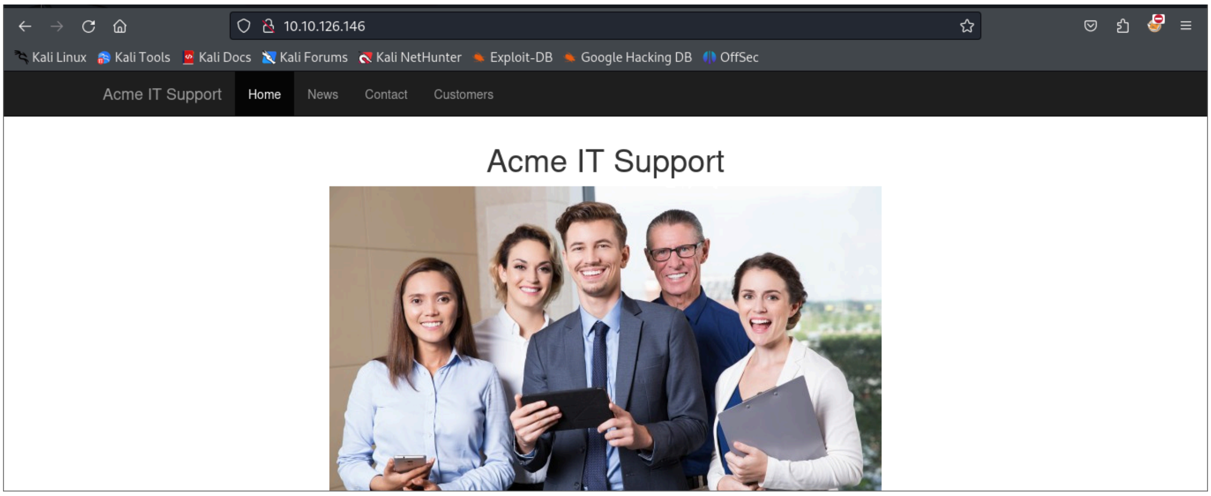
Walking An Application

Manually review a web application for security issues using only your browsers developer tools. Hacking with just your browser, no tools or scripts.

Task 3 Viewing The Page Source

- ➔ I visited the website

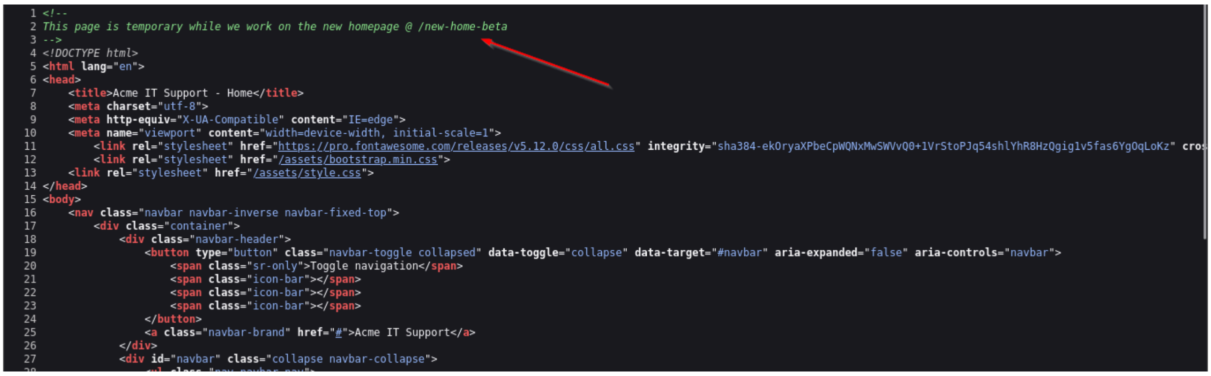


- ➔ I right-click on the page to view the Page Source

What is the flag from the HTML comment?

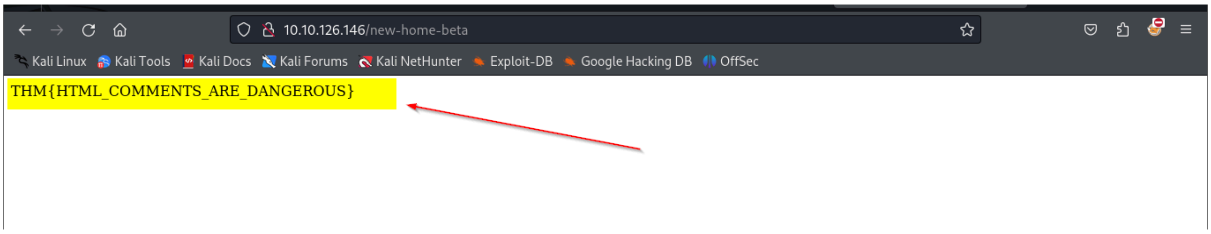
Answer: **THM{HTML_COMMENTS_ARE_DANGEROUS}**

- ➔ In the page source, i found a comment that indicated there is a page called /new-home-beta



```
<!--
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+1VrStoPJq54shlYhR8HzQgig1v5fas6YgOqLoKz" cros
        <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" aria-controls="navbar">
                    <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">
```

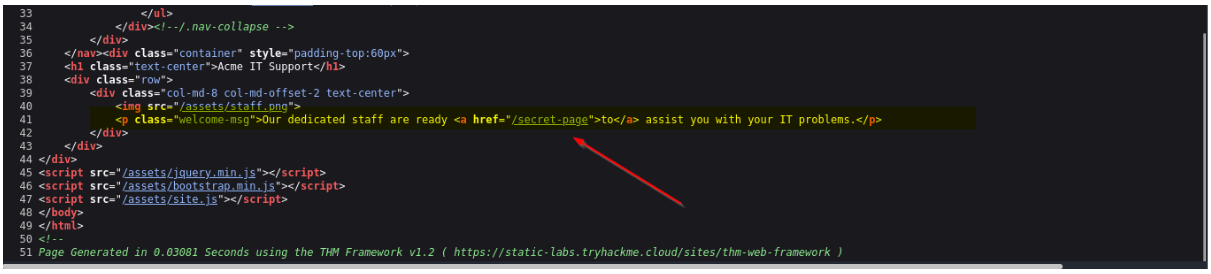
- ➔ I visited the page and found the flag



