KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH:

M. AFRIA ALIM SAPUTRA (09011281520100)

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
PALEMBANG 2018/2019

Website Pemerintah

Detail Infomration

Site : https://ristekdikti.go.id/
Domain : ristekdikti.go.id
IP : 103.56.191.173
Pembukaan perdana : October 2015
Top Level Domain : Indonesia (.go.id)
Tempat Hosting : Indonesia
IP Location :
- Jakarta Raya - Jakarta - Direktorat Jenderal Pendidikan Tinggi
ASN :
AS133826 IDNIC-DIKTI-AS-ID Direktorat Jenderal Pendidikan Tinggi, ID (registered Nov 18, 2014)
Netblock Owner : Direktorat Jenderal Pendidikan Tinggi
Name servers : ns1.rminet.co.id, ns2.rminet.co.id
DNS Admin : yunus@ristekdikti.go.id
Reverse DNS : ristekdikti.go.id
Hosting Company : rminet.co.id
Subdomains : belmawa.ristekdikti.go.id, forlap.ristekdikti.go.id, ijazahln.ristekdikti.go.id, jdih.ristekdikti.go.id, mail.ristekdikti.go.id, phbd.ristekdikti.go.id, puspiptek.ristekdikti.go.id, sinta1.ristekdikti.go.id, webmail.ristekdikti.go.id,
IP Subdomains : belmawa.ristekdikti.go.id (103.56.189.15)
forlap.ristekdikti.go.id (118.98.235.202)
ijazahln.ristekdikti.go.id (103.56.191.166)
jdih.ristekdikti.go.id (103.56.190.31)
mail.ristekdikti.go.id (103.56.190.36)
phbd.ristekdikti.go.id (103.56.190.109)
puspiptek.ristekdikti.go.id (103.56.189.6)
sinta1.ristekdikti.go.id (180.250.152.22)
webmail.ristekdikti.go.id (103.56.191.36)
Server Type :

Netblock owner	IP address	OS	Web server	Last seen Refresh
Direktorat Jenderal Pendidikan Tinggi University / Direct Member IDNIC Gedung KEMDIKNAS Jl. Raya Jendral Sudirman Pintu I, Senayan Jakarta, 10270	103.56.191.173	unknown	Apache/2.4.10 Debian	9-Feb-2019

Whois

```
Domain ID:PANDI-DO589829
Domain Name:RISTEKDIKTI.GO.ID
Created On:21-Apr-2015 03:54:04 UTC
Last Updated On:06-Jun-2018 00:07:48 UTC
Expiration Date:21-Apr-2019 23:59:59 UTC
Status:ok
======================================================
Sponsoring Registrar Organization:Kementerian Komunikasi dan Informa
tika
Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City:Jakarta Pusat
Sponsoring Registrar State/Province:Jakarta
Sponsoring Registrar Postal Code:10110
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:622138433507
Sponsoring Registrar Website:domain.go.id
Sponsoring Registrar Contact Email: hostmaster@pandi.id
Name Server:NS1.RMINET.CO.ID
Name Server:NS2.RMINET.CO.ID
DNSSEC:Unsigned
```

