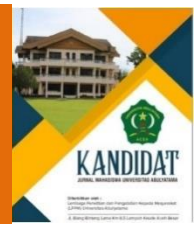
Available online at : http://jurnal.abulyatama.ac.id/index.php/kandidat
ISSN 2715-3126 (Online)
Universitas Abulyatama
Kandidat : Jurnal riset dan inovasi Pendidikan



Analisa Keamanan Web Server dari Serangan *Remote Os Command Injection* pada Instansi Pemerintahan Kota Banda Aceh

Lisa Handasari Yanti[*1], Iqbal[2], Banta Cut[2]

[1]Mahasiswa Program Studi Sistem Informasi, Fakultas Teknik, Universitas Abulyatama, Aceh Besar, 23372, Indonesia.
[2]Dosen Program Studi Sistem Informasi, Fakultas Teknik, Universitas Abulyatama, Aceh Besar, 23372, Indonesia.
*Email korespondensi: lisahandasariyanti@gmail.com[1]

Diterima 27 Desember 2019; Disetujui 3 Desember 2019; Dipublikasi 27 Desember 2019

Abstract: *The development of information technology in the world is rapidly increasing, causing changes in human behavior in finding information. Website is a way to present themselves and information media on the internet. The website of the Banda Aceh City government agency is a website that can be accessed by everyone. So that web server security must really be considered. This research was conducted to test the security of Banda Aceh City Government Agency web server using Remote OS Command Injection technique. Remote OS Command Injection is a form of attack where the attacker's goal is to execute arbitrary commands on the web server through a vulnerable website. This study applies a purposive sampling method using Ow asp Zap version 2.7.0. Based on the analysis carried out the intensity of the attacks on each Banda Aceh City Government Agency differed, the Banda Aceh Social Service was 0.92%, the Aceh Transportation Agency 0.15%, the Aceh Youth and Sports Service 0.71%, the Aceh Food Service 0.11% and the Aceh Library and Archives Service 0.24%.*

Keywords: Remote OS Command Injection 1, Web Server 2, Web Security 3, Data Base 4.

Abstrak:,Perkembangan teknologi informasi didunia semakin pesat sehingga menyebabkan perubahan perilaku manusia dalam mencari informasi. Website adalah cara untuk menampilkan diri dan media informasi di internet. Website instansi Pemerintahan Kota Banda Aceh merupakan website yang bisa diakses oleh semua orang. Sehingga keamanan web server harus benar-benar diperhatikan. Penelitian ini dilakukan untuk menguji kemanan web server Instansi Pemerintahan Kota Banda Aceh dengan menggunakan teknik Remote OS Command Injection. Remote OS Command Injection adalah sebuah bentuk serangan dimana tujuan penyerang adalah untuk mengeksekusi perintah sewenang-wenang di web server melalui website yang rentan. Penelitian ini menerapkan metode purposive sampling dengan menggunakan tools Owasp Zap versi 2.7.0. Berdasarkan analisa yang dilakukan intensitas serangan pada setiap Instansi Pemerintahan Kota Banda Aceh berbeda-beda, pada Dinas Sosial Banda Aceh sebesar 0,92%, Dinas Perhubungan Aceh 0,15%, dinas Pemuda dan Olahraga Aceh 0,71%, Dinas Pangan Aceh 0,11% dan Dinas Perpustakaan dan Kearsipan Aceh 0,24%.

Kata Kunci: Remote OS Command Injection 1, Web Server 2, Keamanan Web 3, Data Base 4

Perkembangan teknologi informasi didunia saat ini semakin pesat sehingga menyebabkan perubahan perilaku manusia dalam mencari informasi, seiring dengan perkembangan teknologi informasi perkembangan sistem informasi juga ikut berkembang pesat untuk dapat memudahkan proses

pengaksesan dan pencarian informasi dari media website.