THM{HTML_COMMENTS_ARE_DANGEROUS}

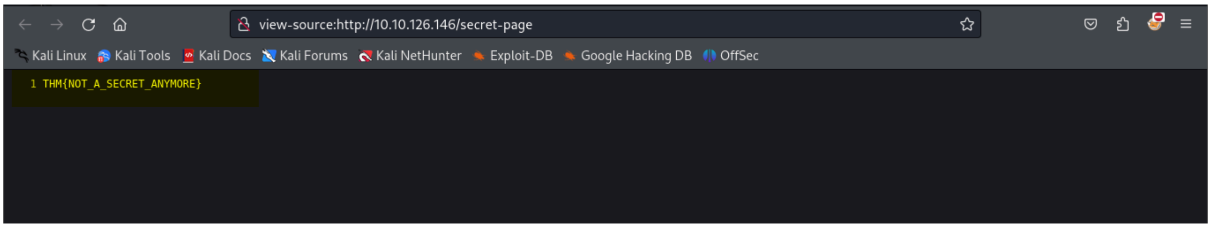
What is the flag from the secret link?

Answer: **THM{NOT_A_SECRET_ANYMORE}**



```
                </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>
<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 0.03081 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )
```

- ➔ I clicked on the secret page link and found the flag



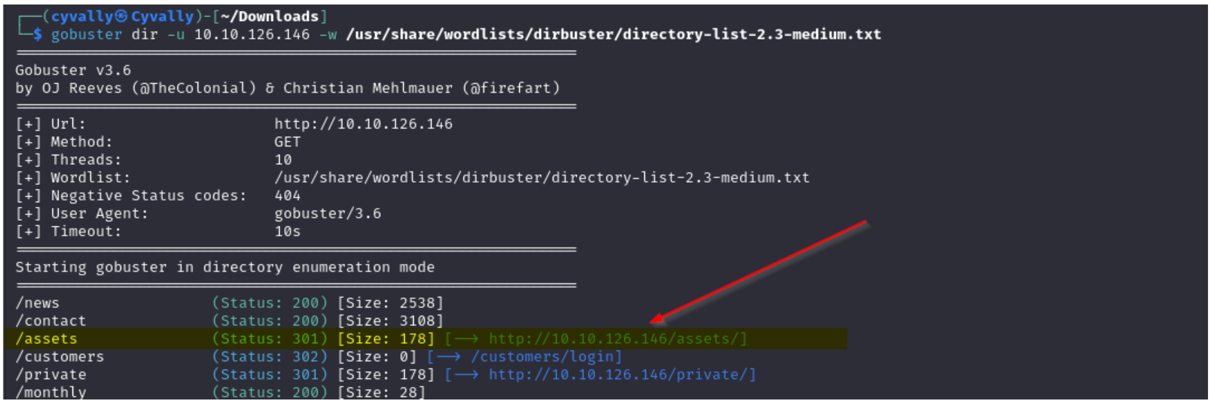
```
THM{NOT_A_SECRET_ANYMORE}
```

What is the directory listing flag?

Answer: **THM{INVALID_DIRECTORY_PERMISSIONS}**

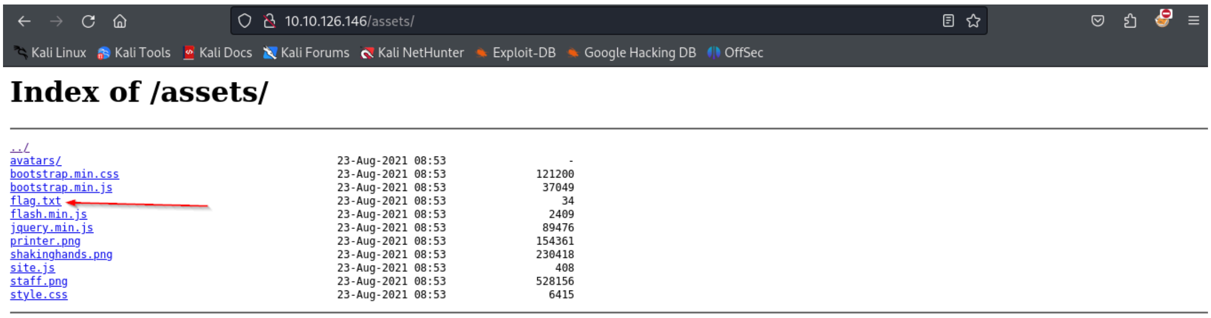
- ➔ I ran gobuster to enumerate directory

Command: **gobuster dir -u 10.10.126.146 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ gobuster dir -u 10.10.126.146 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.126.146
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/news                 (Status: 200) [Size: 2538]
/contact              (Status: 200) [Size: 3108]
/assets               (Status: 301) [Size: 178] [--> http://10.10.126.146/assets/]
/customers            (Status: 302) [Size: 0] [--> /customers/login]
/private              (Status: 301) [Size: 178] [--> http://10.10.126.146/private/]
/monthly              (Status: 200) [Size: 28]
```

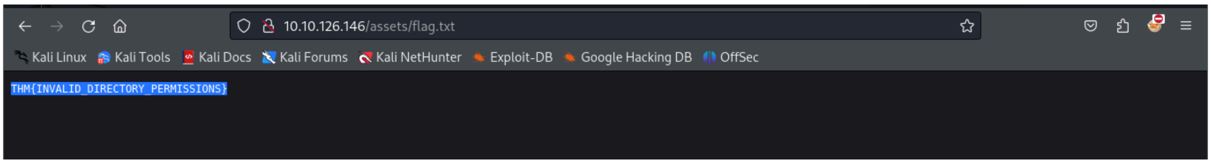
- ➔ Then i ran through each directory and found /assets to be interesting as it lists flag



10.10.126.146/assets/

