Scavenger Hunt

Scavenger Hunt 🔖

👤 | 50 points ✕

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Description

Hints ❓

1

There is some interesting information hidden around this site http://mercury.picoctf.net:27393/. Can you find it?

30,295 solves / 35,657 users attempted (85%)

62%
Liked
👎 👍

🏳 picoCTF{FLAG}

Submit Flag

| Elements | Console | **Sources** | Network | Performance | Memory | Application | Security | Lighthouse | Recorder ⏺ | Performa |

Page » ⋮ ◁ (index) ✕ myjs.js css?family=Open+Sans|Roboto mycss.css KFOmCnqEu92Fr1Mu4mxK.woff2 » ▶|

```
24        <div id="tababout" class="tabcontent">
25            <h3>What</h3>
26            <p>I used these to make this site: <br/>
27            HTML <br/>
28            CSS <br/>
29            JS (JavaScript)
30            </p>
31        <!-- Here's the first part of the flag: picoCTF{t -->
32            </div>
33
34        </div>
35
36    </body>
37 </html>
38
```
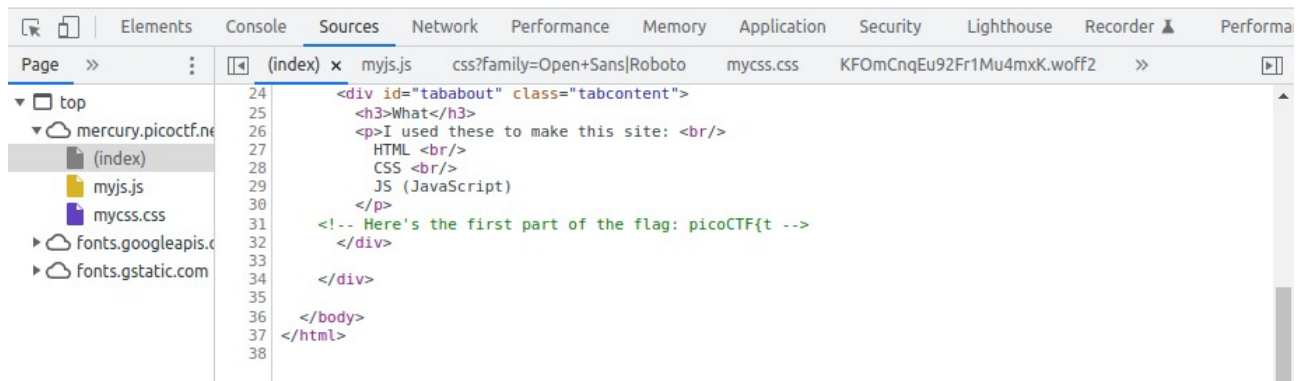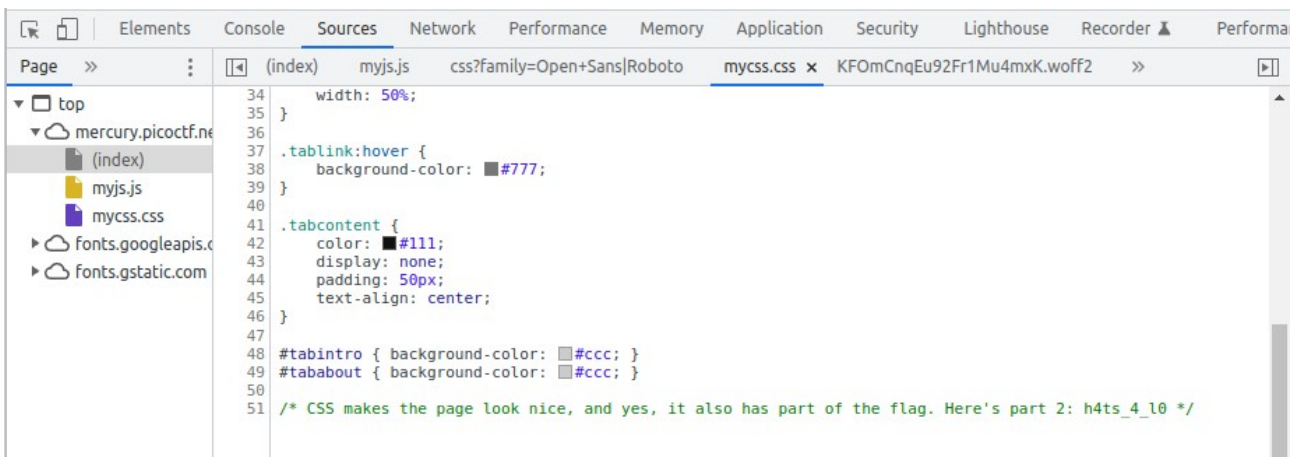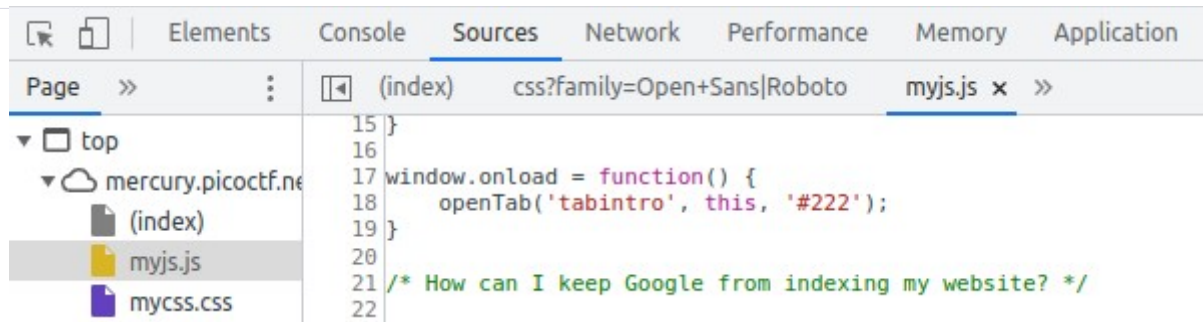
▼ □ top
  ▼ ☁ mercury.picoctf.ne
      📄 (index)
      📙 myjs.js
      📘 mycss.css
  ▷ ☁ fonts.googleapis.c
  ▷ ☁ fonts.gstatic.com

