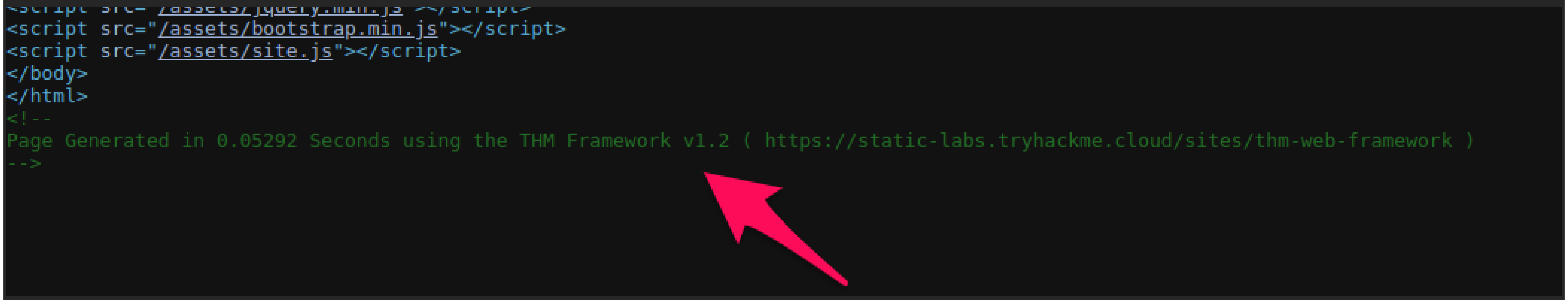
Index of /assets/

all files in same dir and made viewable to anyone

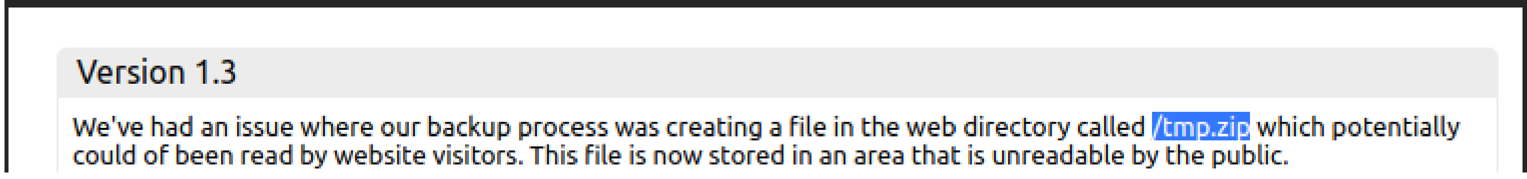
```
../
avatars/                                           23-Aug-2021 08:53                   -
bootstrap.min.css                                  23-Aug-2021 08:53              121200
bootstrap.min.js                                   23-Aug-2021 08:53               37049
flag.txt                                           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
```

```
THM{INVALID_DIRECTORY_PERMISSIONS}
```

What is the framework flag?

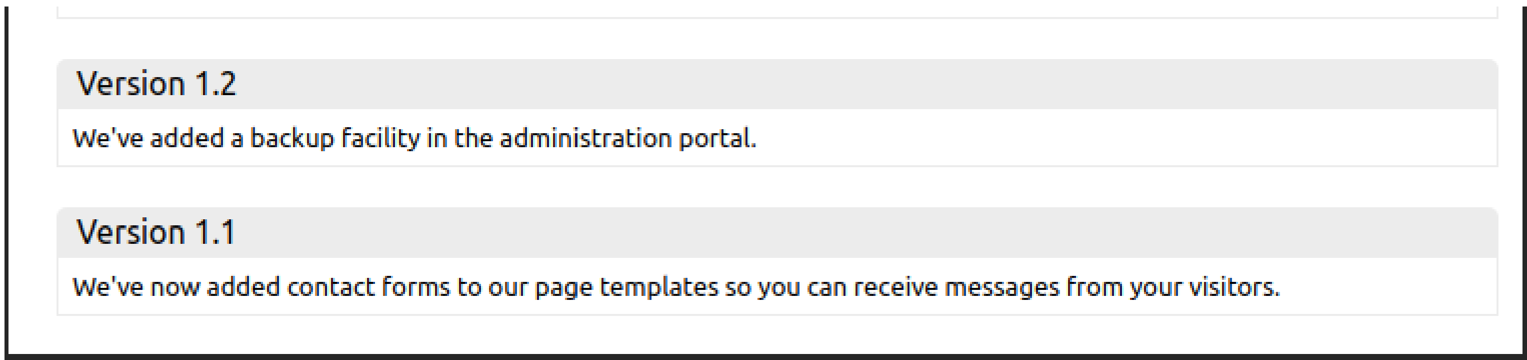


```
<script src="/assets/jquery.min.js"></script>
<script src="/assets/bootstrap.min.js"></script>
<script src="/assets/site.js"></script>
</body>
</html>
<!--
Page Generated in 0.05292 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )
-->
```



