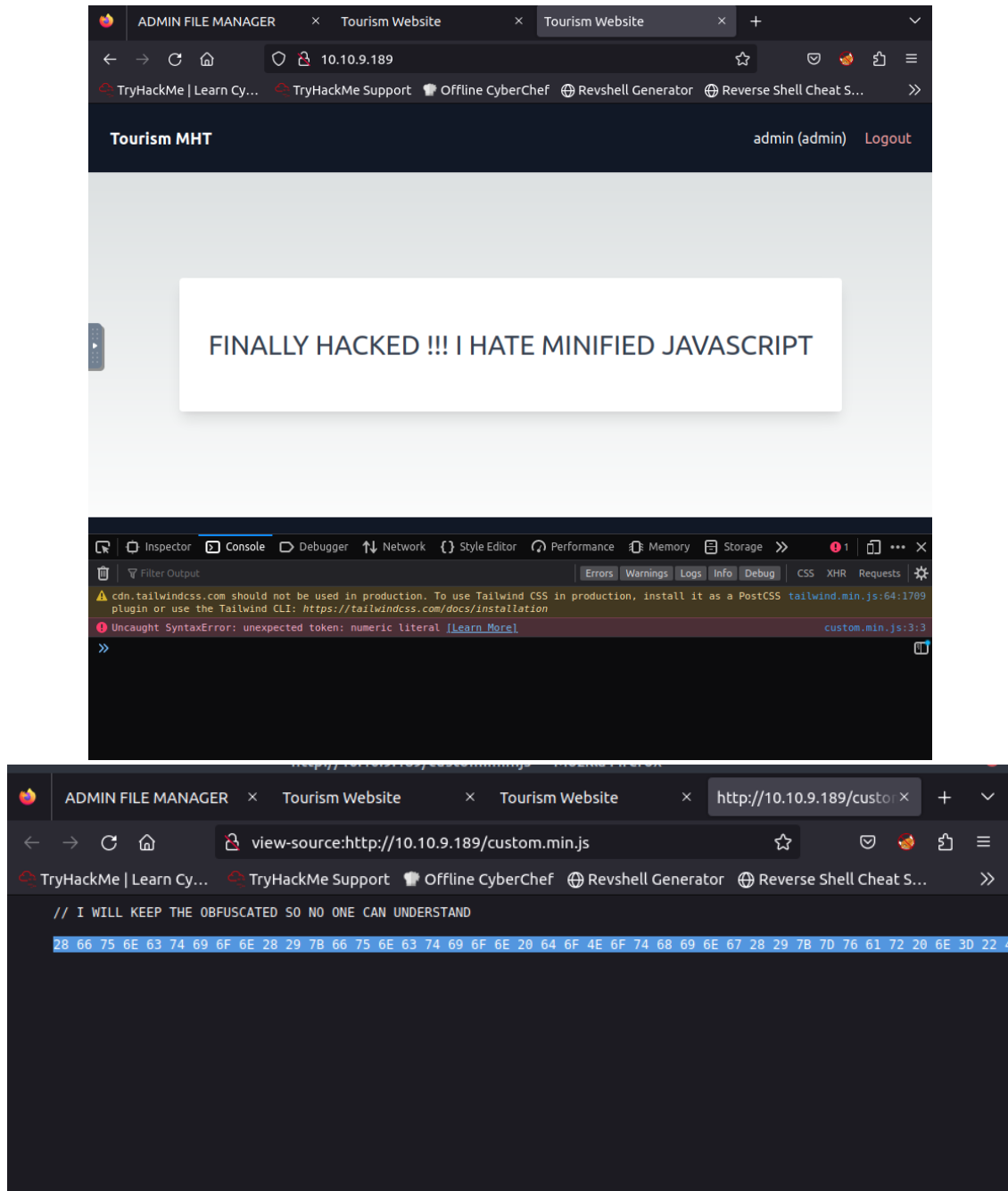


Traverse

Question: What type of encoding is used by the hackers to obfuscate the JavaScript file?

Check the Console tab, we see error message of file **custom.min.js**. Click to read the JS file, we see the type of encoding is used to obfuscate the JS file is HEX.



Answer: Hex

Question: What is the flag value after deobfuscating the file?

Use this [online tool](#) to decode this Hex into Text. After decoding, we see that it is a JS code.