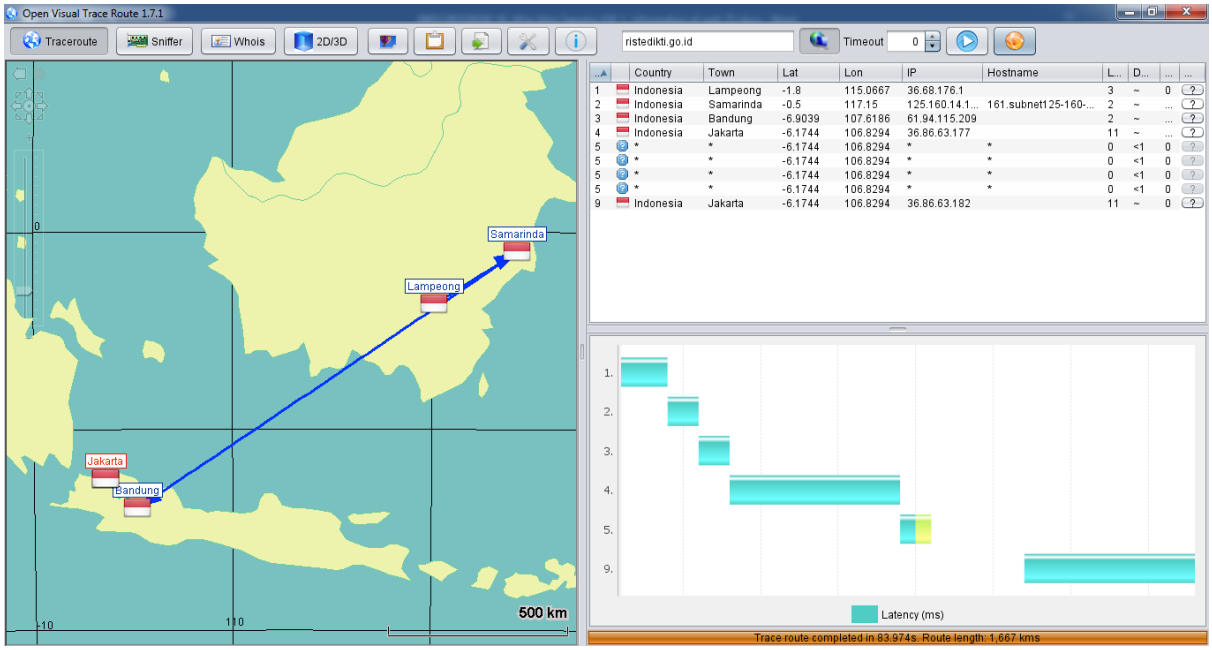
CVE

CVE-2018-1312
In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

CVE-2017-15715
In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

CVE-2018-1283
In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

Traceroute


Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
ristedikti.go.id
Timeout
0
Country
Town
Lat
Lon
IP
Hostname
1 Indonesia Lampeong -1.8 115.0667 36.68.176.1 3 ~ 0
2 Indonesia Samarinda -0.5 117.15 125.160.14.1... 161.subnet125-160-... 2 ~ ...
3 Indonesia Bandung -6.9039 107.6186 61.94.115.209 2 ~ ...
4 Indonesia Jakarta -6.1744 106.8294 36.86.63.177 11 ~ ...
5 * * -6.1744 106.8294 * * 0 <1 0
5 * * -6.1744 106.8294 * * 0 <1 0
5 * * -6.1744 106.8294 * * 0 <1 0
5 * * -6.1744 106.8294 * * 0 <1 0
9 Indonesia Jakarta -6.1744 106.8294 36.86.63.182 11 ~ 0
Samarinda
Lampeong
Jakarta
Bandung
500 km
Latency (ms)
Trace route completed in 83.974s. Route length: 1,667 kms

Website Dalam Negeri

Detail Infomration

Site : http://jurnalotaku.com/
Domain : jurnalotaku.com
IP : 128.199.203.6
Pembukaan perdana : Juni 2013
Top Level Domain : Commercial entities (.com)
Tempat Hosting : Singapore
IP Location : - Singapore - Singapore - Digitalocean Llc
ASN :
AS14061 DIGITALOCEAN-ASN - DigitalOcean, LLC, US (registered Sep 25, 2012)
Netblock Owner : DigitalOcean Cloud
Name servers : ns1.digitalocean.com, ns2.digitalocean.com and ns3.digitalocean.com
DNS Admin : hostmaster@jurnalotaku.com
Nameserver : whois.networksolutions.com
Organisation
Hosting Company : DigitalOcean
Subdomains : mail.jurnalotaku.com, my.jurnalotaku.com, storage.jurnalotaku.com
IP Subdomains : mail.jurnalotaku.com (103.23.20.234)
my.jurnalotaku.com (188.166.250.189)
storage.jurnalotaku.com (128.199.65.252)
Server Type :

