RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

WEBSITE SECURITY VULNERABILITIES

1. **Government Website** (*http://www.palembang.go.id/*)

   - **Common Vulnerabilities and Exposures (CVE)**

	6.8	CVE-2015-8994	An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.	N/A	PHP 5.6.28
	6.5	CVE-2018-19520	An issue was discovered in SDCMS 1.6 with PHP 5.x. app/admin/controller/themecontroller.php uses a check_bad function in an attempt to block certain PHP functions such as eval, but does not prevent use of preg_replace 'e' calls, allowing users to execute arbitrary code by leveraging access to admin template management.	N/A	PHP 5.6.28
	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OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics.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 5.6.28
	7.5	CVE-2016-9935	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.	N/A	PHP 5.6.28
	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 5.6.28

Sumber : https://pentest-tools.com/

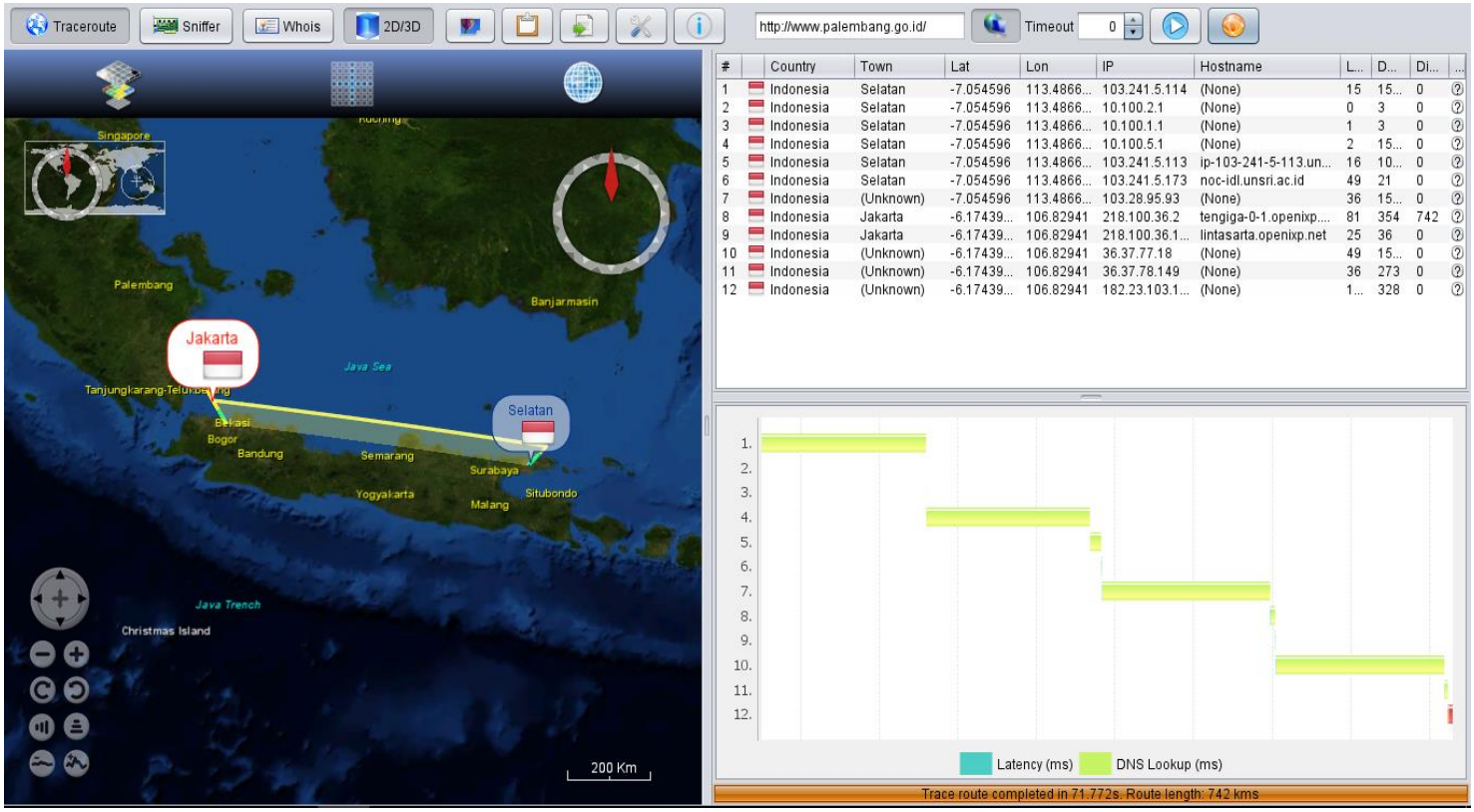
RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

