BAB II

TINJAUAN PUSTAKA

1.1 Penelitian terdahulu

(Cobantoro, 2016)Hasil penelitian sebelumnya yang di lakukan oleh Adi Fajaryanto Cobantoro (2016) berjudul "Penerapan Owaps Versi 4 untuk Uji Kerentanan Web Server (Studi kasus Ejurnal server kampus x Madiun) Meningkatnya penguna internet sejak tahun 2009 dan akan terus meningkat, memudahkan web server dapat di akses kapan saja. Mudahnya akses ini membuat banyak orang maupun instansi membangun sistem web server tanpa memperhatikan keamanan web server tersebut. Gangguan tersebut diantaranya berupa serangan Malicious Code atau Malware. Dalam mengamankan web server dari serangan yang tidak bertanggung jawab maka sebaiknya para pemilik web server melakukan self test terhadap web server mereka sendiri. Salah satu metode self test ini adalah penetration test mengunakan metode Owaps Versi 4.

Berdasarkan hasil penelitian yang dilakukan oleh Muhammad faris (2017) berjudul "Implementasi keamanan owaps terhadap aplikasi berbasis GTFW, *Gamatechno Web Application Framework* atau yang lebih familiar disebut GTFW, merupakan *framework* PHP yang dikembangkan oleh PT Gamatechno Indonesia. Sejak Gamatechno berdiri pada tahun 2005. Bahwa mengamankan aplikasi web dari kerentanan yang memungkinkan pihak yang tidak bertanggung jawab dapat mengakses dan memodifikasi data-data dari

web server yang tersimpan secara online. Adanya bahaya kerentanan dalam suatu web server dapat meningkatkan ancaman bagi pemilik website, hal ini memungkinkan penyerang dapat melakukan hal yang tidak di inginkan terhadap sistem.

(Bella, S.S., 10"., AKAKOM, & Diterbitkan, 2012)Sri Setia Bella (2012) dalam penelitian nya yang berjudul "Membangun aplikasi pembelajaran secure web programming berbasis owasp top 10" Menyatakan Web Aplikasi dengan PHP menjadi hal yang populer dalam akses global terhadap data, pelayanan, dan produk. Akan tetapi, akses global yang memberikan efek keuntungan utama penggunaan web ini juga memberikan kerentanan keamanan yang bisa diakses secara global dan sering disalahgunakan oleh orang yang tidak bertanggung jawab. Memang bukan hal yang sulit untuk membuat Web Aplikasi menggunakan PHP, tetapi aplikasi ini bisa jadi mengandung kerentanan-kerentanan berbahaya tanpa disadari. Kejadian ini ditampilkan oleh banyak Web Aplikasi umum lainnya, termasuk PHP yang ternyata memiliki lubang-lubang keamanan berbahaya.

Berdasarkan hasil penelitian oleh Yunanri W., Imam Riadi, Anton Yudhana, (2016) berjudul (Analisis Keamanan Webserver Mengunakan Metode Penetrasi Testing) Keamanan sistem informasi adalah salah satu permasalahan utama dalam perkembangan teknologi informasi dan komunikasi saat ini.

Dalam memecahkan masalah yang sering terjadi keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data dengan baik, transaksi, dan komunikasi. Dengan tidak adanya keamanan pada sistem maka akan banyak para Hacker yang dengan mudah dapat mengambil alih sistem yang kita bangun.

Dalam membangun sistem informasi berbasis web, keamanan sistem merupakan hal penting yang harus di perhatikan bagi seorang programmer. Dari penelitian terdahulu di atas pada dasarnya sama pada penelitian ini dalam metode atau alalisis fokus pada keamanan sistem informasi tersebut. Ada pun perbedaan penelitian ini dengan penelitian terdahulu dari framework yang di gunakan.

Framework OWASP (Open Web Application Security) versi 4, yang dikeluarkan oleh owaps.org sebuah organisasi yang membahas tentang keamanan aplikasi berbasis sistem informasi secara gratis. Pada penelitian ini penulis fokus pada tahapan Informasi Gethering, Authentication Testing, Authorization Testing dan Session Management Testing.

2.2 Sistem

Suatu jaringan kerja yang saling berhubungan, untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang di tuju.

2.3 Informasi

Informasi adalah Sekumpulan data/ fakta yang diolah sehingga mempunyai arti bagi penerima. Dimana data yang diolah menjadi sesuatu yang dapat di mengerti bagi si penerima dan dapat memberikan keterangan atau pengetahuan. Dengan demikian yang menjadi sumber informasi adalah sebuah data.

