#BugBounty — How I was able to download the Source Code of India's Largest Telecom Service Provider including dozens of more popular websites!

Avinash Jain (@logicbomb_1) Follow
Oct 27, 2018 · 4 min read

Hi Guys,

Recently, we came across a news of source code leakage of Snapchat where hacker downloaded the complete source code of the website and put it over Github. *In the last couple of years, a widespread misconfiguration has come into the picture and being exploited hugely where inexperienced web application developers happened to inadvertently leave key components of their Git repositories publicly accessible—potentially giving anyone access to sensitive*

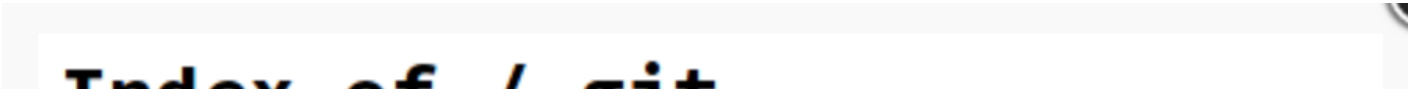
source code, access keys, passwords and more. So under the same light, I started working to discover and find vulnerabilities related to the same Git misconfiguration and through which I was able to access the source code of various companies including the source code of ***India's largest telecom service provider.***

Description in Short

What is Git?

> *Git is a version control system (VCS) for tracking changes in computer files and coordinating work on those files among multiple people. It is primarily used for source code management in software development but it can be used to keep track of changes in any set of files.It allows source code versions to be managed in a logical manner and tracks changes through different 'forks' and 'branches'.*

If an application has misconfigured Git directory which is exposed publically, the directory will look something like this —



Git directory exposed

In order to recursively download every file from the repository, **wget** do this awesomely—wget –r https://www.example.com/.git. Now once you are able to download the complete .git folder, a little git command line knowledge could be fetching the git objects for you. Some of the sites for the reference are-

https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/

https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/

Technical Details

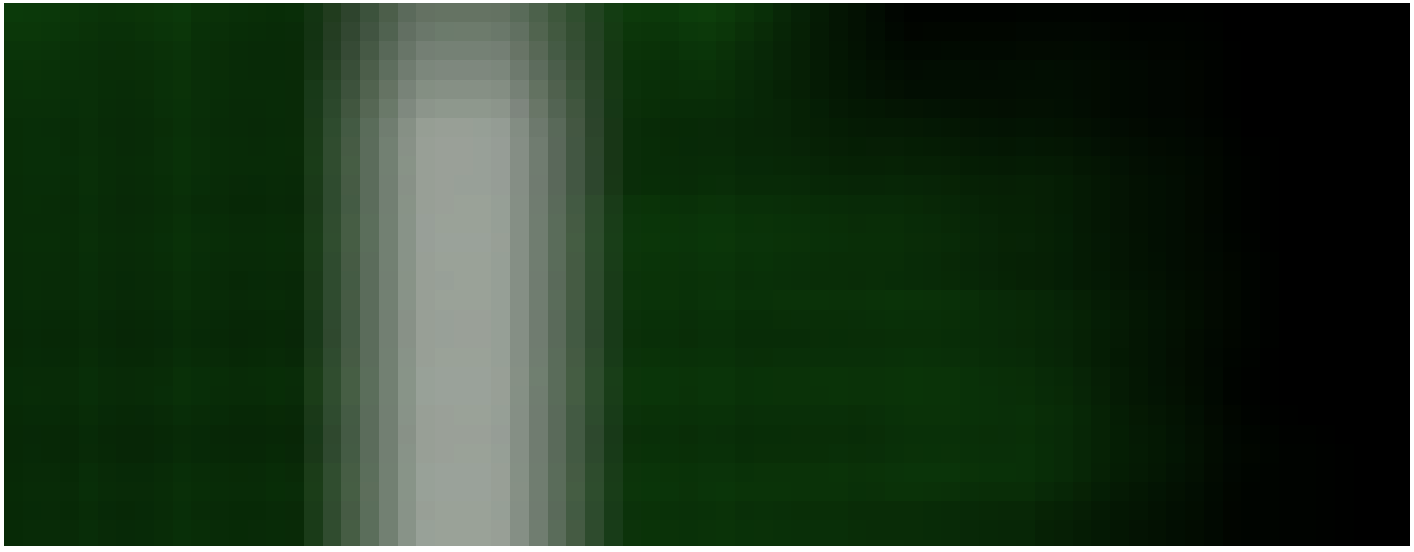
Before jumping into this para, I would advise you to read the above provided links if you don't have good knowledge about git and git commands. Now let's see **How I was able to do the same in various companies including India's largest telecom industry.**