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.

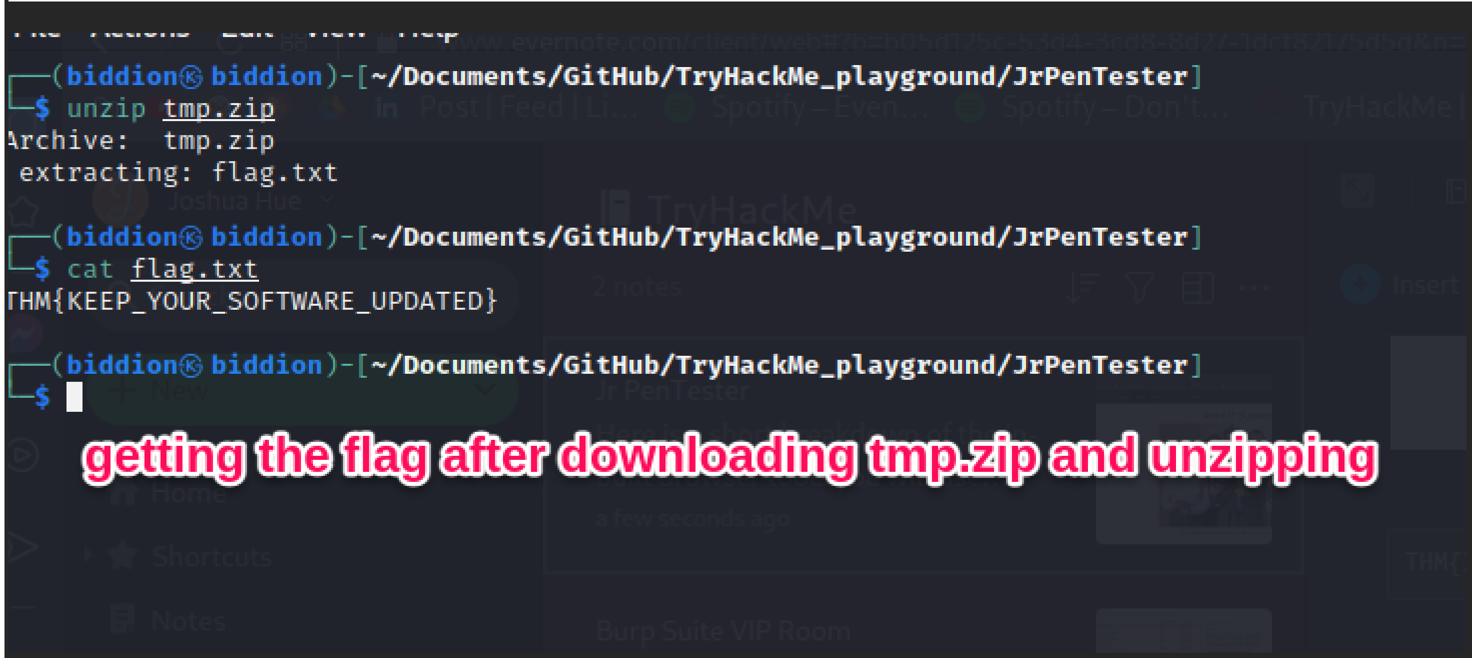


Version 1.2

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.

