TUGAS KEAMANAN JARINGAN KOMPUTER

“FOOTPRINTING RECONNAISSANCE”

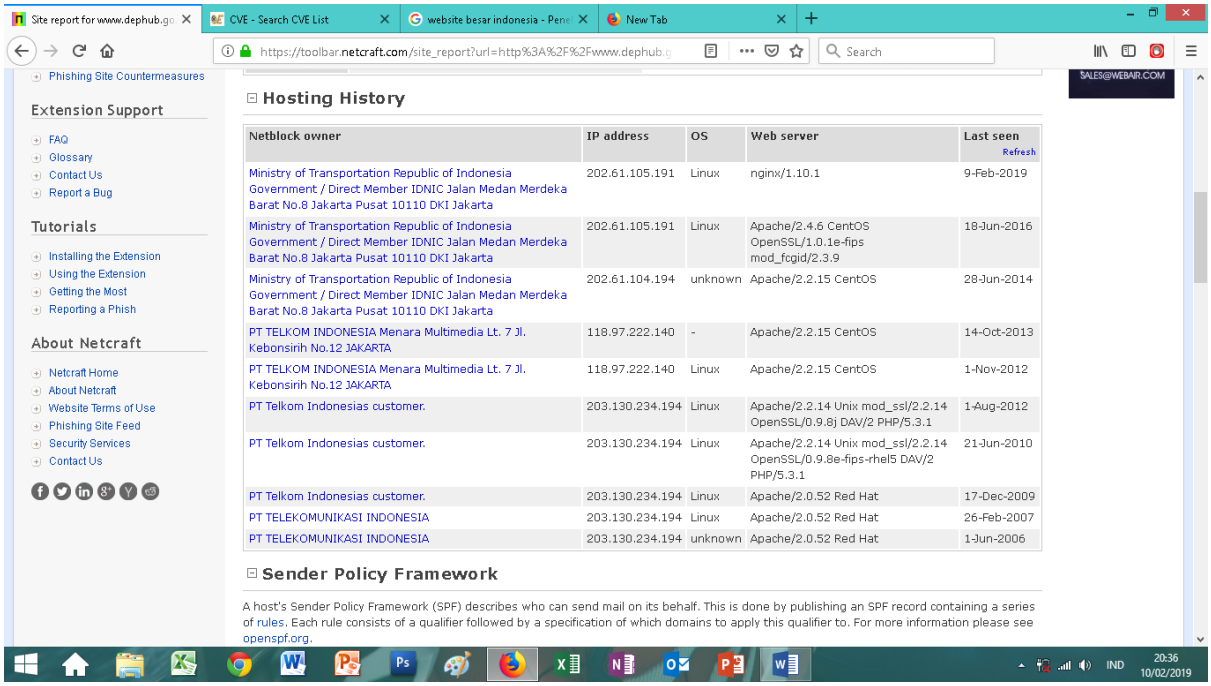
Disusun Oleh:

Nama	: MUHAMMAD FAJAR PUTRA
NIM	: 09011181520009
Kelas	: SK8

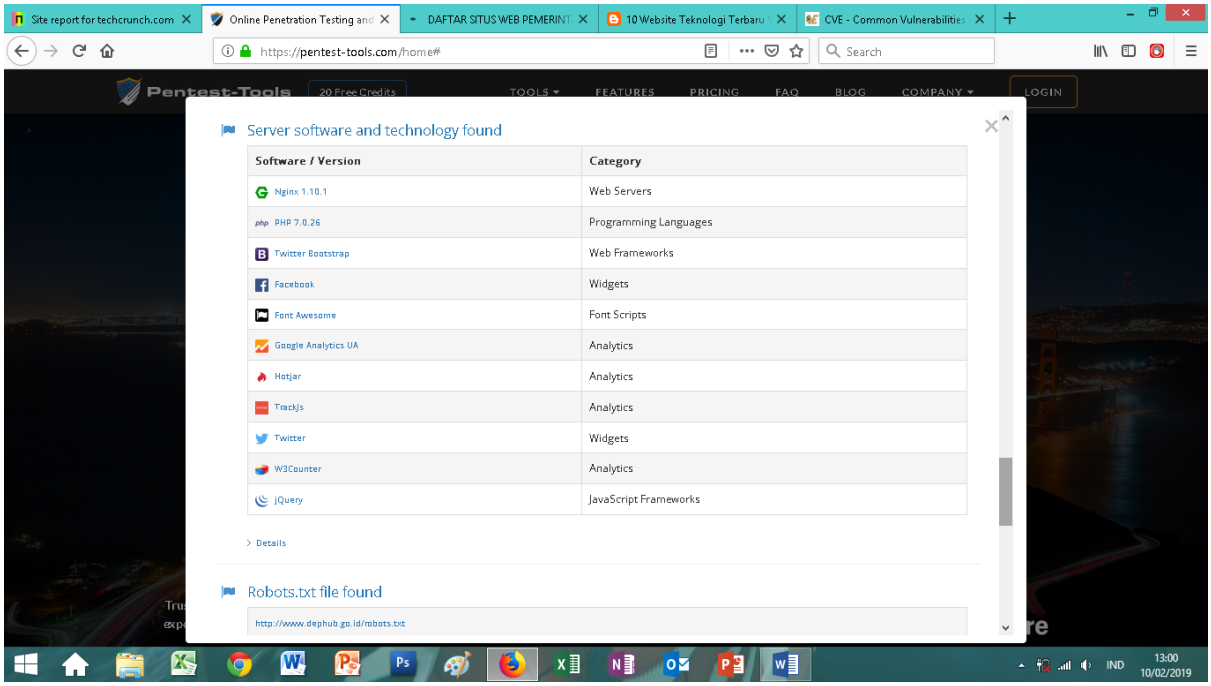
JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2019

1.www.Dephub.go.id (Website Pemerintahan)



