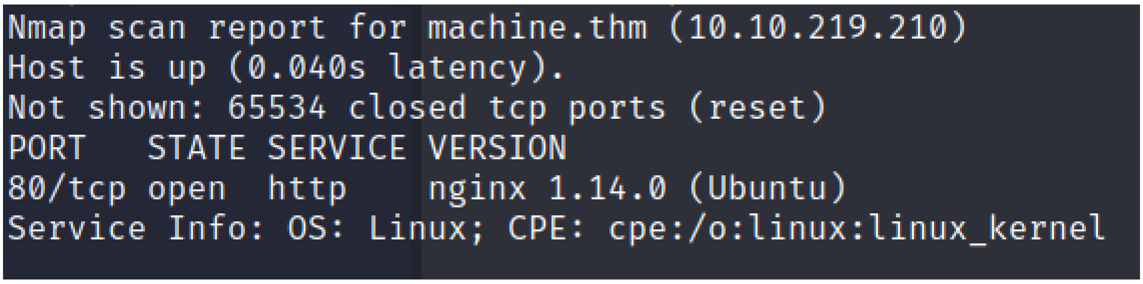
# Writeup TryHackMe – GitHappens

## Reconnaissance

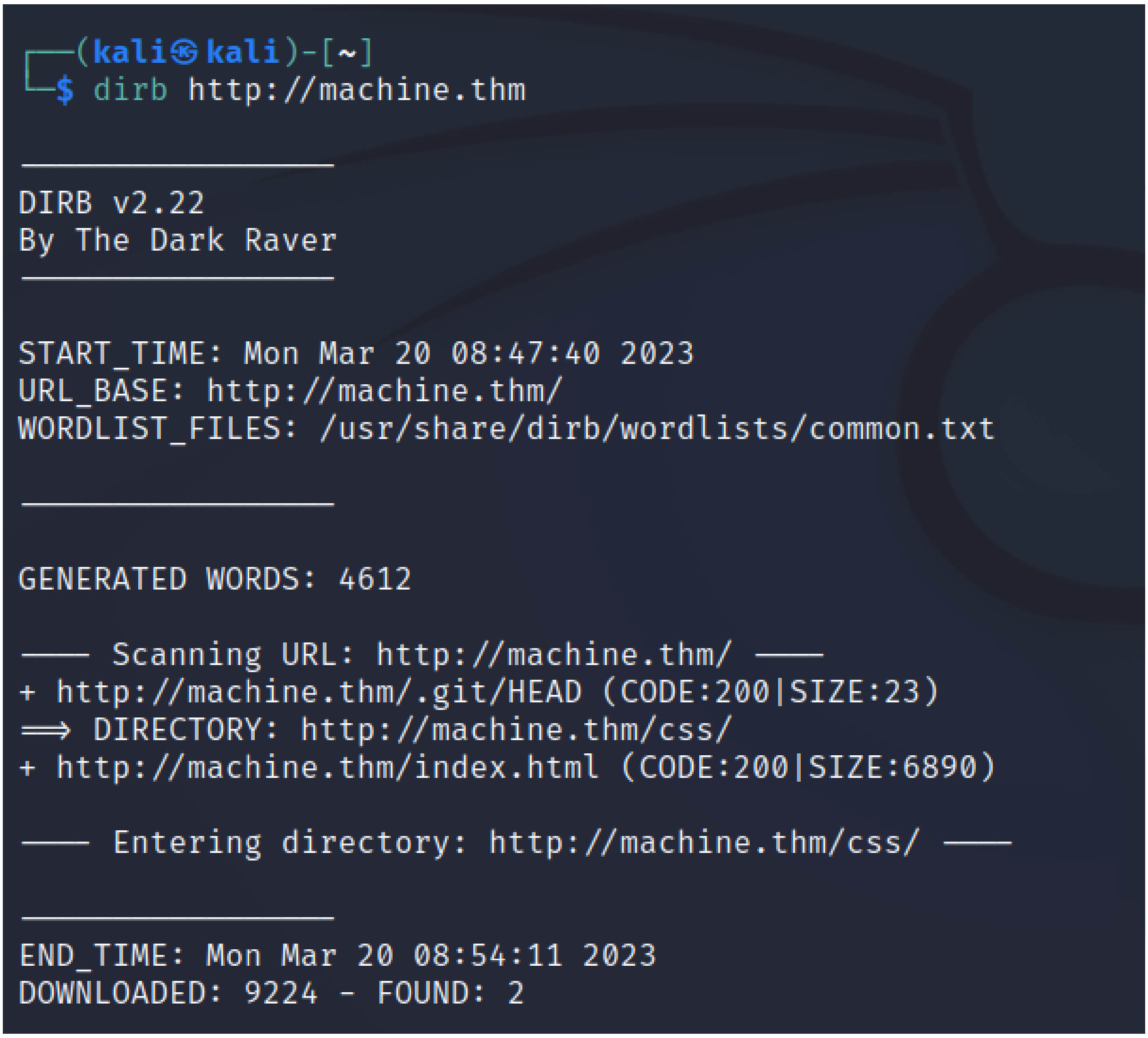
As always I started with an Nmap scan on the target. The output is as follows:



```
Nmap scan report for machine.thm (10.10.219.210)
Host is up (0.040s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I discovered a web service running on port 80. No other open ports were found so let's stick to this.