Dán văn bản bạn muốn hex giải mã ở đây:

```
28 66 75 6E 63 74 69 6F 6E 28 29 7B 66 75 6E 63 74 69 6F 6E 20 64 6F 4E 6F 74 68 69 6E 67 28
29 7B 7D 76 61 72 20 6E 3D 22 44 49 52 45 43 54 4F 52 59 22 3B 76 61 72 20 65 3D 22 4C 49 53
54 49 4E 47 22 3B 76 61 72 20 6F 3D 22 49 53 20 54 48 45 22 3B 76 61 72 20 69 3D 22 4F 4E 4C
59 20 57 41 59 22 3B 76 61 72 20 66 3D 6E 75 6C 6C 3B 76 61 72 20 6C 3D 66 61 6C 73 65 3B 76
61 72 20 64 3B 69 66 28 66 3D 3D 3D 6E 75 6C 6C 29 7B 63 6F 6E 73 6F 6C 65 2E 6C 6F 67 28 22
46 6C 61 67 3A 22 2B 6E 2B 22 20 22 2B 65 2B 22 20 22 2B 6F 2B 22 20 22 2B 69 29 3B 64 3D 75
6E 64 65 66 69 6E 65 64 7D 65 6C 73 65 20 69 66 28 74 79 70 65 6F 66 20 66 3D 3D 3D 22 75 6E
64 65 66 69 6E 65 64 22 29 7B 64 3D 75 6E 64 65 66 69 6E 65 64 7D 65 6C 73 65 7B 69 66 28 6C
29 7B 64 3D 75 6E 64 65 66 69 6E 65 64 7D 65 6C 73 65 7B 28 66 75 6E 63 74 69 6F 6E 28 29 7B
69 66 28 64 29 7B 66 6F 72 28 76 61 72 20 6E 3D 30 3B 6E 3C 31 30 3B 6E 2B 2B 29 7B 63 6F 6E
73 6F 6C 65 2E 6C 6F 67 28 22 54 68 69 73 20 63 6F 64 65 20 64 6F 65 73 20 6E 6F 74 68 69 6E
67 2E 22 29 7D 64 6F 4E 6F 74 68 69 6E 67 28 29 7D 65 6C 73 65 7B 64 6F 4E 6F 74 68 69 6E 67
28 29 7D 7D 29 28 29 7D 7D 29 28 29 3B
```

Hex Decode!

Hex vào văn bản

[Download file](#)

Sao chép văn bản giải mã hex của bạn ở đây:

```
(function(){function doNothing(){var n="DIRECTORY";var e="LISTING";var o="IS THE";var i="ONLY
WAY";var f=null;var l=false;var d;if(f===null){console.log("Flag:"+n+" "+e+" "+o+"
");d=undefined}else if(typeof f==="undefined"){d=undefined}else{if(l){d=undefined}else{(function()
{if(d){for(var n=0;n<10;n++){console.log("This code does nothing.")doNothing();}else{doNothing();}}
)}}}());
```



js-beautify

(v1.14.9)

Beautify JavaScript, JSON, React.js, HTML, CSS, SCSS, and SASS

```
(function() {
  function doNothing() {}
  var n = "DIRECTORY";
  var e = "LISTING";
  var o = "IS THE";
  var i = "ONLY WAY";
  var f = null;
  var l = false;
  var d;
  if (f === null) {
    console.log("Flag:" + n + " " + e + " " + o + " " + i);
    d = undefined
  } else if (typeof f === "undefined") {
    d = undefined
  } else {
    if (1) {
      d = undefined
    } else {
      (function() {
        if (d) {
          for (var n = 0; n < 10; n++) {
            console.log("This code does nothing.")
          }
          doNothing()
        } else {
          doNothing()
        }
      })()
    }
  }
})();
```

This code is a function to create a Flag, we can use any tool to execute the script. Here I use [online tool](#) to execute this code then I got the Flag.



```
index.html × script.js ×
1  (function() {
2      function doNothing() {}
3      var n = "DIRECTORY";
4      var e = "LISTING";
5      var o = "IS THE";
6      var i = "ONLY WAY";
7      var f = null;
8      var l = false;
9      var d;
10     if (f === null) {
11         console.log("Flag:" + n + " " + e + " " + o + " " + i);
12         d = undefined
13     } else if (typeof f === "undefined") {
14         d = undefined
15     } else {
16         if (l) {
17             d = undefined
18         } else {
19             (function() {
20                 if (d) {
21                     for (var n = 0; n < 10; n++) {
22                         console.log("This code does nothing.")
23                     }
24                 }
25             })()
26         }
27     }
28 })()
```

Console × ...

Flag:DIRECTORY LISTING IS THE ONLY WAY

Answer: DIRECTORY LISTING IS THE ONLY WAY

Question: Logging is an important aspect. What is the name of the file containing email dumps?



By reading source we see a command for folder `./logs` that navigate to `/logs`.

```
18
19 <body>
20 <!-- Navigation Bar -->
21 <nav class="bg-gray-900 text-white p-6">
22 <div class="flex justify-between items-center">
23 <a href="/" class="text-lg font-bold">Tourism MHT </a>
24 <ul class="flex items-center gap-5">
25 <!-- <li><a href="/img" class="hover:text-gray-300">Logs</a></li> Please keep all images in this folder -->
26 <!-- <li><a href="/logs" class="hover:text-gray-300">Logs</a></li> DevOps team to check and remove it later on -->
27
28
```

← → ↻ 🏠 🔒 10.10.9.189/logs/ ☆

TryHackMe | Learn Cy... TryHackMe Support 📄 Offline CyberChef 🌐 Revshell Generator 🌐 Reverse S

Index of /logs

| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
|  Parent Directory | | - | |
|  email_dump.txt | 2023-05-26 06:11 | 450 | |

Apache/2.4.41 (Ubuntu) Server at 10.10.9.189 Port 80

Answer: email_dump.txt

Question: The logs folder contains email logs and has a message for the software team lead. What is the name of the directory that Bob has created?