- **Server Software and Technology Found**

Software / Version	Category
Apache 2	Web Servers
PHP 5.6.28	Programming Languages
Twitter Bootstrap	Web Frameworks
Google Font API	Font Scripts
Google Maps	Maps
YouTube	Video Players
jQuery 1.9.1	JavaScript Frameworks

Sumber : https://pentest-tools.com/

- **Visual Trace Route**



RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

2. Domestic Website *(http://djarum.com/)*

➢ Common Vulnerabilities and Exposures (CVE)

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 5.6.24
●	7.5	CVE-2016-7129	The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.	N/A	PHP 5.6.24
●	7.5	CVE-2016-7127	The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.	N/A	PHP 5.6.24
●	7.5	CVE-2016-7126	The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.	N/A	PHP 5.6.24
●	7.5	CVE-2016-7124	ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.	N/A	PHP 5.6.24

Sumber : https://pentest-tools.com/

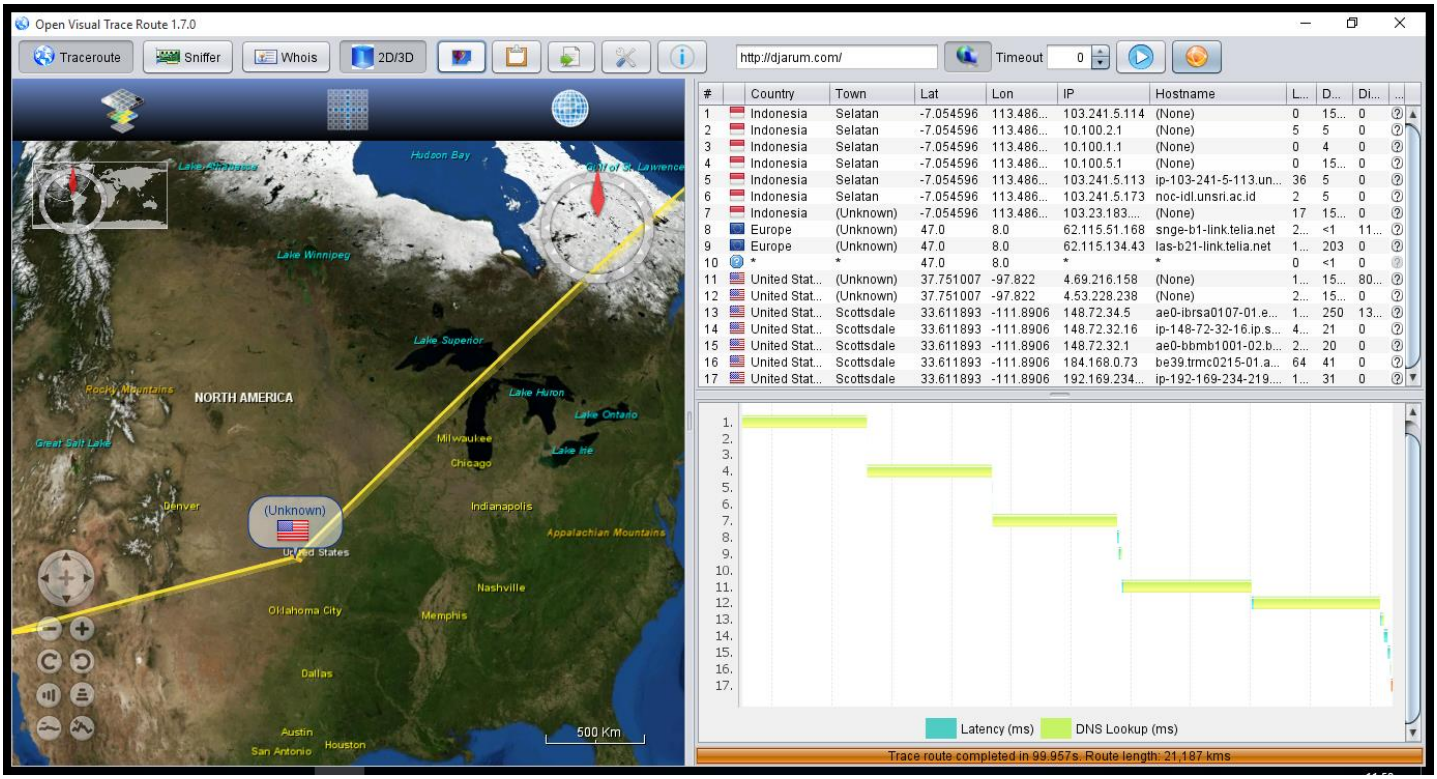
➢ Server Software and Technology Found

Software / Version	Category
Apache	Web Servers
PHP 5.6.24	Programming Languages
TYPO3 CMS	CMS
SWFObject	Miscellaneous
Google Analytics	Analytics
jQuery 2.1.1	JavaScript Frameworks

