

**Tugas Keamanan Jaringan
Reconnaissance**



**Disusun Oleh:
Juanda Fahrizal
09011181520006**

**Universitas Sriwijaya
Fakultas Ilmu Komputer
Jurusan Sistem Komputer
2019**

1. Website Pemerintahan (<http://www.pangkalpinangkota.go.id>)

Deskripsi Website menggunakan tools Robtex :

QUICK INFO

Quick summary of the host name

www.pangkalpinangkota.go.id quick info

General	
FQDN	www.pangkalpinangkota.go.id
Host Name	www
Domain Name	pangkalpinangkota.go.id
Registry	go.id
TLD	id
Domain DNS	
Name servers	ns1.iixmedia.com ns2.iixmedia.com
Mail servers	mail.pangkalpinangkota.go.id
IP Numbers	103.28.22.117

Sistem Operasi yang digunakan menggunakan Pantest-tools:

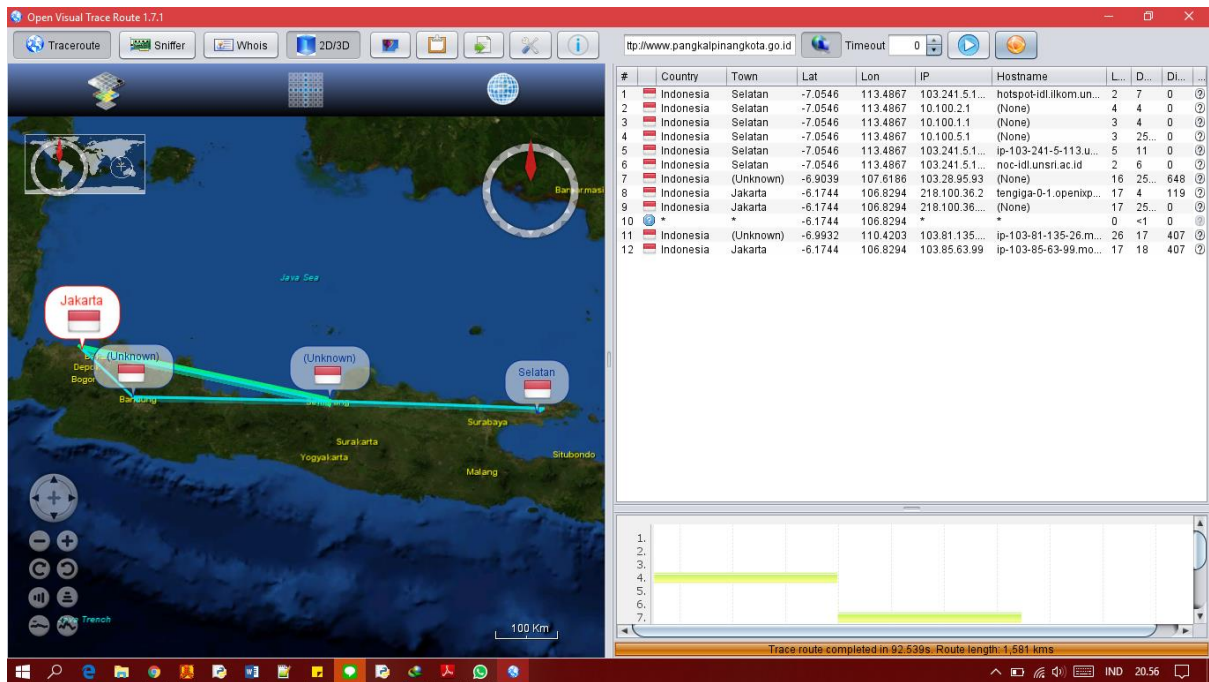
Software / Version	Category
CentOS	Operating Systems
Apache 2.4.6	Web Servers
PHP 5.4.16	Programming Languages
WordPress 5.0.3	CMS, Blogs
Font Awesome	Font Scripts
Google Analytics UA	Analytics
Google Font API	Font Scripts
Lightbox	JavaScript Frameworks
Twitter Emoji (Twemoji)	JavaScript Graphics
Yoast SEO	Marketing Automation
jQuery	JavaScript Frameworks
prettyPhoto	JavaScript Frameworks

CVE yang terdeteksi menggunakan Pantest-tools :

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
	7.5	CVE-2014-9912	The <code>get_icu_disp_value_src_php</code> function in <code>ext/intl/locale/locale_methods.c</code> in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU <code>uresbund.cpp</code> component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a <code>locale_get_display_name</code> call with a long first argument.	N/A	PHP 5.4.16
	7.5	CVE-2014-3515	The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) <code>ArrayObject</code> and (2) <code>SPLObjectStorage</code> .	N/A	PHP 5.4.16
	7.5	CVE-2014-3669	Integer overflow in the <code>object_custom</code> function in <code>ext/standard/var_unserializer.c</code> in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the <code>unserialize</code> function that triggers calculation of a large length value.	N/A	PHP 5.4.16
	7.5	CVE-2015-0231	Use-after-free vulnerability in the <code>process_nested_data</code> function in <code>ext/standard/var_unserializer.re</code> in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted <code>unserialize</code> call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.	N/A	PHP 5.4.16
	7.5	CVE-2014-9427	<code>sapi/cgi/cgi_main.c</code> in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when <code>mmap</code> is used to read a <code>.php</code> file, does not properly consider the mapping's length during processing of an invalid file that begins with a <code>#</code> character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers	N/A	PHP 5.4.16

			to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.		
7.5	CVE-2017-7679		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.	N/A	http_server 2.4.6
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 replay 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 2.4.6
6.8	CVE-2017-15715		In Apache httpd 2.4.0 to 2.4.29, the expression specified in 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 externally blocked, but only by matching the trailing portion of the filename.	N/A	http_server 2.4.6
6.8	CVE-2014-0226		Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.	EDB-ID:34133	http_server 2.4.6
6.4	CVE-2017-9788		In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.	N/A	http_server 2.4.6