```
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
```

- ➔ I opened the file and got the flag



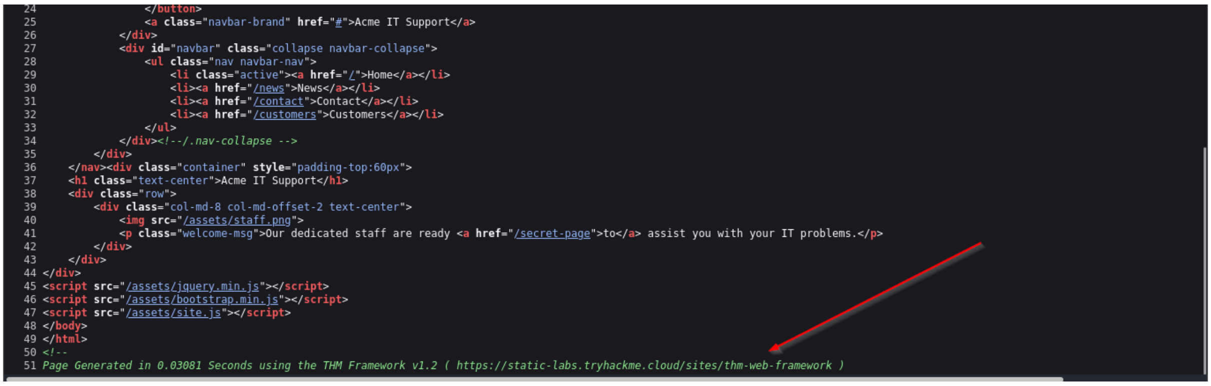
10.10.126.146/assets/flag.txt

```
THM{INVALID_DIRECTORY_PERMISSIONS}
```

What is the framework flag?

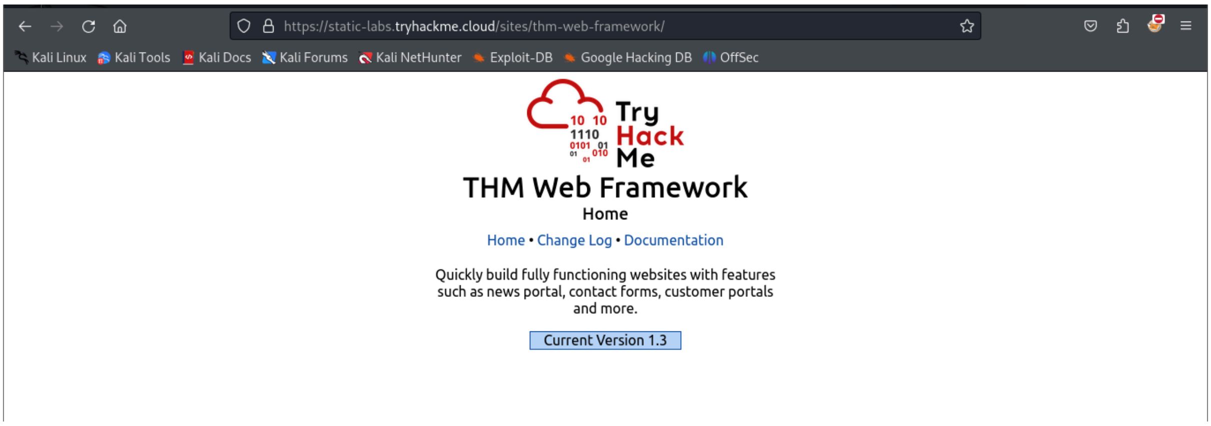
Answer: THM{KEEP_YOUR_SOFTWARE_UPDATED}

- ➔ I found a comment on the page source on the main website page



```
                </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>
<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 0.03081 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )
```

→ I visited the website in the comment



THM Web Framework

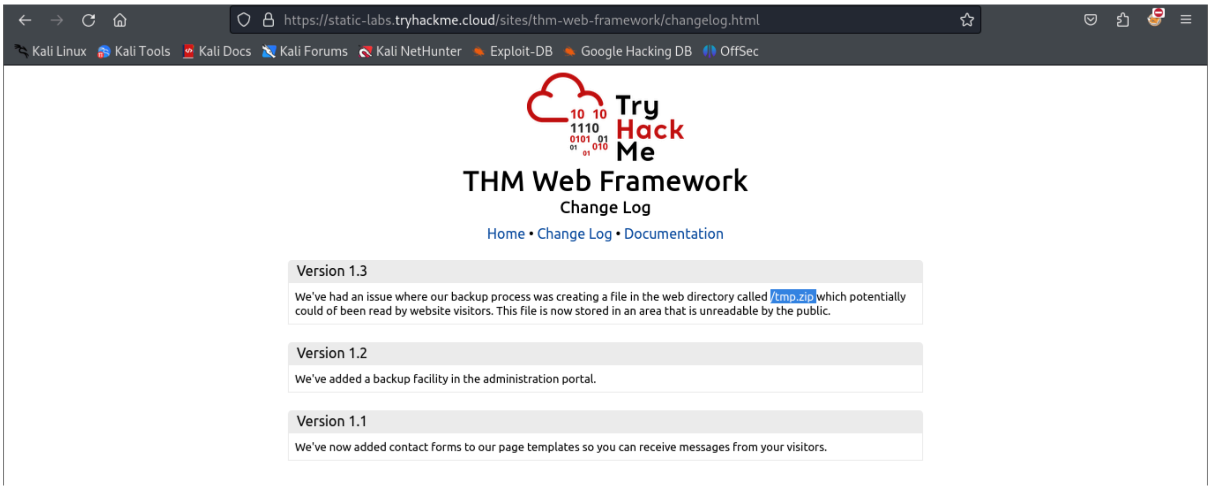
Home

Home • Change Log • Documentation

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

Current Version 1.3

→ I clicked on change log and found something interesting in it, it said the backup process was creating a file in the web directory called /tmp.zip.



THM Web Framework

Change Log

Home • Change Log • Documentation

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.

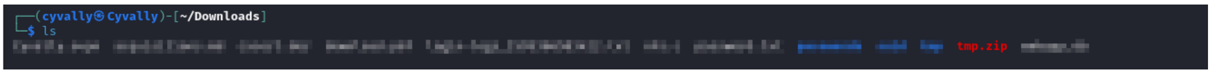
Version 1.2

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

Version 1.1

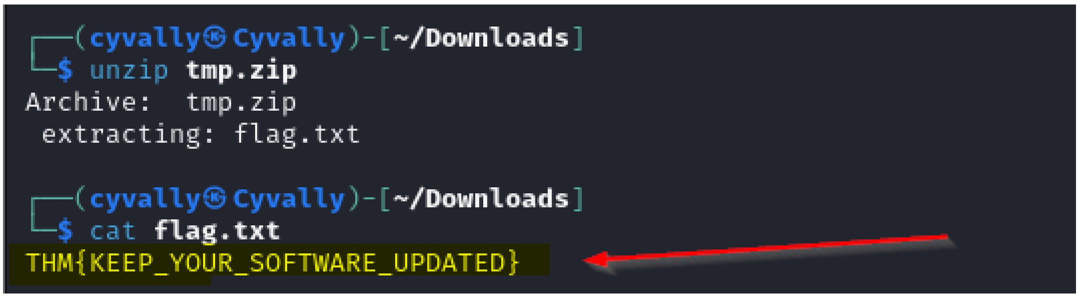
We've now added contact forms to our page templates so you can receive messages from your visitors.

→ I visited http://10.10.126.146/tmp.zip page and the file was downloaded



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ ls
[redacted] tmp.zip [redacted]
```