By reading the email, and understanding the SSDLC so first phase is **Planning**

```
From: Bob <bob@tourism.mht>
To: Mark <mark@tourism.mht>
Subject: API Credentials

Hey Mark,

Sorry I had to rush earlier for the holidays, but I have created the directory for you with all the required information for the API.
You loved SSDLC so much, I named the API folder under the name of the first phase of SSDLC.
This page is password protected and can only be opened through the key. THM{100100111}

See ya after the holidays

Bob.
```

Answer: Planning

Question: What is the key file for opening the directory that Bob has created for Mark?

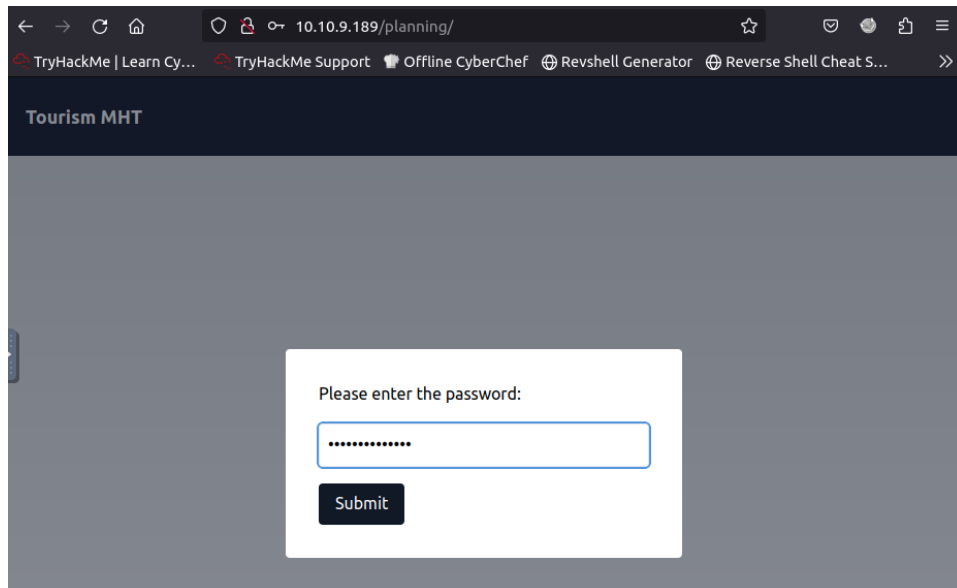
By reading the content of the email, I can see the flag

Answer: THM{100100111}

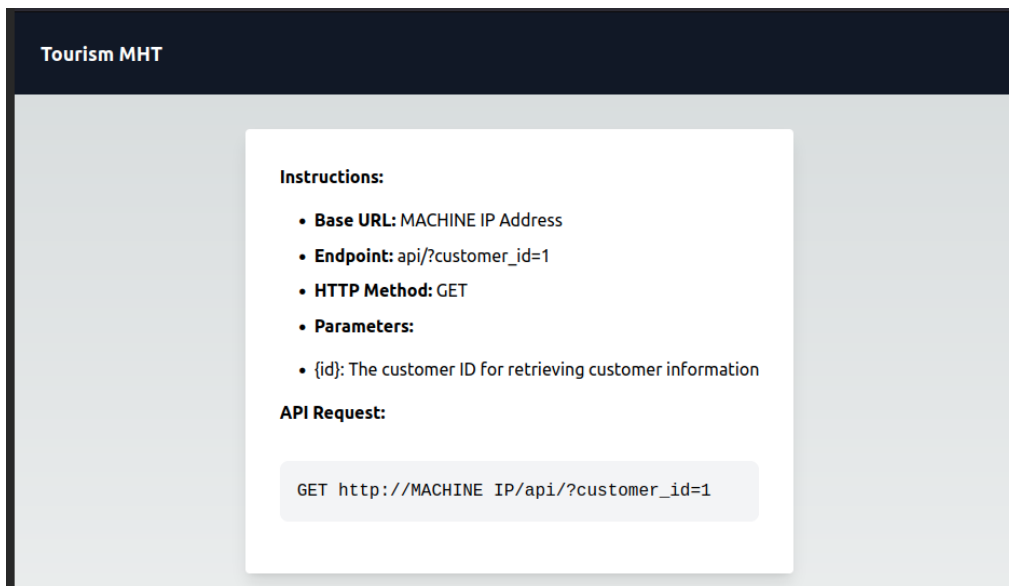
Question: What is the email address for ID 5 using the leaked API endpoint?