Netblock owner	IP address	OS	Web server	Last seen Refresh
DigitalOcean Cloud	128.199.203.6	Linux	nginx/1.4.6 Ubuntu	3-Feb-2019
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	174.37.68.45	Linux	Apache	23-Feb-2014

Whois

```
Domain Name: JURNALOTAKU.COM
Registry Domain ID: 1796002276_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2018-07-13T06:40:24
Creation Date: 2013-04-23T09:42:49
Registrar Registration Expiration Date: 2019-04-23T09:42:49
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Reseller: PT. Master Web Network
Domain Status: clientTransferProhibited https://icann.org/epp#client
TransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUp
dateProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 0134311893
Registrant Organization: Contact Privacy Inc. Customer 0134311893
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M6K 3M1
Registrant Country: CA
Registrant Phone: +1.4165385457
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jurnalotaku.com@contactprivacy.com
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 0134311893
Admin Organization: Contact Privacy Inc. Customer 0134311893
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M6K 3M1
Admin Country: CA
Admin Phone: +1.4165385457
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jurnalotaku.com@contactprivacy.com
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 0134311893
Tech Organization: Contact Privacy Inc. Customer 0134311893
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M6K 3M1
Tech Country: CA
Tech Phone: +1.4165385457
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
```

Tech Email: jurnalotaku.com@contactprivacy.com
Name Server: ns1.digitalocean.com
Name Server: ns2.digitalocean.com
Name Server: ns3.digitalocean.com

Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

"For more information on Whois status codes, please visit https://icann.org/epp"

Registration Service Provider:

PT. Master Web Network, hostmaster@masterweb.net
62215266899
http://www.masterweb.net
* No. 1 Leading Hosting in Indonesia
* The Trust For Your Online Business

CVE

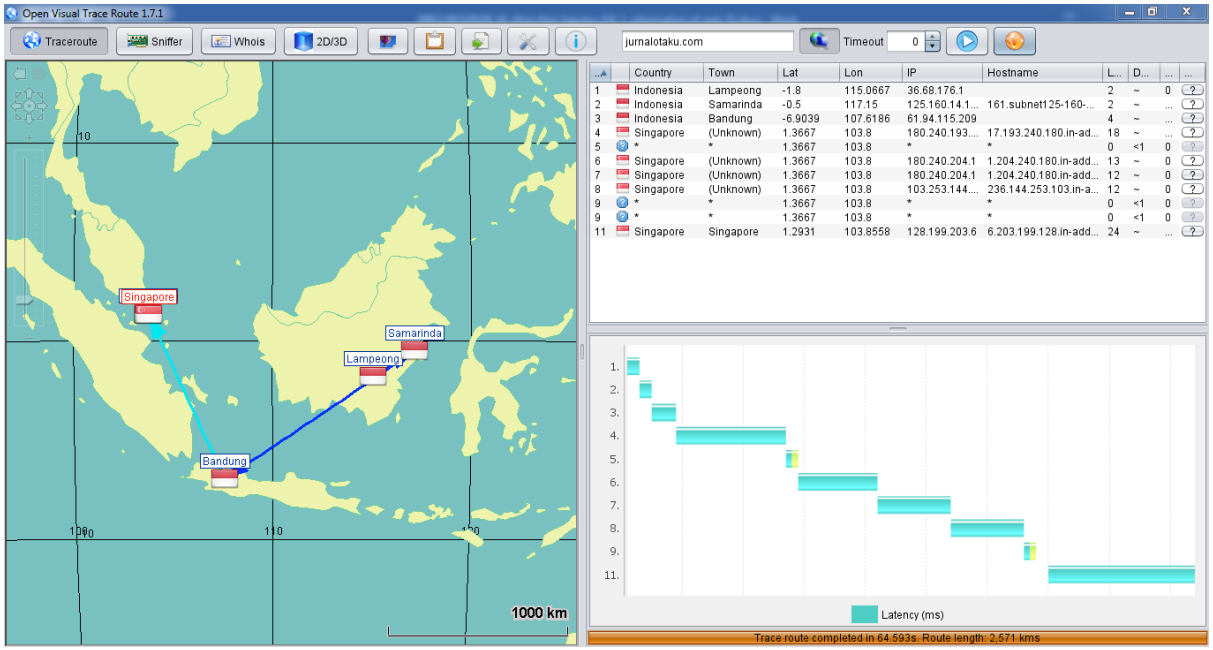
CVE-2018-16845
nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