→ I unzipped it and got my flag



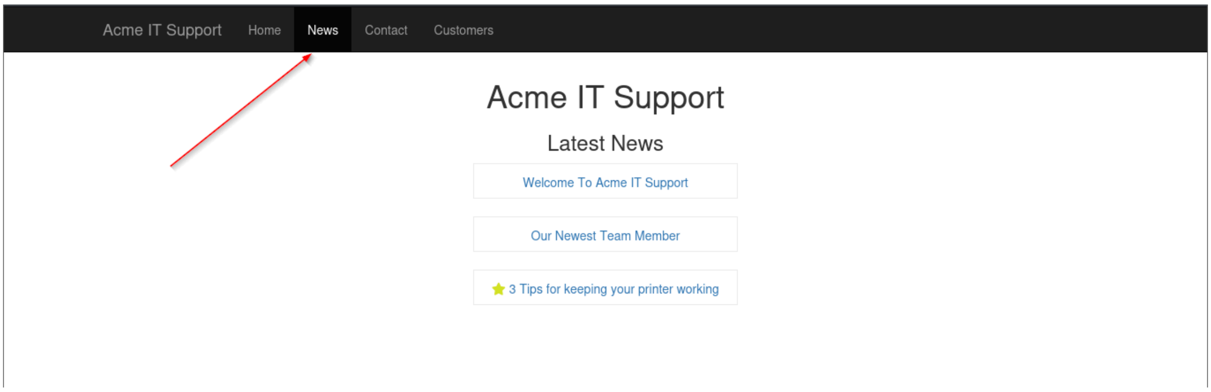
```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ unzip tmp.zip
Archive:  tmp.zip
 extracting: flag.txt

┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ cat flag.txt
THM{KEEP_YOUR_SOFTWARE_UPDATED}
```

Task 4 Developer Tools - Inspector

What is the flag behind the paywall?

Answer:THM{NOT_SO_HIDDEN}

- I clicked on the news page and found three articles



Acme IT Support

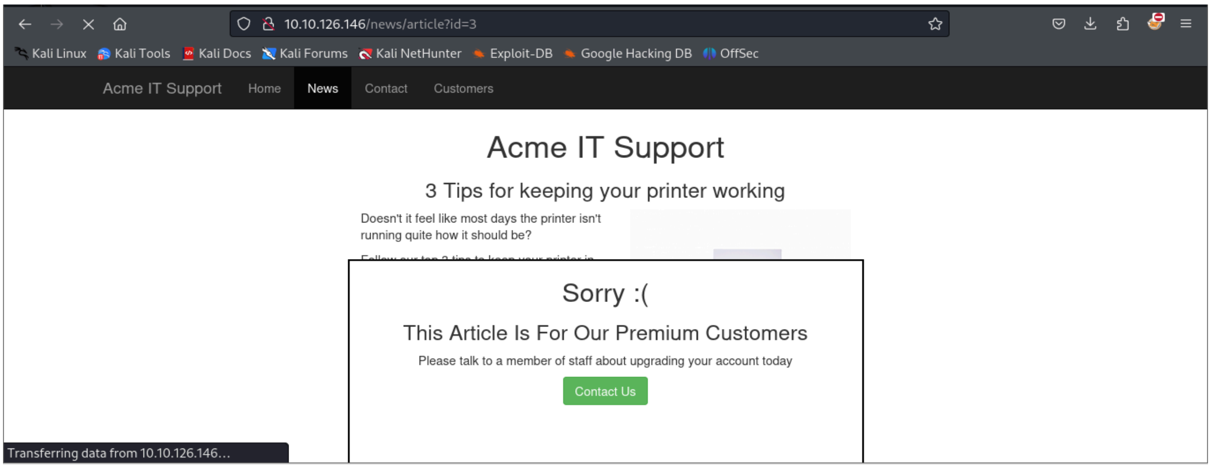
Latest News

Welcome To Acme IT Support

Our Newest Team Member

3 Tips for keeping your printer working

- I found the first two articles readable, but the third has been blocked with a floating notice above the content stating I have to be a premium customer to view the article.



