Implementasi Web Analitik Untuk Deteksi, Analisa dan Evaluasi Keamanan Website (Studi Kasus PT. David System)

[1]Sartana, [2]Marice Hotnauli Simbolon

AMIK Medan Business Polytechnic, Jl. Jamin Ginting No. 285-287 Padang Bulan Medan

[3]Program Studi Manajemen Informatika, [2]Teknik Informatika
e-mail: [1]sartanasinurat@gmail.com, [2]simbolonice@gmail.com

Abstrak

David GroupTM merupakan perusahaan yang multi-divisi yang bergerak dibeberapa bidang jasa antara adalah cyber security, telekomunikasi, teknologi, software dan program customizer. Web Analitik merupakan suatu software yang berfungsi untuk mendeteksi, menganalisis, dan mengevaluasi keamanan sebuah website. Pengguna layanan Web dan internet akan menuntut keamanan dan kenyamanan dalam bertransaksi pada setiap website komersial seperti pembayaran atau data pribadi pada website. Web Analitik yang akan dirancang diharapkan mampu membantu PT. David Sistem Group memberikan implementasi analitik keamanan, pemetaan potensi jenis dan karakteristik serangan, nilai evaluasi terhadap tingkat keamanan website

Kata kunci*—David Sistem, Web Analitik, Keamanan Siber*

Abstract

David GroupTM is a multi-divisional company that is engaged in several services, including cyber security, telecommunications, technology, software and customizer programs. Web Analytics is a software that functions to detect, analyze, and evaluate the security of a website. Users of Web and internet services will demand security and convenience in transacting on any commercial website such as payment or personal data on the website. The Analytical Web that will be designed is expected to be able to help PT. David System Group provides implementation of security analytics, mapping of potential types and characteristics of attacks, evaluating the value of website security levels

Keywords—*Web Analytic, David System, Cyber Security*

1. PENDAHULUAN

PT. David Sistem Group merupakan perusahaan perseroan terbatas yang berdedikasi pada stabilitas keamanan siber global dan disahkan pada tanggal 27 mei 2019 oleh menteri hukum dan hak asasi manusia (HAM) Indonesia dengan nomor AHU-0026807.AH.01.01.TAHUN 2019. Software analitik website merupakan suatu software untuk mendeteksi, menganalisis, dan mengevaluasi keamanan sebuah website yang digunakan agar suatu website tidak mudah terserang oleh pihak lain, baik atau tidaknya sebuah website terdiri dari keamanan website, kecepatan website, SEO, dan hal lainnya.

Banyak orang yang tidak mengetahui apakah website yang dibangun aman atau tidak. Bahkan sebagian orang tidak mengetahui bagaimana menutup dan mengevaluasi keamanan

sistem tersebut jika website tersebut telah terserang. Pengguna Jasa Internet dan web pasti menuntut keamanan dan kenyamanan bertransaksi dari Setiap website komersial yang mendukung sistem pembayaran atau penyimpanan data pribadi pada website, selama ini pihak perusahaan yang menyelenggarakan bisnis komersial dalam penjualan barang dan jasa biasanya menggunakan aplikasi pendukung dan tools dalam memonitoring dan memanajemen transahsi onlinenya.

Dari uraian diatas maka peneliti ingin membantu PT. David System dalam memberikan kemudahan dalam memberikan layanan keamanan bagi website para nasabah dan mitra kerja.

2. METODE PENELITIAN

Untuk memenuhi kebutuhan materi yang diperlukan dalam penelitian ini Peneliti melakukan beberapa penerapan metode penelitian untuk menyelesaikan permasalahan,. Metodemetode yang dilakukan dalam penelitian ini adalah sebagai berikut
:

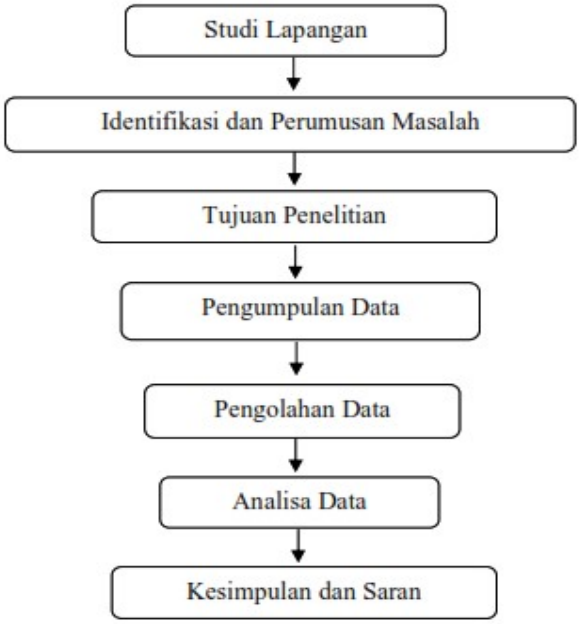
1. Studi Literatur
   Pada tahap ini dilakukan dengan mempelajari buku-buku referensi atau sumber-sumber Yang berkaitan dengan skripsi ini. Baik text book atau internet.

2. Tahap Analisa dan Pengumpulan Data
   Pada tahapan ini, akan dilakukan penelitian yang bertujuan untuk memperoleh data secara langsung dari perusahaan. Tahapan ini berupa:
   a. Pengumpulan sampel dokumentasi yang berhubungan dengan masalah Deteksi, Analisa dan Evaluasi Keamanan Website
   b. Mewawancarai pihak perusahaan PT. David Group System yang bekerja dibagian lapangan dalam masalah Web Analitik yang akan direkomendasikan.

3. Tahap Perancangan
   Pada tahapan ini, berguna untuk merancang sistem yang dapat menyelesaikan permasalahan yang terdapat pada sistem yang sedang berjalan.Yang bertujuan untuk meminimalisasikan kekurangan yang terdapat pada sistem yang lama dengan menggunakan sistem yang baru.

4. Tahap Pemrograman
   Adapun tahapan ini, bertujuan untuk menghasilkan tampilan visual dari web analitik deteksi, analsa dan evaluasi keamanan website pada PT. David Group Sistem