CVE-2016-1247
The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx ebuild before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.

CVE-2018-17197
A carefully crafted or corrupt sqlite file can cause an infinite loop in Apache Tika's SQLite3Parser in versions 1.8-1.19.1 of Apache Tika.

CVE-2018-17195
The template upload API endpoint accepted requests from different domain when sent in conjunction with ARP spoofing + man in the middle (MiTM) attack, resulting in a CSRF attack. The required attack vector is complex, requiring a scenario with client certificate authentication, same subnet access, and injecting malicious code into an unprotected (plaintext HTTP) website which the targeted user later visits, but the possible damage warranted a Severe severity level. Mitigation: The fix to apply Cross-Origin Resource Sharing (CORS) policy request filtering was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.

Traceroute


Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
jurnalotaku.com
Timeout
0
Country
Town
Lat
Lon
IP
Hostname
1 Indonesia Lampeong -1.8 115.0667 36.68.176.1
2 Indonesia Samarinda -0.5 117.15 125.160.14.1... 161.subnet125-160-...
3 Indonesia Bandung -6.9039 107.6186 61.94.115.209
4 Singapore (Unknown) 1.3667 103.8 180.240.193.... 17.193.240.180.in-ad...
5 * * 1.3667 103.8 * *
6 Singapore (Unknown) 1.3667 103.8 180.240.204.1 1.204.240.180.in-add...
7 Singapore (Unknown) 1.3667 103.8 180.240.204.1 1.204.240.180.in-add...
8 Singapore (Unknown) 1.3667 103.8 103.253.144.... 236.144.253.103.in-a...
9 * * 1.3667 103.8 * *
9 * * 1.3667 103.8 * *
11 Singapore Singapore 1.2931 103.8558 128.199.203.6 6.203.199.128.in-add...
Singapore
Samarinda
Lampeong
Bandung
1000 km
Latency (ms)
Trace route completed in 64.593s. Route length: 2,571 kms

Website Luar Negeri

Detail Infomration

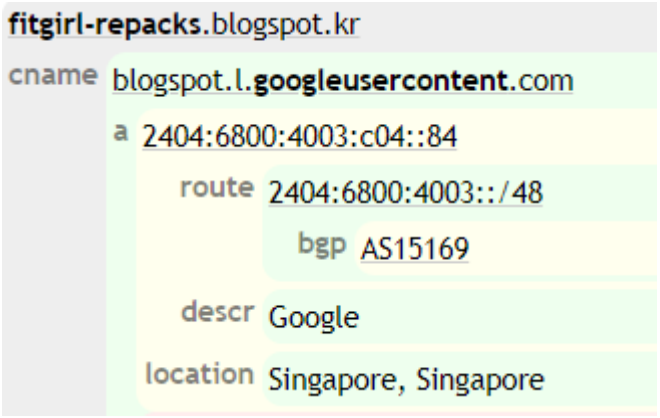
Site : http://fitgirl-repacks.site
Domain : fitgirl-repacks.site
IP : 104.24.126.50, 104.24.127.50
IPv6 : 2606:4700:30:0:0:0:6818:7f32, 2606:4700:30::6818:7e32
Pembukaan perdana : November 2016
Top Level Domain : Site (.site)
Tempat Hosting : San Francisco, United States
IP Location : - California - San Francisco - Cloudflare Inc.
ASN : AS13335 CLOUDFLARENET - Cloudflare, Inc., US (registered Jul 14, 2010)
Netblock Owner : Cloudflare, Inc.
Name servers : tani.ns.cloudflare.com, woz.ns.cloudflare.com
DNS Admin : dns@cloudflare.com
Nameserver : whois.cloudflare.com
Organisation
Hosting Company : *unknown*
Other Domains :
fitgirl-repacks.com

