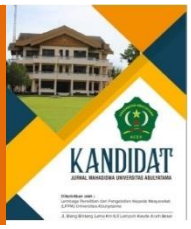
Available online at : http://jurnal.abulyatama.ac.id/index.php/kandidat
ISSN 2715-3126 (Online)
Universitas Abulyatama
Kandidat : Jurnal Riset dan Inovasi Pendidikan



Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga

Neng Ita Sopia Fazriani*[1], Banta Cut[2], Sanusi[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: sopiafazriani@gmail.com

Diterima 27 Agustus 2019 ; Disetujui 4 Oktober 2019; Dipublikasi 18 Oktober 2019

Abstract: *Website security is very important because website is targeted hacker to exploit actions that can harm the website itself. One of them is a Path Traversal attack that allows an attacker to access file, directory and commands that are potentially outside the root directory of web document. To find out how a website was broken or in other words hack with Path Traversal technique, then make an analysis of the Path Traversal attack. The purpose of this research is to study Path Traversal attack, find out how to anallyze website security and find solutions to overcome wibsite security problem against Path Traversal attack. In this research conducted using the OWASP ZAP scaning application program to clearly see the vulnerability on a website. Based on the analysis of Path Traversal attack on the citizens collection website, it can be seen that when access to the directory is not protected it will be a gap for the attacker can access or retrieve important files in the app. To minimize Path Traversal attack add an .htaccess file or index.php of all folder.*

Keywords: Website security, Path traversal, Hacker

Abstrak: Keamanan website sangat penting dilakukan mengingat website menjadi sasaran peretas untuk melakukan tindakan pengeksploitasian yang dapat merugikan website itu sendiri. Salah satunya adalah serangan Path Traversal yang memungkinkan penyerang mengakses file, direktori dan perintah yang berpotensi diluar direktori root dokumen web. Untuk mengetahui bagaimana sebuah website di jebol atau dengan kata lain di hack dengan teknik Path Traversal, maka dibuatlah sebuah analisa serangan path traversal. Tujuan dari penelitian ini untuk mempelajari serangan Path Traversal, mengetahui cara menganalisis keamanan website dan mengetahui solusi untuk mengatasi masalah keamanan website terhadap serangan Path Traversal. Dalam penelitian kali ini dilakukan dengan menggunakan program Aplikasi Scaning OWASP ZAP untuk melihat secara jelas kerentanan pada sebuah website. Berdasarkan hasil analisa pengujian serangan Path Traversal pada website pendataan warga dapat diketahui bahwa ketika akses ke direktori tidak diproteksi maka akan menjadi celah untuk attacker bisa mengakses atau mengambil file-file penting yang ada pada aplikasi tersebut. Untuk meminimalisir serangan Path Traversal tambahkan file .htaccess atau file index.php pada setiap folder.

Kata kunci : Keamanan Website, *Path traversal, hacker*

Saat ini dunia maya sudah berkembang pesat disegala bidang khususnya di bidang website. Website adalah halaman informasi yang disediakan melalui jalur internet sehingga bisa diakses di seluruh dunia selama terkoneksi dengan jaringan internet. Mengingat website ini dapat diakses secara luas, maka perlu memperhatikan keamanan website. Apalagi ada beberapa website yang rawan akan kejahatan internet khususnya dalam penyerangan *path traversal*. Saat ini untuk mengamankan website sangat penting karena semakin banyak terbukanya pengetahuan *hacking* dan *cracking*, didukung dengan banyaknya *tools* yang tersedia dengan mudah dan kebanyakan *free*, semakin mempermudah untuk melakukan aksi penyusupan ataupun serangan. Terjadinya penyusupan atau serangan dapat mengakibatkan masalah pada keberlangsungan sistem yang diserang oleh *attacker* (Kurniawan dkk, 2016). Salah satunya serangan *path traversal*.

Serangan *path traversal* merupakan sebuah serangan yang memungkinkan penyerang mengakses file, direktori dan perintah yang berpotensi berada diluar direktori root dokumen web. Penyerang dapat memanipulasi URL sedemikian rupa sehingga situs web akan mengeksekusi atau mengungkapkan isi file sewenang-wenangnya (Auger, 2010).

KAJIAN PUSTAKA

Website

Website merupakan sebuah kumpulan halaman-halaman web beserta file-file pendukungnya seperti file gambar, video dan file digital lainnya yang dapat disimpan pada sebuah web server yang umumnya dapat diakses melalui internet. Atau dengan kata lain, website adalah sekumpulan folder dan file yang mengandung banyak perintah dan fungsi-fungsi tertentu seperti fungsi tampilan, fungsi menangani penyimpanan data (Hartono, 2014).