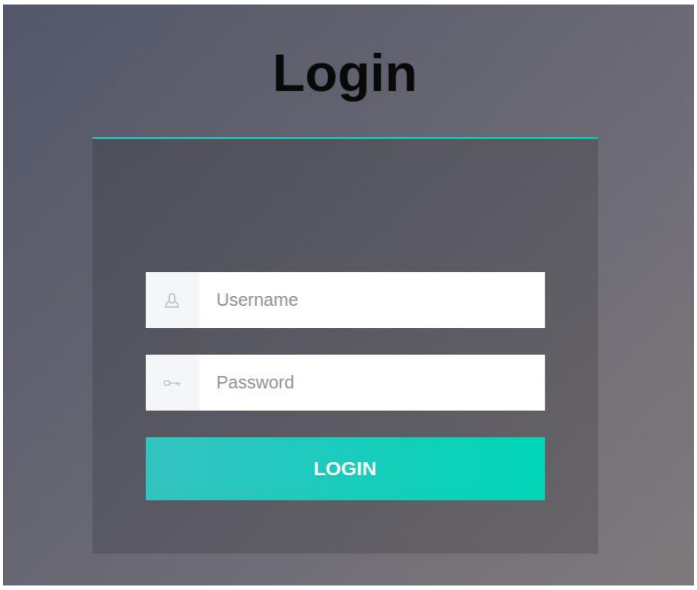
I then began with the enumeration of the web service using dirb:



```
┌──(kali㉿kali)-[~]
└─$ dirb http://machine.thm

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Mar 20 08:47:40 2023
URL_BASE: http://machine.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://machine.thm/ ----
+ http://machine.thm/.git/HEAD (CODE:200|SIZE:23)
==> DIRECTORY: http://machine.thm/css/
+ http://machine.thm/index.html (CODE:200|SIZE:6890)