Go to the **/planning** and enter the password above, we will see an API Document. Enter the key in previous question, we can login into the Planning page. We can see that there is a guide for us to get something form API Request:

GET http://MACHINE IP/api/?customer_id=1



A screenshot of a web browser window. The address bar shows the URL `10.10.9.189/planning/`. The browser's tab bar includes several tabs: 'TryHackMe | Learn Cy...', 'TryHackMe Support', 'Offline CyberChef', 'Revshell Generator', and 'Reverse Shell Cheat S...'. The page header is dark blue with the text 'Tourism MHT'. The main content area is a light gray. In the center, there is a white rectangular box containing the text 'Please enter the password:' above a password input field with a blue border and a series of dots. Below the input field is a dark blue 'Submit' button.



A screenshot of the 'Tourism MHT' web application. The header is dark blue with 'Tourism MHT' in white. The main content area is light gray. A white box in the center contains the following information:

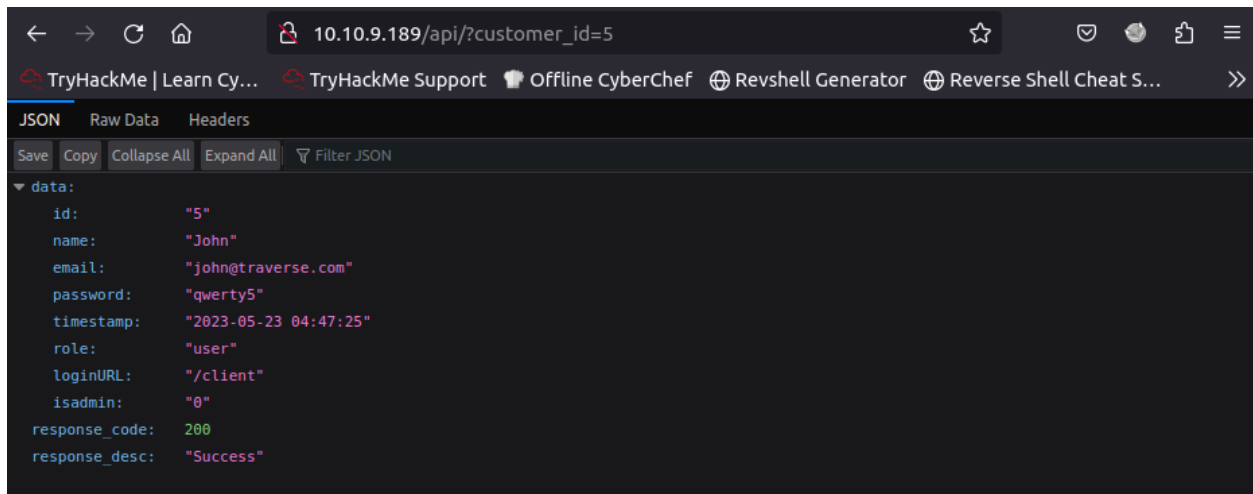
Instructions:

- **Base URL:** MACHINE IP Address
- **Endpoint:** api/?customer_id=1
- **HTTP Method:** GET
- **Parameters:**
 - {id}: The customer ID for retrieving customer information

API Request:

```
GET http://MACHINE IP/api/?customer_id=1
```

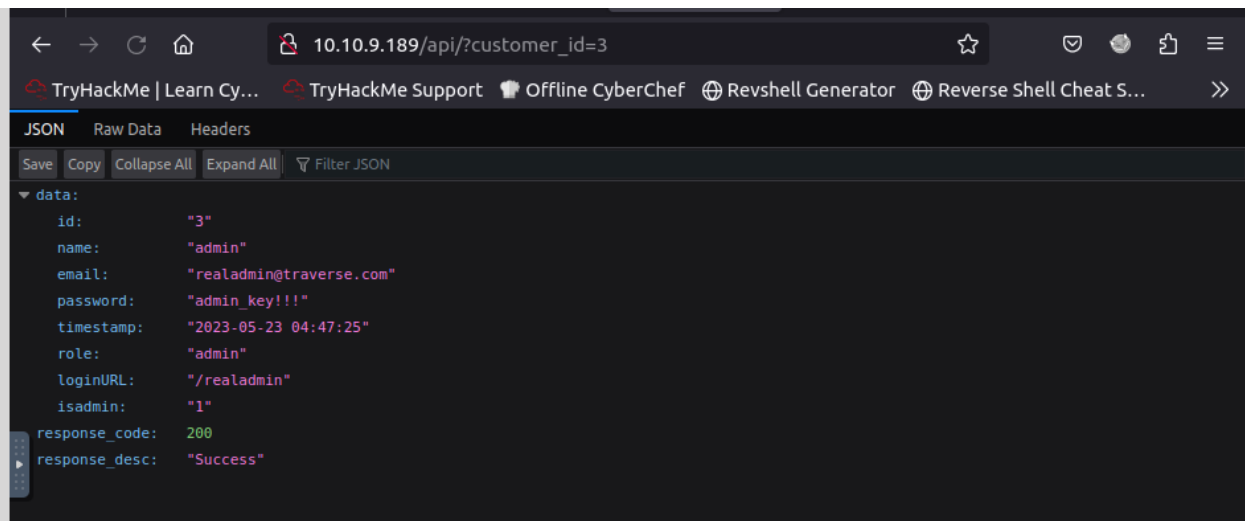
Then we make a request to id=5. We can see that the return is the information of the customer with id=5. There are some sensitive information such as email, password.



```
10.10.9.189/api/?customer_id=5
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
data:
  id: "5"
  name: "John"
  email: "john@traverse.com"
  password: "qwerty5"
  timestamp: "2023-05-23 04:47:25"
  role: "user"
  loginURL: "/client"
  isAdmin: "0"
  response_code: 200
  response_desc: "Success"
```

