Reconnaisance Website

Tugas 1 Keamanan Jaringan Komputer

Oleh :

Muhammad Fikri Rabbani

09011181621013

Kelas : SK8P Indralaya

Dosen pengampu : Deris Stiawan, M.T., Ph.D.

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

WWW.ADVANDIGITAL.COM (dalam negeri)

1. Server Specification

a. Network

- Site : www.advandigital.com
- Domain : advandigital.com
- IP address : 103.3.61.107
- Ipv6 Address : -
- Domain Registrar : PublicDomainRegistry.com
- Organisation : P. Jayakarta No. 46, Jakarta, 10730, ID
- Top level domain : komersial (.com)
- Hosting country : Singapore
- Netblock Owner : 329 E. Jimmie Leeds Road Suite A
- Nameserver : ns1.iixmedia.com
- DNS admin : webmaster@iixmedia.com
- Reverse DNS : webarq.org
- Nameserver organisation : whois.PublicDomainRegistry.com
- Hosting company : Linode
- DNS Security Extensions : -

b. Registrar Information

- Domain Name : ADVANDIGITAL.COM
- Registry Domain ID : 1342683022_DOMAIN_COM-VRSN
- Registrar WHOIS Server : whois.publicdomainregistry.com
- Registrar URL : www.publicdomainregistry.com
- Registrar Registration Expiration Date : 2023-11-27T03:42:49Z
- Registrar : PDR Ltd. d/b/a PublicDomainRegistry.com
- Registrar IANA ID : 303
- Domain Status : OK https://icann.org/epp#OK
- Registry Registrant ID : Not Available From Registry
- Registrant Name : Chandra T
- Registrant Organization : None
- Registrant Street : P. Jayakarta No. 46
- Registrant City : Jakarta
- Registrant State/Province : Jakarta
- Registrant Postal Code : 10730
- Registrant Country : ID
- Registrant Phone : +00.6265830222
- Registrant Phone Ext :
- Registrant Fax :

- Registrant Fax Ext :
- Registrant Email : chandra@advancedigitals.com
- Registry Admin ID : Not Available From Registry
- Admin Name : Chandra T
- Admin Organization : None
- Admin Street : P. Jayakarta No. 46
- Admin City : Jakarta
- Admin State/Province : Jakarta
- Admin Postal Code : 10730
- Admin Country : ID
- Admin Phone : +00.6265830222
- Admin Phone Ext :
- Admin Fax :
- Admin Fax Ext :
- Admin Email : chandra@advancedigitals.com
- Registry Tech ID : Not Available From Registry
- Tech Name : Chandra T
- Tech Organization : None
- Tech Street : P. Jayakarta No. 46
- Tech City : Jakarta
- Tech State/Province : Jakarta
- Tech Postal Code : 10730
- Tech Country : ID
- Tech Phone : +00.6265830222
- Tech Phone Ext :
- Tech Fax :
- Tech Fax Ext :
- Tech Email : chandra@advancedigitals.com
- Name Server : ns5.7flow.com
- Name Server : ns6.7flow.com
- DNSSEC : Unsigned
- Registrar Abuse Contact Email : abuse-contact@publicdomainregistry.com
- Registrar Abuse Contact Phone : +1.2013775952

c. Hosting

- PT. Varnion Technology Semesta Gedung Cyber Lt.3 Jl. Kuningan Barat No.8 Jakarta Selatan 12710
    - IP address : 111.68.116.10
    - OS : Linux
    - Webserver : Apache
    - Tanggal : 27-Jun-2016

d. Site Technology

- Server Side : SSL
- Client side : Javascript
- Client side scripting framework : Google Tag Manager
- Character Encoding : UTF8
- HTTP Compression : Gzip Content Encoding
- Web Browser Targeting : Strict Transport Security
- Doctype : HTML5, HTML
- HTML 5 : Viewport meta tag