Acme IT Support

3 Tips for keeping your printer working

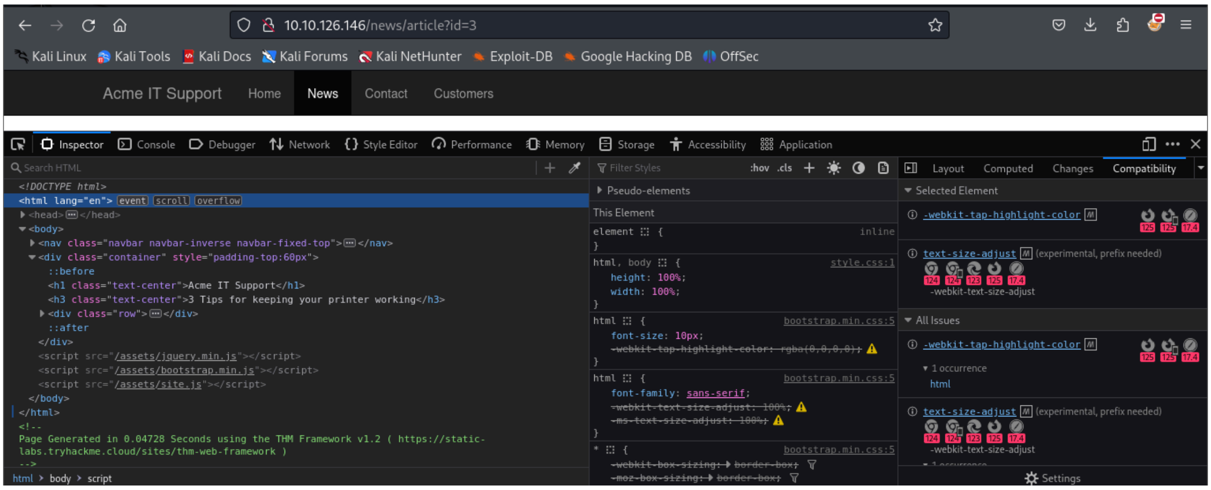
Doesn't it feel like most days the printer isn't running quite how it should be?

Sorry :(

This Article Is For Our Premium Customers

Please talk to a member of staff about upgrading your account today

- ➔ I opened the developer tools on this page and saw the elements/HTML that make up the website

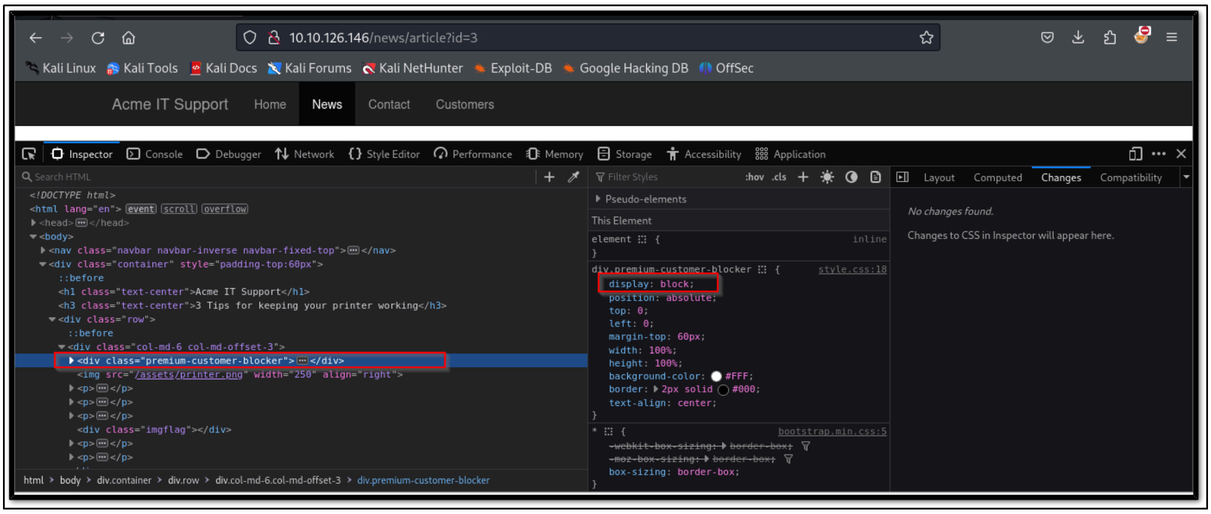


10.10.126.146/news/article?id=3

```
<!DOCTYPE html>
<html lang="en"> event scroll overflow
  <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">⋯</div>
      ::after
    </div>
    <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 0.04728 Seconds using the THM Framework v1.2 ( https://static-
labs.tryhackme.cloud/sites/thm-web-framework )
-->
```

```
element {                                         inline
}
html, body {                                style.css:1
  height: 100%;
  width: 100%;
}
html {                              bootstrap.min.css:5
  font-size: 10px;
  -webkit-tap-highlight-color: rgba(0,0,0,0);
}
html {                              bootstrap.min.css:5
  font-family: sans-serif;
  -webkit-text-size-adjust: 100%;
  -ms-text-size-adjust: 100%;
}
* {                                 bootstrap.min.css:5
  -webkit-box-sizing: border-box;
  -moz-box-sizing: border-box;
```

- ➔ I located the DIV element with the class premium-customer-blocker and clicked on it. I see the display: block.



10.10.126.146/news/article?id=3

```
<!DOCTYPE html>
<html lang="en"> event scroll overflow
  <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">⋯</div>
          <img src="/assets/printer.png" width="250" align="right">
          <p>⋯</p>
          <p>⋯</p>
          <p>⋯</p>
          <div class="imgflag"></div>
          <p>⋯</p>
          <p>⋯</p>
```