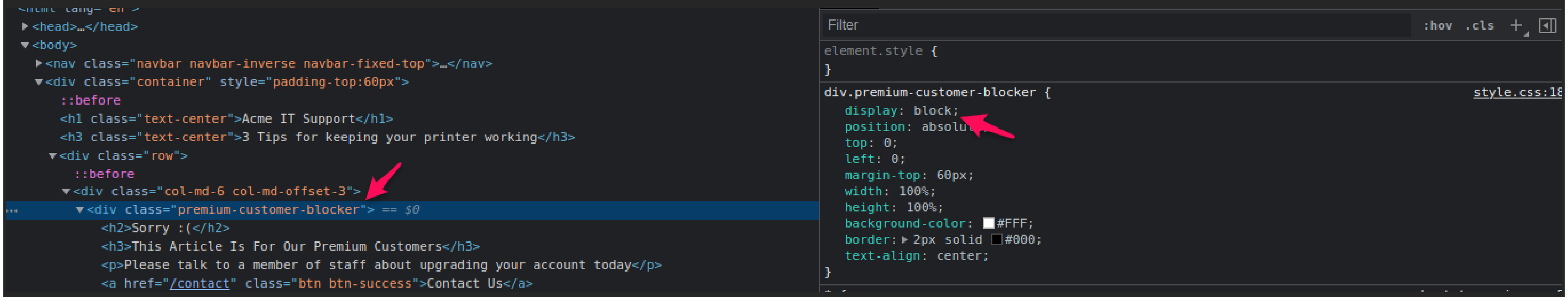


```
┌──(biddion㉿biddion)-[~/Documents/GitHub/TryHackMe_playground/JrPenTester]
└─$ unzip tmp.zip
Archive:  tmp.zip
 extracting: flag.txt

┌──(biddion㉿biddion)-[~/Documents/GitHub/TryHackMe_playground/JrPenTester]
└─$ cat flag.txt
THM{KEEP_YOUR_SOFTWARE_UPDATED}

┌──(biddion㉿biddion)-[~/Documents/GitHub/TryHackMe_playground/JrPenTester]
└─$ ▌
```