---- Entering directory: http://machine.thm/css/ ----

-----------------
END_TIME: Mon Mar 20 08:54:11 2023
DOWNLOADED: 9224 - FOUND: 2
```

Dirb discovered a ".git" subfolder. This seems interesting.

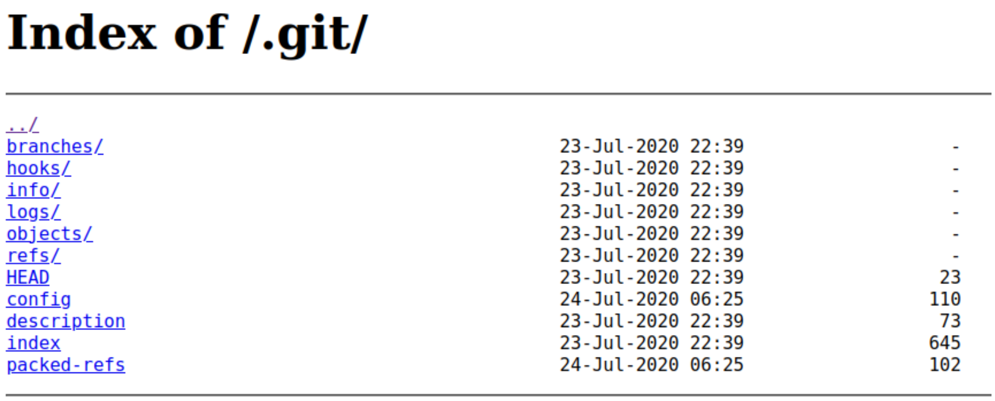
But first visit the webpage to have a look on its content:



A login mask shows up.

## Analyze .git:

Let’s have a look on „.git“:



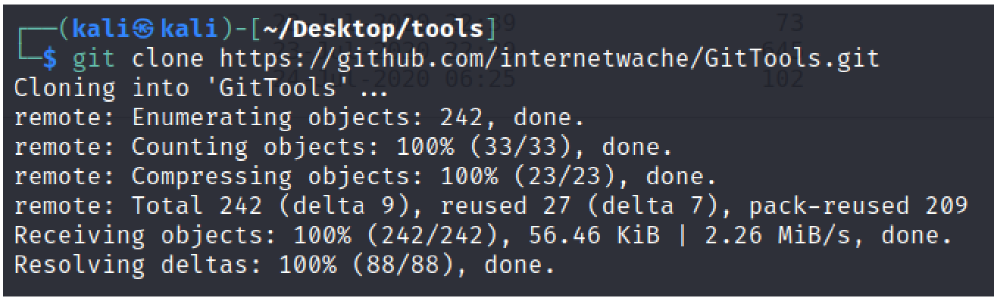
# Index of /.git/