Website merupakan cara untuk menunjukkan diri ke internet dan sarana untuk memberi informasi kepada pengguna intenet. Beberapa website yang sering diakses oleh masyarakat diantaranya search engine, e-commerce, social networking, forum, portal berita dan lain – lain. Dengan adanya website maka masyarakat pun akan semakin mudah untuk mengakses berita ataupun kebutuhan yang lainnya. Akan tetapi dibalik kemudahan layanan yang disediakan oleh setiap website tersebut, ternyata terdapat beberapa masalah pada celah keamanan.

Hampir semua instansi Pemerintahan Kota Banda Aceh memiliki Web Server sendiri yang digunakan sebagai media untuk sarana publikasi informasi. Mengingat website ini dapat diakses secara luas oleh pengguna internet, maka diperlukan perhatian khusus mengenai keamanan web server. Terdapat banyak cara yang bisa digunakan untuk melakukan pengujian terhadap keamanan sebuah web server. Salah satunya adalah dengan cara menggunakan Remote OS Command Injection.

Analisa ini melakukan scanning port dengan aplikasi Owasp Zap, menggunakan teknik penyerangan Remote OS Command Injection. Penulis memilih teknik serangan Remote OS Command Injection karena serangan jenis ini berdampak langsung ke server seperti mematikan server, melihat isi direktori web, menghapus direktori web server, dll. Ditambah lagi dengan banyaknya sistem operasi dan aplikasi web server yang bisa digunakan sehingga makin sulit untuk menjaga keamanan server. Contohnya saja untuk pengkodingan website yang sama, namun tetap memiliki kerentanan yang berbeda jika di upload ke server yang berbeda type, seperti OS Linux dan windows yang menggunakan web server Apache type yang berbeda. Sehingga sampai saat ini belum ada web server yang bisa dijamin keamananya.

Berdasarkan uraian diatas penulis tertarik untuk menganalisa keamanan web server pemerintahan Kota Banda Aceh yang akan penulis tuangkan ke dalam skripsi yang berjudul "Analisa Keamanan Web Server dari Serangan Remote OS Command Injection Pada Instansi Pemerintahan Kota Banda Aceh ". Penulis berharap dapat menyelesaikan proses analisa ini dengan baik dan bisa memberikan manfaat dalam melakukan pengamanan.

KAJIAN PUSTAKA

WEB SERVER

Web Server atau server web merupakan perangkat lunak (software) yang berfungsi untuk menerima permintaan (request) berupa halaman web melalui protokol HTTP atau HTTPS dari client atau yang lebih dikenal dengan nama browser, kemudian mengirimkan kembali atau merespon hasil permintaan tersebut ke dalam bentuk halaman-halaman web yang pada umumnya berupa dokumen HTML atau php. Dapat di simpulkan web server merupakan pemberi layanan bagi browser supaya browser bisa menampilkan data atau halaman yang di request pengguna layana internet.[1]

Fungsi utama web server adalah untuk menstransferkan atau mimindahkan data yang diminta oleh pengguna internet melalui protokol komunikasi tertentu. Di dalam sebuah website biasanya terdiri dari berbagai macam jenis berkas seperti gambar, teks, video, audio dan lain sebagainya, maka pemanfaatan web server di sini

adalah untuk mentransferkan seluruh aspek data pemberkas dalam halaman tersebut. [2]

WEBSITE

Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan gabungan dari semuanya baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait, yang masing-masing dihubungkan dengan jaringan-jaringan halaman. Halaman website biasanya berupa dokumen yang ditulis dalam format Hyper Text Markup Language (HTML), yang bisa diakses melalui HTTP, HTTPS adalah suatu protokol yang menyampaikan berbagai informasi dari server website untuk ditampilkan kepada para user atau pemakai melalui web browser.[3]

REMOTE OS COMMAND INJECTION

Remote Os Command Injection adalah sebuah bentuk serangan dimana tujuan penyerang adalah untuk mengeksekusi perintah sewenang-wenang di web server melalui aplikasi web yang rentan. Serangan ini bisa terjadi ketika aplikasi berbasis web menyediakan kolom input yang rentan dan tidak aman kepada pengguna untuk memasukkan data. Serangan Remote OS Command Injection terjadi dikarenakan lemahnya atau tidak memadai validasi dari input dan adanya data yang tidak dipercaya dikirim ke bagian perintah atau query. Data yang dikirim dapat mengelabui intepreter untuk mengeksekusi atau mengakses data tanpa otoritas yang tepat.[4]