Answer: john@traverse.com

Question: What is the ID for the user with admin privileges?



```
10.10.9.189/api/?customer_id=3
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
data:
  id: "3"
  name: "admin"
  email: "realadmin@traverse.com"
  password: "admin_key!!!"
  timestamp: "2023-05-23 04:47:25"
  role: "admin"
  loginURL: "/realadmin"
  isAdmin: "1"
  response_code: 200
  response_desc: "Success"
```

Answer: 3

Question: What is the endpoint for logging in as the admin? Mention the last endpoint instead of the URL. For example, if the answer is URL is tryhackme.com/admin - Just write /admin.

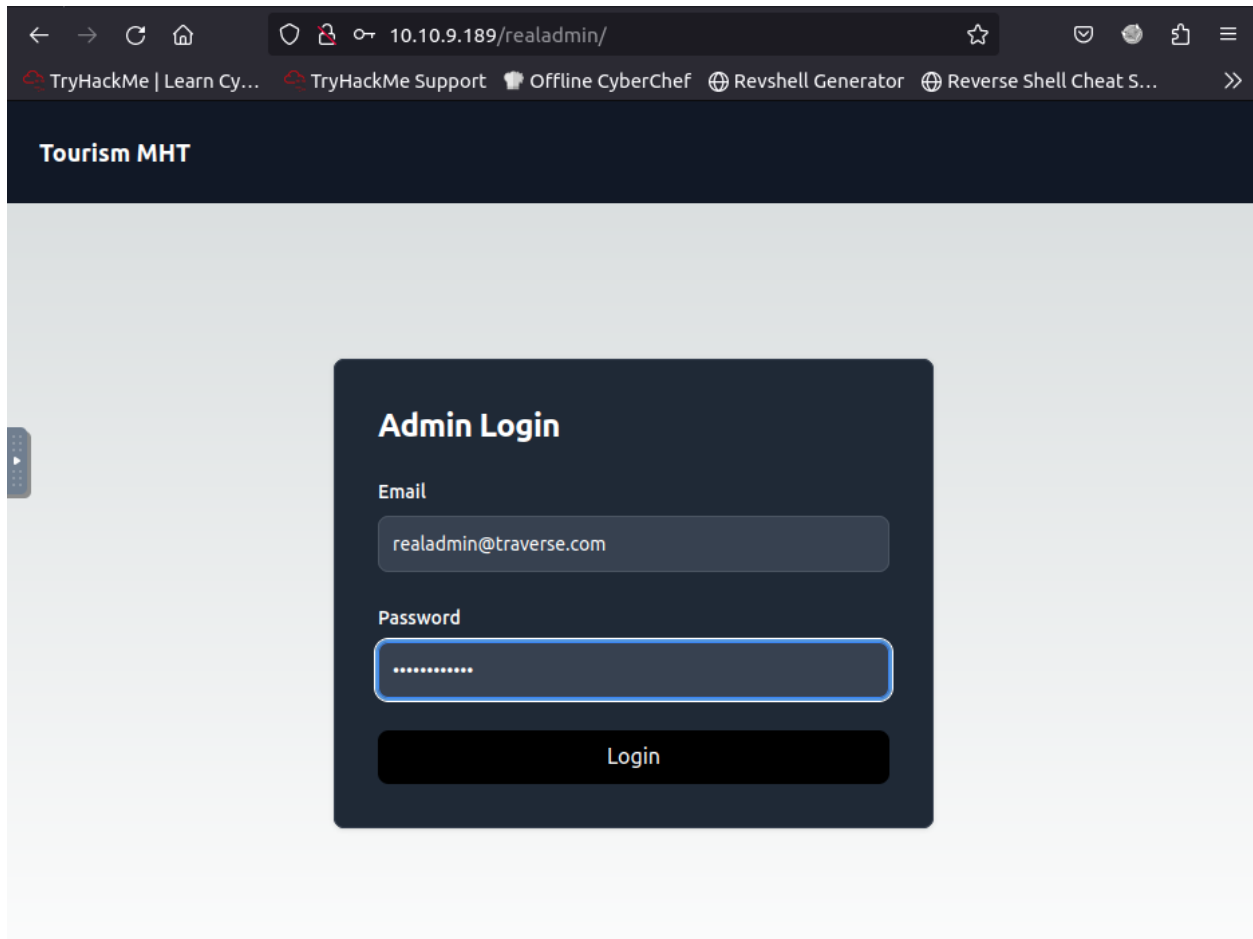
Answer: /readladmin

Question: The attacker uploaded a web shell and renamed a file used for managing the server. Can you find the name of the web shell that the attacker has uploaded?

Answer: thm_shell.php