```
../
branches/                                          23-Jul-2020 22:39                   -
hooks/                                             23-Jul-2020 22:39                   -
info/                                              23-Jul-2020 22:39                   -
logs/                                              23-Jul-2020 22:39                   -
objects/                                           23-Jul-2020 22:39                   -
refs/                                              23-Jul-2020 22:39                   -
HEAD                                               23-Jul-2020 22:39                  23
config                                             24-Jul-2020 06:25                 110
description                                        23-Jul-2020 22:39                  73
index                                              23-Jul-2020 22:39                 645
packed-refs                                        24-Jul-2020 06:25                 102
```

The content of the “.git” folder is shown. Let’s investigate this further. To clone the “.git” folder to my machine I used GitTools from https://github.com/internetwache/GitTools.

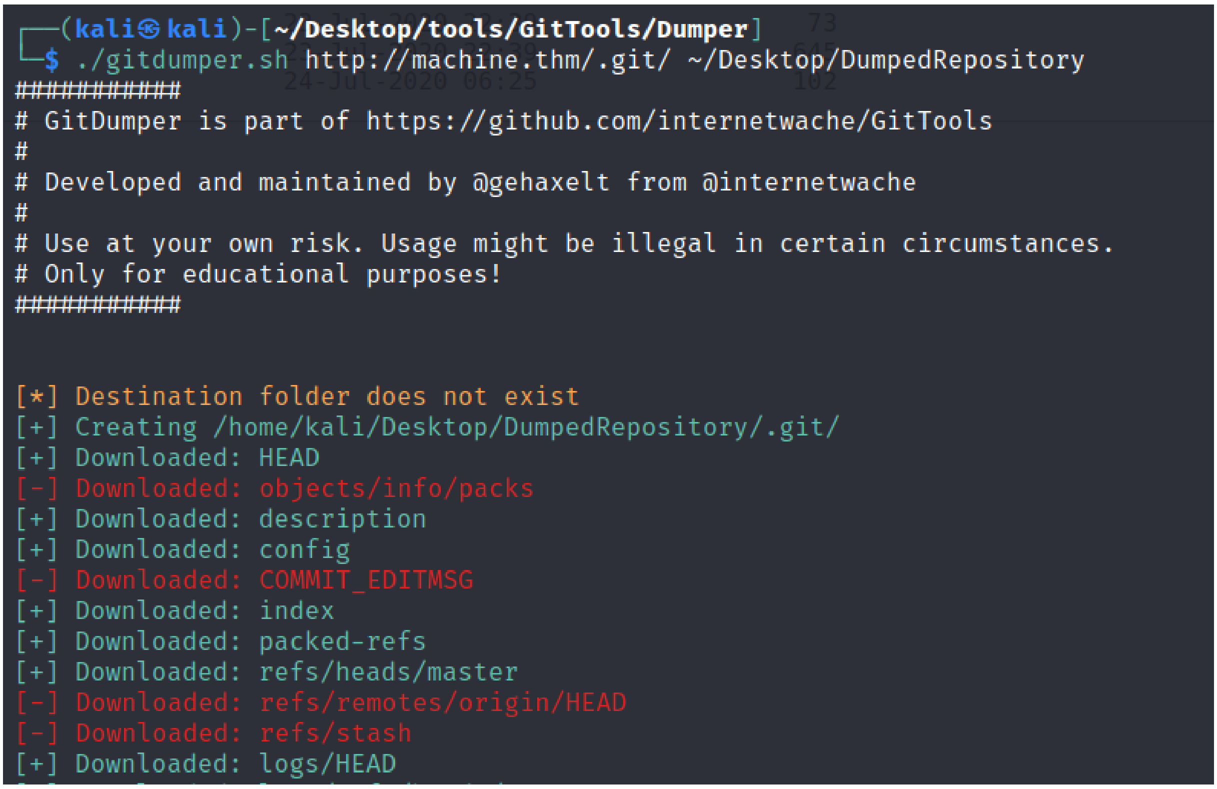
### GitTools:

Clone it from GitHub:



```
┌──(kali㉿kali)-[~/Desktop/tools]
└─$ git clone https://github.com/internetwache/GitTools.git
Cloning into 'GitTools'...
remote: Enumerating objects: 242, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (23/23), done.
remote: Total 242 (delta 9), reused 27 (delta 7), pack-reused 209
Receiving objects: 100% (242/242), 56.46 KiB | 2.26 MiB/s, done.
Resolving deltas: 100% (88/88), done.
```

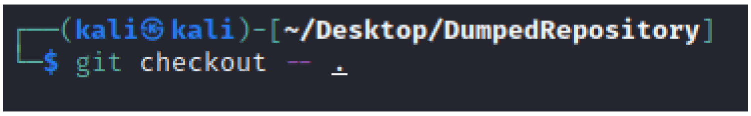
Dump the repository:



```
┌──(kali㉿kali)-[~/Desktop/tools/GitTools/Dumper]
└─$ ./gitdumper.sh http://machine.thm/.git/ ~/Desktop/DumpedRepository
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating /home/kali/Desktop/DumpedRepository/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[-] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[+] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
```

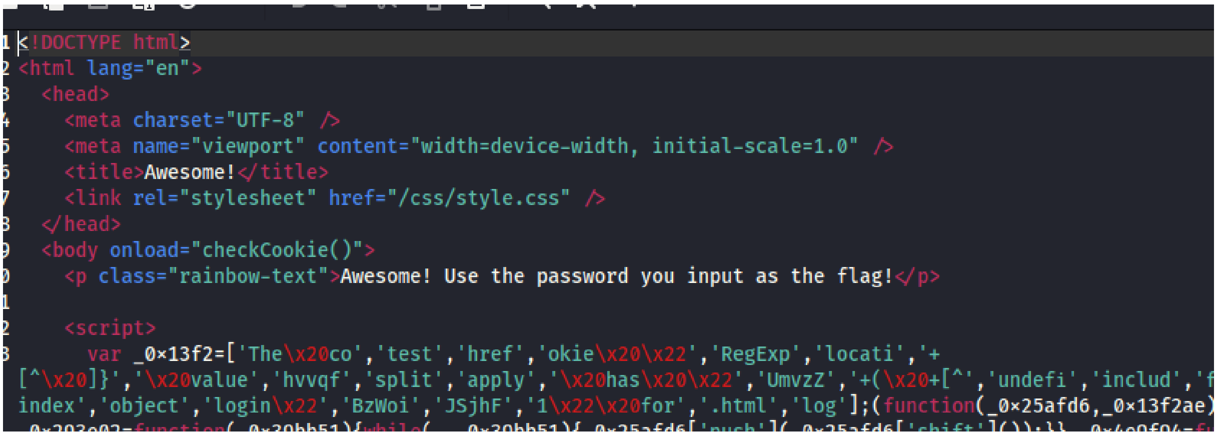
## Analyze Files:

Change in dumped repository and get files



```
┌──(kali㉿kali)-[~/Desktop/DumpedRepository]
└─$ git checkout -- .
```

Accessed „dashboard.html“:

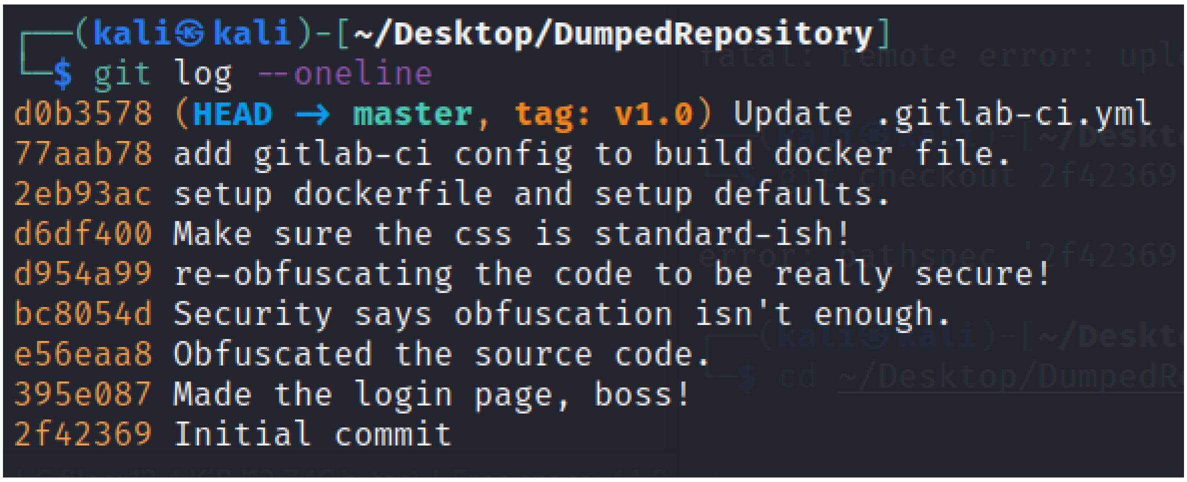


```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Awesome!</title>
    <link rel="stylesheet" href="/css/style.css" />
  </head>
  <body onload="checkCookie()">
    <p class="rainbow-text">Awesome! Use the password you input as the flag!</p>

    <script>
      var _0x13f2=['The\x20co','test','href','okie\x20\x22','RegExp','locati','+
[^\x20]}','\x20value','hvvqf','split','apply','\x20has\x20\x22','UmvzZ','+(\x20+[^','undefi','includ','f
index','object','login\x22','BzWoi','JSjhF','1\x22\x20for','.html','log'];(function(_0x25afd6,_0x13f2ae)
```

So we need to get the password of the login mask which is the flag we need.

I had a look on the login logic on the “index.html” file. I could discover that no request was made to a server so the login is hardcoded. But the login code is obfuscated.

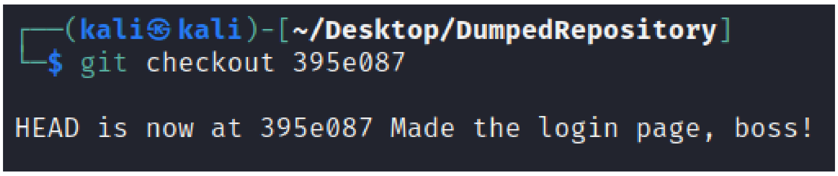
Checked previous commits:



```
┌──(kali㉿kali)-[~/Desktop/DumpedRepository]
└─$ git log --oneline
d0b3578 (HEAD → master, tag: v1.0) Update .gitlab-ci.yml
77aab78 add gitlab-ci config to build docker file.
2eb93ac setup dockerfile and setup defaults.
d6df400 Make sure the css is standard-ish!
d954a99 re-obfuscating the code to be really secure!
bc8054d Security says obfuscation isn't enough.
e56eaa8 Obfuscated the source code.
395e087 Made the login page, boss!
2f42369 Initial commit
```

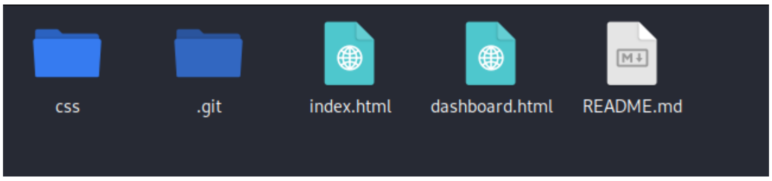
Seems like that in commit 935e087 the login page is created. In commit e56eaa8 the source code gets obfuscated. So the commit 935e087 is interesting to us.

Let's checkout the commit before the source code gets obfuscated:

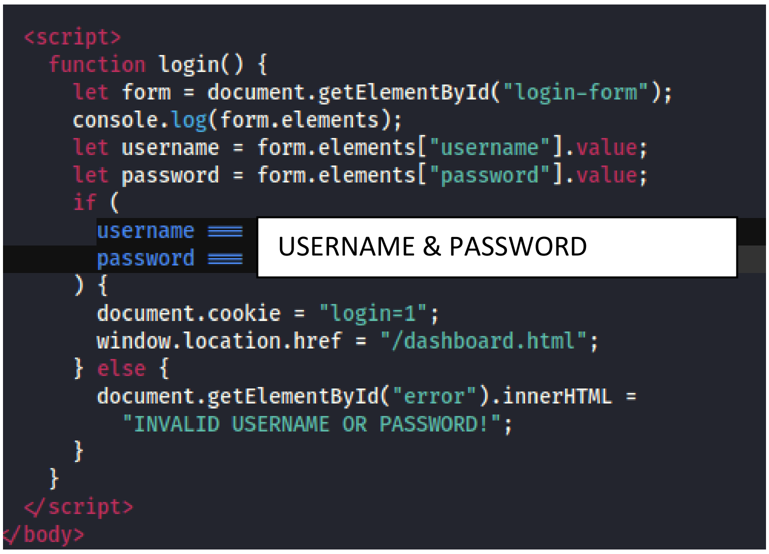


```
┌──(kali㉿kali)-[~/Desktop/DumpedRepository]
└─$ git checkout 395e087

HEAD is now at 395e087 Made the login page, boss!
```

Files of commit:



Inside index.html:



```
  <script>
    function login() {
      let form = document.getElementById("login-form");
      console.log(form.elements);
      let username = form.elements["username"].value;
      let password = form.elements["password"].value;
      if (
        username ==  USERNAME & PASSWORD
        password ==
      ) {
        document.cookie = "login=1";
        window.location.href = "/dashboard.html";
      } else {
        document.getElementById("error").innerHTML =
          "INVALID USERNAME OR PASSWORD!";
      }
    }
  </script>
</body>
```

We found the password and are done!