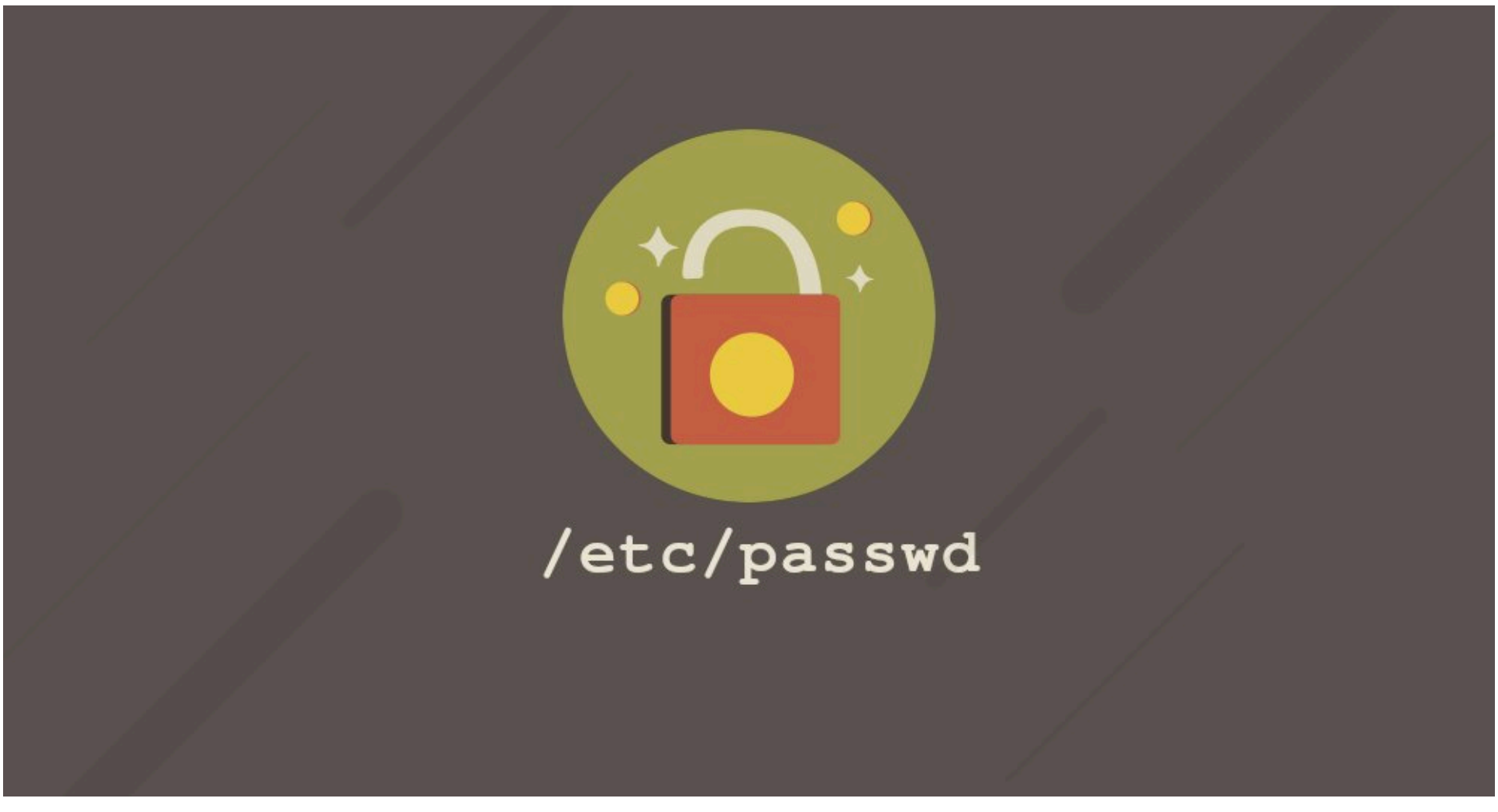
noobSecurity

One mistake can make you crazy

Blankon33 Follow

Peternak kudanil

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 methode dari https://snyk.io/vuln/npm:wangshuai:20170910

Langkah-langkah untuk mencari subdomain (`enumeration`) bisa menggunakan:

- Aquatone

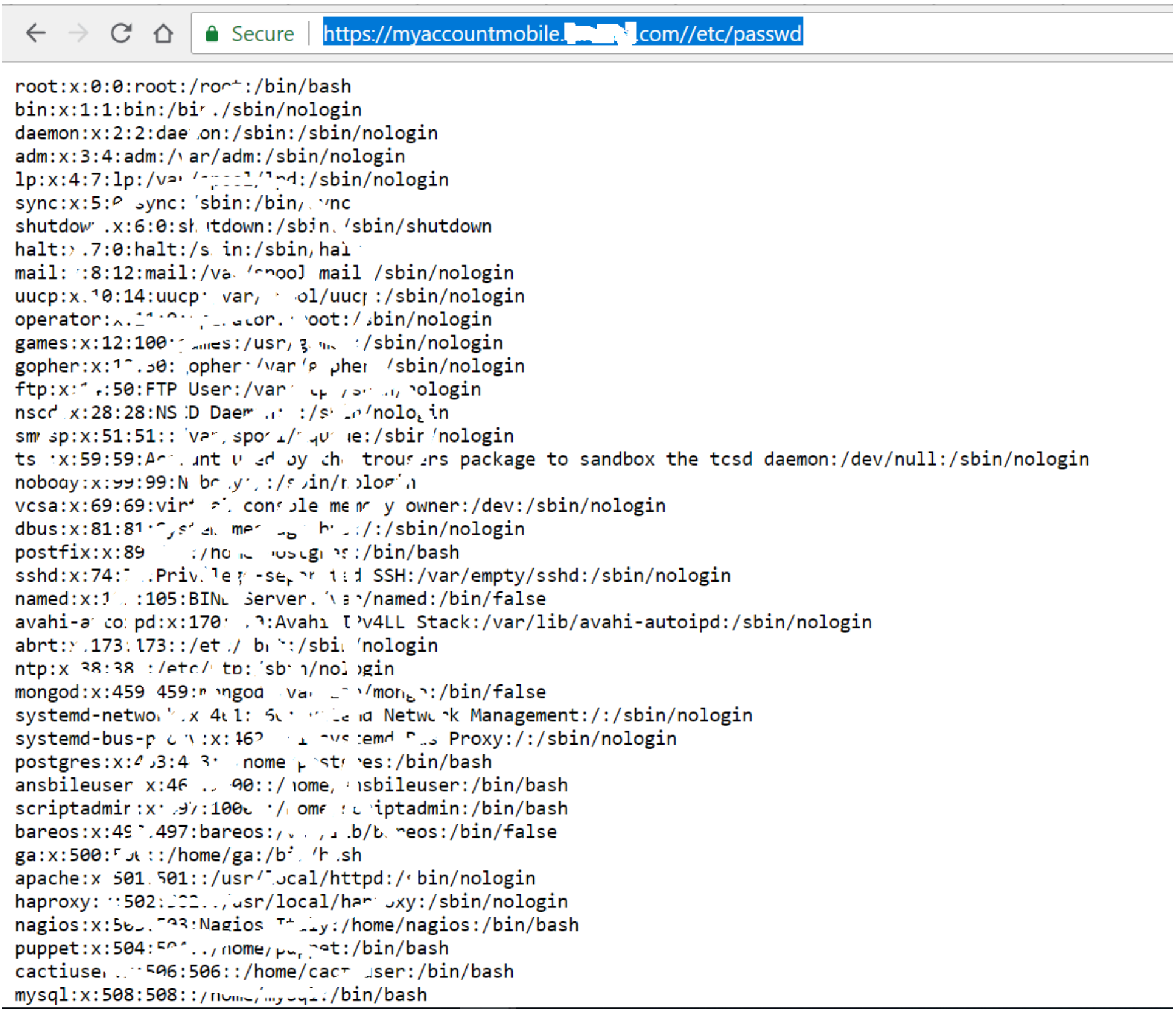
```
aquatone-discover --domain domain.com
```

