Nama : AHMAD RIDWAN

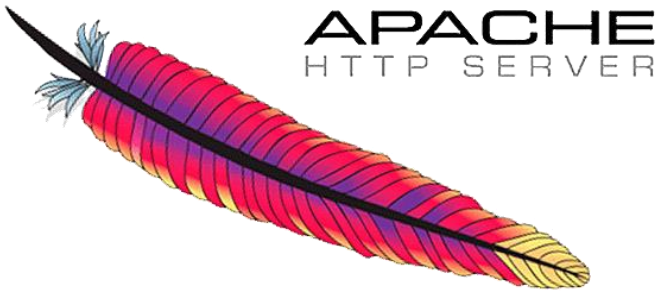
NIM : 09011281419042

COMMON VULNERABILITIES AND EXPOSURES (CVE)

APACHE HTTP SERVER 2.2.15

Server HTTP Apache atau Server Web/WWW Apache adalah server web yang dapat dijalankan di banyak sistem operasi (Unix, BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Apache web server yang bertanggung jawab pada request-response HTTP dan logging informasi secara detail (kegunaan basicnya). Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigur, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah.



Gambar 1. Apache HTTP Server

Penulis mengambil contoh website Pemerintah Provinsi Sumatera Selatan yaitu http://www.sumselprov.go.id/ . Kemudian penulis mencari informasi terkait sistem operasi dan web server yang digunakan melalui website netcraft dan didapatkan informasi sebagai berikut:

Netblock owner	IP address	OS	Web server	Last seen Refresh
Dinas Perhubungan Kominfo Provinsi Sumatera Selatan Government / Direct member IDNIC Jl. Kapten A. Rivai No. 51 Palembang - Sumatera Selatan	103.239.165.80	Linux	Apache/2.2.15 CentOS	14-Oct-2016

Dapat dilihat bahwa update terakhir menggunakan OS Linux dan Web server Apache 2.2.15 CentOS dengan alamat IP 103.239.165.80.

Dengan memanfaatkan website CVE, kemudian dicari menggunakan kata kunci Apache 2.2.15 maka akan didapatkan beberapa hasil sebagai berikut :

#	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	2018-01-18	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	2018-01-04	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	2018-01-18	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	2018-01-04	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-2014-0231	399		DoS	2014-07-20	2017-12-08	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.														
6	CVE-2014-0098	20		DoS	2014-03-18	2017-12-08	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.														
7	CVE-2013-6438	20		DoS	2014-03-18	2017-12-08	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.														
8	CVE-2013-2249				2013-07-23	2017-01-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.														
9	CVE-2013-1896	264		DoS	2013-07-10	2017-09-18	4.3	None	Remote	Medium	Not required	None	None	Partial
mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.														

Gambar 2. CVE Apache 2.2.15

CVE merupakan sebuah Sistem Common Vulnerabilities and Exposures (CVE) yang menyediakan metode referensi untuk kerentanan keamanan dan eksposur informasi yang diketahui atau dapat dikatakan CVE adalah sebuah katalog ancaman keamanan yang telah dikenali dan telah dilaporkan oleh seseorang, baik yang telah diperbaiki ataupun masih dalam proses perbaikan hole/celah tersebut.

Kemudian penulis mengambil salah satu data CVE dengan identitas **CVE-2012-0053.**

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	264

Gambar 3. CVE-2012-0053

Dijelaskan hole/celah yaitu protocol.c di Apache HTTP Server 2.2.x sampai 2.2.21 tidak membatasi informasi header selama pembuatan dokumen kesalahan Bad Request (alias 400), yang memungkinkan penyerang jarak jauh mendapatkan nilai cookie HTTPOnly melalui vektor yang melibatkan (1) header panjang atau (2) rusak bersama dengan skrip web yang dibuat.

Atribut Secure dan HttpOnly tidak memiliki nilai terkait. Sebaliknya, kehadiran hanya nama atribut mereka menunjukkan bahwa perilaku mereka harus diaktifkan.

Atribut Secure dimaksudkan untuk menjaga komunikasi cookie terbatas pada transmisi terenkripsi, mengarahkan browser untuk menggunakan cookies hanya melalui koneksi yang aman / terenkripsi. Namun, jika server web menyetel kuki dengan atribut aman dari sambungan tidak aman, kuki masih dapat disadap saat dikirim ke pengguna oleh serangan man-in-the-middle. Oleh karena itu, untuk keamanan maksimum, cookies dengan atribut Secure hanya boleh diatur melalui koneksi yang aman.

Atribut HttpOnly mengarahkan browser untuk tidak mengekspos cookie melalui saluran selain permintaan HTTP (dan HTTPS). Ini berarti cookie tidak dapat diakses melalui bahasa script sisi klien (terutama JavaScript), dan oleh karena itu tidak dapat dicuri dengan mudah melalui skrip cross-site (teknik serangan yang menyebar luas).