fitgirl-repacks.com
- a 2400:cb00:2048:1::681f:5235
  - route 2400:cb00:2048::/48
    - bgp AS13335
      - asname CLOUDFLARENET-AS CloudFlare, Inc.
  - descr CloudFlare, Inc.
  - location United States

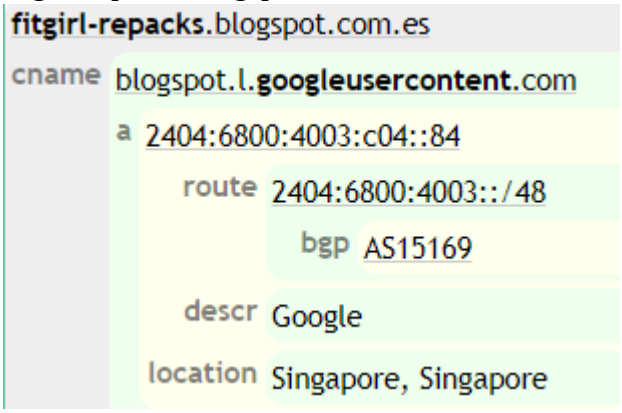
fitgirl-repacks.online

fitgirl-repacks.online
- a 2400:cb00:2048:1::681b:b6dc
  - route 2400:cb00:2048::/48
    - bgp AS13335
      - asname CLOUDFLARENET-AS CloudFlare, Inc.
  - descr CloudFlare, Inc.
  - location United States

fitgirl-repacks.blogspot.kr



fitgirl-repacks.blogspot.com.es



Server Type :

Netblock owner	IP address	OS	Web server	Last seen Refresh
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.24.126.50	Linux	cloudflare	11-Feb-2019
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.182.26	Linux	cloudflare-nginx	18-Mar-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.183.26	Linux	cloudflare-nginx	15-Mar-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.182.26	Linux	cloudflare-nginx	14-Mar-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.183.26	Linux	cloudflare-nginx	11-Mar-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.182.26	Linux	cloudflare-nginx	11-Feb-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.183.26	Linux	cloudflare-nginx	9-Feb-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.182.26	Linux	cloudflare-nginx	8-Feb-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.183.26	Linux	unknown	7-Feb-2017
Cloudflare, Inc. 101 Townsend Street San Francisco CA US 94107	104.27.183.26	Linux	cloudflare-nginx	6-Feb-2017

Whois

Domain Name: FITGIRL-REPACKS.SITE
Registry Domain ID: D36010193-CNIC
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: https://publicdomainregistry.com
Updated Date: 2018-09-24T09:40:06.0Z
Creation Date: 2016-09-01T16:43:23.0Z
Registry Expiry Date: 2019-09-01T23:59:59.0Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: ok https://icann.org/epp#ok
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant State/Province: MA
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: WOZ.NS.CLOUDFLARE.COM
Name Server: TANI.NS.CLOUDFLARE.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