Question: What is the name of the file renamed by the attacker for managing the web server?

Login with admin using admin login URL



The screenshot shows a web browser window with the address bar displaying `10.10.9.189/realadmin/`. The browser's address bar and tabs are visible at the top. The page has a dark blue header with the text "Tourism MHT". The main content area is light gray and contains a dark blue login form titled "Admin Login". The form has two input fields: "Email" with the value `realadmin@traverse.com` and "Password" with a masked password represented by dots. A "Login" button is located at the bottom of the form.

← → ↻ 🏠 10.10.9.189/realadmin/ ☆ 📧 📁 ☰

TryHackMe | Learn Cy... TryHackMe Support 🍷 Offline CyberChef 🌐 Revshell Generator 🌐 Reverse Shell Cheat S... >>

Tourism MHT

Admin Login

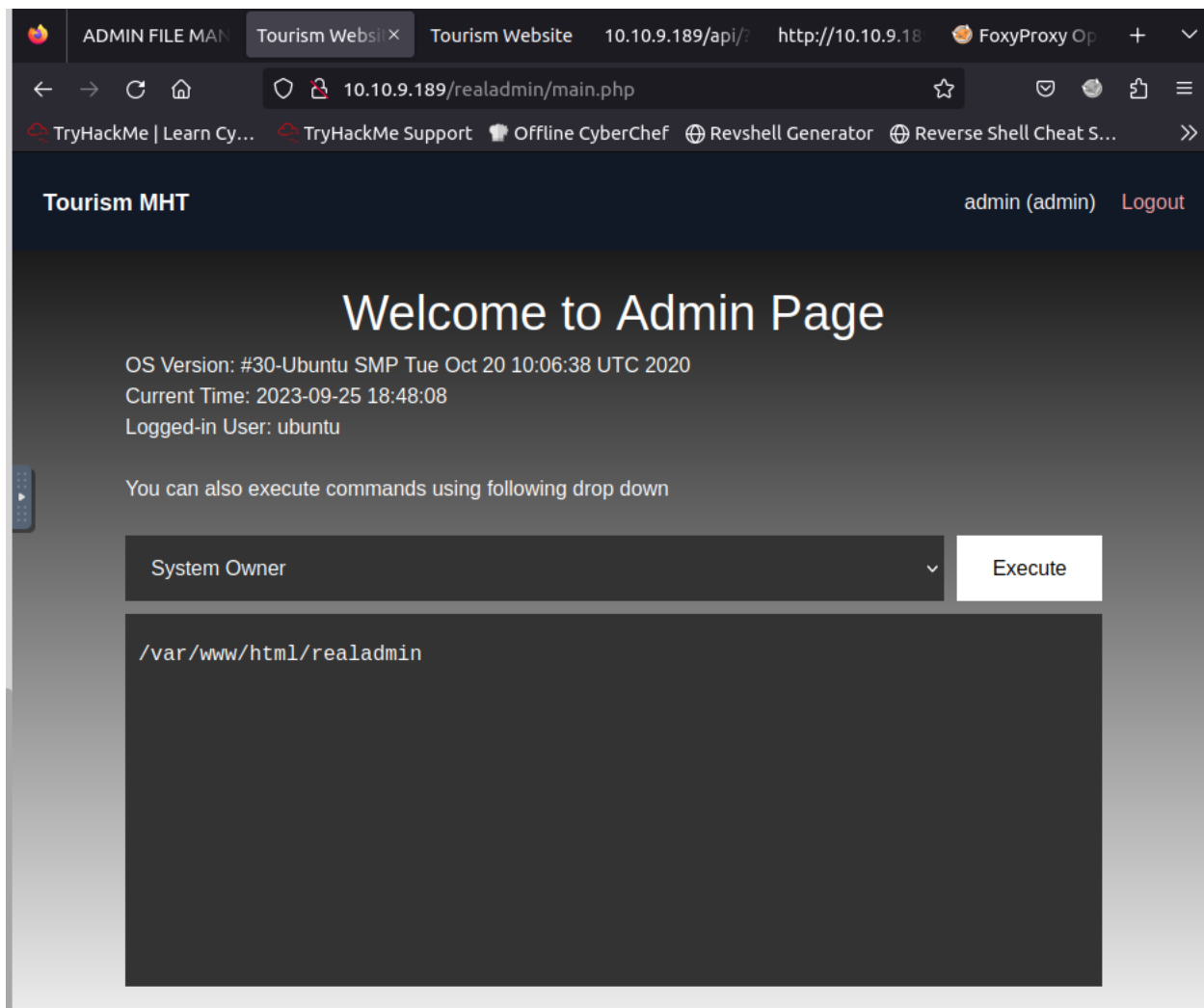
Email

realadmin@traverse.com

Password

.....