getting the flag after downloading tmp.zip and unzipping

Task 4 Developer Tools - Inspector

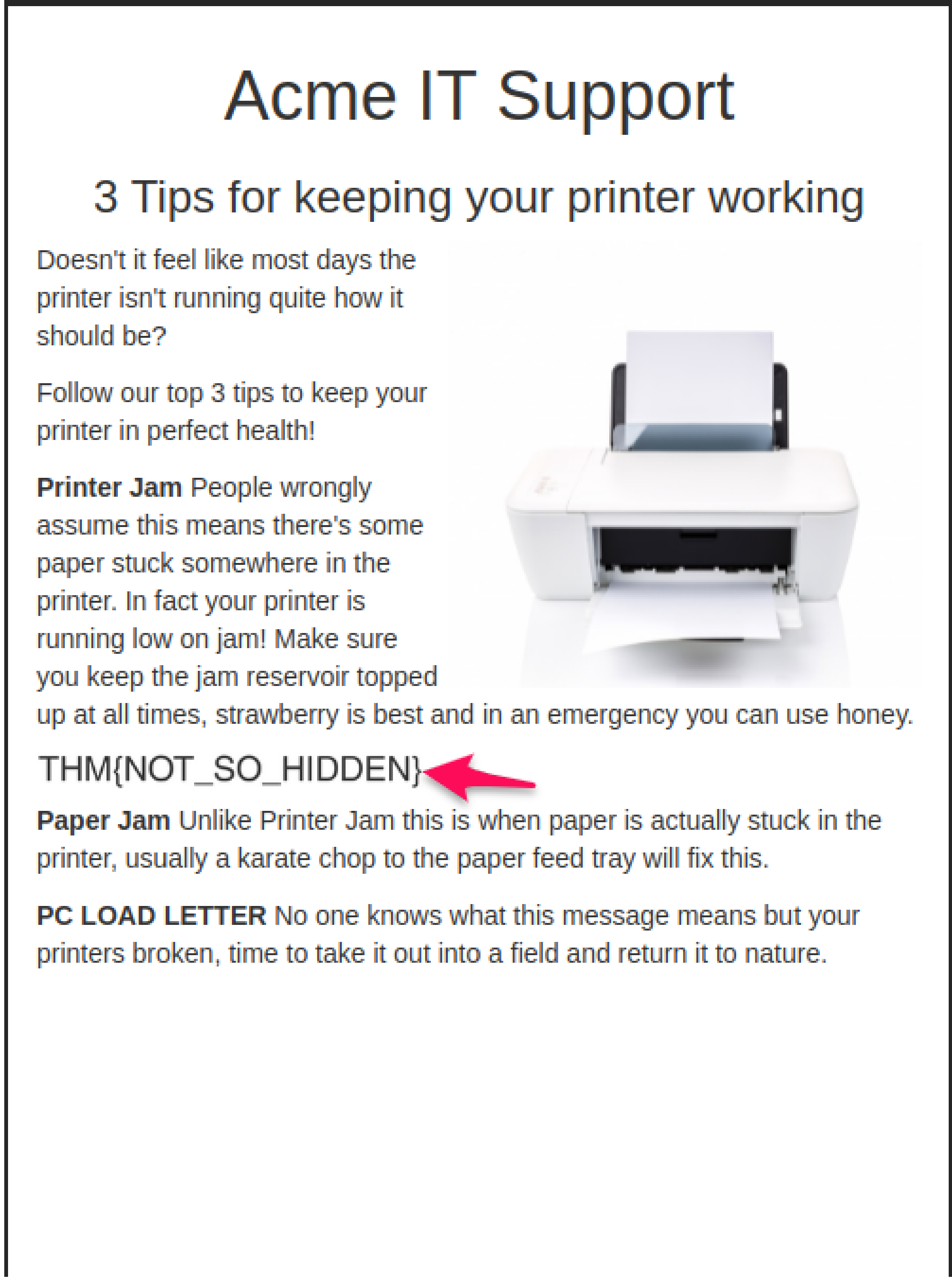
What is the flag behind the paywall?



```
 ▸<head>…</head>
 ▾<body>
   ▸<nav class="navbar navbar-inverse navbar-fixed-top">…</nav>
   ▾<div class="container" style="padding-top:60px">
       ::before
       <h1 class="text-center">Acme IT Support</h1>
       <h3 class="text-center">3 Tips for keeping your printer working</h3>
     ▾<div class="row">
         ::before
       ▾<div class="col-md-6 col-md-offset-3">
…        ▾<div class="premium-customer-blocker"> == $0
             <h2>Sorry :(</h2>
             <h3>This Article Is For Our Premium Customers</h3>
             <p>Please talk to a member of staff about upgrading your account today</p>
             <a href="/contact" class="btn btn-success">Contact Us</a>
```

```
Filter                                             :hov .cls +
element.style {
}
div.premium-customer-blocker {                     style.css:18
    display: block;
    position: absolu
    top: 0;
    left: 0;
    margin-top: 60px;
    width: 100%;
    height: 100%;
    background-color: □#FFF;
    border: ▸ 2px solid ■#000;
    text-align: center;
}
```

After changing "block" to "none" this appears:



Acme IT Support

3 Tips for keeping your printer working

Doesn't it feel like most days the printer isn't running quite how it should be?

Follow our top 3 tips to keep your printer in perfect health!

Printer Jam People wrongly assume this means there's some paper stuck somewhere in the printer. In fact your printer is running low on jam! Make sure you keep the jam reservoir topped up at all times, strawberry is best and in an emergency you can use honey.