Tampilan tracking data pada software Open Visual Traceroute :











2. Website Dalam Negri (<http://www.sinarmas.com/>)

Deskripsi Website menggunakan tools Robtex :

QUICK INFO	
Quick summary of the host name	
www.sinarmas.com quick info	
General	
FQDN	www.sinarmas.com
Host Name	www
Domain Name	sinarmas.com
Registry	com
TLD	com
DNS	
IP numbers	66.96.249.137
Domain DNS	
Name servers	ns1.eikonwebstar.com ns2.eikonwebstar.com ns3.eikonwebstar.com ns4.eikonwebstar.com
Mail servers	mail.sinarmas.com mx1.bsd.simasfinance.co.id mx2.bsd.simasfinance.co.id mx3.lbk.simasfinance.co.id mx4.lbk.simasfinance.co.id
IP Numbers	66.96.249.137

Sistem Operasi yang digunakan menggunakan Pantest-tools:

Server software and technology found

Software / Version	Category
 Ubuntu	Operating Systems
 Apache 2.4.7	Web Servers
 PHP 5.5.9	Programming Languages
 Twitter Bootstrap	Web Frameworks
 DreamWeaver	Editors
 Twitter	Widgets
 YouTube	Video Players
 jQuery 1.11.3	JavaScript Frameworks

:

CVE yang terdeteksi menggunakan Pantest-tools

isk Level	CVSS	CVE	Summary	Exploit	Affected software
	10.0	CVE-2015-4642	The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.	N/A	PHP 5.5.9
	10.0	CVE-2015-4603	The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.	N/A	PHP 5.5.9
	10.0	CVE-2015-4602	The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.	N/A	PHP 5.5.9
	10.0	CVE-2015-5589	The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.	N/A	PHP 5.5.9
	10.0	CVE-2015-4599	The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of	N/A	PHP 5.5.9

			service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.		
7.5	CVE-2017-7679	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.	N/A	http_server 2.4.7	
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 replay 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 2.4.7	
6.8	CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in 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 externally blocked, but only by matching the trailing portion of the filename.	N/A	http_server 2.4.7	
6.8	CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.	EDB-ID:34133	http_server 2.4.7	
6.4	CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to	N/A	http_server 2.4.7	

leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

Tampilan tracking data pada software Open Visual Traceroute

The screenshot displays the Open Visual Traceroute 1.7.1 application interface. The left pane shows a 3D map of Indonesia with a red path tracing the route from Jakarta to Surabaya. A red circle highlights the starting point in Jakarta, and another red circle highlights the destination in Surabaya. The right pane shows a detailed table of traceroute data.

#	Country	Town	Lat	Lon	IP	Hostname	L...	D...	Di...
1	Indonesia	Selatan	-7.0546	113.4867	103.241.5.1...		5	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		2	0	?
4	Indonesia	Selatan	-7.0546	113.4867	10.100.5.1		3	0	?
5	Indonesia	Selatan	-7.0546	113.4867	103.241.5.1...		2	0	?
6	Indonesia	Selatan	-7.0546	113.4867	103.241.5.1...		3	0	?
7	Indonesia	(Unknown)	-6.9039	107.6186	103.28.95.93		16	648	?
8	Indonesia	Jakarta	-6.1744	106.8294	218.100.36.2		50	119	?
9	Indonesia	Jakarta	-6.1744	106.8294	218.100.36....		17	0	?
...	Indonesia	Jakarta	-6.1744	106.8294	103.47.134....		16	0	?
...	Indonesia	Jakarta	-6.1744	106.8294	103.47.132....		17	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?
...	*	*	-6.1744	106.8294	*	*	0	0	?

Trace route incomplete. Reached max number of hops. This number can be changed in the settings.

3. Website Luar Negeri (<https://www.logitechg.com/en-au>)

Deskripsi Website menggunakan tools Robtex :

QUICK INFO	
Quick summary of the host name	
www.logitechg.com quick info	
General	
FQDN	www.logitechg.com
Host Name	www
Domain Name	logitechg.com
Registry	com
TLD	com
Domain DNS	
Name servers	ns-1.logitech.com ns-2.logitech.com
Mail servers	aspmx.l.google.com alt1.aspmx.l.google.com alt2.aspmx.l.google.com alt3.aspmx.l.google.com alt4.aspmx.l.google.com
IP Numbers	107.21.26.162 107.23.199.237

Sistem Operasi yang digunakan menggunakan Pantest-tools:

Software / Version	Category
 Nginx 1.12.1	Web Servers
 Amazon Cloudfront	CDN
 Tealium	Advertising Networks
 jQuery	JavaScript Frameworks

CVE yang terdeteksi menggunakan Pantest-tools :

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
	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 1.12.1
	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 1.12.1
	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 1.12.1

Tampilan tracking data pada software Open Visual Traceroute