| Elements | Console | **Sources** | Network | Performance | Memory | Application | Security | Lighthouse | Recorder ⏺ | Performa |

Page » ⋮ ◁ (index) myjs.js css?family=Open+Sans|Roboto **mycss.css** ✕ KFOmCnqEu92Fr1Mu4mxK.woff2 » ▶|

```
34        width: 50%;
35 }
36
37 .tablink:hover {
38      background-color: ▮#777;
39 }
40
41 .tabcontent {
42      color: ▮#111;
43      display: none;
44      padding: 50px;
45      text-align: center;
46 }
47
48 #tabintro { background-color: ▯#ccc; }
49 #tababout { background-color: ▯#ccc; }
50
51 /* CSS makes the page look nice, and yes, it also has part of the flag. Here's part 2: h4ts_4_l0 */
```

▼ □ top
  ▼ ☁ mercury.picoctf.ne
      📄 (index)
      📙 myjs.js
      📘 mycss.css
  ▷ ☁ fonts.googleapis.c
  ▷ ☁ fonts.gstatic.com

```
15 }
16
17 window.onload = function() {
18     openTab('tabintro', this, '#222');
19 }
20
21 /* How can I keep Google from indexing my website? */
22
```

Indexing is the process by which search engines like Google, Bing, and others gather and store information about web pages on the internet. Search engines use web crawlers, also known as spiders or bots, to automatically scan websites and follow links to other pages on the internet.

During this process, the web crawler analyzes the content of the page, including text, images, and other media, and adds this information to a database called an index. The index allows search engines to quickly retrieve information about a particular website or web page when a user enters a search query.

When a user types a search query into a search engine, the search engine uses the index to find relevant web pages and ranks them in order of relevance. This ranking is based on a variety of factors, including the content on the page, the number and quality of links pointing to the page, and the overall reputation of the website.