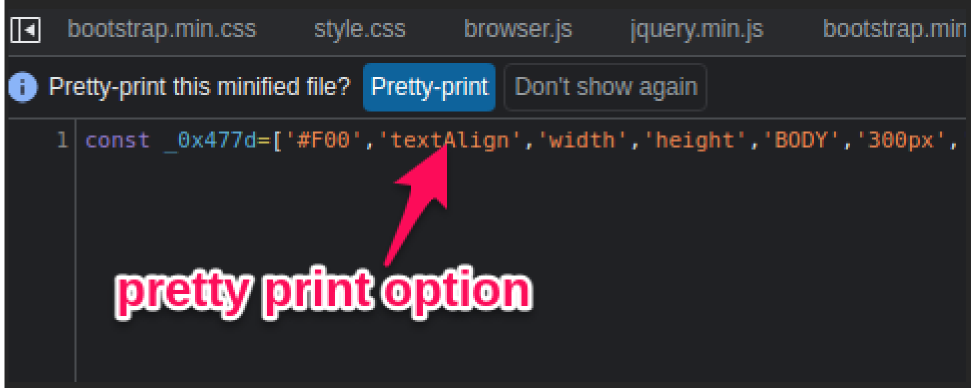
THM{NOT_SO_HIDDEN}

Paper Jam Unlike Printer Jam this is when paper is actually stuck in the printer, usually a karate chop to the paper feed tray will fix this.

PC LOAD LETTER No one knows what this message means but your printers broken, time to take it out into a field and return it to nature.

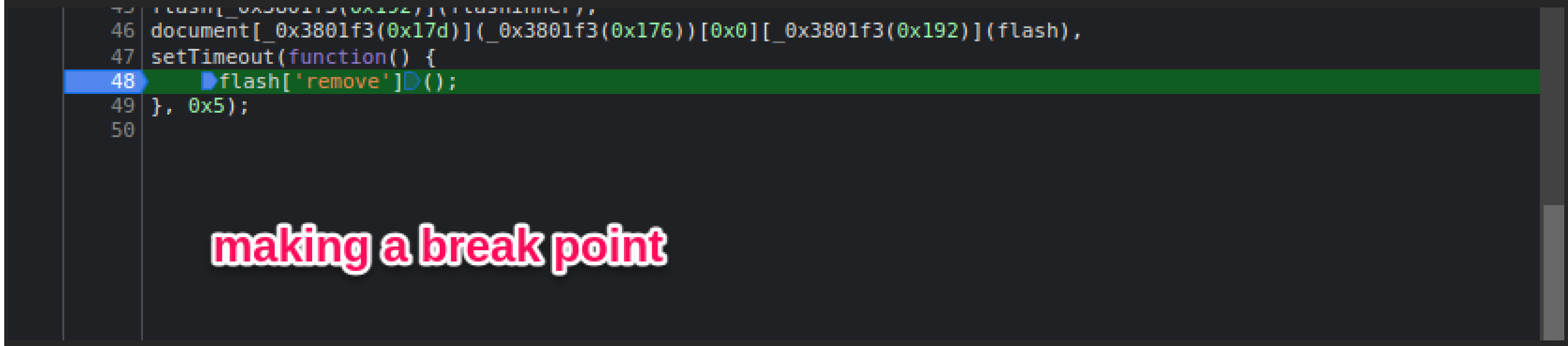
Task 5 Developer Tools - Debugger

What is the flag in the red box?