Internet

internet adalah sebuah perpustakaan besar yang didalamnya terdapat jutaan (bahkan milyaran) informasi atau data yang dapat berupa teks, grafik, audio maupun animasi dan lain lain dalam bentuk media elektronik (Zabar dan Novianto, 2015).

Keamanan Jaringan

Keamanan jaringan internet adalah manajemen pengelolaan keamanan yang bertujuan mencegah, mengatasi dan melindungi berbagai sistem informasi dari resiko terjadinya tindakan ilegal, seperti penggunaan tanpa izin, penyusupan dan perusakan terhadap berbagai informasi yang dimiliki (Academia, 2019).

Keamanan Website

Keamanan website sangat erat kaitannya dengan jaringan, karena untuk mengakses sebuah website pasti dibutuhkan koneksi jaringan. Saat ini sangat pesat sekali perkembangan teknologi website, jaringan dan bermacam ancaman keamanan yang dihadapi, seperti ancaman terhadap kerahasiaan yang sering dihadapi oleh *hacker* (Universitas Pasundan, 2012).

Web Aplikasi

Web aplikasi adalah aplikasi yang diakses menggunakan web *browser* melalui jaringan internet. Ada 2 bagian pokok dalam web aplikasi, yang pertama adalah sisi client dan yang kedua adalah sisi server. Sisi client dalam hal ini adalah PC atau perangkat mobile yang terhubung kejaringan internet, client dapat mengangkses aplikasi web melalui web browser. Server adalah perangkat komputer dengan spesifikasi yang bagus digunakan untuk menyimpan aplikasi web beserta database server yang siap untuk diakses oleh client (Smartsoft, 2014).

Path Traversal

Serangan *path traversal* memungkinkan *hacker* mengakses file, direktori dan perintah yang berpotensi berada diluar direktori root dokumen web. Penyerang dapat memanipulasi URL sedemikian rupa sehingga situs web akan mengeksekusi atau mengungkapkan konten file sewenang-wenang dimana pun di server web (Auger, 2010).

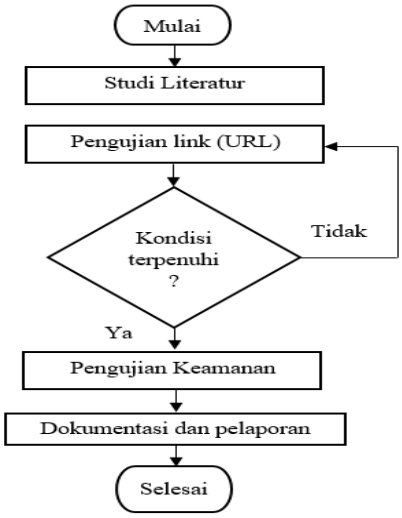
OWASP ZAP

OWASP ZAP adalah sebuah *tools vulnerabilities scanner* yang dibuat oleh organisasi OWASP *tool* ini adalah suatu proyek dari OWASP yang paling aktif karena terus dikembangkan. *Tool* ini bersifat *opensource* sehingga siapa saja bisa mengembangkan *tool* ini (OWASP ZAP, 2016).

METODE PENELITIAN

Dalam melakukan penelitian terhadap website pendataan warga dengan url http://skripsiwarga.000webhost.com. Pada penelitian ini terdapat tahapan pengumpulan data. Teknik yang digunakan pada tahapan pengumpulan data adalah studi literatur atau biasa disebut dengan studi pustaka dan studi dokumen. Studi pustaka merupakan Sebuah proses pengumpulan data dan informasi berupa teori-teori yang berkaitan dengan masalah yang diteliti (Muryandi, 2018). Sedangkan studi dokumen adalah Jenis pengumpulan data yang meneliti berbagai macam dokumen yang berguna untuk bahan analisis (Universitas Ciputra, 2016).