- Sublister

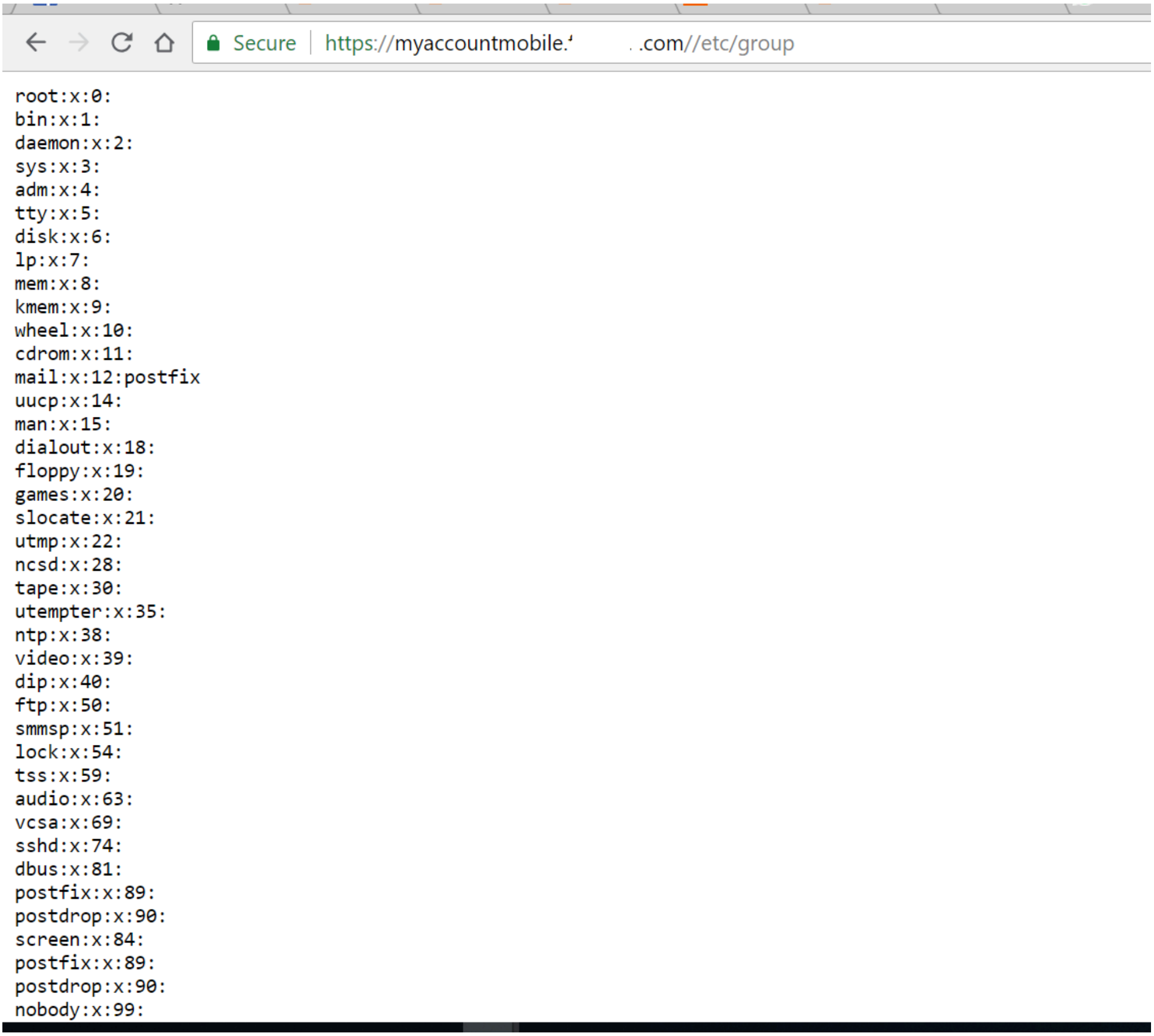
```
./Sublist3r.py -d domain.com
```

- dsb.

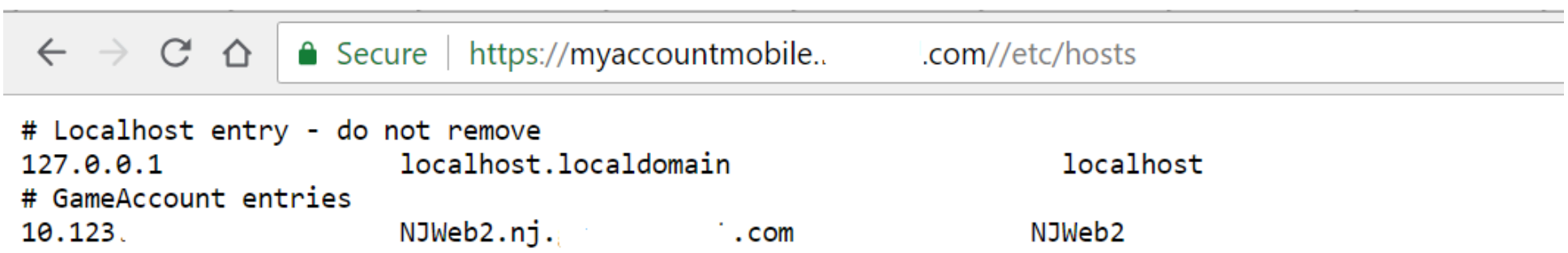
kami mendapatkan satu subdomain yaitu myaccount.redacted.com. Lalu kami mencoba dengan memasukkan payload directory traversal https://myaccount.redacted.com//etc/passwd. Diluar ekspektasi kami, muncul file /etc/passwd.



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



dan /etc/hosts



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 missconfig pentesting

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

Bagaimana menurutmu?

30Respons

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 respondnya 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)