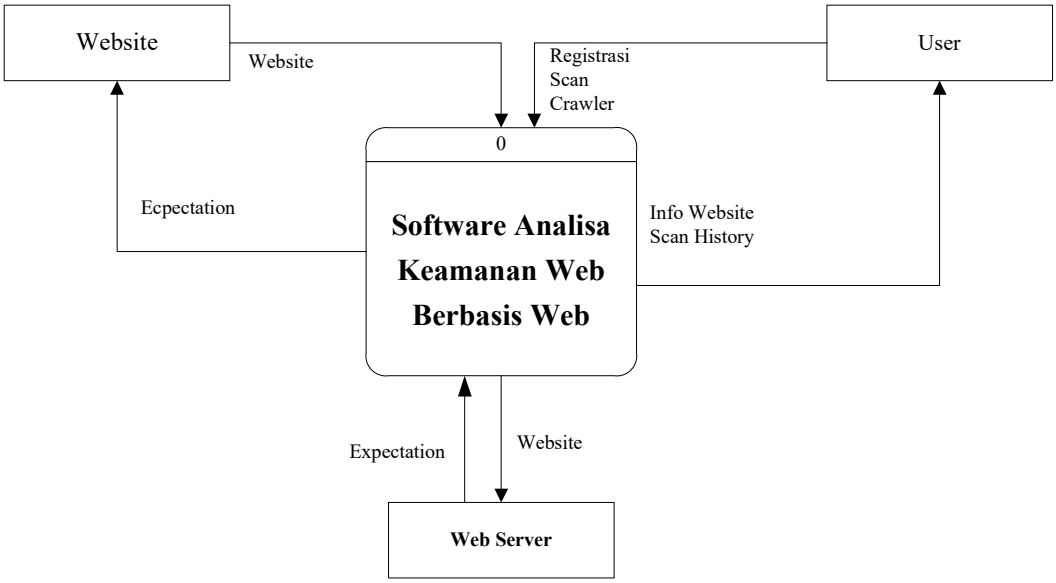
a. Diagram Alir Langkah Penelitian



Gambar 1. Diagram Alir Penelitian

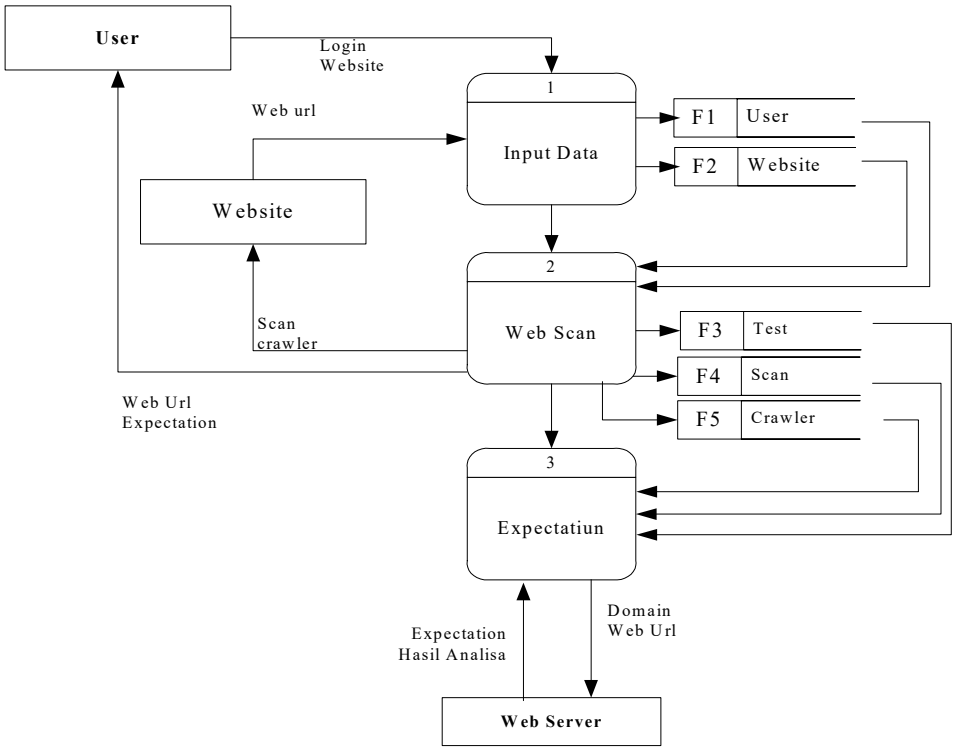
3. HASIL DAN PEMBAHASAN

3.1 DFD Level 0



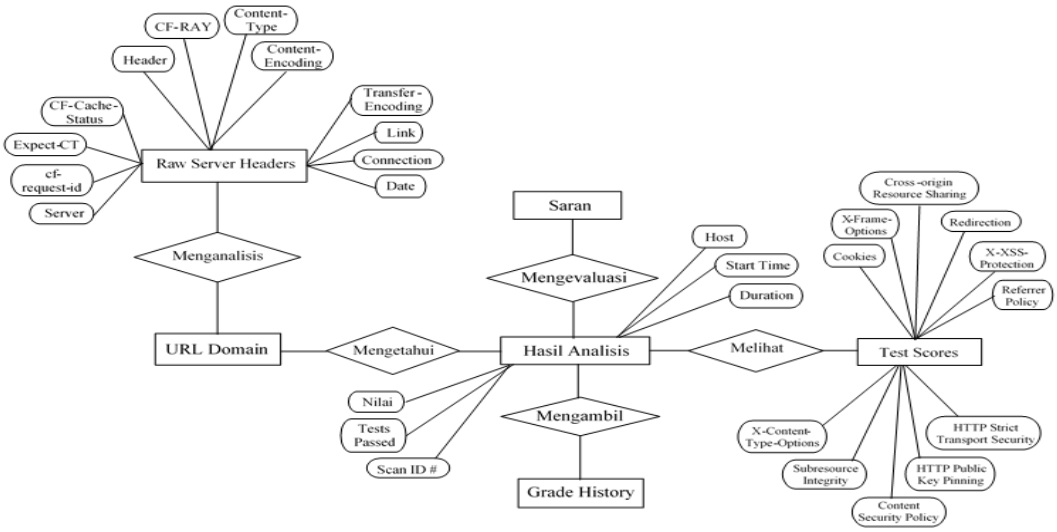
Gambar 2 DFD Level 0 Web Analitik

3.2 DFD Level 1