Flowchart Tahapan Penelitian

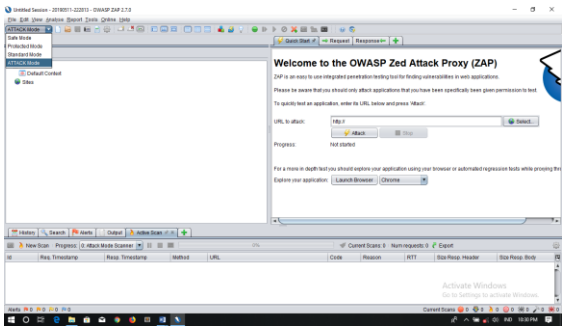


Gambar 1. Flowchart Tahapan Penelitian

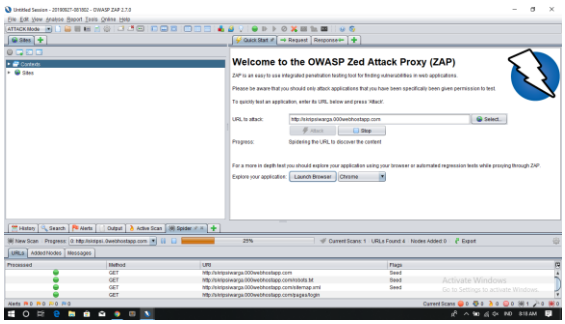
Proses Analisa

Pada tahap ini peneliti akan memberikan contoh bagaimana melakukan pengujian menggunakan *tool* OWASP ZAP pada website yang rentan terhadap serangan *path traversal*.

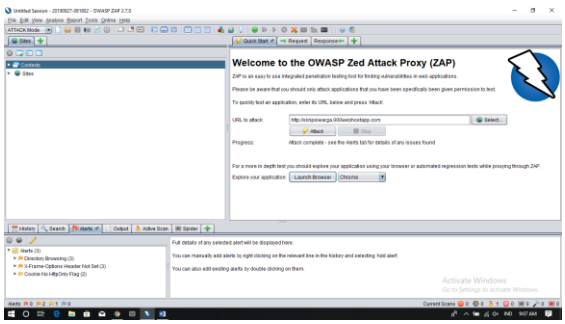
Berikut ini langkah-langkah melakukan proses analisa :



Gambar 2. Tampilan Awal OWASP ZAP



Gambar 3. Tampilan Proses Analisa



Gambar 4. Tampilan Hasil Analisa

HASIL DAN PEMBAHASAN

Pembahasan

Pada bagian ini akan diuraikan hasil yang telah dilakukan berdasarkan analisis yang telah dikemukakan pada bab sebelumnya. Pembahasan diarahkan pada permasalahan terhadap keamanan website dengan serangan *path traversal* yang ada pada website pendataan warga.

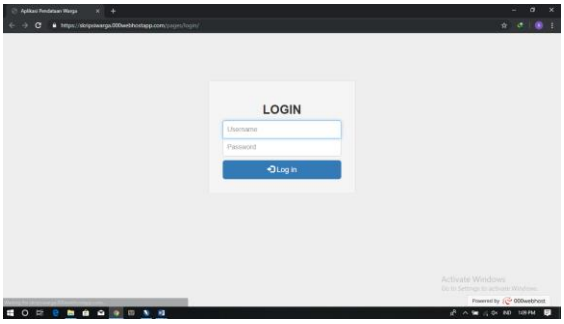
Hasil Analisa

Tabel 1. Hasil Analisa

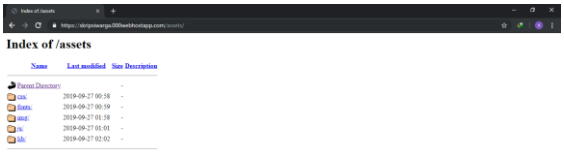
No	Nama Website	Celah dan Solusi	
		Celah	Solusi
1.	http://skripsiwarga.000webhostapp.com	Path tidak ditutup sehingga user bisa mengakses tanpa hak akses	- Menambahkan folder .htaccess dan memasukkan kode Options-Indexes - Menambahkan folder index.php

Implementasi Serangan Path Traversal

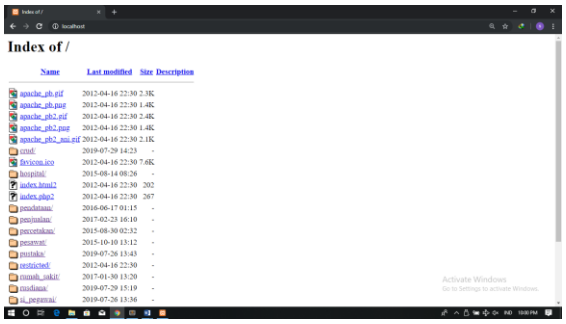
Berikut ini adalah implementasi dari serangan Path Traversal, penulis lakukan pada Aplikasi Pendataan Warga dengan url http://skripsiwarga.000webhostapp.com.