If you want to prevent Google from indexing your website, there are several ways to do it:

1. Use the robots.txt file: This is a file that is placed in the root directory of your website, and it tells search engines which pages and files they are allowed to crawl and index. You can use this file to exclude certain pages or directories from being indexed by Google.

2. Use a "noindex" meta tag: You can add a meta tag to the head section of your web pages that tells search engines not to index that particular page. The tag looks like this: <meta name="robots" content="noindex">

3. Password-protect your website: If your website is behind a password-protected area, search engines won't be able to access it and therefore won't index it.

4. Use a "disallow" directive in the robots.txt file: If you want to exclude a specific URL or directory from being indexed by Google, you can use the "disallow" directive in the robots.txt file. For example: Disallow: /directory-name/

It's important to note that while these methods can help prevent Google from indexing your website, they are not foolproof. Some search engines may still index your site even if you use these methods. If you want to be absolutely sure that your site is not indexed by search engines, you may want to consider making it completely private or not putting it online at all.

```
← → C ⌂    ⚠ Not secure | mercury.picoctf.net:27393/robots.txt    < ☆

User-agent: *
Disallow: /index.html
# Part 3: t_0f_pl4c
# I think this is an apache server... can you Access the next flag?
```

An Apache server is a web server software that is widely used to serve websites and web applications. It is an open-source software that is maintained by the Apache Software Foundation and runs on various operating systems including Windows, Linux, and macOS.

Apache server is highly customizable and configurable, allowing administrators to set up and manage complex websites and web applications with ease. It supports a wide range of features such as SSL/TLS encryption, dynamic content generation through server-side scripting, and URL rewriting for search engine optimization.Apache server is also extensible through modules that can be added to enhance its functionality, such as mod_rewrite for URL manipulation and mod_ssl for encryption. Its popularity and extensive documentation make it a preferred choice for many web developers and administrators.Apache server is not only used to host websites but also used for other purposes such as serving files and media, streaming audio and video, and as a proxy server. Its flexibility and versatility make it a key component of many web-based systems and applications.

Accessing hidden files on a Mac-based Apache server from a link is not recommended, as it can be a security risk and may not be possible without the proper credentials and access permissions.
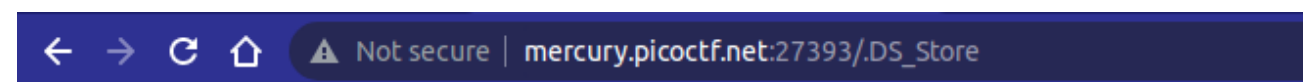
If you have access to the server via SSH or an FTP client, you can navigate to the directory where the hidden files are located and view them. Common hidden files on a Mac-based Apache server include:

1. .htaccess: This file is used to control access to specific directories or files on the server.

2. .htpasswd: This file contains usernames and hashed passwords for users who are authorized to access password-protected areas of the server.

3. .bash_profile: This file contains user-specific configurations for the Bash shell, which is commonly used on Mac-based servers.

4. .DS_Store: This file is created by the macOS operating system and stores metadata about the contents of a directory.

5. .svn: This directory is used in Subversion version control systems to store metadata and configuration information.

It's important to note that accessing and modifying hidden files on a server without proper knowledge or permission can cause issues and compromise security. Only authorized personnel with the necessary credentials and access permissions should interact with these files. As such, accessing hidden files on a Mac-based Apache server from a link may not be possible or advisable.

← → C ⌂ ⚠ Not secure | mercury.picoctf.net:27393/.htaccess
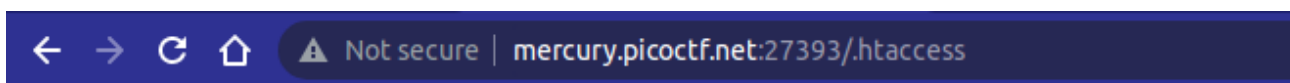
```
# Part 4: 3s_2_l00k
# I love making websites on my Mac, I can Store a lot of information there.
```

← → C ⌂ ⚠ Not secure | mercury.picoctf.net:27393/.DS_Store

```
Congrats! You completed the scavenger hunt. Part 5: _d375c750}
```