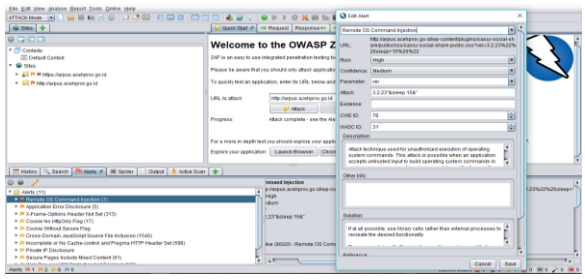
METODE PENELITIAN

Dalam penelitian ini membutuhkan dua aspek yang sangat penting yaitu software (Tools Owasp versi2.7.0, Java 8 update 131 dan OS windows 10 pro 64-bit) dan hardware (Laptop, prosessor intel dan RAM 2 GB).

Metode yang digunakan dalam penelitian ini yaitu metode *Purposive Sampling*, dimana metode ini adalah salah satu teknik sampling non random, dimana peneliti menentukan pengambilan sampel dengan cara menetapkan ciri-ciri khusus yang sesuai dengan tujuan penelitian sehingga diharapkan dapat menjawab permasalahan penelitian.

HASIL DAN PEMBAHASAN

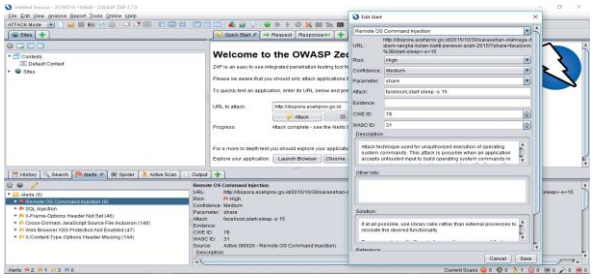
HASIL



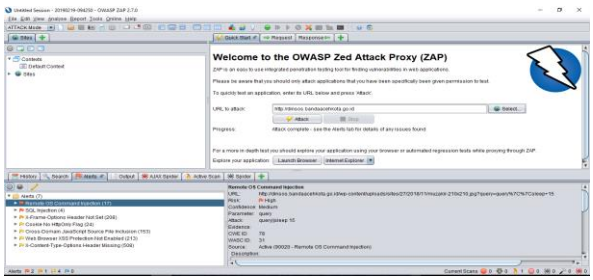
Gambar 1 : Hasil Scanner Website Dinas Perpustakaan dan Kearsipan Aceh

Gambar 2 : Hasil Scanner Website Dinas Pangan Aceh

Gambar 3 : Hasil Scanner Website Dinas Perhubungan Aceh



Gambar 4 : Hasil Scanner Website Dinas Pemuda dan Olahraga Aceh



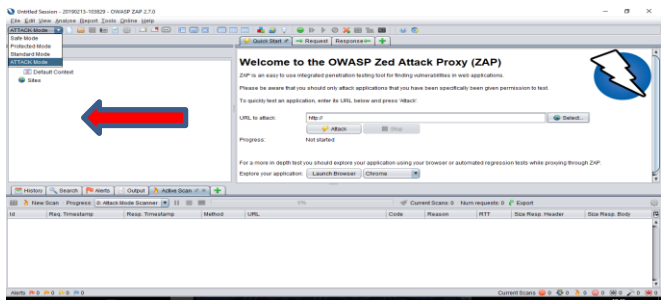
Gambar 5 : Hasil Scanner Website Dinas Sosial Aceh