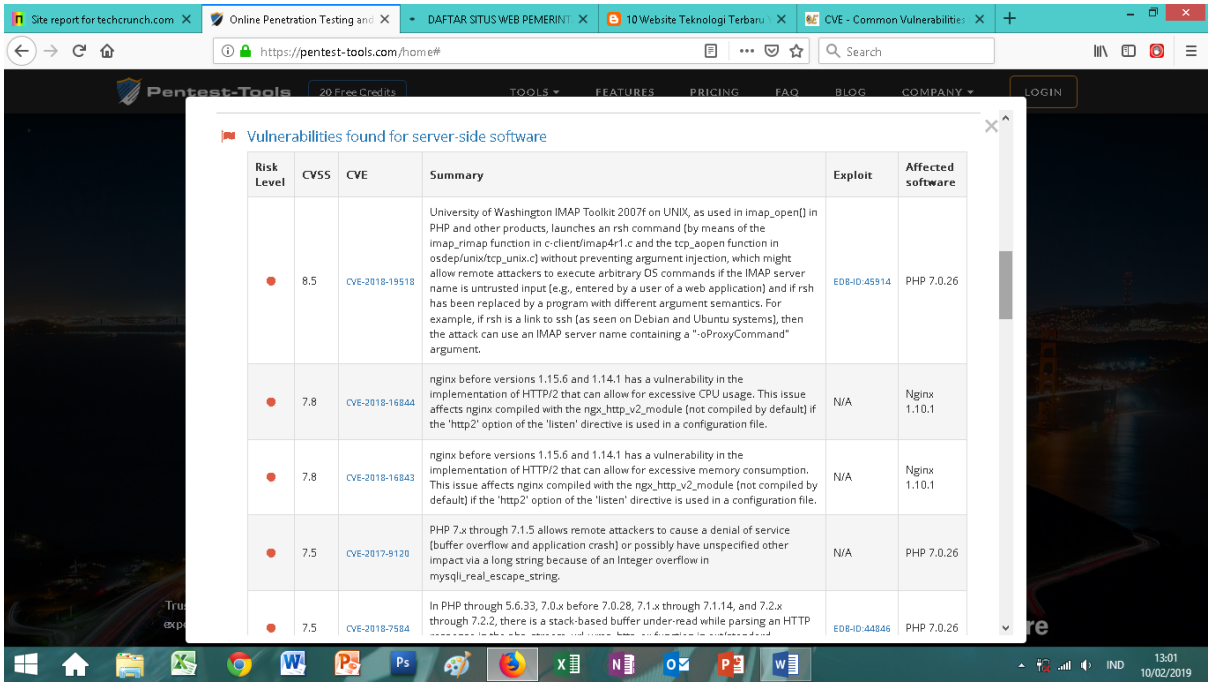
Operating Systemnya menggunakan Linux



Web servernya menggunakan Nginx 1.10.1,

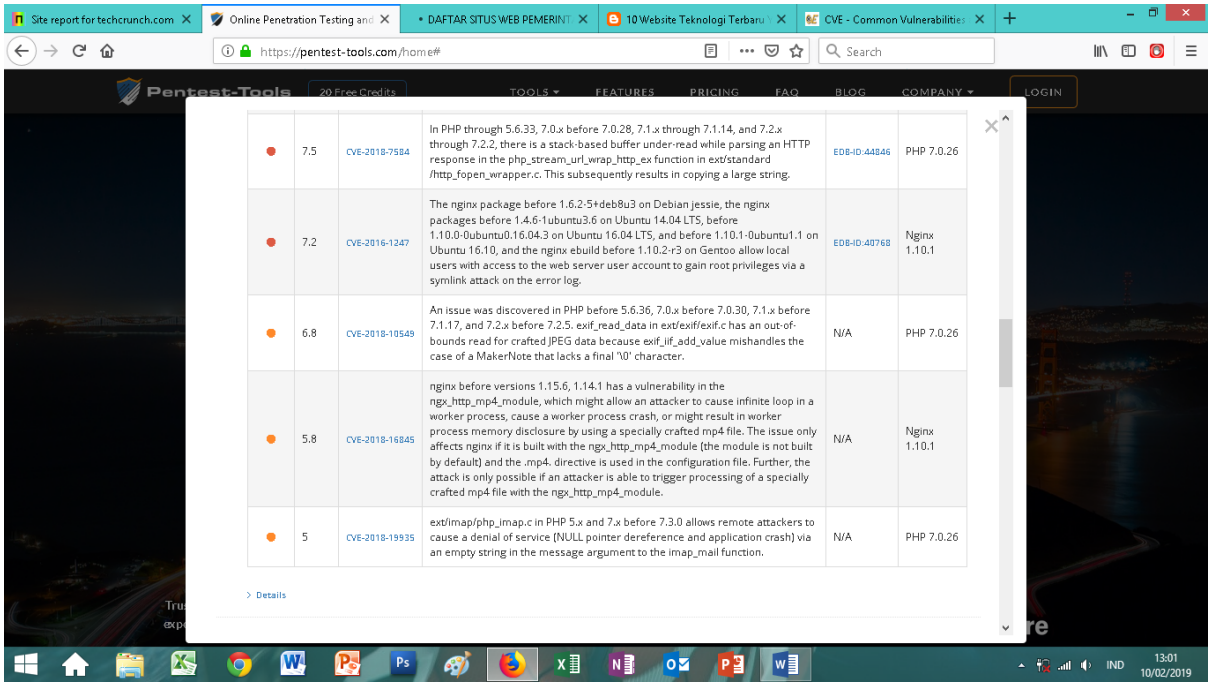
Bahasa Pemrogramannya menggunakan PHP 7.0.26

CVE List:



Vulnerabilities found for server-side software

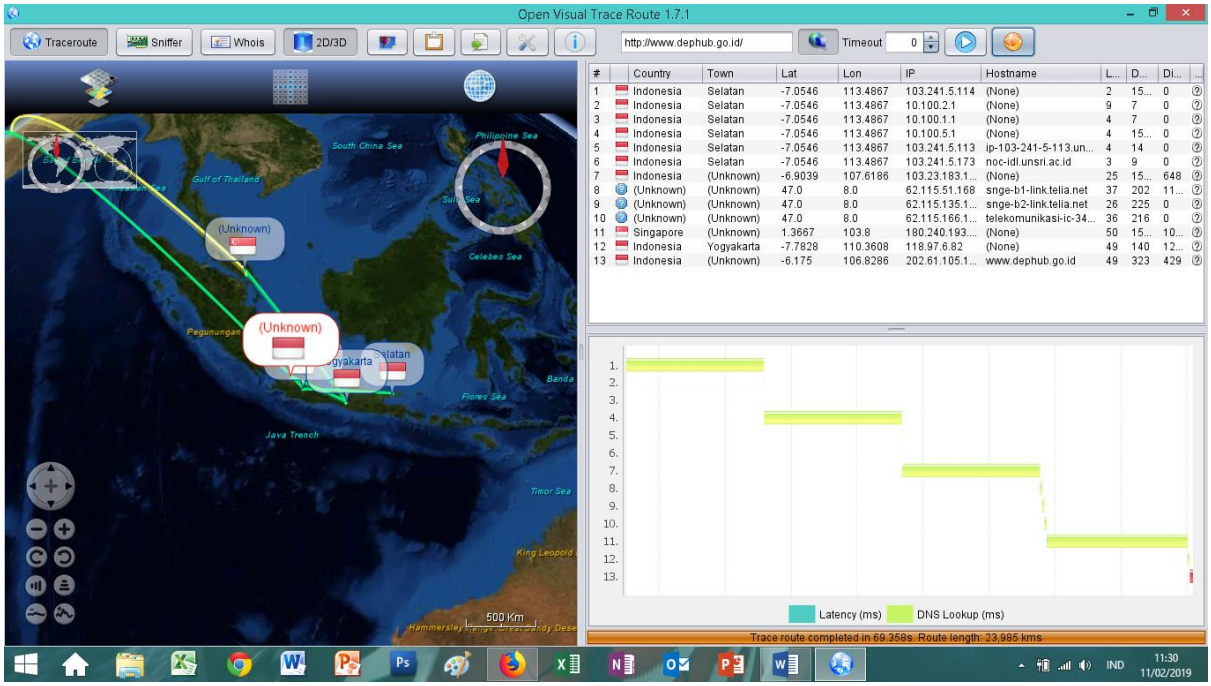
Risk Level	CVSS	CVE	Summary	Exploit	Affected software
	8.5	CVE-2018-19518	University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.	EDB-ID:45914	PHP 7.0.26
	7.8	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.	N/A	Nginx 1.10.1
	7.8	CVE-2018-16843	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. 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.	N/A	Nginx 1.10.1
	7.5	CVE-2017-9120	PHP 7.x through 7.1.5 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a long string because of an Integer overflow in mysqli_real_escape_string.	N/A	PHP 7.0.26
	7.5	CVE-2018-7584	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP	EDB-ID:44846	PHP 7.0.26



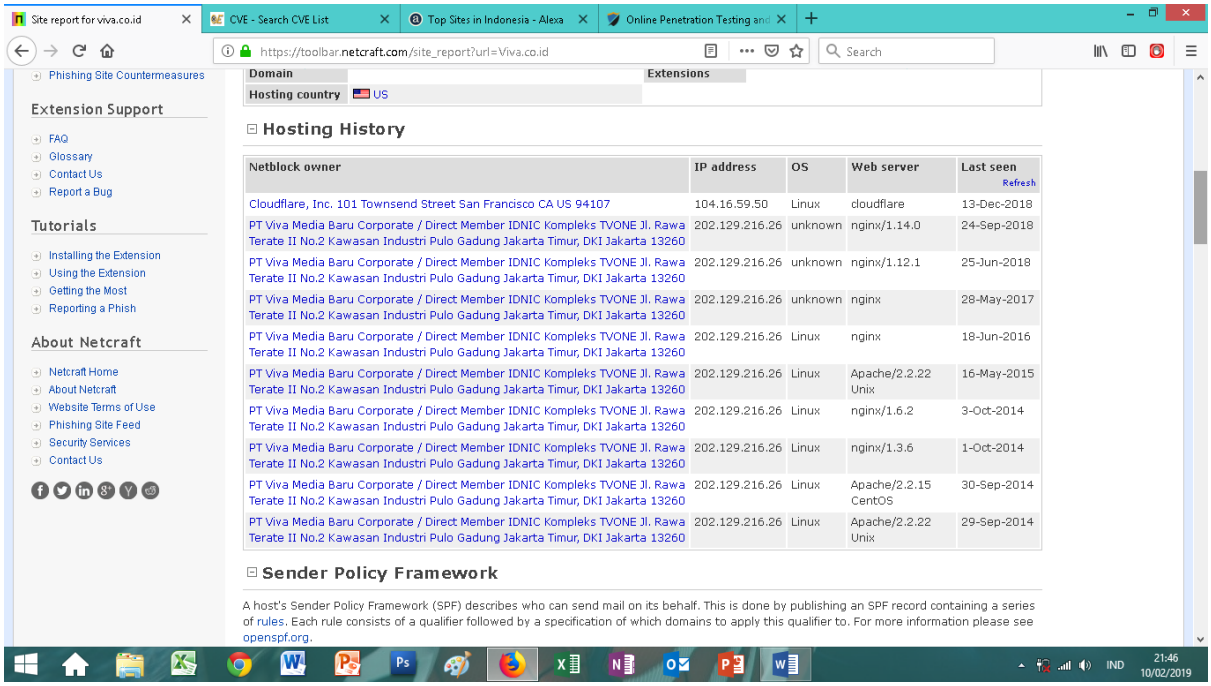
	7.5	CVE-2018-7584	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard /http_fopen_wrapper.c. This subsequently results in copying a large string.	EDB-ID:44846	PHP 7.0.26
	7.2	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.	EDB-ID:40768	Nginx 1.10.1
	6.8	CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.	N/A	PHP 7.0.26
	5.8	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.	N/A	Nginx 1.10.1
	5	CVE-2018-19935	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.	N/A	PHP 7.0.26