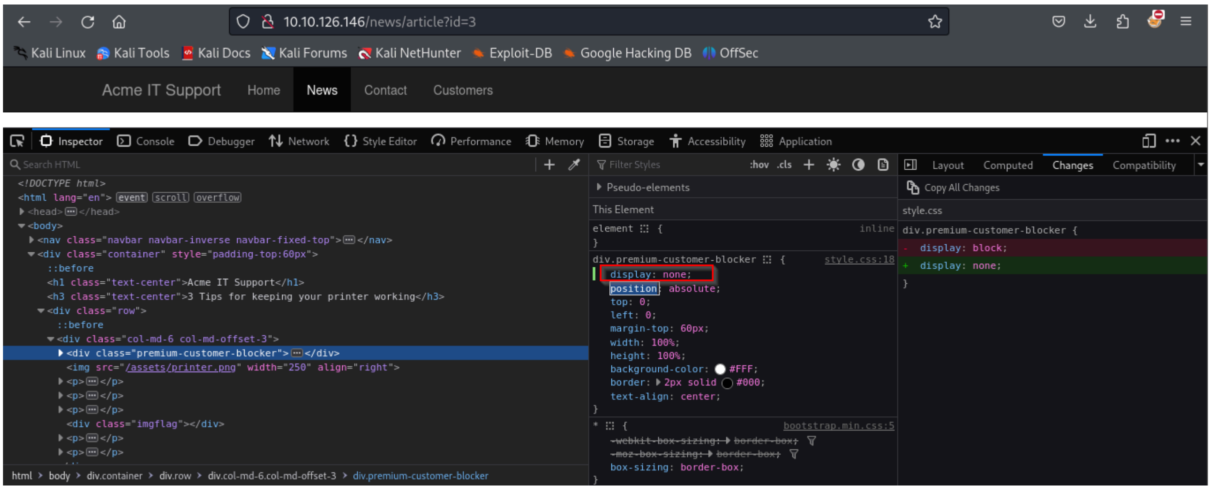
html › body › div.container › div.row › div.col-md-6.col-md-offset-3 › div.premium-customer-blocker

```
element {                                         inline
}
div.premium-customer-blocker {             style.css:18
  display: block;
  position: absolute;
  top: 0;
  left: 0;
  margin-top: 60px;
  width: 100%;
  height: 100%;
  background-color: #FFF;
  border: 2px solid #000;
  text-align: center;
}
* {                                 bootstrap.min.css:5
  -webkit-box-sizing: border-box;
  -moz-box-sizing: border-box;
  box-sizing: border-box;
}
```

No changes found.

Changes to CSS in Inspector will appear here.

- ➔ I clicked on the word block and I typed “none”, this made the box disappear, revealing the content underneath it and a flag.

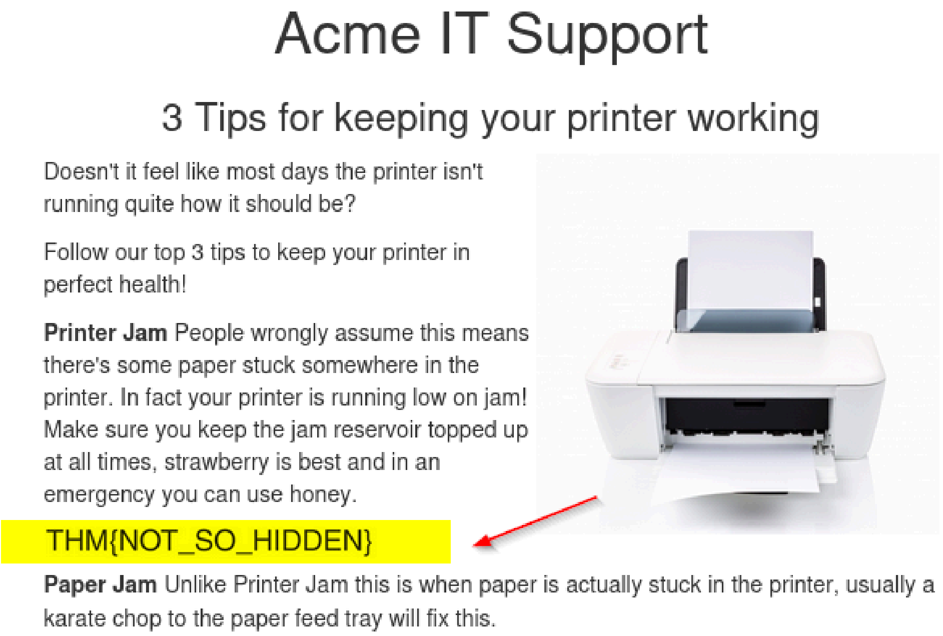


```
<!DOCTYPE html>
<html lang="en"> event scroll overflow
 <head>…</head>
 <body>
  <nav class="navbar navbar-inverse navbar-fixed-top">…</nav>
  <div class="container" style="padding-top:60px">
    ::before
    <h1 class="text-center">Acme IT Support</h1>
    <h3 class="text-center">3 Tips for keeping your printer working</h3>
   <div class="row">
     ::before
    <div class="col-md-6 col-md-offset-3">
     <div class="premium-customer-blocker">…</div>
      <img src="/assets/printer.png" width="250" align="right">
     <p>…</p>
     <p>…</p>
     <p>…</p>
      <div class="imgflag"></div>
     <p>…</p>
     <p>…</p>
html > body > div.container > div.row > div.col-md-6.col-md-offset-3 > div.premium-customer-blocker
```

```
Pseudo-elements
This Element
element {                                        inline
}
div.premium-customer-blocker {              style.css:18
  display: none;
  position: absolute;
  top: 0;
  left: 0;
  margin-top: 60px;
  width: 100%;
  height: 100%;
  background-color: #FFF;
  border: 2px solid #000;
  text-align: center;
}
* {                                      bootstrap.min.css:5
  ~~-webkit-box-sizing: border-box;~~
  ~~-moz-box-sizing: border-box;~~
  box-sizing: border-box;
}
```

```
style.css
div.premium-customer-blocker {
-  display: block;
+  display: none;
}
```

