Tugas

Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Sigit Wijaya Pramono

NIM : 09011181419012

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

CVE (*Common Vulnerabilities and Exposures*) Apache

Server HTTP 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. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Apache sendiri bersifat open source, yang artinya dapat digunakan secara bebas oleh semua pengguna. Apache di kenal memiliki fitur-fitur canggih seperti penanganan pesan kesalahan yang dapat di konfigurasi serta otentikasi berbasis basis data, dan memiliki tampilan GUI yang memungkinkan penanganan server menjadi mudah. Web serbver Apache akan bekerja saat pengguna mengetikkan request melalui protocol http:// untuk membuka suatu halaman. Apache akan menjawab request yang di ketikkan user dan kemudian menampilkan halaman yang di minta.

Pada tugas ini saya menggunakan contoh website http://www.pusri.co.id untuk mencari informasi seputar sistem operasi dan web server yang digunakan oleh pusri dan melihat update terbaru yang dilakukan pada website tersebut dengan menggunakan bantuan dari website netcraft, dan memperoleh hasil seperti capture di bawah :

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.4.120	Linux	Apache/2.2.16 Debian	19-Feb-2018
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	-	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	25-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	unknown	24-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	22-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.1 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	3-Oct-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.0 Unix DAV/2 mod_ssl/2.2.0 OpenSSL/0.9.8a PHP/5.1.2 mod_apreq2-20050712/2.1.3-dev mod_perl/2.0.2 Perl/v5.8.7	12-Mar-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache	4-Jun-2006
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache/2.0.54	17-Sep-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	-	Apache/2.0.52 Unix mod_perl/1.99_17 Perl/v5.8.4 mod_ssl/2.0.52 OpenSSL/0.9.7d PHP/4.3.10	4-Mar-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	Linux	Apache/1.3.28 Unix PHP/4.3.2 mod_gzip/1.3.19.1a mod_fastcgi/2.2.12 mod_perl/1.27	9-May-2004

Dari capture diatas kita bisa melihat web server yang terakhir digunakan yaitu Apache/2.2.16 Debian pada sistem operasi Linux.

Pada tahap tugas selanjutnya yaitu mencari *data hole* Apahe dengan menggunakan CVE, dari banyak nya hasil search *data hole* Apache pada CVE saya mengambil salah satu diantaranya yaitu CVE-2017-12636 :

Dalam deskripsi data hole CVE-2017-12636 menjelaskan bahwa Pengguna administratif CouchDB dapat mengkonfigurasi server database via HTTP (S). Beberapa opsi konfigurasi mencakup jalur untuk binari tingkat sistem operasi yang kemudian diluncurkan oleh CouchDB. Hal ini memungkinkan pengguna admin di Apache CouchDB sebelum 1.7.0 dan 2.x sebelum 2.1.1 untuk mengeksekusi perintah shell sewenang-wenang sebagai pengguna CouchDB, termasuk mendownload dan menjalankan skrip dari internet publik. Beberapa kerentanan telah ditemukan di CouchDB. Seorang *remote attacker* bisa mengeksekusi perintah shell yang sewenang-wenang atau hak istimewa yang meningkat. Kerentanan juga terdapat pada *Authentication*, dengan *Single System* kerentanan mengharuskan penyerang untuk masuk ke sistem (seperti pada baris perintah atau melalui sesi desktop atau antarmuka web).

Setelah mendapatkan *data hole* selanjutnya yaitu menentukan *how to attack* dengan memanfaatkan *hole* yang teah diketahui. Dalam penjelasan dari CVE-2017-12636 salah satu *attack* yang dapat diakukan yaitu dengan melalui _user. Dalam kasus database _user *allowing duplicate keys* memungkinkan attacker untuk mengirimkan dokumen _users dengan dua tombol ‘role’. Yang pertama bisa termasuk apapun peran yang ditugaskan sendiri, karena fungsi validasi JavaScript hanya akan pernah terlihat. Kunci kedua ketika mengautentikasi pengguna pada permintaan berikutnya, kunci ‘role’ dibaca dari representasi Erlang-JSON dan dalam implementasi itu, tombol ‘role’ pertama dikembalikan. Yang sekarang bisa mencakup peran apa pun, termasuk peran _admin khusus, memberi hak istimewa kepada pengguna admin.