> Details

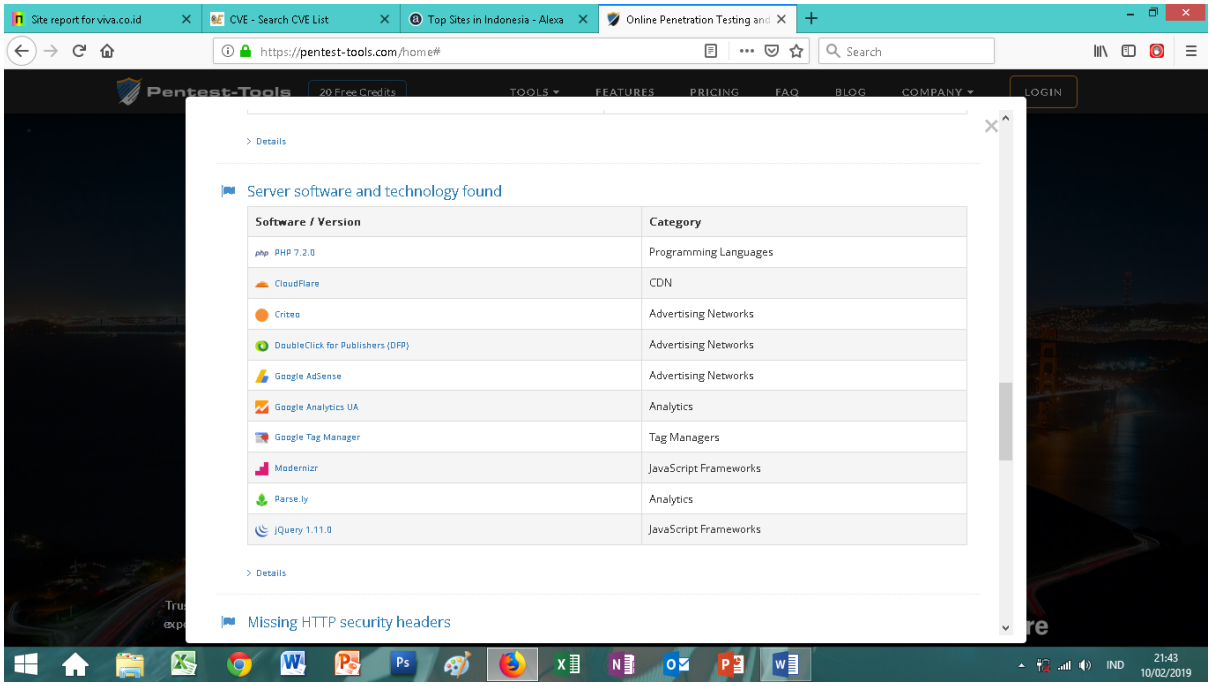
TraceRoute:


Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
http://www.dephub.go.id/
Timeout
0
Country Town Lat Lon IP Hostname L... D... Di...
1 Indonesia Selatan -7.0546 113.4867 103.241.5.114 (None) 2 15... 0
2 Indonesia Selatan -7.0546 113.4867 10.100.2.1 (None) 9 7 0
3 Indonesia Selatan -7.0546 113.4867 10.100.1.1 (None) 4 7 0
4 Indonesia Selatan -7.0546 113.4867 10.100.5.1 (None) 4 15... 0
5 Indonesia Selatan -7.0546 113.4867 103.241.5.113 ip-103-241-5-113.un... 4 14 0
6 Indonesia Selatan -7.0546 113.4867 103.241.5.173 noc-idl.unsri.ac.id 3 9 0
7 Indonesia (Unknown) -6.9039 107.6186 103.23.183.1... (None) 25 15... 648
8 (Unknown) (Unknown) 47.0 8.0 62.115.51.168 snge-b1-link.telia.net 37 202 11...
9 (Unknown) (Unknown) 47.0 8.0 62.115.135.1... snge-b2-link.telia.net 26 225 0
10 (Unknown) (Unknown) 47.0 8.0 62.115.166.1... telekomunikasi-ic-34... 36 216 0
11 Singapore (Unknown) 1.3667 103.8 180.240.193.... (None) 50 15... 10...
12 Indonesia Yogyakarta -7.7828 110.3608 118.97.6.82 (None) 49 140 12...
13 Indonesia (Unknown) -6.175 106.8286 202.61.105.1... www.dephub.go.id 49 323 429
South China Sea
Philippine Sea
Gulf of Thailand
Celebes Sea
(Unknown)
Pegunungan
Flores Sea
Banda
Java Trench
Timor Sea
King Leopold
500 Km
Latency (ms)
DNS Lookup (ms)
Trace route completed in 69.358s. Route length: 23,985 kms
IND
11:30
11/02/2019

2.www.viva.co.id (Website Dalam Negeri)



