Reconnaissance

Pemerintahan : http://www.imigrasi.go.id/

Web server : nginx 1.9.3
Apache 2.2.25

Operating Systems : UNIX
Limiter Modules
OpenSSL
CentOS
Red Hat Enterprise Linux

Framework : PHP

IP	222.124.200.172	**Hostname**	imigrasi.go.id	**ASN**	17974
Country	Indonesia (ID)	**Provider**	PT Telekomunikasi Indonesia	**Continent Code**	AS
City	Jakarta	**Latitude**	-6.1744	**Continent Name**	Asia
Region	Jakarta (JK)	**Longitude**	106.8294	**TimeZone**	Asia/Jakarta
Postal Code		**Metro Code**		**DateTime**	2019-02-11 17:04:01

Luar negri : https://www.aon.com/

Web server : Apache Tomcat Coyote
Apache 2.2.25

Operating Systems : UNIX
mod_ssl 2.2.17
OpenSSL 0.9.8

Framework : J2EE
Adobe Dreamweaver

IP	168.87.112.148	**Hostname**	168.87.112.148	**ASN**	19647
Country	United States (US)	**Provider**	Hewlett-Packard Company	**Continent Code**	NA
City		**Latitude**	37.751	**Continent Name**	North America
Region		**Longitude**	-97.822	**TimeZone**	
Postal Code		**Metro Code**		**DateTime**	

Name: Wayne Rideout
Tel: +62 21 2985 8550
Email: wayne.rideout@aon.com

Dalam negri : https://www.grand-indonesia.com/

Web server : Apache 2.225

Operating System : Linux
Unix mod_ssl 2.2.25
OpenSSL 1.0.0-fips

Framework : PHP

IP	103.200.7.91	**Hostname**	103.200.7.91	**ASN**	134451
Country	Indonesia (ID)	**Provider**	NewMedia Express Pte Ltd	**Continent Code**	AS
City	Jakarta	**Latitude**	-6.1744	**Continent Name**	Asia
Region	Jakarta (JK)	**Longitude**	106.8294	**TimeZone**	Asia/Jakarta
Postal Code		**Metro Code**		**DateTime**	2019-02-11 17:02:17

Dear valued customers,

Your feedback is important and a valuable insight for us so we can serve you better. Please write your suggestion to customerservice@grand-indonesia.com or you may call us at 021 2358 0001

CVE

Apache » Http Server » 2.2.25 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.2.25*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-7679	119		Overflow	2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	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	20			2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	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	CVE-2017-3169	476			2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	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	CVE-2017-3167	287		Bypass	2017-06-19	2018-06-02	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	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	20			2018-03-09	2018-06-02	3.3	None	Local Network	Low	Not required	None	None	Partial
	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	93		Http R.Spl.	2018-08-14	2018-10-19	4.3	None	Remote	Medium	Not required	None	Partial	None
	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).													
7	CVE-2014-0231	399		DoS	2014-07-20	2018-10-30	5.0	None	Remote	Low	Not required	None	None	Partial
	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.													
8	CVE-2014-0098	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.													
9	CVE-2013-6438	20		DoS	2014-03-18	2018-10-09	5.0	None	Remote	Low	Not required	None	None	Partial
	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.													
10	CVE-2013-2249				2013-07-23	2017-01-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

Apache » Coyote Http Connector » 1.1 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:coyote_http_connector:1.1*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2005-2090			XSS Bypass	2005-07-05	2018-10-19	4.3	None	Remote	Medium	Not required	None	Partial	None
	Jakarta Tomcat 5.0.19 (Coyote/1.1) and Tomcat 4.1.24 (Coyote/1.0) allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes Tomcat to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."													

Total number of vulnerabilities : **1** Page : 1 (This Page)

Nginx » Nginx » 1.9.3 : Security Vulnerabilities

Cpe Name:*cpe:/a:nginx:nginx:1.9.3*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-16844	400			2018-11-07	2018-12-12	7.8	None	Remote	Low	Not required	None	None	Complete
	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.													
2	CVE-2017-7529	190		Overflow +Info	2017-07-13	2018-01-04	5.0	None	Remote	Low	Not required	Partial	None	None
	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.													
3	CVE-2016-0747	399		DoS	2016-02-15	2018-10-30	5.0	None	Remote	Low	Not required	None	None	Partial
	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.													
4	CVE-2016-0746			DoS	2016-02-15	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	Use-after-free vulnerability in the resolver in nginx 0.6.18 through 1.8.0 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.													
5	CVE-2016-0742			DoS	2016-02-15	2018-10-30	5.0	None	Remote	Low	Not required	None	None	Partial
	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.													

Total number of vulnerabilities : **5** Page : 1 (This Page)