➔ Back to the page, and i get the flag



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}

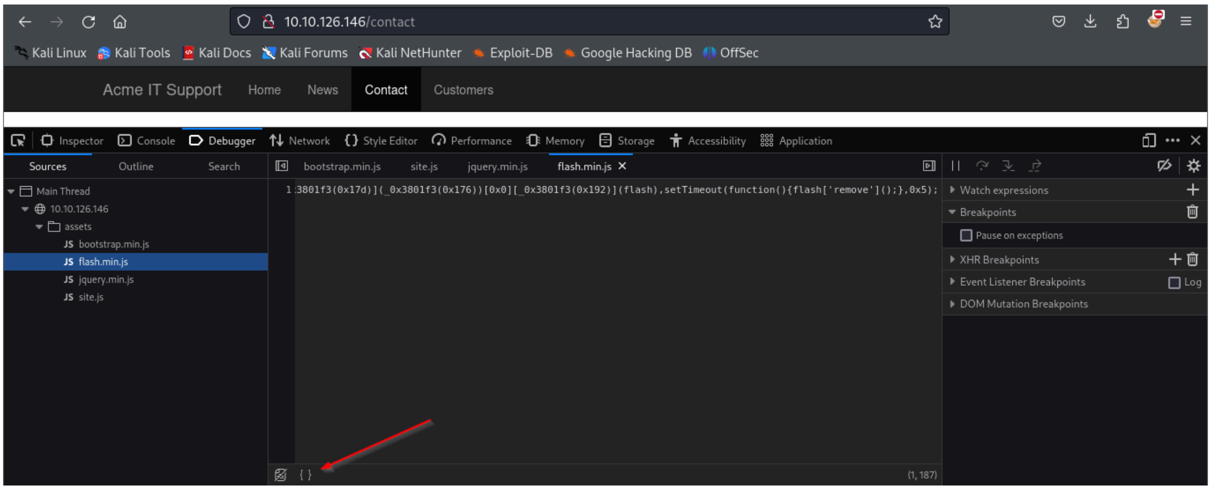
Paper Jam Unlike Printer Jam this is when paper is actually stuck in the printer, usually a karate chop to the paper feed tray will fix this.

Task 5 Developer Tools - Debugger

What is the flag in the red box?

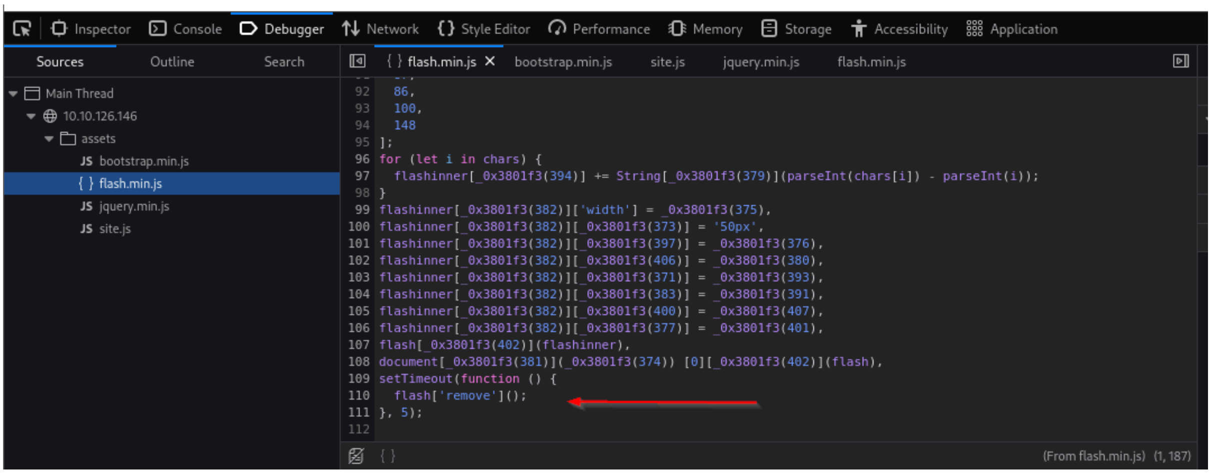
Answer: **THM{CATCH_ME_IF_YOU_CAN}**

➔ On the Acme IT Support website,i clicked on the contact page and opened the developer tools



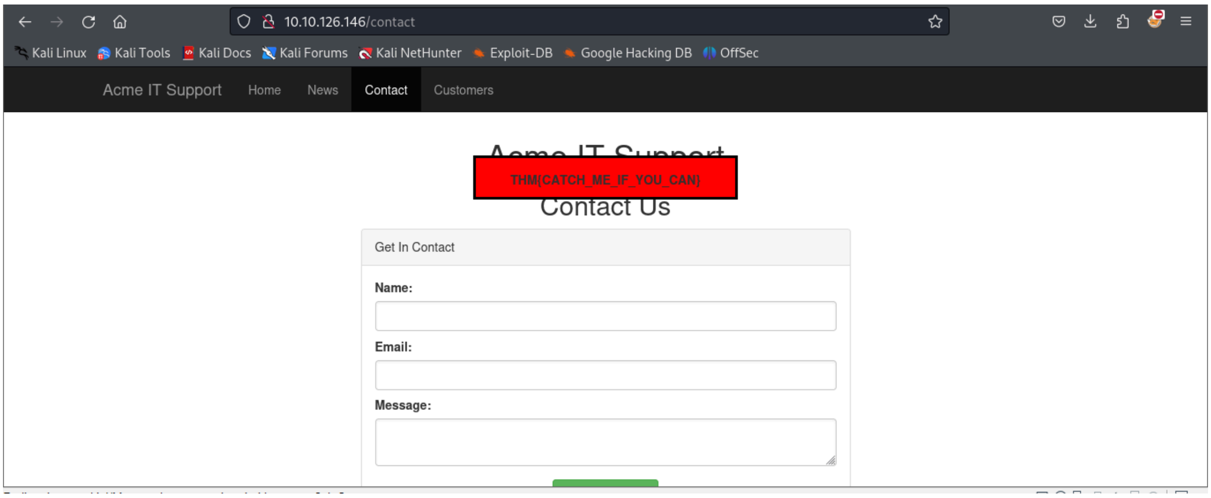
```
3801f3(0x17d)](_0x3801f3(0x176))[0x0][_0x3801f3(0x192)](flash),setTimeout(function(){flash['remove']();},0x5);
```