2.4 Sistem Informasi

Suatu sekumpulan komponen yang mempunyai keterkaitan antara satu komponen dengan komponen lainnya yang mempunyai tujuan suatu informasi dalam suatu bidang tertentu. Dalam sistem informasi diperlukannya klasifikasi alur informasi, dalam sistem informasi dibutuhkannya keanekaragaman akan suatu informasi oleh pengguna informasi. Kriteria dari sistem informasi antara lain, fleksibel, efektif dan efisien.

2.5 Website

Website biasa disebut dengan web page dan link, website merupakan dapat memungkinkan pengguna bisa mengunakan berpindah dari satu page ke page lain (hyper text), baik diantara page yang disimpan di dalam server yang sama ataupun server diseluruh dunia. Pages yang diakses dan dibaca melalui browser seperti Netscape Navigator, Internet Explorer, Mozila Firefox, Google Chrome dan aplikasi browser lainnya.

2.6 Open Web Application Security Project (OWASP)

(OWASP, 2014)Open Web Application Security Project (OWASP) adalah sebuah organisasi internasional yang bersifat non-profit, didirikan oleh OWASP foundation pada 21 April 2004 di Ameriaka Serikat. Pada OWASP merupakan peningkatan keamanan perangkat lunakdi dalam mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi terpercaya untuk menjamin dapat keamanan yang telah di buat atau pun yang di kembangkan. OWASP sendiri memiliki tujuan dalam keamanan untuk mengamankan software, sehingga orang-orang dan organisasi dapat membuat keputusan terhada resiko yang telah ditemukan dalam keamanan yang benar.

2.6.1 OWASP Testing Guide

OWASP Testing Project telah dikembangkan dan di pergunakan selama bertahun tahun dalam keamanan aplikasi web. Dalam OWASP ini memiliki tahapan kerangka pengujian yang sangat lengkap dalam memakukan pengetesan saat uji coba mencari kerentanan sistim. Melainkan OWASP merupakan sebagai *template* untuk membangun keamanan dalam program pengujian yang di lakukan. Dalam panduan tahapan OWASP pengujian dijelaskan secara rinci baik kerangka pengujian umum dan teknik yang dilakukan untuk menerapkan kerangka dalam praktik uji coba keamanan aplikasi web.

Tujuan Pengujian aplikasi ini merupakan untuk menemukan kerentanan keamanan yang ada, tanpa mengetahui inner dari aplikasi itu sendiri yang disebut pengujian penetrasi, tester bertindak sebagai seorang penyerang dan berupaya untuk menemukan dan mengeksploitasi kerentanan aplikasi web. Kerentanan yang ditemukan saat penetrasi dapat dikategori yaitu low, medium dan high.

2.6.2 Information Gathering

Pengumpulan informasi adalah suatu proses dalam penetration testing yang digunakan untuk mengumpulkan data dan informasi penting tentang target yang akan di serang.

2.6.3 Authentication Testing

Otentikasi adalah proses menetapkan atau mengkonfirmasi sesuatu yang dibuat itu dapat di percaya. Dalam keamanan komputer merupakan bentuk komunikasi web browser sebagai client dan Web server sebagai website.

2.6.4 Authorization Testing

Otorisasi merupakan pencarian, apakah penguna sudah diidentifikasi melewati otentikasi dengan identitas resmi untuk melakukan akses dan memanipulasi ke sumber daya.

2.6.5 Session Management Testing

Session Management Testing didefinisikan sebagai himpunan semua kontrol antara client dan aplikasi berbasis web. Aplikasi paling populer, seperti ASP dan PHP, menyediakan pengembang dengan rutinitas penanganan sesi built-in. Beberapa jenis token identifikasi biasanya akan dikeluarkan, yang akan disebut sebagai "ID Sesi" atau Cookie.

2.7 Kali Linux

Kali Linux merupakan reinkarnasi dari BackTrack, sebuah distro Linux yang dibuat khusus untuk mengunakan keperluan dalam penetration dan testing pada sebuah sistem keamanan komputer. Kali Linux sudah dilengkapi dengan berbagai tools Linux yang dapat digunakan untuk melakukan penetration testing untuk keamanan aplikasi web. Kali Linux merupakan pengujian keamanan yang tidak perlu melakukan men-install atau membuat kode program/script baru. Kali linuk bisa di gunakan hacker yang dapat memahami setiap aksi yang dilakukannya dan mampu membuat tool/script-nya sendiri dalam penetrasi testing (www.kali.org).