Operating Systemnya menggunakan Linux



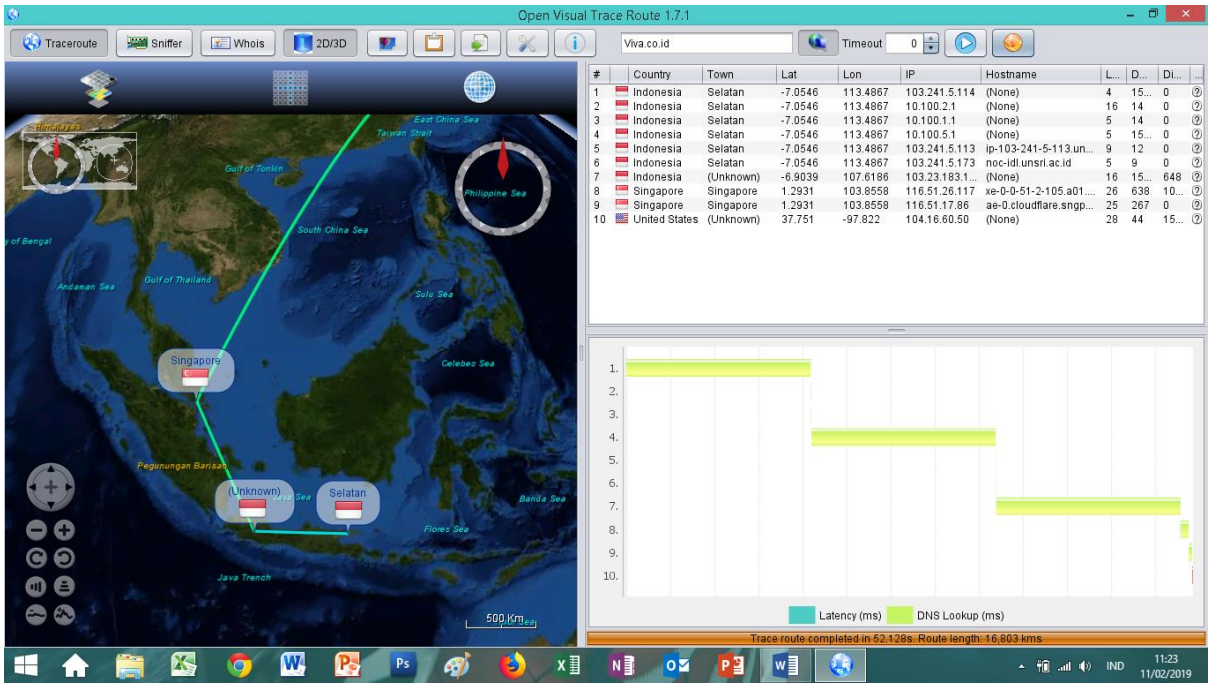
Menggunakan bahasa pemrograman PHP 7.2.0, dan menggunakan CloudFlare

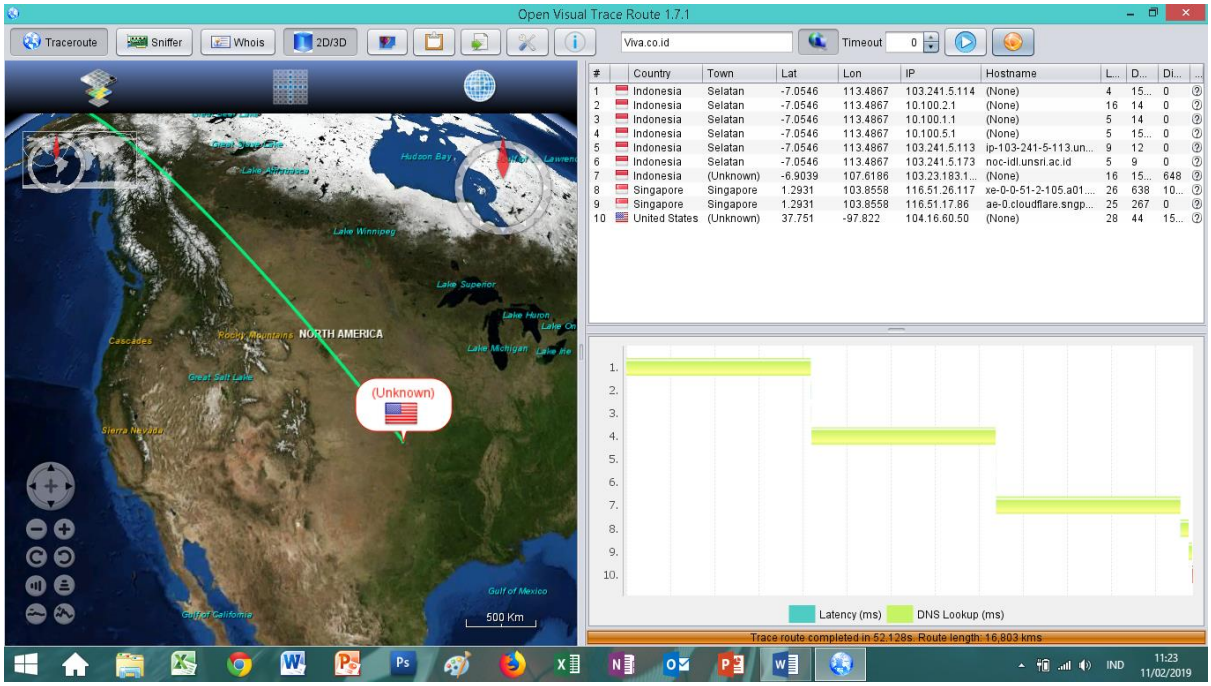
CVE List:

Vulnerabilities found for server-side software

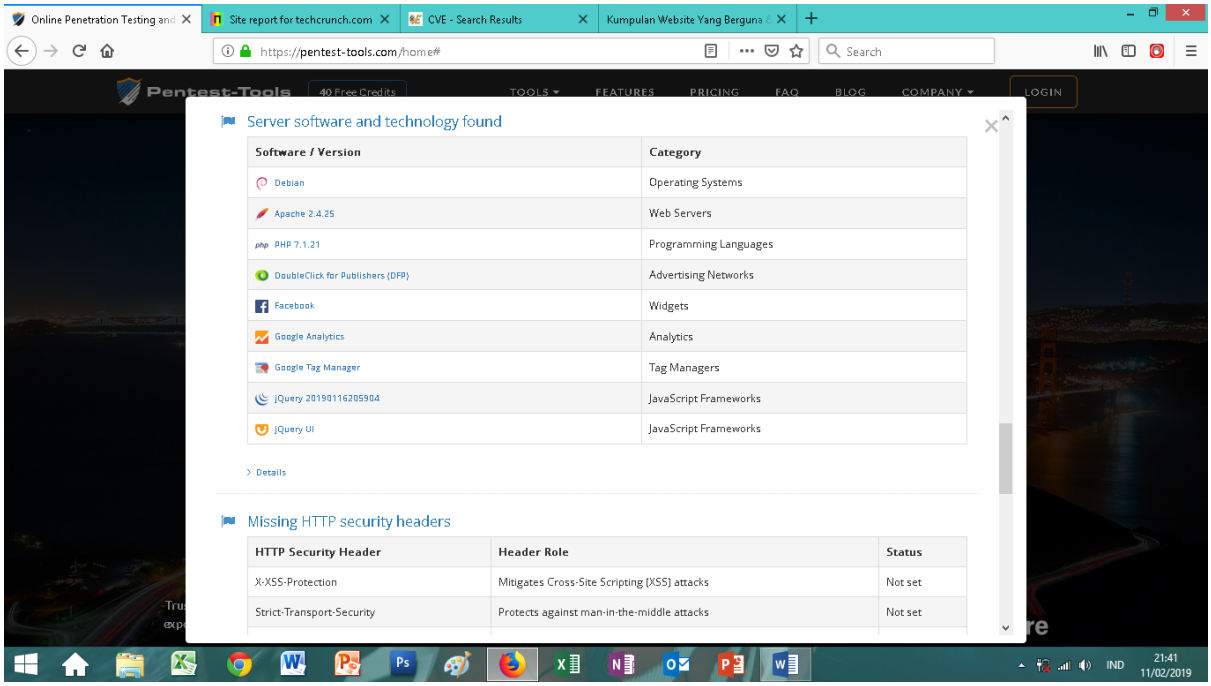
Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	8.5	CVE-2018-19518	University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.	EDB-ID:45914	PHP 7.2.0
●	7.5	CVE-2018-11756	In PHP Runtime for Apache OpenWhisk, a Docker action inheriting one of the Docker tags openwhisk/action-php-v7.2:1.0.0 or openwhisk/action-php-v7.1:1.0.1 (or earlier) may allow an attacker to replace the user function inside the container if the user code is vulnerable to code exploitation.	N/A	PHP 7.2.0
●	7.5	CVE-2018-12882	exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.	N/A	PHP 7.2.0
●	7.5	CVE-2018-7584	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard /http_fopen_wrapper.c. This subsequently results in copying a large string.	EDB-ID:44846	PHP 7.2.0
●	6.8	CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final \0' character.	N/A	PHP 7.2.0

TraceRoute:



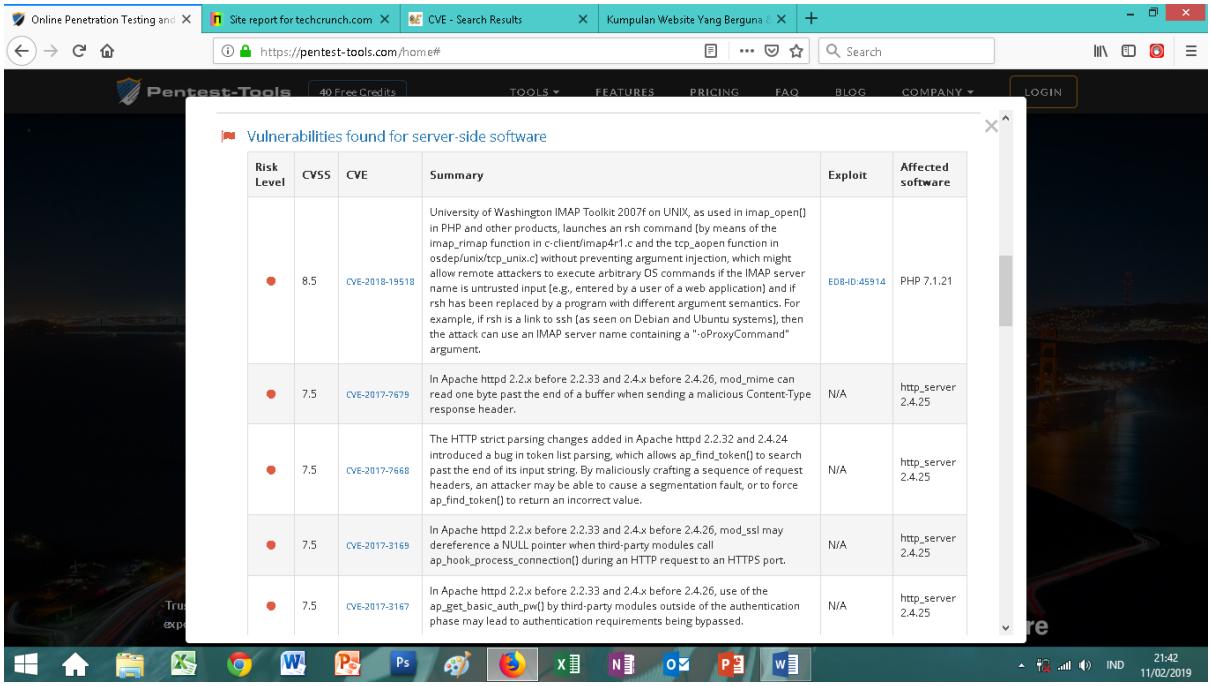

Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
Viva.co.id
Timeout
0
Country Town Lat Lon IP Hostname L... D... Di...
1 Indonesia Selatan -7.0546 113.4867 103.241.5.114 (None) 4 15... 0
2 Indonesia Selatan -7.0546 113.4867 10.100.2.1 (None) 16 14 0
3 Indonesia Selatan -7.0546 113.4867 10.100.1.1 (None) 5 14 0
4 Indonesia Selatan -7.0546 113.4867 10.100.5.1 (None) 5 15... 0
5 Indonesia Selatan -7.0546 113.4867 103.241.5.113 ip-103-241-5-113.un... 9 12 0
6 Indonesia Selatan -7.0546 113.4867 103.241.5.173 noc-idl.unsri.ac.id 5 9 0
7 Indonesia (Unknown) -6.9039 107.6186 103.23.183.1... (None) 16 15... 648
8 Singapore Singapore 1.2931 103.8558 116.51.26.117 xe-0-0-51-2-105.a01.... 26 638 10...
9 Singapore Singapore 1.2931 103.8558 116.51.17.86 ae-0.cloudflare.sngp... 25 267 0
10 United States (Unknown) 37.751 -97.822 104.16.60.50 (None) 28 44 15...
NORTH AMERICA
(Unknown)
500 Km
Latency (ms)
DNS Lookup (ms)
Trace route completed in 52.128s. Route length: 16,803 kms
IND
11:23
11/02/2019