Tabel 1. Jumlah Serangan pada Setiap Website

No.	Nama Website	Url Bermasalah	Jumlah Seluruh Url
1	http://dinsos.acehprov.go.id	17	758
2	http://arpus.acehprov.go.id	7	2.904
3	http://dinaspangan.acehprov.go.id	8	7.311
4	http://dishub.acehprov.go.id	13	8.538
5	http://dispora.acehprov.go.id	9	1.267
	Jumlah	54	20.778

PEMBAHASAN 1

Pengujian dilakukan menggunakan Tool Owasp Zap versi 2.7.0 dengan domain http://dinsos.bandaacehkota.go.id, berikut adalah tahapan melakukuan pengujian keamanan website pada Dinas Sosial Banda Aceh :



Gambar 6: Tampilan awal aplikasi Owasp

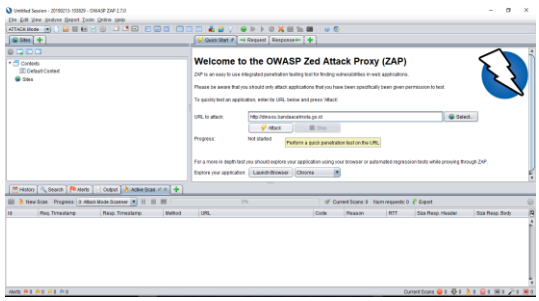
Pada gambar diatas dapat dilihat bagaimana tampilan awal dari tools owasp, untuk memulai melakukan uji coba penulis memilih mode Attack Mode yang tujuannya adalah untuk mengetahui semua kelemahan yang ada didalam website yang akan di uji coba. Setelah memilih Attack Mode maka akan muncul kotak Active Scan, setelah kotak active Scan muncul berarti ini menandakan bahwa sofware Owasp sudah siap untuk melakukan uji coba kerentanan sebuah website. Adapun beberapa mode yang sudah disediakan oleh sofware owasp ini yaitu sebagai berikut :

1. Safe Mode berfungsi untuk memperbaiki kerusakan website.
2. Protected Mode berfungsi untuk membantu mencegah perangkat lunak berbahaya dari

mengeksploitasi kelemahan terhadap website.

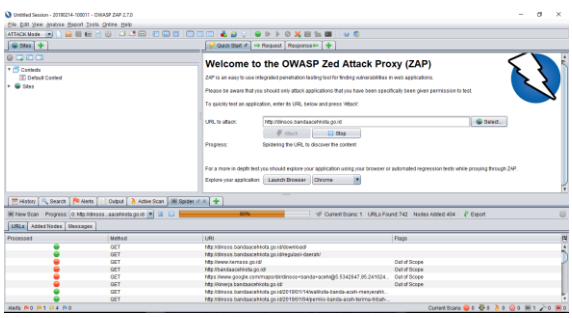
3. Standar Mode berfungsi untuk menguji keselamatan sebuah website terhadap serangan dari luar secara tidak mendalam.
4. Attack Mode berfungsi untuk menganalisis sebuah website secara mendalam dengan cara melakukan serangan terus-menerus sehingga dapat diketahui titik lemah yang dapta dimanfaatkan oleh penyerang

Setelah salah satu dari mode diatas dipilih, maka Active scan disini akan berfungsi untuk memantau pergerakan dari sebuah website. Dalam menganalisis sebuah website



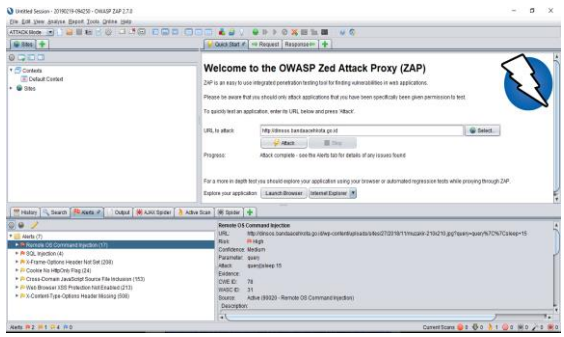
Gambar 7: Tampilan untuk pengisian alamat website

Setelah memilih Attack Mode pada proses sebelumnya, maka selanjutnya penulis mengisi alamat website yang akan dilakukan analisis keamanannya. Setelah memasukkan nama domain dikotak URL to attack kemudian klik tombol Attack untuk menjalankan proses analisis.