Login



Using dropdown command to excute, we see that the current directory → Using bursuite to intercept the request

Intercepted request to http://10.10.9.189:80

Forward Drop Intercept is on Action Open browser

Raw

```
1 POST /realadmin/main.php HTTP/1.1
2 Host: 10.10.9.189
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 15
9 Origin: http://10.10.9.189
10 Connection: close
11 Referer: http://10.10.9.189/realadmin/main.php
12 Cookie: PHPSESSID=mr5d3dhqdgjbgsh5af8f5mrf6; filemanager=huhbe8rt2hvr cbg56ndgbq5ccl
13 Upgrade-Insecure-Requests: 1
14
15 commands=pwd
```

Change the command into 'ls' to list all the files.

Intercepted request to http://10.10.9.189:80

Forward Drop Intercept is on Action Open browser

Raw

```
1 POST /realadmin/main.php HTTP/1.1
2 Host: 10.10.9.189
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 12
9 Origin: http://10.10.9.189
10 Connection: close
11 Referer: http://10.10.9.189/realadmin/main.php
12 Cookie: PHPSESSID=mr5d3dhqdgjbgsh5af8f5mrf6; filemanager=huhbe8rt2hvr cbg56ndgbq5ccl
13 Upgrade-Insecure-Requests: 1
14
15 commands=ls
```

Welcome to Admin Page

OS Version: #30-Ubuntu SMP Tue Oct 20 10:06:38 UTC 2020

Current Time: 2023-09-25 18:49:46

Logged-in User: ubuntu

You can also execute commands using following drop down

System Owner



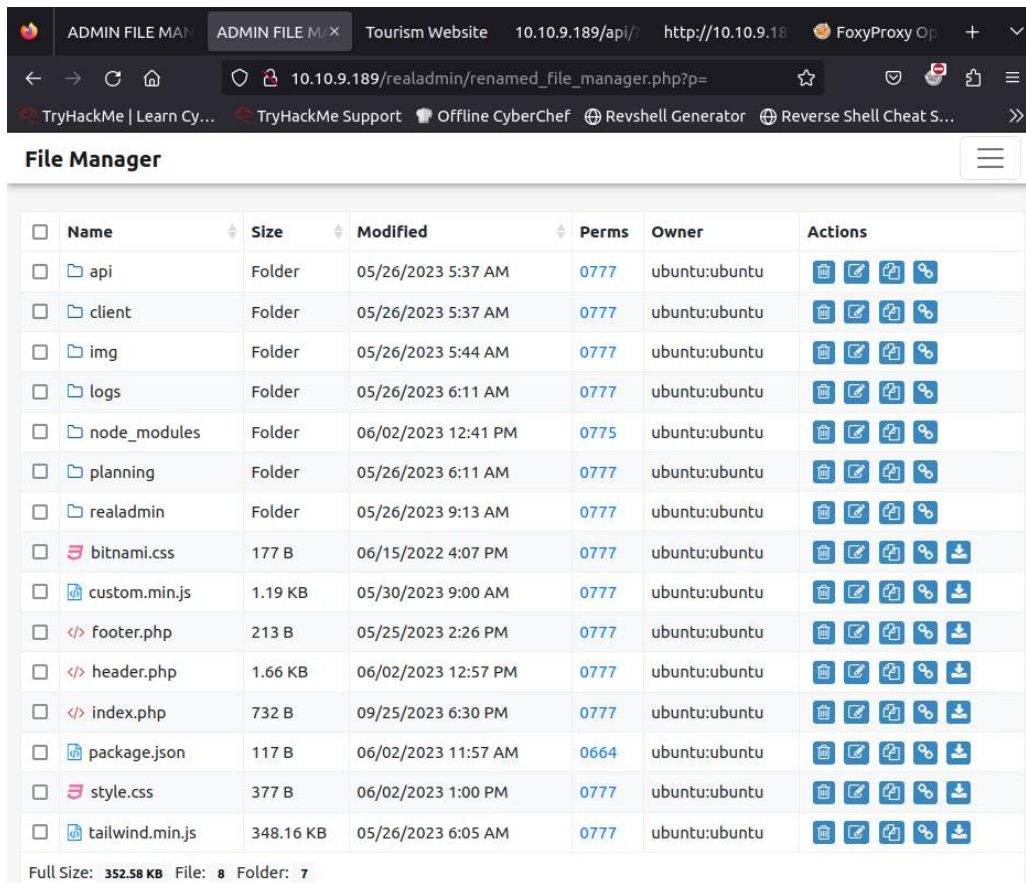
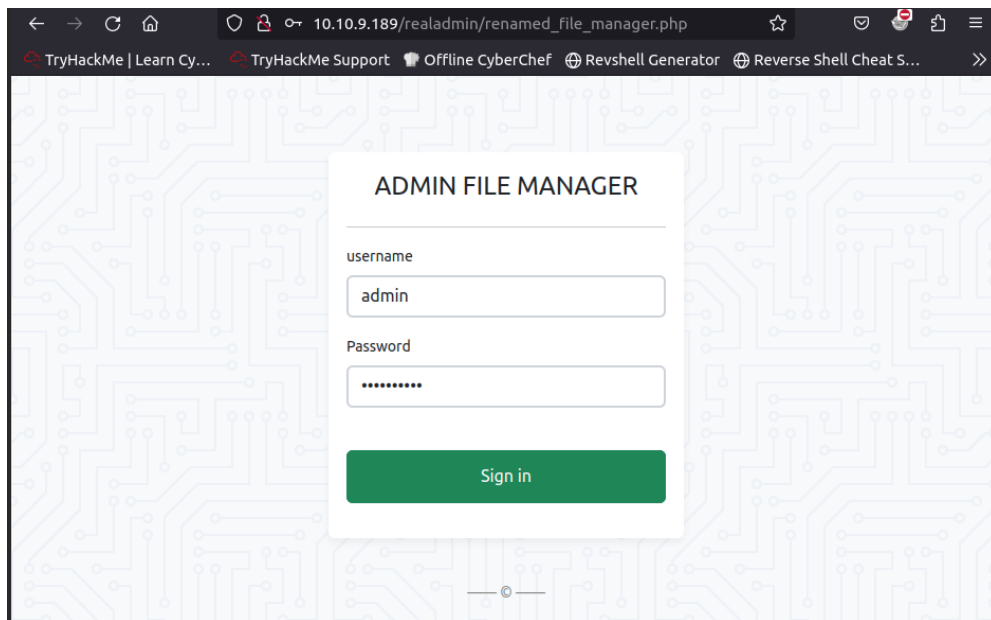
Execute

```
Password for accessing original file manager: THM{10101}  
index.php  
main.php  
renamed_file_manager.php  
thm_shell.php
```