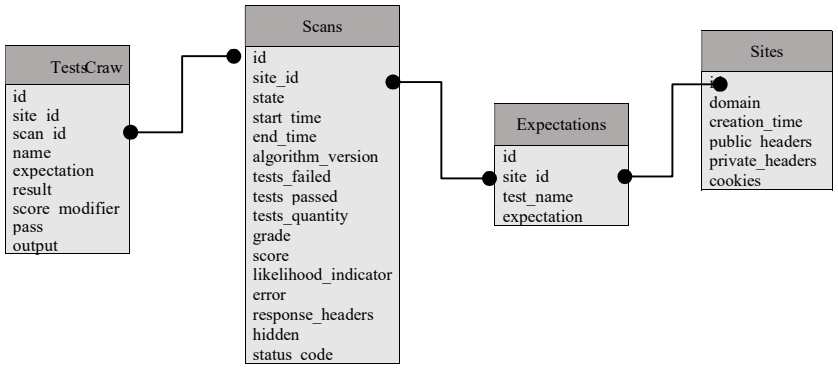
Gambar 3. DFD Level 1 Web Analitik

3.3 ERD Implementasi Web Analitik



Gambar 4. ERD Lengkap Implementasi Web Analitik

3.4 Relasi Tabel Database

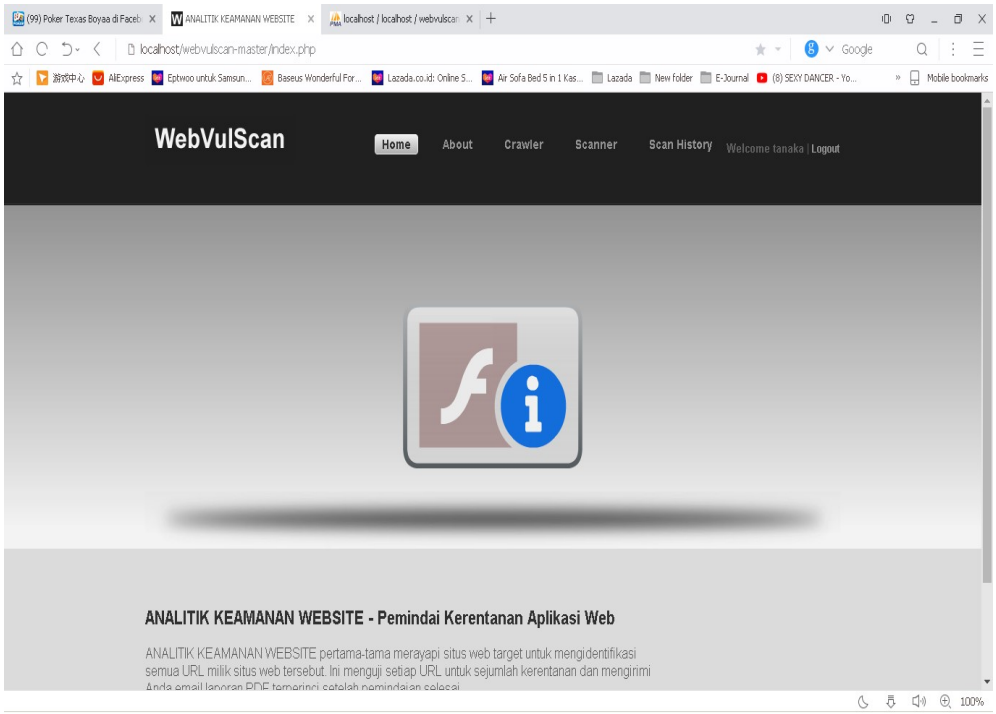


Gambar 5. Relasi Tabel Data Web Analitik

3.4 Hasil Uji Coba Dan Implementasi Sistem