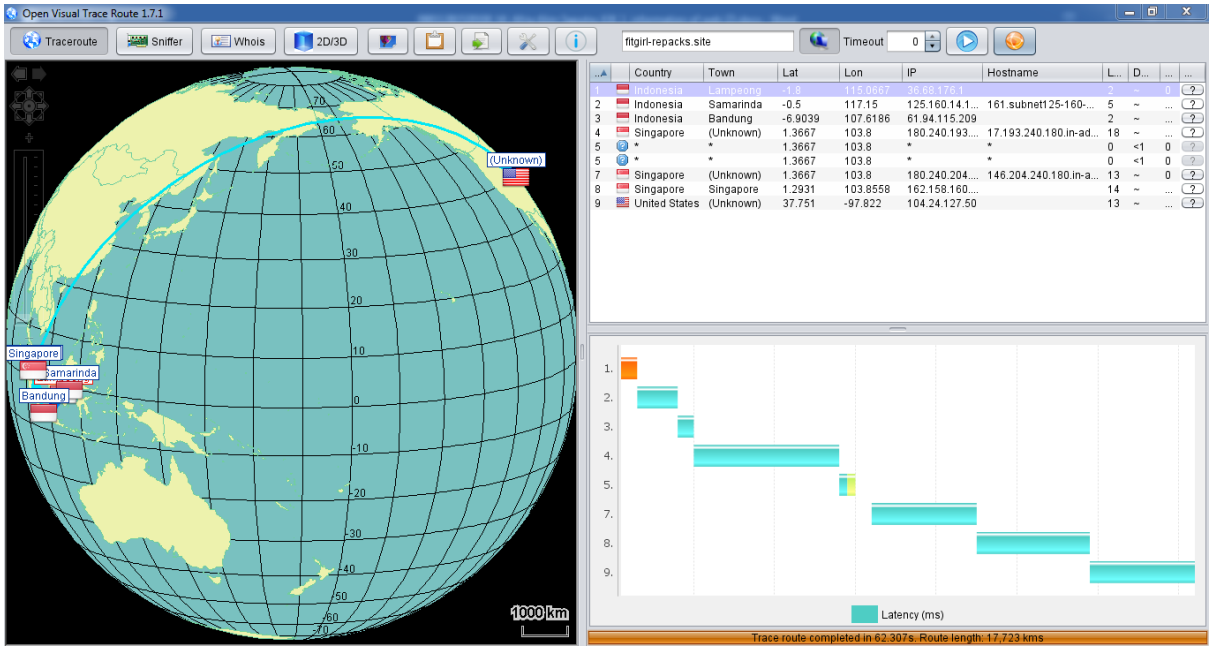
CVE

CVE-2017-7235
An issue was discovered in cloudflare-scrape 1.6.6 through 1.7.1. A malicious website owner could craft a page that executes arbitrary Python code against any cfscrape user who scrapes that website. This is fixed in 1.8.0.

CVE-2018-16844
nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

CVE-2017-7235
An issue was discovered in cloudflare-scrape 1.6.6 through 1.7.1. A malicious website owner could craft a page that executes arbitrary Python code against any cfscrape user who scrapes that website. This is fixed in 1.8.0.

Traceroute


Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
fitgirl-repacks.site
Timeout
0
Country
Town
Lat
Lon
IP
Hostname
1 Indonesia Lampeong -1.8 115.0667 36.68.176.1
2 Indonesia Samarinda -0.5 117.15 125.160.14.1... 161.subnet125-160-...
3 Indonesia Bandung -6.9039 107.6186 61.94.115.209
4 Singapore (Unknown) 1.3667 103.8 180.240.193.... 17.193.240.180.in-ad...
5 * * 1.3667 103.8 * *
5 * * 1.3667 103.8 * *
7 Singapore (Unknown) 1.3667 103.8 180.240.204.... 146.204.240.180.in-a...
8 Singapore Singapore 1.2931 103.8558 162.158.160....
9 United States (Unknown) 37.751 -97.822 104.24.127.50
(Unknown)
Singapore
Samarinda
Bandung
1000 km
Latency (ms)
Trace route completed in 62.307s. Route length: 17,723 kms