2. CVE

a. Apache 2.4.22

No	CVE ID	Vulnerability type	Publish date	Update date	Description
1	CVE-2018-11763		2018-09-25	2019-01-22	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
2	CVE-2018-1333	DOS	2018-06-18	2018-11-13	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
3	CVE-2018-1312		2018-03-26	2018-11-13	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.
4	CVE-2018-1283		2018-03-26	2018-11-13	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.
5	CVE-2017-15715		2018-03-26	2018-11-13	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.
6	CVE-2017-7679	Overflow	2017-06-19	2018-06-02	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

3. Traceroute

#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Palembang	-2.9167	104.75	192.168.10...		19	~	0	
2		Indonesia	Palembang	-2.9167	104.75	10.37.0.1		4	~	0	
3		Indonesia	Bogor	-6.5944	106.7892	103.47.134...	host-103-47-134-...	14	~	467	
4		Indonesia	Bogor	-6.5944	106.7892	172.16.11.12		12	~	0	
5		Indonesia	Jakarta	-6.1744	106.8294	103.47.134...		14	~	46	
6		Indonesia	(Unknown)	-6.5191	105.8078	119.110.11...	IP-117-1.MCS.inte...	63	~	119	
7		Indonesia	(Unknown)	-6.5191	105.8078	119.110.11...	IP-116-165.MCS.i...	26	~	0	
8		Singapore	Singapore	1.2931	103.8558	27.111.228...	63949.sgw.equini...	1...	~	896	
9		Singapore	Singapore	1.2931	103.8558	139.162.0.14		2...	~	0	
...		Singapore	Singapore	1.2931	103.8558	103.3.61.107	webarq.org	1...	~	0	

WWW.SUMSELPROV.GO.ID (pemerintah)

1. Server Specification

a. Network

- Site : http://www.sumselprov.go.id
- Domain : sumselprov.go.id
- IP address : 103.239.165.80
- Ipv6 Address : -
- Domain Registrar : -
- Organisation : -
- Top level domain : Indonesia (.go.id)
- Hosting country : Indonesia
- Netblock Owner : Dinas Perhubungan Kominfo Provinsi Sumatera Selatan
- Nameserver : ns3.sumselprov.go.id
- DNS admin : hostmaster@sumselprov.go.id
- Reverse DNS : -
- Nameserver organisation : -
- Hosting company : -
- DNS Security Extensions : -

b. Registrar

- Domain Name: sumselprov.go.id
- Top Level Domain: ID (Indonesia)
- Domain ID:PANDI-DO55582
- Domain Name:SUMSELPROV.GO.ID
- Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
- 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:NS3.SUMSELPROV.GO.ID
- Name Server:NS1.SUMSELPROV.GO.ID
- DNSSEC:Unsigned

c. Hosting

- Dinas Perhubungan Kominfo Provinsi Sumatera Selatan Government / Direct member IDNIC Jl. Kapten A. Rivai No. 51 Palembang - Sumatera Selatan

- IP address : 103.239.165.80
- OS : Linux
- Webserver : Apache/2.2.15 CentOS
- Tanggal : 17 – Dec – 2018