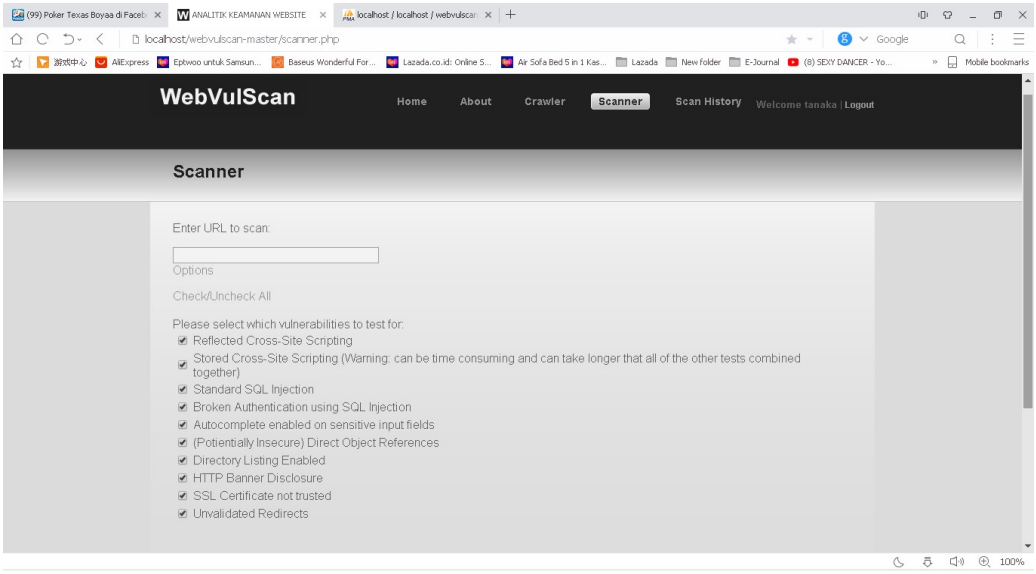
Dalam proses ujicoba dan implementasi sistem web analitik, akan ditampilkan Fitur-fitur serta menu interaktif yang memudahkan pengguna untuk mendapatkan layanan dan fasilitas yang telah tersedia dalam halaman web yang terdiri dari

a. Halaman Utama (Home Page)