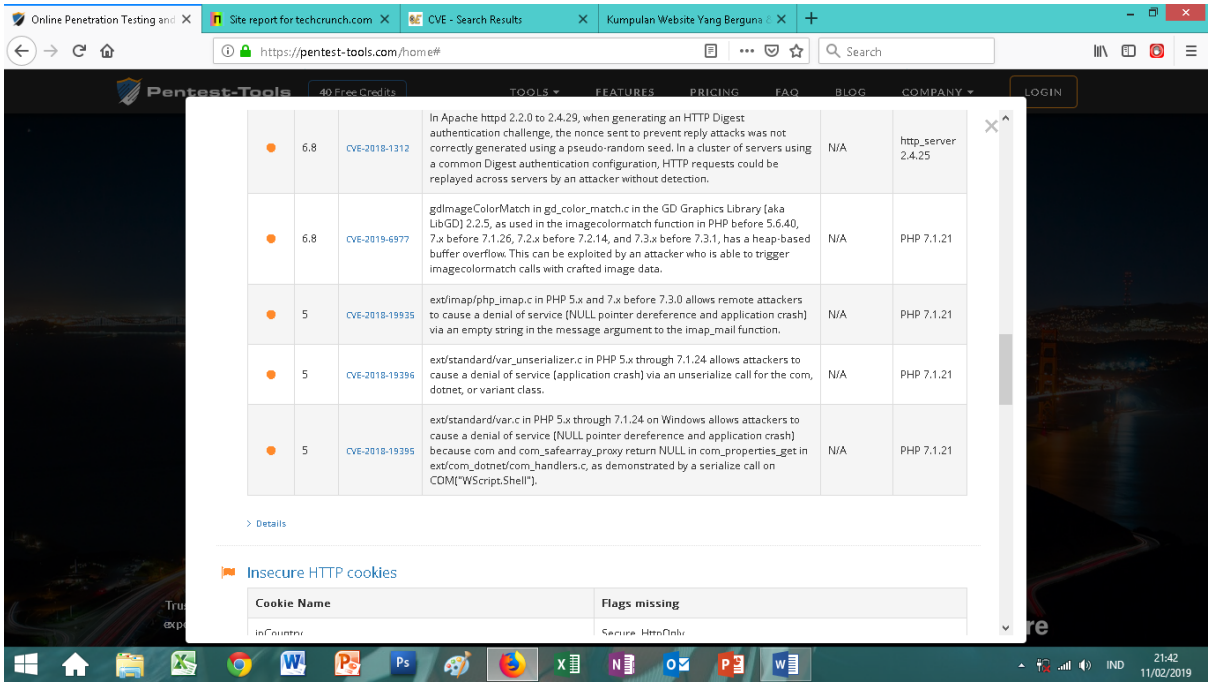
3.www.seatguru.com (Website Luar Negeri)



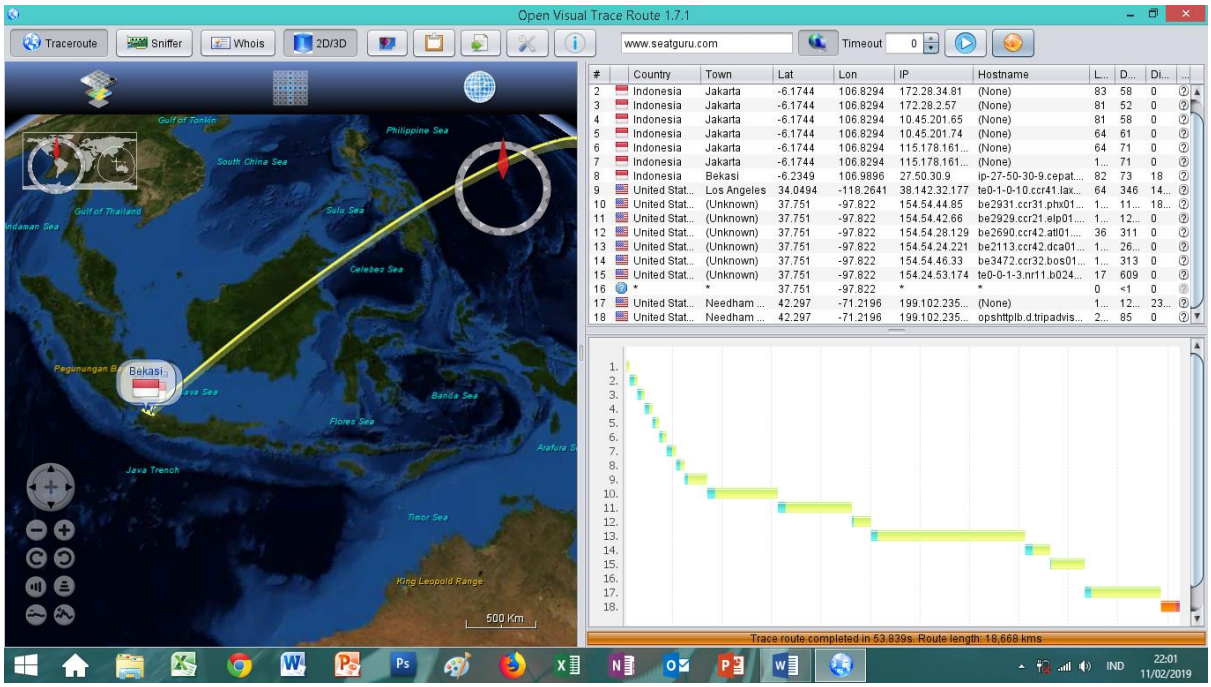
Website ini menggunakan Sistem operasi Debian, menggunakan Apache 2.4.25 sebagai web servernya, dan menggunakan PHP 7.1.21 sebagai bahasa pemrogramannya.