Answer: renamed_file_manager.php

Question: Can you use the file manager to restore the original website by removing the "FINALLY HACKED" message? What is the flag value after restoring the main website?

Using URL to navigate to `/realadmin/renamed_file_manager.php`



Execute remove “FINALLY HACKED” of \$message

File Manager

Charset: utf-8

[Download](#) [Open](#) [Edit](#) [Advanced Editor](#) [Back](#)

```
<!-- Rest PHP code and html content -->
<?php
include './api/login.php';
$basePath = "/";
?>

<!DOCTYPE html>
<html lang="en">

<?php
include 'header.php';
$message = "FINALLY HACKED";
?>

<!-- Main Content -->
<main class="mx-auto py-8 h-[80vh] flex items-center justify-center">

  <div class="rounded overflow-hidden shadow-lg bg-white p-8 flex ">
    <?php
      if($message != "FINALLY HACKED"){
        echo '<h1 class="text-gray-700 text-3xl py-6"> SUCCESSFULLY RESTORED WEBSITE FLAG: THM{WEBSITE_RES
      }
    }
    else{
      ?>
      <h2 class="text-gray-700 text-3xl py-6"> <?php echo $message; ?> !!! I HATE MINIFIED JAVASCRIPT</h2>
    }
  }
  ?>
</div>
</main>
```

```
<!-- Rest PHP code and html content -->
<?php
include './api/login.php';
$basePath = "/";
?>

<!DOCTYPE html>
<html lang="en">

<?php
include 'header.php';
$message = "";
?>

<!-- Main Content -->
<main class="mx-auto py-8 h-[80vh] flex items-center justify-center">

  <div class="rounded overflow-hidden shadow-lg bg-white p-8 flex ">
    <?php
      if($message != "FINALLY HACKED"){
        echo '<h1 class="text-gray-700 text-3xl py-6"> SUCCESSFULLY RESTORED WEBSITE FLAG: THM{WEBSITE_RESTORED}
      }
    }
    else{
      ?>
      <h2 class="text-gray-700 text-3xl py-6"> <?php echo $message; ?> !!! I HATE MINIFIED JAVASCRIPT</h2>
    }
  }
  ?>
</div>
</main>
```

SUCCESSFULLY RESTORED WEBSITE FLAG:
THM{WEBSITE_RESTORED}

Answer: THM{WEBSITE_RESTORED}