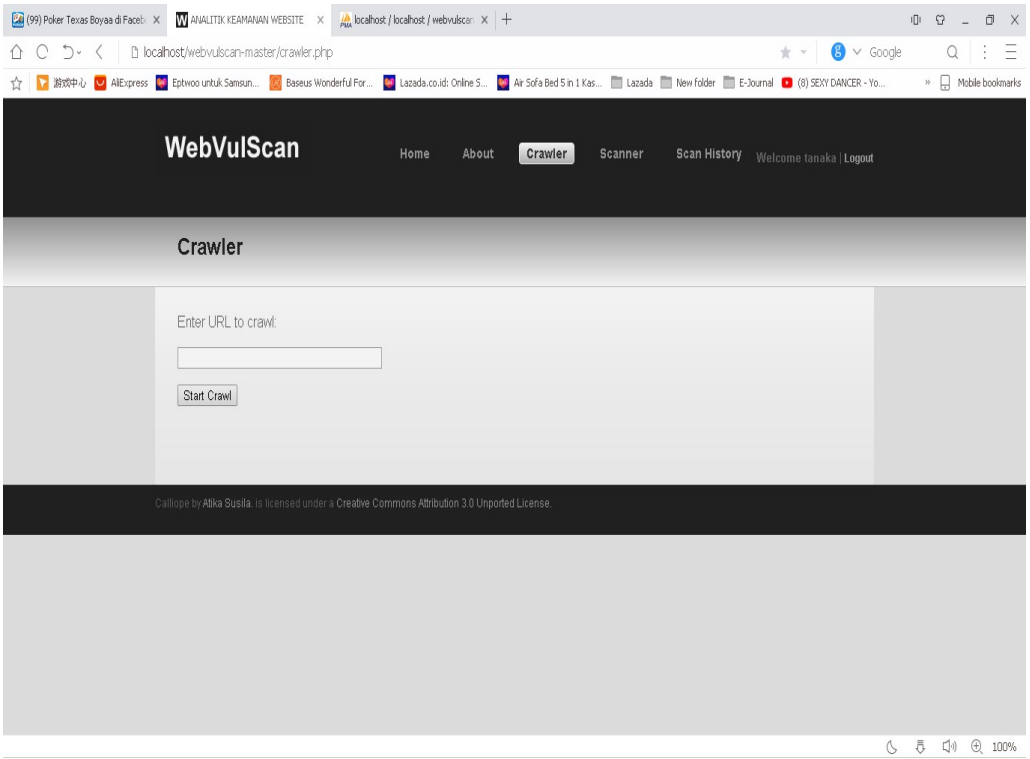
Gambar 6. Tampilan Hompage Web Analitik

b. Proses Web Scanning



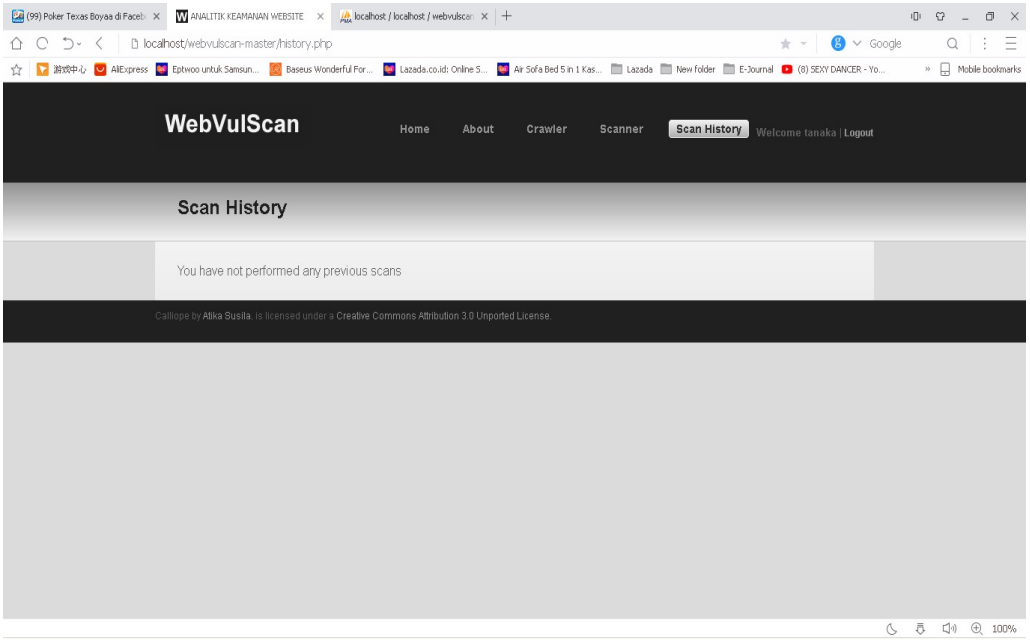
Gambar 7. Proses Analisa Keamanan Web dengan Teknik Scanning