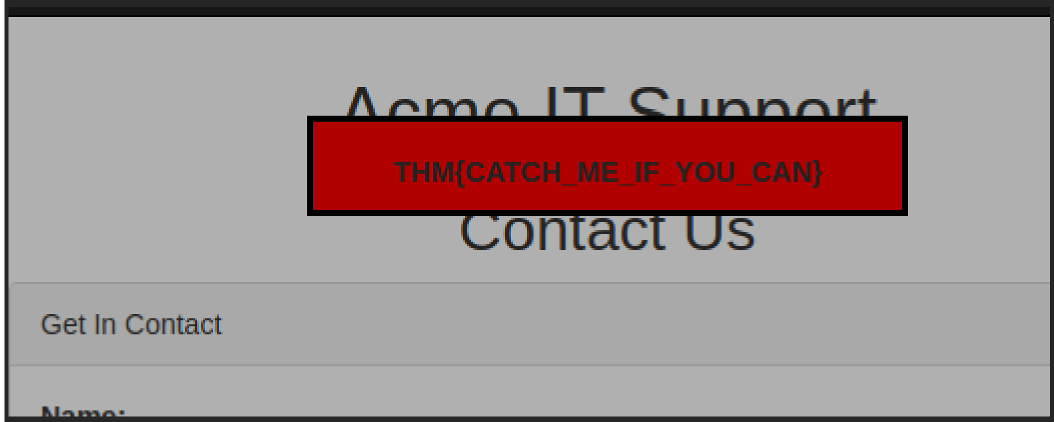
```
const _0x477d=['#F00','textAlign','width','height','BODY','300px',
```

pretty print option



```
document[_0x3801f3(0x17d)](_0x3801f3(0x176))[0x0][_0x3801f3(0x192)](flash),
setTimeout(function() {
    flash['remove']();
}, 0x5);
```

making a break point



Acme IT Support

THM{CATCH_ME_IF_YOU_CAN}

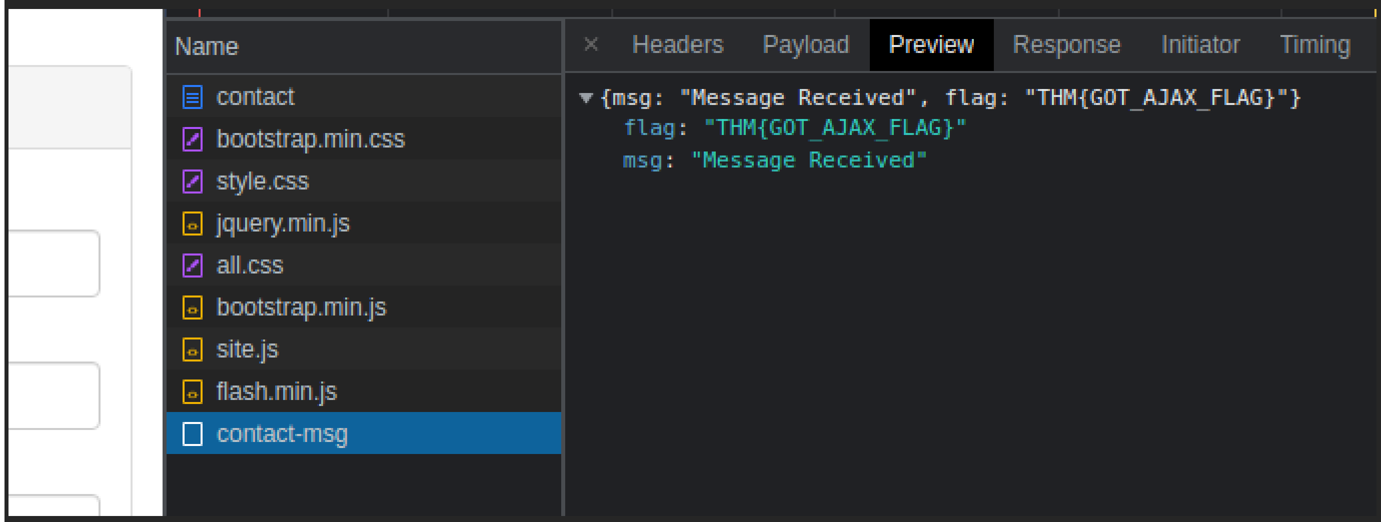
Contact Us

Get In Contact

Name:

Task 6 Developer Tools - Network

What is the flag shown on the contact-msg network request?
By filling the form I see a contact-msg reply in the inspector that I would not have seen without it.



```
▾{msg: "Message Received", flag: "THM{GOT_AJAX_FLAG}"}
   flag: "THM{GOT_AJAX_FLAG}"
   msg: "Message Received"
```