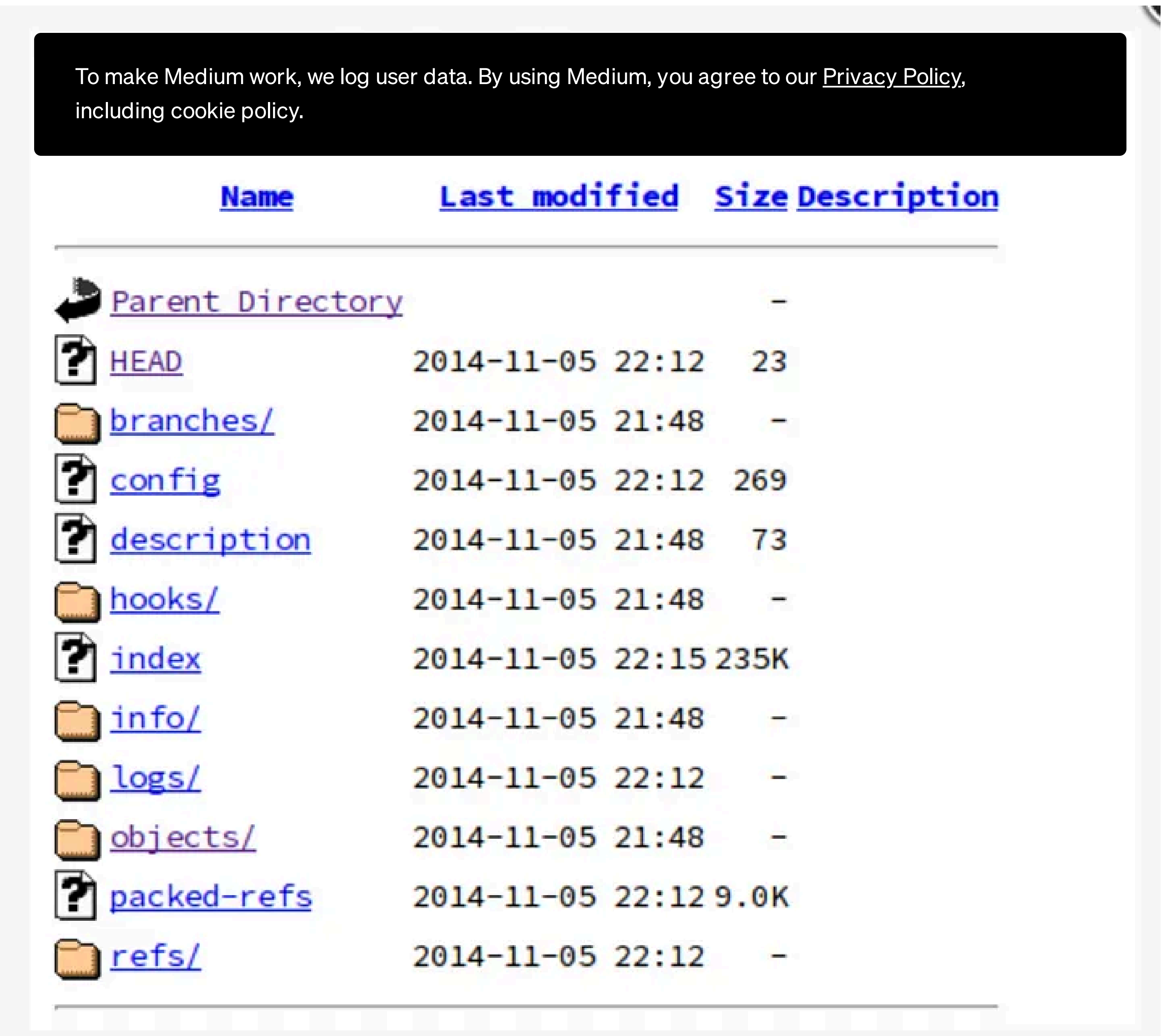
#BugBounty — How I was able to download the Source Code of India's Largest Telecom Service Provider including dozens of more popular websites!

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

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



To make Medium work, we log user data. By using Medium, you agree to our Privacy Policy, including cookie policy.

Name	Last modified	Size	Description
Parent Directory		-	
HEAD	2014-11-05 22:12	23	
branches/	2014-11-05 21:48	-	
config	2014-11-05 22:12	269	
description	2014-11-05 21:48	73	
hooks/	2014-11-05 21:48	-	
index	2014-11-05 22:15	235K	
info/	2014-11-05 21:48	-	
logs/	2014-11-05 22:12	-	
objects/	2014-11-05 21:48	-	
packed-refs	2014-11-05 22:12	9.0K	
refs/	2014-11-05 22:12	-	

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-wetool- Sublist3r which basically enumerate subdomain of a parent domain fr

als

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 —

```
(avi) ➜ git-domain git:(0540930) ✗ python3 git-domain.py domain_list.txt
```

and rest what I got is the complete git folder downloaded of dozens of

co

la

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*

Written by Avinash Jain (@logicbomb)

Follow

4.8K Followers

Security Engineer @Microsoft | DevSecOps | Speaker | Breaking stuff to learn | Featured in Forbes, BBC| Acknowledged by Google, NASA, Yahoo, UN etc

More from Avinash Jain (@logicbomb)

Avinash Jain (@logicbomb)

#BugBounty —” Database hacked of India's Popular Sports...

Hi Guys,

Jun 6, 2018 584 7

Avinash Jain (@logicbomb) in InfoSec Write-ups

#BugBounty — Exploiting CRLF Injection can lands into a nice...

Hi Guys,

Feb 17, 2018 762 6

Recommended from Medium

loyalonlytoday in InfoSec Write-ups

How to find bugs in Microsoft iis page.

>> NOTE : HERE IS THE LINK FOR NON-PAID MEMBERS → CLICKHERE <<

5d ago 289

Jayvin Gohel

Bypassed an Admin Panel Using SQL Payloads

It’s been a while since I last wrote a blog post, but I’ve got something interesting to share...

Sep 8 143 2

Lists

Medium's Huge List of Publications Accepting...
378 stories · 3812 saves

Staff Picks
755 stories · 1415 saves

Jonathan Mondaut

Desiree Peralta in Publishous

Ho
Ha

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

Jun 18 1.6K 53

Oct 8 17.5K 350

See more recommendations