c. Proses Web Crawler



Gambar 8. Proses Alanisa Keamanan Wem dengan Teknik Crawler

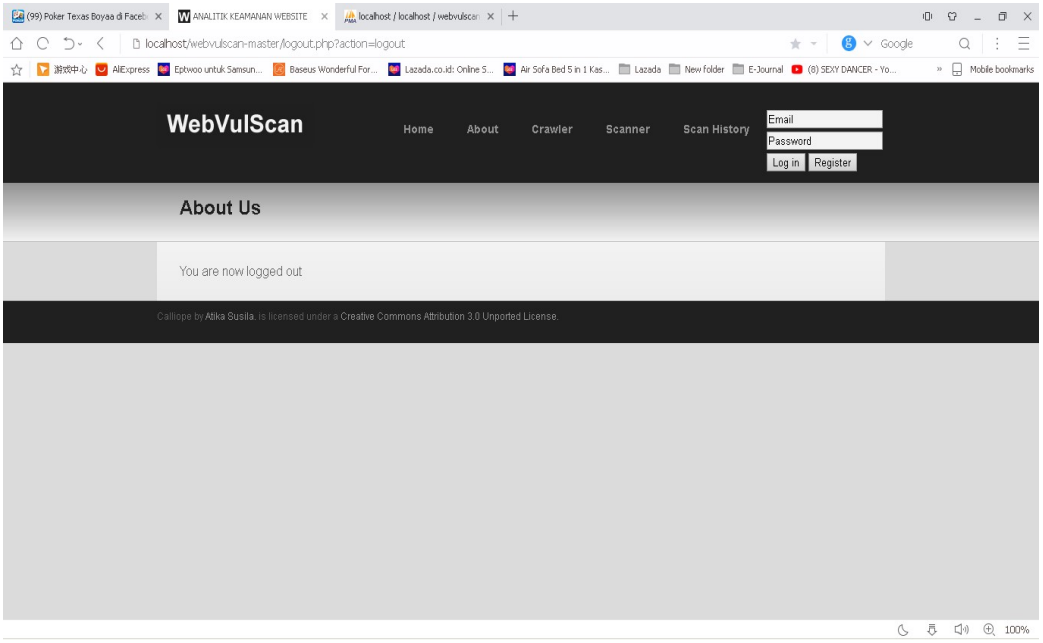
d. Proses Scan History



Gambar 9. Tampilan Riwayat Hasil Scan Web yang pernah di Analisis

e. Log Out User

\



Gambar 10. Tampilan Keluar dari Web Analitik Sistem

4. KESIMPULAN

1. Sistem Deteksi dapat berjalan dengan baik terutama pada website yang menggunakan WordPress. Dari 54 website data replikasi, sistem yang dibangun menemukan celah keamanan pada 53 website. Celah keamanan pada WordPress banyak ditemukan pada versi WordPress dan versi plugin yang digunakan. Sedangkan pada PHP manual/framework hasilnya tidak efektif, dari 6 data website, hanya 3 website yang ditemukan memiliki celah keamanan.
2. Deteksi celah keamanan berdasarkan jenis website cukup efektif terutama pada website jenis CMS dikarenakan celah keamanan pada CMS yang beragam sesuai dengan versi yang digunakan sehingga dapat dibuat database berisi informasi versi yang digunakan beserta celah keamanannya. Namun metode ini memiiliki kelemahan dimana terbatasnya informasi celah keamanan yang digunakan untuk jenis website tertentu.Sistem yang dibangun mampu memberikan informasi inventaris barang dengan mudah dan cepat.

5. SARAN

1. Sistem yang dibangunharus mampu menampilkan gambar grafik dan persen kelemahan dari website target yang dicrawler maupun discan
2. Sistem yang dibangun dapat dikembangkan dengan menambahkan fitur-fitur yang lebih lengkap seperti traffic tracking, open and close port number, menghapus jejak scanner dan membangun backdoor pada web target
3. Sistem yang dibangun dapat dikembangkan lagi untuk multi platform sistem operasi dan multi device (Sistem operasi Android dan Aplikasi untuk Mobile smartphone).

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada semua pihak yang telah memberi dukungan terhadap penelitian ini, sehingga Peneliti dapan menyelesaikannya dengan baik, tentu masih banyak kekurangan didalam penelitian ini oleh sebab itu Peneliti meminta keritikan dan masukan untuk penelitian berikutnya, terima kasih juga buat segenap rekan-rekan yang telah banyak membantu peneliti dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] Kadir, Abdul, Dasr Penmrograman Web Dinamis Menggunakan PHP, Andi, Yogyakarta, 2002.
[2] Ariyus, Dony. 2007. Intrusion Detection System.Yogyakarta: Andi Offset.
[3] Diansyah, Tengku M., 2014. Analisa Mekanisme Snort dalam Menangani Serangan Flooding. pada Prosiding Snastikom 2014 hal. 9
[4] IBISA, 2011, Keamanan Sistem Informasi, Yogyakarta: Andi Offset.
[5] Jamaluddin, 2012. Modul Praktikum Keamanan Web dan Virus Komputer. Medan: Lab.Komputer FE-UMI.
[6] Manimaran, G. 2004. Internet Infrastructure Security in High Performance Interconnects, pada Proceedings of 12 th Annual IEEE Symposium on 2004, p.109.
[7] Rafiudin, Rahmat. 2010. Mengganyang Hacker dengan Snort, Yogyakarta: Andi Offset.

[8] Sofana, Iwan. 2008. Membangun Jaringan Komputer, Bandung: Informatika.
[9] Tanenbaun, Andrew S., 1989. Computer Network. Englewood: Prentice-Hall International, inc.
[10] Apriawan, Dwi N.H. 2015. Protokol Jaringan Komputer . http://ilmukomputer.com/hendra protokol jaringan.pdf diakses tanggal 27 April 2015.
[11] Clancy Malcolm, Ten Security Check For PHP, Website, http://www.onlamp.com/pub/a/php/2003/03/20/php_security.htm
[12] Guidelines on Securing Public Web Servers **http://csrc.nist.gov/publications/nistpubs/800-44ver2/SP800-44v2.pdf**
[13] Jordan Dimov,On The Security Of PHP, Website http://www.developer.com/lang/php/article.php/922871
[14] John Coggeshall ,PHP Security,Website http://www.onlamp/pub/au/135
[15] Sufehmi, Harry, Security di PHP, Website http://www.tf.itb.ac.id/~eryan/Php/PHPSecurity.txt