Sumber : https://pentest-tools.com/

RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

- **Visual Trace Route**



RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

3. Foreign Website (*https://fly10.emirates.com*)

➢ Common Vulnerabilities and Exposures (CVE)

Name	Description
CVE-2019-1673	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. For information about fixed software releases, consult the Cisco bug ID at https://quickview.cloudapps.cisco.com/quickview/bug/CSCvn64652. When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories and Alerts page, to determine exposure and a complete upgrade solution.
CVE-2019-1653	A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability.
CVE-2018-9920	Server side request forgery exists in the runtime application in K2 smartforms 4.6.11 via a modified hostname in an https://*/Identity/STS/Forms/Scripts URL.
CVE-2018-8025	CVE-2018-8025 describes an issue in Apache HBase that affects the optional "Thrift 1" API server when running over HTTP. There is a race-condition which could lead to authenticated sessions being incorrectly applied to users, e.g. one authenticated user would be considered a different user or an unauthenticated user would be treated as an authenticated user. https://issues.apache.org/jira/browse/HBASE-20664 implements a fix for this issue. It has been fixed in versions: 1.2.6.1, 1.3.2.1, 1.4.5, 2.0.1.
CVE-2018-8016	The default configuration in Apache Cassandra 3.8 through 3.11.1 binds an unauthenticated JMX/RMI interface to all network interfaces, which allows remote attackers to execute arbitrary Java code via an RMI request. This issue is a regression of CVE-2015-0225. The regression was introduced in https://issues.apache.org/jira/browse/CASSANDRA-12109. The fix for the regression is implemented in https://issues.apache.org/jira/browse/CASSANDRA-14173. This fix is contained in the 3.11.2 release of Apache Cassandra.
CVE-2018-7295	ffxivlauncher.exe in Square Enix Final Fantasy XIV 4.21 and 4.25 on Windows is affected by Improper Enforcement of Message Integrity During Transmission in a Communication Channel, allowing a man-in-the-middle attacker to steal user credentials because a session retrieves global.js via http before proceeding to use https. This is fixed in Patch 4.3.
CVE-2018-6849	In the WebRTC component in DuckDuckGo 4.2.0, after visiting a web site that attempts to gather complete client information (such as https://ip.voidsec.com), the browser can disclose a private IP address in a STUN request.
CVE-2018-6608	In the WebRTC component in Opera 51.0.2830.55, after visiting a web site that attempts to gather complete client information (such as https://ip.voidsec.com), the browser can disclose a private IP address in a STUN request.
CVE-2018-6018	Fixed sizes of HTTPS responses in Tinder iOS app and Tinder Android app allow an attacker to extract private sensitive information by sniffing network traffic.
CVE-2018-5721	Stack-based buffer overflow in the ej_update_variables function in router/httpd/web.c on ASUS routers (when using software from https://github.com/RMerl/asuswrt-merlin) allows web authenticated attackers to execute code via a request that updates a setting. In ej_update_variables, the length of the variable action_script is not checked, as long as it includes a "_wan_if" substring.
CVE-2018-5542	F5 BIG-IP 13.0.0-13.0.1, 12.1.0-12.1.3.6, or 11.2.1-11.6.3.2 HTTPS health monitors do not validate the identity of the monitored server.

Sumber : https://cve.mitre.org/

➢ Server Software and Technology Found

Software / Version	Category
Microsoft ASP.NET	Web Frameworks
SDL Tridion	CMS
Akamai	CDN
Google Tag Manager	Tag Managers
Modernizr	JavaScript Frameworks
Twitter typeahead.js	JavaScript Frameworks
jQuery 1.6.4	JavaScript Frameworks

Sumber : https://pentest-tools.com/

RIDHO ILHAM RENALDO
09011181520021 (SK8PIL)
KEAMANAN JARINGAN KOMPUTER

- **Visual Trace Rout**