d. Site technology

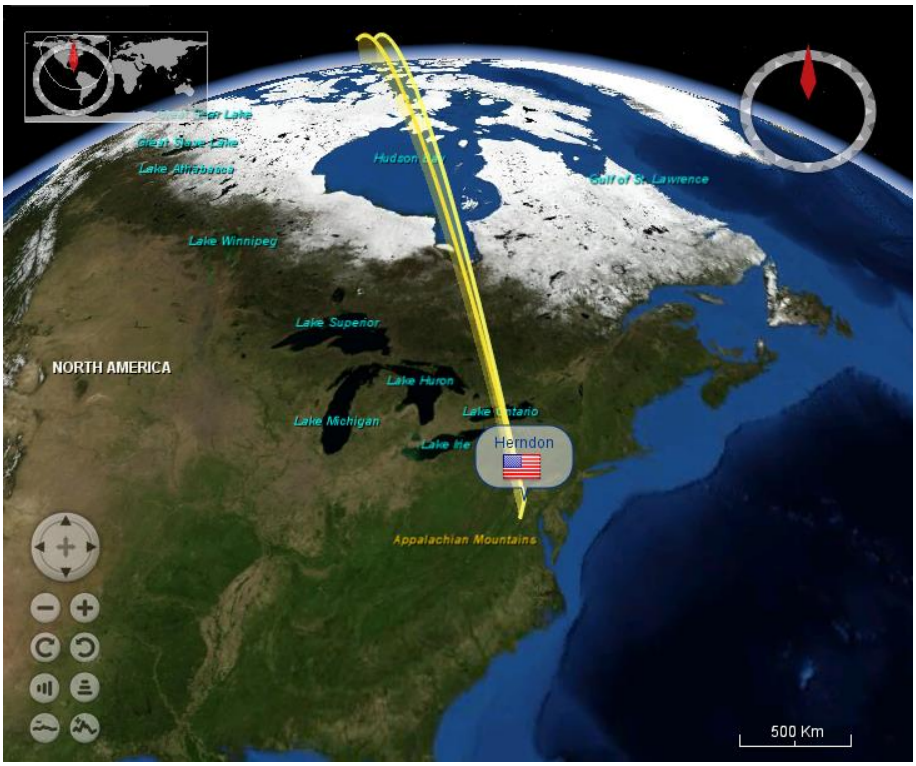
- Application server : CentOS, Apache
- Server side : PHP enabled, PHP
- Client side : Javascript
- Client side scripting framework : Jquery, Font Awesome web font
- Web stat : Google webmaster tool
- Character encoding : ISO-8859-1, UTF8
- Doctype : HTML5
- HTML 5 : Viewport meta tag
- CSS usage : External, CSS media query

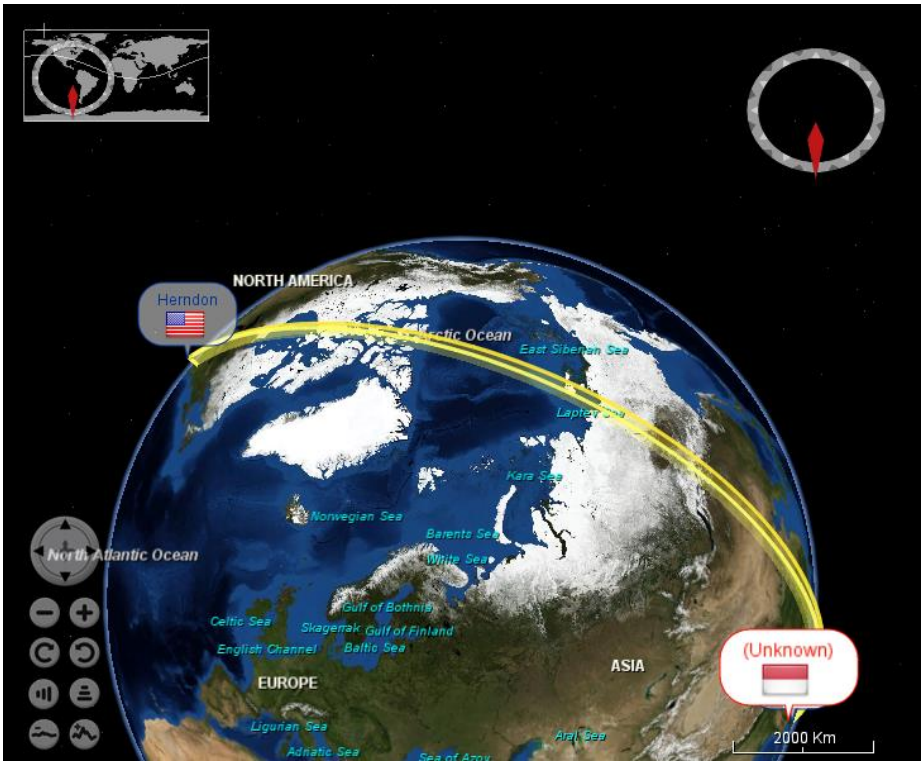
2. CVE

a. Apache 2.2.15

No	CVE ID	Vulnerability type	Publish date	Update date	Description
1	CVE-2017-7679	Overflow	2017-06-19	2018-06-02	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
2	CVE-2017-7668		2017-06-19	2018-06-02	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.3
3	CVE-2017-3169		2017-06-19	2018-06-02	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.4
4	CVE-2017-3167	Bypass	2017-06-19	2018-06-02	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
5	CVE-2016-8612		2018-03-09	2018-06-02	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.
6	CVE-2016-4975	Http R.Spl.	2018-08-14	2018-10-19	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