Gambar 5. Tampilan Awal Aplikasi Pendataan Warga

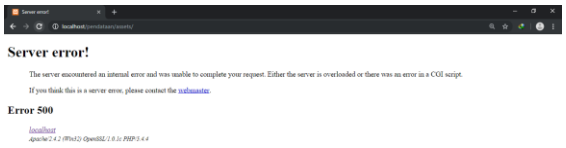


Gambar 6. Tampilan Path Yang Tidak Ditutup



Gambar 7. Tampilan Ke Server

Gambar 8. Tampilan Penambahan .htaccess



Gambar 9. Tampilan Setelah Ditambahkan .htaccess

Gambar 10. Tampilan Penambahan index.php

Gambar 11. Tampilan Setelah Ditambahkan index.php

Antisipasi Serangan Path Traversal

Untuk mencegah serangan Path Traversal, harus dilakukan proteksi pada website agar tidak bisa diakses tanpa ada hak akses dengan cara menutup file/folder penting agar tidak bisa diakses diluar jalur akses. Berikut ini ada dua cara menutup akses ke direktori, antara lain sebagai berikut :

1. .htaccess

   Yang pertama adalah membuat dulu file .htaccess pada file/folder yang penting dan memasukkan kode dibawah ini :

   ```
   Options-Indexes
   ```

   Kode diatas untuk menutup akses direktori sehingga ketika dijalankan akan muncul *Warning Access Forbidden*.

2. index.php

   Yang kedua dengan membuat file index.php pada setiap file/folder yang penting dan bisa menambahkan kata-kata yang diinginkan sebagai tanda bahwa file tidak bisa diakses.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil kegiatan "Uji Keamanan Website Terhadap Serangan Path Traversal : Studi Kasus Website Pendataan Warga" dapat diketahui bahwa saat ini tingkat kerentanan website cukup rawan diserang oleh attacker. Berdasarkan hasil analisa maka dapat dibuat kesimpulan sebagai berikut :

1. Hasil implementasi serangan Path Traversal pada Aplikasi Pendataan Warga, yaitu ketika akses ke direktori tidak ditutup akan menjadi celah untuk melakukan serangan Path Traversal sehingga attacker bisa mengakses atau mengambil file penting dari direktori pada aplikasi tersebut. Dengan menambahkan file .htaccess atau file index.php bisa menutup akses ke direktori

sehingga file-file penting tidak bisa diakses oleh attacker.

2. Serangan Path Traversal cukup berbahaya karena attacker bisa mengakses file tanpa memiliki hak akses sehingga attacker bisa mengambil file-file penting pada direktori.

Saran

1. Melakukan perawatan dan penjagaan website secara teratur menggunakan aplikasi scanning OWASPZAP agar diketahui jika website memiliki kerentanan serta melakukan pemeriksaan dan mengupdate bahasa program secara berkala.
2. Kelemahan website terletak pada bahasa pemrogramannya atau sintaks yang digunakan masih belum sempurna. Cara memperbaikinya adalah dengan menyempurnakan sintaks seperti yang penulis jelaskan sebelumnya.

DAFTAR PUSTAKA

Academia. (2019). *Keamanan Jaringan*. Diperoleh dari http://academia.edu. (diakses 20 juni).

Auger, Robert. (2010). *Path Traversal*. Diperoleh dari http://projects.webappsec.org. (diakses 4 mei).

Hartono, Hamzah. (2014). *Pengertian Website dan Fungsinya*. Ilmu Teknologi Informasi.

Kurniawan, Iwan, dkk. (2016). *Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2ban*. Jurnal Infomatek. 18: 96.

Muryandi, AMP. (2018). *Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web*. Skripsi. Tidak diterbitkan. Teknik Informatika Universitas Islam Indonesia.

OWASP ZAP. (2016). Diperoleh dari https://www.owasp.org. (diakses 20 Juni).

Smartsoft. (2014). *Pengertian Atau Definisi Web Application (Aplikasi Web).* Diperoleh dari http://smartsoftstudio.com. (diakses 15 Februari).

Universitas Ciputra. (2016). *Metode Pengumpulan Data*. Diperoleh dari http://ciputrauceo.net. (diakses 21 Juni).

Universitas Pasundan. (2012). *Keamanan Web*. Diperoleh dari http://www.unpas.ac.id. (diakses 20 Juni).

Zabar, AA dan Novianto, F. (2015). *Keamanan HTTP dan HTTPS Berbasis Web Menggunakan Sistem Informasi Kali Linux.*Vol. 4 N. 2. Hal 69-70.