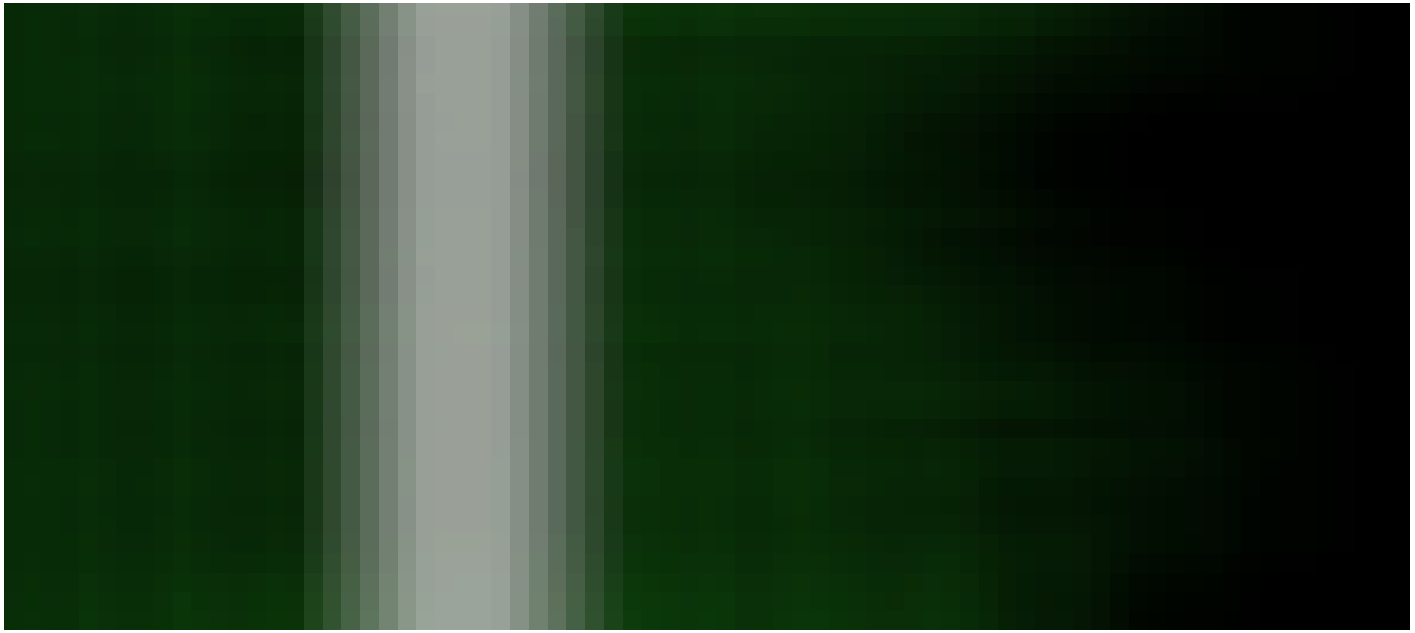
Subdomains are as important as the main domain and that's why one of the most important part in reconnaissance is Subdomain enumeration. It is not always necessary that git misconfiguration can occur only in main domain, it can be present in subdomains too so in order to find which all domains/subdomains/companies have inadvertently left their git repo public, I combined both the techniques of subdomain enumeration and .git folder download. There is an awesome open source subdomain enumeration tool- Sublist3r which basically enumerate subdomain of a parent domain from various different sources and give you the list as an output. There is also one more cool tool to check and download publically exposed git directory named as Git-dumper which in actual checks whether the .git directory is being indexed and then download the git directory. I basically merged the code of both the scripts, made some small changes in the code named it as *git-domian.py* and which does the following things for me —

1. git-domain.py expect a file as an input containing the list of all the main domains separated by a line.
2. It traverses each domain(line) one by one to find it's subdomain and check for .git directory if publically exposed or not in each of the subdomains.

3. If yes, then it recursively downloads the complete git folder of the particular subdomain and saves it in a folder.

So this is what I did, prepared a list of various large, medium, and small scaled popular companies having public/private bug bounty program/responsible disclosure policies, give it to git-domain.py —





Git directory check on each subdomain of the main domain

and rest what I got is the complete git folder downloaded of dozens of companies having misconfigured git directory which also included ***India's largest telecom service provider*** from where I then escalated to access the **complete source code of their website** some of which had their main domain source code leaked while some of them have the same misconfiguration in their subdomain.

Git directory files

Source code access

Mitigation Step

Web server administrator or developers have to make sure that the .git directory is not being indexed and the directory, sub-directories, and all files are inaccessible using server permission rules. Furthermore, the .gitignore file should be used to ensure sensitive files are properly ignored and not mistakenly added. The simplest way to mitigate this is to just deny access to `.git` folders.

> *<DirectoryMatch "^/.*/\.git/">*
>
> *Require all denied*

> *</DirectoryMatch>*

. . .

Thanks for reading!

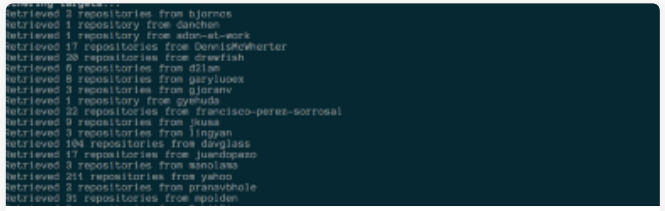
~Logicbomb (https://twitter.com/logicbomb_1)

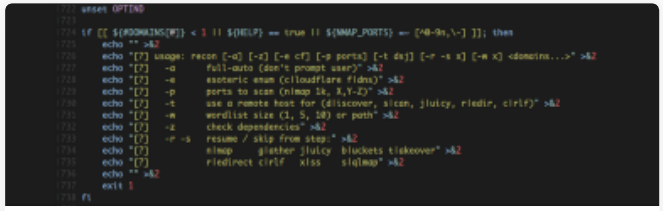
Git | Hacking | Bug Bounty | Ethical Hacking | Information Security

845 claps

Avinash Jain (@logicbomb_1)

Lead Infrastructure Security Engineer @groferseng | DevSecops | Part time BugBounty Hunter | Acknowledged by Google, NASA, Yahoo, United Nations, BBC etc.





More from Avinash Jain (@logicbomb_1)

Credentials leaked in public? Here's what Grofers implemented to...

Avinash Jain (@log...
Nov 3, 2018 · 4 min re

1.3K

Related reads

h1–702 CTF — Web Challenge Write Up

Amal Murali
Jul 1, 2018 · 12 min rea

907

Related reads

Reconnaissance: a eulogy in three acts

europa
Feb 11, 2018 · 8 min re

1.3K

Responses

Write a response...

Show all responses