3. Traceroute





#		Enter an hostname or IP to traceroute		Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Selatan	-7.0546	113.4867	103.241.5....	hotspot-idl.ilkom....	2	~	0	
2		Indonesia	Selatan	-7.0546	113.4867	10.100.2.1		5	~	0	
3		Indonesia	Selatan	-7.0546	113.4867	10.100.1.1		18	~	0	
4		Indonesia	Selatan	-7.0546	113.4867	10.100.5.1		5	~	0	
5		Indonesia	Selatan	-7.0546	113.4867	103.241.5....	ip-103-241-5-113...	4	~	0	
6		Indonesia	Selatan	-7.0546	113.4867	103.241.5....	noc-idl.unsri.ac.id	35	~	0	
7		Indonesia	(Unknown)	-6.9039	107.6186	103.23.18...		14	~	648	
8		*	*	-6.9039	107.6186	*	*	0	<1	0	
8		*	*	-6.9039	107.6186	*	*	0	<1	0	
...		United St...	Herndon	38.9841	-77.3827	63.218.22...	63-218-229-110....	1...	~	1...	
...		Indonesia	Jakarta	-6.1744	106.8294	103.66.19...		99	~	1...	
...		*	*	-6.1744	106.8294	*	*	0	<1	0	
...		*	*	-6.1744	106.8294	*	*	0	<1	0	
...		Indonesia	(Unknown)	-6.175	106.8286	103.239.1...		58	~	0	

WWW.SPACEJAM.COM (luar negeri)

1. Server Specification

a. Network

- Site : www.spacejam.com
- Domain : spacejam.com
- IP address : 54.192.29.6
- Ipv6 Address : 2600:9000:200a:f000:17:45f:7100:93a1
- Domain Registrar : -
- Organisation : -
- Top level domain : komersial (.com)
- Hosting country : US
- Netblock Owner : Amazon.com, Inc.
- Nameserver : ns1-a8.warnerbros.com
- DNS admin : wbol-hostmaster@warnerbros.com
- Reverse DNS : server-54-192-29-6.dub2.r.cloudfront.net
- Nameserver organisation : -
- Hosting company : -
- DNS Security Extensions : -

b. Registrar Information

- Domain Name: spacejam.com
- Registry Domain ID: 2039205_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.markmonitor.com
- Registrar URL: http://www.markmonitor.com
- Updated Date: 2019-02-11T02:10:44-0800
- Creation Date: 1996-03-14T00:00:00-0800
- Registrar Registration Expiration Date: 2021-03-13T23:00:00-0800
- Registrar: MarkMonitor, Inc.
- Registrar IANA ID: 292
- Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
- Registrar Abuse Contact Phone: +1.2083895740
- Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
- Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
- Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
- Registrant Organization: Warner Bros. Entertainment Inc.
- Registrant State/Province: CA

- Registrant Country: US
- Admin Organization: Warner Bros. Entertainment Inc.
- Admin State/Province: CA
- Admin Country: US
- Tech Organization: Warner Bros. Entertainment Inc.
- Tech State/Province: CA
- Tech Country: US
- Name Server: ns1-a8.warnerbros.com
- Name Server: ns3-a8.warnerbros.com
- Name Server: ns2-a8.warnerbros.com
- Name Server: ns4-a8.warnerbros.com
- DNSSEC: unsigned

c. Hosting

- Time Warner Enterprise Infrastructure Services LLC 10 Columbus Circle New York City NY US 10019
    - IP address : 168.161.242.18
    - OS : Linux
    - Web server : Apache
    - Tanggal : 6 - May – 2015

d. Site Technology

- Cloud & PaaS : Amazon Web Services – CloudFront, Amazon Web Services - S3
- Client-Side : JavaScript
- Content Delivery Network : Cloudfront
- Doctype : HTML