Gambar 8: Tampilan informasi analisis yang berjalan

Di dalam kotak spider akan membaca data yang keseluruhan analisis yang sedang berjalan, pada point merah yang method GET adalah informasi hasil untuk mengetahui bahwa server log memiliki informasi sensitif yang dapat disalahgunakan oleh penyerang.



Gambar 9: Hasil dari analisis yang dilakukan

Setelah selesai melakukan scanner website Dinas Sosial Banda Aceh dengan menggunakan Tools Owasp zap versi 2.7.0 dengan memakan waktu kurang lebih 7 jam dengan kecepatan internet atau bandwith 2-3 Mbps. Dalam proses ini sangat berpengaruh terhadap kecepatan internet, karena lama atau cepatnya proses scanner tergantung pada kecepan internet. Hasil dari proses scanner ini dapat dilihat pada kotak Alerts yaitu memliki 17 kelemahan, yang tiap-tiap kelemahan mempunyai warna dan informasi yang berbeda yaitu sbb :

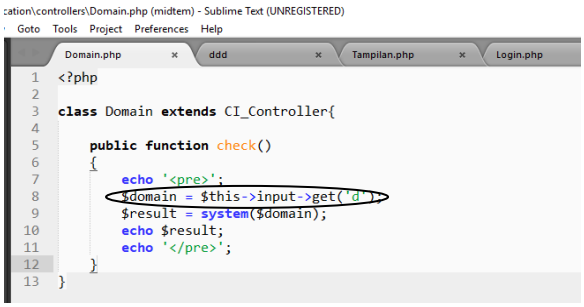
1. Warna merah atau disebut dengan High Priority alert yang berarti tingkat kerentanan sangat fatal terhadap serangan dari luar.
2. Warna orange atau disebut dengan Medium Priority alert yang berarti tingkat kerentanan tidak terlalu beresiko akan tetapi juga tidak terlalu aman dari serangan.
3. Warna kuning atau disebut juga Low Priority alert yang berarti tingkat kerentanan sulit untuk di serang atau sudah diminimalkan.

4. Warna biru atau disebut dengan Information Priority alert yaitu untuk menampilkan informasi tentang keamanan website tersebut.

Menurut hasil scanner yang ditemukan oleh Owasp zap 2.7.0 terdapat 2 kondisi yang sangat fatal yang dikategorikan High Priority alert yaitu Remote Os Command Injection dan SQL Injection yang kedua kondisi ini sangat rentan terhadap serangan dari luar. Maka dari tu kondisi yang akan diangkat penulis adalah Remote Os Command Injection

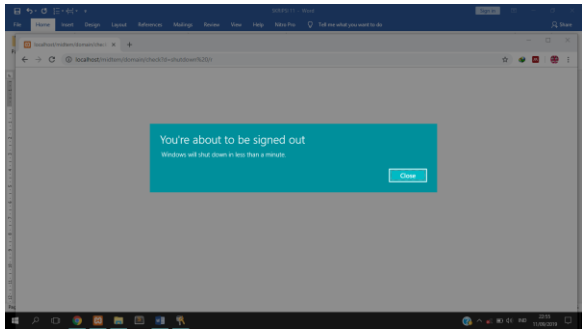
PEMBAHASAN 2

Penulis mengimplementasikan serangan Remote OS Injection pada website yang dibangun oleh penulis sendiri, dikarenakan penulis tidak bisa mendapatkan coding website dari Instansi Pemerintahan Kota Banda Aceh karena tidak diperbolehkan duplikat website untuk komsumsi publik.