- ➔ Everything was on one line, but I used the "Pretty Print" option, which looks like two braces { } to make it a little more readable.
- ➔ I scroll to the bottom of the flash.min.js file and i see the line: flash['remove']();



```
  86,
  100,
  148
];
for (let i in chars) {
  flashinner[_0x3801f3(394)] += String[_0x3801f3(379)](parseInt(chars[i]) - parseInt(i));
}
flashinner[_0x3801f3(382)]['width'] = _0x3801f3(375),
flashinner[_0x3801f3(382)][_0x3801f3(373)] = '50px',
flashinner[_0x3801f3(382)][_0x3801f3(397)] = _0x3801f3(376),
flashinner[_0x3801f3(382)][_0x3801f3(406)] = _0x3801f3(380),
flashinner[_0x3801f3(382)][_0x3801f3(371)] = _0x3801f3(393),
flashinner[_0x3801f3(382)][_0x3801f3(383)] = _0x3801f3(391),
flashinner[_0x3801f3(382)][_0x3801f3(400)] = _0x3801f3(407),
flashinner[_0x3801f3(382)][_0x3801f3(377)] = _0x3801f3(401),
flash[_0x3801f3(402)](flashinner),
document[_0x3801f3(381)](_0x3801f3(374)) [0][_0x3801f3(402)](flash),
setTimeout(function () {
  flash['remove']();
}, 5);
```

- ➔ I clicked the line number that contains the code,flash['remove']();
- ➔ it turns blue; meaning i have inserted a breakpoint on this line.
- ➔ I refreshed the page, and noticed the red box stays on the page instead of disappearing, and it contains a flag.



Acme IT Support

THM{CATCH_ME_IF_YOU_CAN}

Contact Us

Get In Contact

Name:

Email:

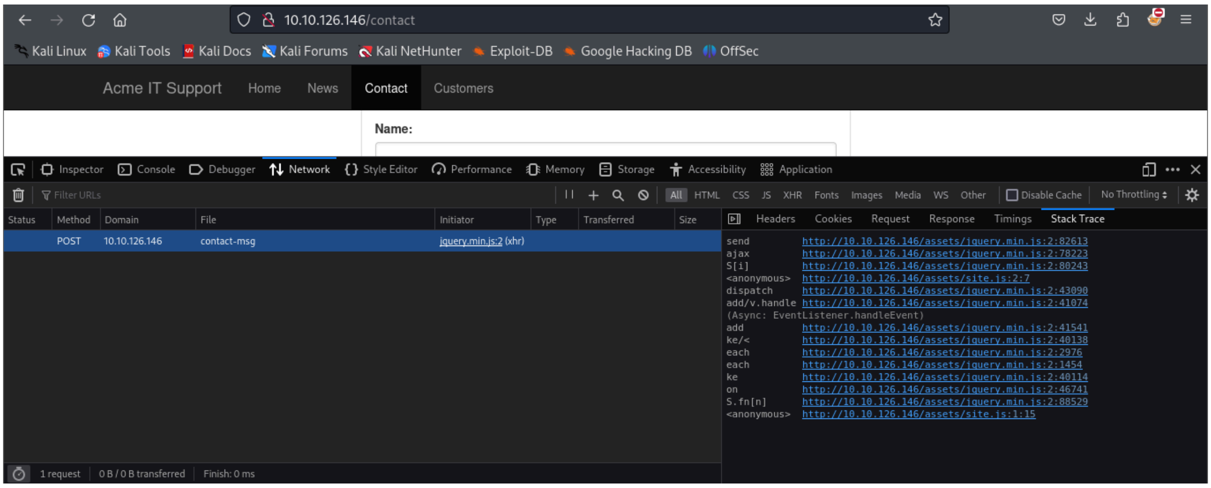
Message:

Task 6 Developer Tools - Network

What is the flag shown on the contact-msg network request?

Answer: **THM{GOT_AJAX_FLAG}**

- ➔ With the network tab open, i filled the contact form and pressed the Send Message button

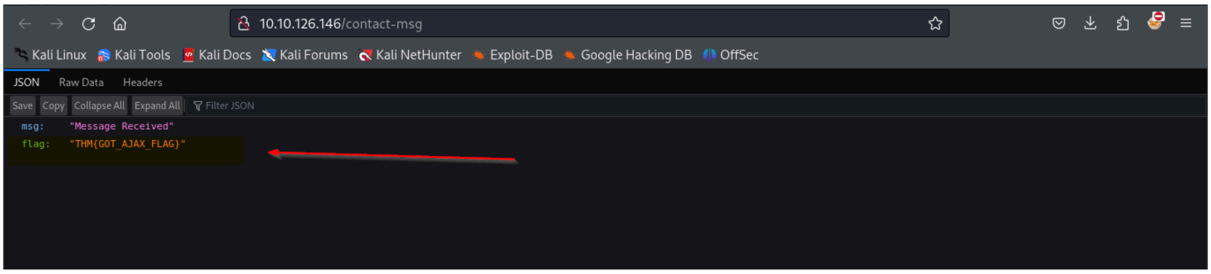


Status	Method	Domain	File	Initiator	Type	Transferred	Size
	POST	10.10.126.146	contact-msg	jquery.min.js:2 (xhr)			

```
send          http://10.10.126.146/assets/jquery.min.js:2:82613
ajax          http://10.10.126.146/assets/jquery.min.js:2:78223
S[i]          http://10.10.126.146/assets/jquery.min.js:2:80243
<anonymous>   http://10.10.126.146/assets/site.js:2:7
dispatch      http://10.10.126.146/assets/jquery.min.js:2:43090
add/v.handle  http://10.10.126.146/assets/jquery.min.js:2:41074
(Async: EventListener.handleEvent)
add           http://10.10.126.146/assets/jquery.min.js:2:41541
ke/<          http://10.10.126.146/assets/jquery.min.js:2:40138
each          http://10.10.126.146/assets/jquery.min.js:2:2976
each          http://10.10.126.146/assets/jquery.min.js:2:1454
ke            http://10.10.126.146/assets/jquery.min.js:2:40114
on            http://10.10.126.146/assets/jquery.min.js:2:46741
S.fn[n]       http://10.10.126.146/assets/jquery.min.js:2:88529
<anonymous>   http://10.10.126.146/assets/site.js:1:15
```

1 request | 0 B / 0 B transferred | Finish: 0 ms

- ➔ I examined the new entry on the network tab that the contact form created and viewed the page(by clicking on the link on the contact-msg) the data was sent to in order to reveal a flag.



10.10.126.146/contact-msg

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

END!!!