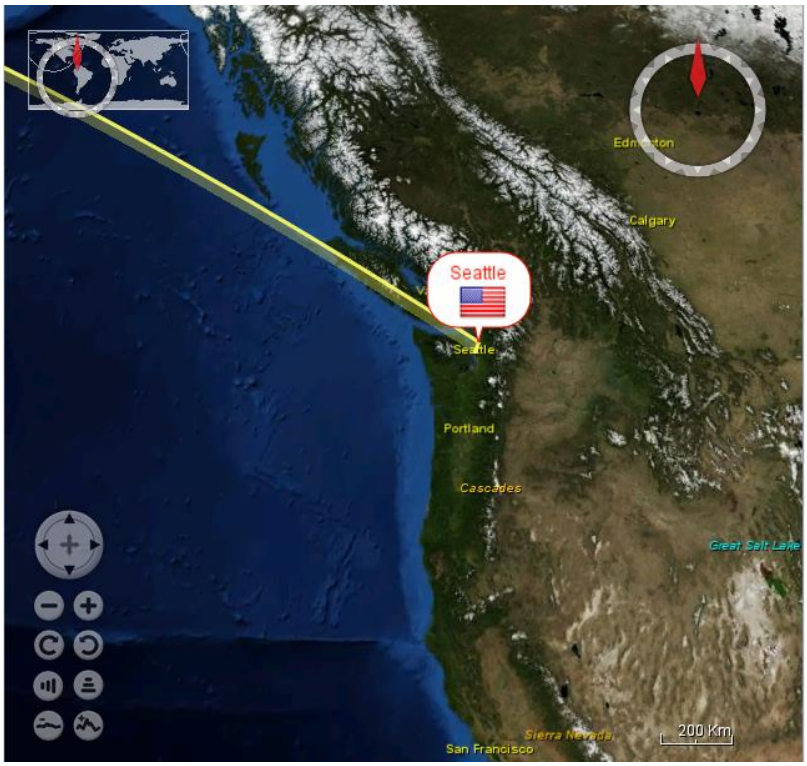
2. CVE

a. Apache 2.4.20

No	CVE ID	Vulnerability type	Publish date	Update date	Description
1	CVE-2018-11763		2018-09-25	2019-01-22	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
2	CVE-2018-1333	DoS	2018-06-18	2018-11-13	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
3	CVE-2018-1312		2018-03-26	2018-11-13	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.
4	CVE-2018-1283		2018-03-26	2018-11-13	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.
5	CVE-2017-15715		2018-03-26	2018-11-13	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.
6	CVE-2017-15710	DoS	2018-03-26	2018-11-13	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

3. Traceroute



#		Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...	...
1		Indonesia	Palembang	-2.9167	104.75	192.168.100.1		1	~	0	
2		Indonesia	Palembang	-2.9167	104.75	10.37.0.1		3	~	0	
3		Indonesia	Jakarta	-6.1744	106.8294	103.47.132.37	host-103-47-132-37....	32	~	429	
4		Indonesia	Jakarta	-6.1744	106.8294	172.16.10.12		20	~	0	
5		Indonesia	Jakarta	-6.1744	106.8294	103.47.132.2...	host-103-47-132-245....	14	~	0	
6		In	Jakarta	-6.1744	106.8294	172.17.0.9		41	~	0	
7		Singapore	Singapore	1.2931	103.8558	103.6.148.233	103-6-148-233.myrep...	36	~	894	
8		Singapore	Singapore	1.2931	103.8558	52.93.8.142		45	~	0	
9		Singapore	Singapore	1.2931	103.8558	52.93.11.169		34	~	0	
10		*	*	1.2931	103.8558	*	*	0	<1	0	
10		*	*	1.2931	103.8558	*	*	0	<1	0	
10		*	*	1.2931	103.8558	*	*	0	<1	0	
10		*	*	1.2931	103.8558	*	*	0	<1	0	
10		*	*	1.2931	103.8558	*	*	0	<1	0	
15		United States	Seattle	47.6103	-122.3341	54.192.151.82	server-54-192-151-82...	52	~	12...	

Indonesia