BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2. 1. Tinjauan Pustaka

Dalam tinjauan pustaka ini terdapat lima referensi dan satu referensi dari penulis. Penelitian sebelumnya telah dilakukan oleh Sri Setia Bella dengan hasil website dengan code yang aman berdasarkan OWASP TOP 10 dan Saiful Azhari Muhammad yang menghasilkan website yang bisa menangkal serangan *SQL Injection*.

2.1 Tabel Tinjauan Pustaka

Parameter / Penulis	Objek	Metode	Bahasa Pemrograman	Database	Map
Sri Setia Bella(2013)	Pengguna Umum	- OWASP TOP 10	- PHP - CSS - HTML	MySQL	Graphical User Interface (GUI)
Saiful Azhari Muhammad (2014)	Pengguna Umum	- Pengenalan String - Encoding Parameter - Pengenalan Pola Serangan	- PHP - CSS - HTML	MySQL	Graphical User Interface (GUI)
KM. Syarif Haryana (2008)	Pengguna Umum	- Validasi Login - HTTPS Protokol - Enkripsi MD5	- PHP	-	Graphical User Interface (GUI)
Sri Wahyuni (2012)	Pengguna Umum	- WSP, WTP, WTLS dan WDP	- PHP - HTML	-	Graphical User Interface (GUI)
Suluh Sri W (2009)	Auditor Situs Web	- Pengukuran yang	- ASP	MySQL	Graphical User

Parameter / Penulis	Objek	Metode	Bahasa Pemrograman	Database	Map
		digunakan adalah : fa = ∑bi . gi			Interface (GUI)
Ikhwan Dirga Pratama (2017)	Pengembang Situs Web	- Pengenalan String - Encoding Parameter - Pengenalan Pola serangan - Validasi Login - Enkripsi Base64	- PHP - HTML - CSS - JavaScript	JSON	Graphical User Interface (GUI)

Sistem yang dibuat ini merupakan sistem berbasis web dimana pengguna harus menyisipkan salah satu berkas php kedalam situs web yang akan di pantau, dan melakukan *login* untuk memantau jalannya aplikasi pengaman web ini.

Pembeda dari aplikasi lainnya adalah:

1) Adanya Laporan yang menggunakan Informasi Geografis untuk menampilkan IP penyerang berdasarkan lokasi negara.
2) Perbaikan UI dan UX menjadi lebih responsif
3) Memberikan keamanan pada kode program dengan pemberian enkripsi base64.

2. 2. Dasar Teori

Dasar teori digunakan untuk memahami definisi, pengertian dasar dan istilah yang digunakan dalam penelitian ini. Berikut dasar teori yang digunakan:

2.2.1. PHP

PHP merupakan Bahasa pemrograman serv*er-side scripting* yaitu sintaks dan perintah yang dijalankan di server dan disertakan pada dokumen HTML. Sehingga dapat digunakan untuk membuat halaman web yang dinamis. PHP (Personal home Page) sendiri merupakan Bahasa pemrogramman dan HTML dalah sebagai pembangun halaman web. Pada saat akan membuka suatu situs yang menggunakan fasilitas *server-side scripting* PHP, maka terlebih dahulu server yang bersangkutan akan memproses semua perintah PHP di server lalu mengirimkan hasilnya dalam format HTML ke web browser. PHP merupakan *software* yang *open source* dan dapat digunakan pada sistem operasi dan web server apapun. (Wahyuni, 2010)

2.2.2. JSON

JSON (*JavaScript Object Notation*) adalah format pertukaran data yang ringan, mudah dibaca dan ditulis oleh manusia, serta mudah diterjemahkan dan dibuat (generate) oleh komputer. Format ini dibuat berdasarkan bagian dari Bahasa Pemprograman *JavaScript*, Standar ECMA-262 Edisi ke-3 - Desember 1999. JSON merupakan format teks yang tidak bergantung pada bahasa pemprograman apapun karena menggunakan gaya bahasa yang umum digunakan oleh programmer keluarga C termasuk C, C++, C*#, Java, JavaScript, Perl, Python* dll.

2.2.3. Htmlentities

Htmlentities adalah suatu fungsi PHP yang berfungsi umtuk mengubah karakter menjadi HTML entities. *Htmlentities* dapat digunakan untuk mengamankan parameter input dari serangan XSS dan *SQL Injection*

2.2.4. Escapeshellarg

Escapeshellarg adalah fungsi PHP yang berfungsi untuk menambah tanda petik pada *string* yang memungkinkan untuk mengakses langsung perintah *shell*. Fungsi ini digunakan untuk mengamankan parameter yang mengandung perintah *shell* dari inputan user.

2.2.5. Brute Force

Brute force adalah suatu metode untuk bisa masuk ke suatu situs web dengan menggunakan *username* dan *password* secara acak. Metode ini menggunakan daftar *username* dan *password* yang kemudian digunakan untuk mencoba masuk kedalam halaman web. Proses ini dilakukan secara berulan-ulang sampai didapatkan *username* dan *password* yang benar.

2.2.6. SQL Injection

SQL Injection adalah jenis serangan yang memungkinkan penyerang untuk memanipulasi perintah SQL melalui URL atau isian *form* yang dikirimkan oleh aplikasi web ke server.

2.2.7. Cross Site Scripting

Kelemahan *Cross Site Scripting* atau XSS terjadi ketika aplikasi mengambil data yang tidak dapat dipercaya dan mengirimnya ke suatu web *browser* tanpa validasi yang memadai, XSS memungkinkan penyerangan mengeksekusi *script-script* di dalam browser korban, yang dapat membajak sesi pengguna, mengubah tampilan website, atau mengarahkan pengguna ke situs-situs jahat.

2.2.8. Command Execution

Command execution merupakan celah keamanan yang memungkinkan penyerangan untuk menyisipkan perintah-perintah *shell* untuk dieksekusi oleh web server. Fungsi PHP yang berpotensi menyebabkan celah *command execution* adalah exec(), system(), shell_exec(), passthru().

2.2.9. Arbitrary File Upload

Arbitrary file upload adalah celah keamanan dimana fitur upload tidak membatasi extensi apa saja yang diizinkan, sehingga penyerang dapat mengupload berkas berbahaya seperti PHP *backdoor* maupun *executable file* yang lain.