Laporan Bug Bounty Cilsy Fiolution

https://vuln.cilsy.id

Local File Disclosure

24 Juli 2022

Oleh Samuel Dasmianus

Issue Description

Local File Disclosure (LFD) is type of vulnerability which attacker can access/download sensitive file in web application server such as password.txt and group.txt.

Issue Identified

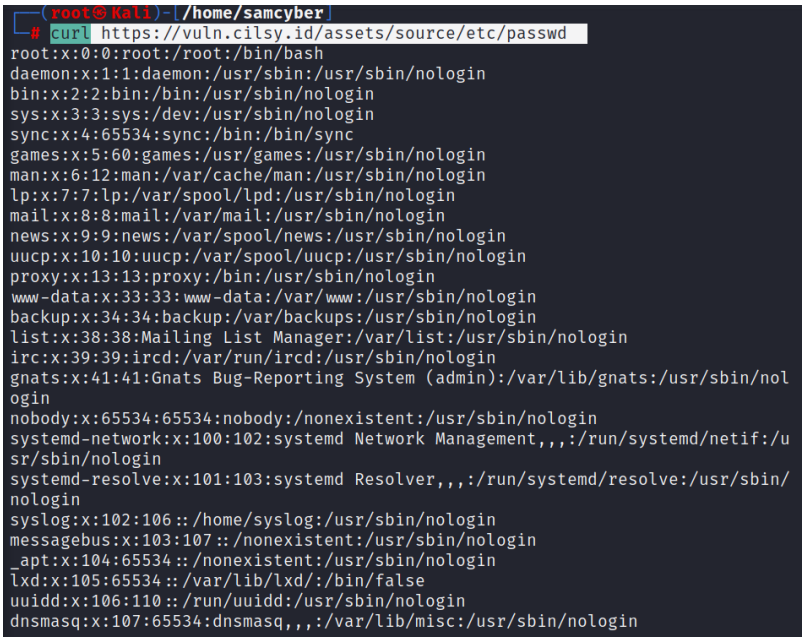
The attacker point to the path of web application which contain private file of website in this case path https://vuln.cilsy.id/assets/source/etc/password & https://vuln.cilsy.id/assets/source/etc/group

Risk Breakdown

- Risk:**High**
- CVSS v3 Score:**7.5** (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

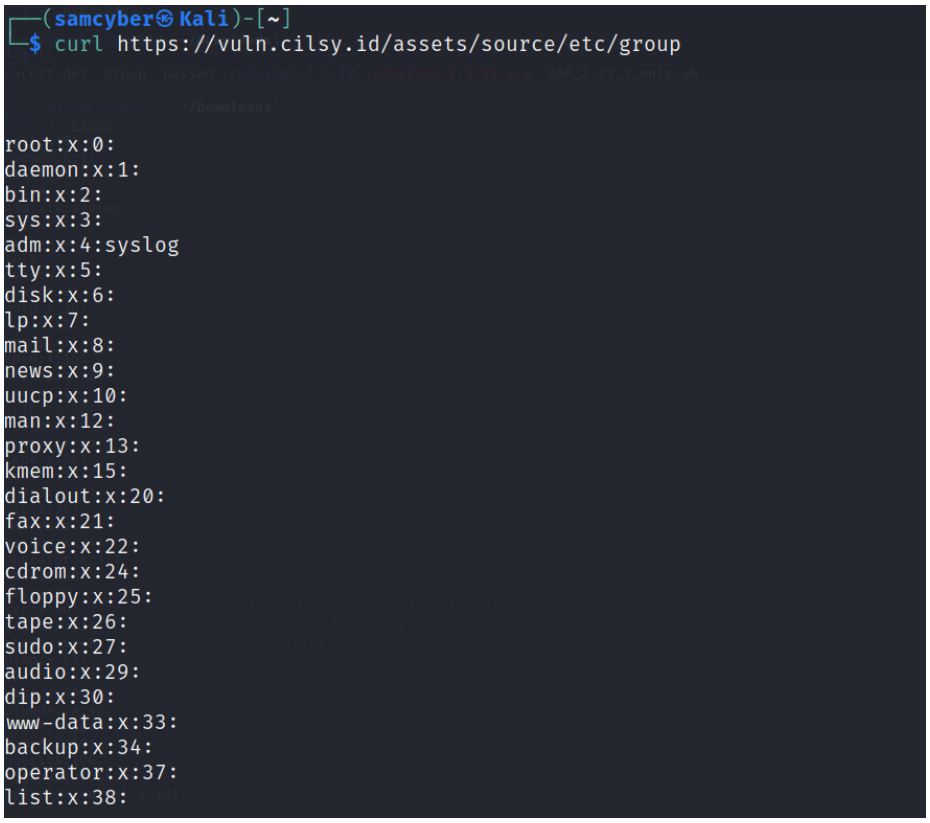
Affected URLs & POC

- https://vuln.cilsy.id/assets/source/etc/password



File password.txt

- https://vuln.cilsy.id/assets/source/etc/group



File group.txt

Steps to Reproduce

Step 1: Access file in web app server using **curl** command in kali linux terminal which is https://vuln.cilsy.id/assets/source/etc/passwd & https://vuln.cilsy.id/assets/source/etc/group

Step 2: capture the result show in kali linux terminal or you can just download the file passwd and group from url which you can access from your own browser

Affected Demographic

Attacker can access/download critical file such as passwd.txt and group.txt which contain credential user and should not read by general user.

Recommendation

Make restricted access and download to general user which set the permission folder and file to public.

References

For more information on remediation steps check out reference [1].

- [1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-3394