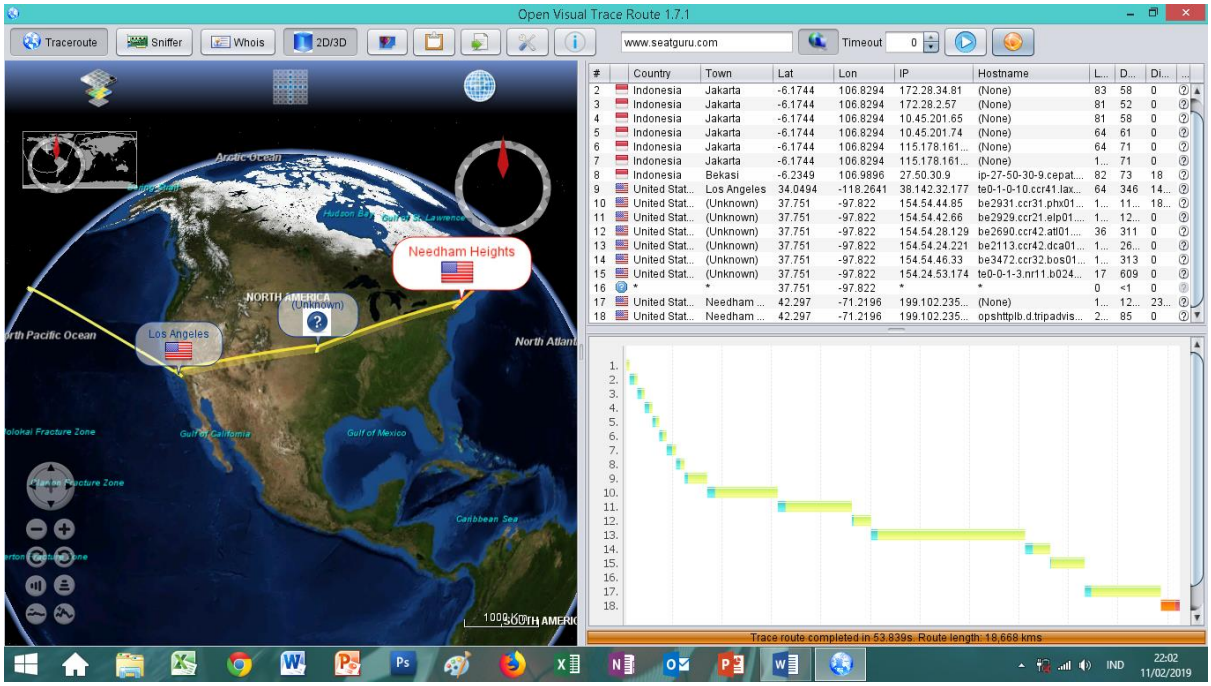
CVE List:




Online Penetration Testing and
Site report for techcrunch.com
CVE - Search Results
Kumpulan Website Yang Berguna &
https://pentest-tools.com/home#
Search
Pentest-Tools
40 Free Credits
TOOLS
FEATURES
PRICING
FAQ
BLOG
COMPANY
LOGIN
6.8 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. N/A http_server 2.4.25
6.8 CVE-2019-6977 gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data. N/A PHP 7.1.21
5 CVE-2018-19935 ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function. N/A PHP 7.1.21
5 CVE-2018-19396 ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class. N/A PHP 7.1.21
5 CVE-2018-19395 ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM("WScript.Shell"). N/A PHP 7.1.21
Details
Insecure HTTP cookies
Cookie Name
Flags missing
IND
21:42
11/02/2019

TraceRoute:


Open Visual Trace Route 1.7.1
Traceroute
Sniffer
Whois
2D/3D
www.seatguru.com
Timeout
Gulf of Tonkin
Philippine Sea
South China Sea
Gulf of Thailand
Sulu Sea
Celebes Sea
Bekasi
Banda Sea
Flores Sea
Java Trench
Timor Sea
King Leopold Range
500 Km
Trace route completed in 53.839s. Route length: 18,668 kms
IND
22:01
11/02/2019



#	Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...
2	Indonesia	Jakarta	-6.1744	106.8294	172.28.34.81	(None)	83	58	0
3	Indonesia	Jakarta	-6.1744	106.8294	172.28.2.57	(None)	81	52	0
4	Indonesia	Jakarta	-6.1744	106.8294	10.45.201.65	(None)	81	58	0
5	Indonesia	Jakarta	-6.1744	106.8294	10.45.201.74	(None)	64	61	0
6	Indonesia	Jakarta	-6.1744	106.8294	115.178.161...	(None)	64	71	0
7	Indonesia	Jakarta	-6.1744	106.8294	115.178.161...	(None)	1...	71	0
8	Indonesia	Bekasi	-6.2349	106.9896	27.50.30.9	ip-27-50-30-9.cepat....	82	73	18
9	United Stat...	Los Angeles	34.0494	-118.2641	38.142.32.177	te0-1-0-10.ccr41.lax...	64	346	14...
10	United Stat...	(Unknown)	37.751	-97.822	154.54.44.85	be2931.ccr31.phx01....	1...	11...	18...
11	United Stat...	(Unknown)	37.751	-97.822	154.54.42.66	be2929.ccr21.elp01....	1...	12...	0
12	United Stat...	(Unknown)	37.751	-97.822	154.54.28.129	be2690.ccr42.atl01....	36	311	0
13	United Stat...	(Unknown)	37.751	-97.822	154.54.24.221	be2113.ccr42.dca01....	1...	26...	0
14	United Stat...	(Unknown)	37.751	-97.822	154.54.46.33	be3472.ccr32.bos01....	1...	313	0
15	United Stat...	(Unknown)	37.751	-97.822	154.24.53.174	te0-0-1-3.nr11.b024....	17	609	0
16	*	*	37.751	-97.822	*	*	0	<1	0
17	United Stat...	Needham ...	42.297	-71.2196	199.102.235...	(None)	1...	12...	23...
18	United Stat...	Needham ...	42.297	-71.2196	199.102.235...	opshttplb.d.tripadvis....	2...	85	0