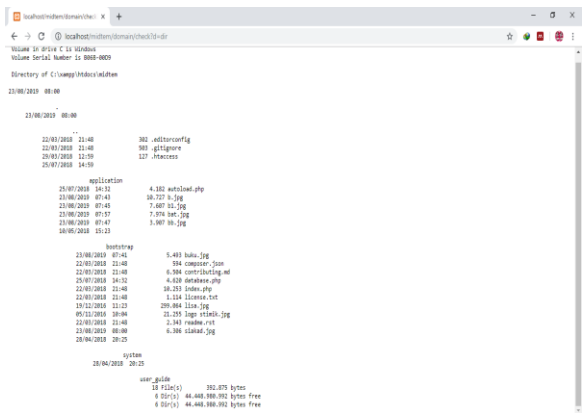
Pada sintaks "$domain = $this->input->get('d');" diatas menunjukkan bahwa kita bisa menjalankan perintah-perintah command prompt melalui sebuah website, dan dampaknya yaitu kita bisa mematikan atau melakukan hal-hal lain sesuai perintah yang kita berikan setelah variabel "d".

Adapun perintah untuk mematikan server http://localhost/midtem/domain/check?d=shutdown /r, setelah melakukan perintah shutdown /r maka proses yang terjadi adalah menshutdownkan komputer.



Gambar 6: Layout Hasil Perintah Pengshutdownan Komputer

Untuk mengetahui semua folder yang ada didalam website, bisa menjalankan perintah "http://localhost/midtem/domain/check?d=dir", setelah melakukan perintah dir maka proses yang terjadi adalah seperti gambar dibawah.



Gambar 7: Layout Hasil Perintah Dir

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian dapat disimpulkan bahwa :

1. Dari analisis yang telah dilakukan menggunakan metode purposive sampling, hasil persentase kerentanan website pada webserver Dinas Sosial Banda Aceh sebesar

0,92%, Dinas perhubungan 0,15%, Dinas Pemuda dan Olahraga 0,71%, Dinas Pangan 0,11%, dan Dinas Perpustakaan dan Kearsipan aceh 0,24%.

2. Dari hasil analisis yang telah dilakukan didapatkan hasil persentase tingkat kerentangan Remote OS Command Injection yang paling tinngi adalah web server Dinas Sosial Banda Aceh.
3. Dari analisis yang dilakukan maka dapat disimpulkan bahwa web server Pemerintahan Kota Banda aceh masih belum aman dari serangan Remote OS Command Injection.

Saran

Adapun saran yang dapat disampaikan setelah melakukan penelitian ini yaitu :

1. Diharapkan supaya analisa yang telah dilakukan dapat dimanfaatkan dan digunakan sebagai pedoman untuk meningkatkan keamanan pada Web Server.
2. Dalam menjaga keamanan web server perlu memperhatikan perawatan atau melakukan service web server secara teratur.
3. Memilih web server yang tingkat keamanan dan versi web server nya bagus dan baik.
4. Mewaspadai aktifitas yang berusaha masuk ke sistem jaringan melalui notifikasi alert IDS Snort, meskipun aktifitas tersebut hanya untuk melihat-lihat website yang aktif.
5. Developer hendaknya melakukan validasi terhadap Url dan memfilter bentuk request yang mengarah terhadap tinjakan Remote OS.
6. Lakukan audit sendiri dengan berbagai macam tools yang ada.
7. Kelemahan website terdapat pada pencodingan sintaks pemrogramannya, oleh sebab itu perbaiki dan sempurnakan sintaks pemrogramannya.

DAFTAR PUSTAKA

[I] Journal and S. Engineering, "Volume 1 No 1 – 2015 Lppm3.bsi.ac.id/jurnal IJSE – Indonesian Journal on Software Engineering," vol. 1, no. 1, pp. 1–10, 2015.

[2] P. S. Ke-, "UMK (Universitas Muria Kudus) dengan domain umk.ac.id merupakan," pp. 251–258, 2015.

[3] J. T. Elektro and P. N. Medan, "Perancangan Website pada PT . Ratu Enim Palembang," pp. 15–27

[4] V. Chapela, "Remote Os Command Injection," 2005.