1. Pendahuluan

Latar Belakang

PHP merupakan salah satu dari bahasa pemrograman web yang sangat popular, bahasa pemrograman PHP digunakan oleh 79,0% dari semua situs web [1]. Banyak aplikasi web telah disediakan untuk layanan online dalam beberapa tahun terakhir, seperti perbankan. Tetapi, kerentanan keamanan masih menjadi masalah utama pada aplikasi web. Menurut laporan Risk Based Security [2]. Pada tahun 2018 terjadi kerentanan keamanan pada website seluruh dunia mencapai 17.308 serangan, termasuk didalamnya serangan XSS dan SQL Injection. Penyebab kerentanan terhadap serangan biasanya terjadi karena adanya Script PHP yang tidak difilter, salah satu cara untuk mengatasinya adalah menggunakan htmlentities.

Static Analysis biasanya digunakan untuk mendeteksi kerentanan keamanan pada suatu program atau website, karena Static Analysis dapat melakukan analisis terhadap suatu Script tanpa kita harus menjalankan program atau website kita terlebh dahulu [3]. Namun, akurasi pendeteksian PHP Vulnerability masih rendah pada beberapa penelitian masih menghasilkan false positive yang tinggi. Akurasi yang didapat saat ini hanya mencapai 88% [4].

Maka dalam menangani permasalahan kerentanan keamanan pada suatu Script PHP dan rendahnya akurasi pendeteksian pada tugas akhir ini akan melakukan analisis terhadap Script PHP menggunakan metode Static Forward Taint Data analysis. Metode Static Forward Taint Data analysis dapat melakukan analisis terhadap Script PHP tanpa harus menjalankan program tersebut terlebih dahulu atau kita melakukan analisis secara White Box serta dapat meningkatkan akurasi pendeteksian kerentanan pada Script PHP.

Beberapa langkah untuk melakukan analisis menggunakan metode Static Forward Taint Data analysis adalah pertama kita melakukan tracing per-baris dan memisahkan antara script yang rentan terhadap serangan dan script yang tidak rentan terhadap serangan lalu menyimpannya kedalam array sesuai kategori atau konteksnya, langkah kedua melakukan tracing per-Array dan melakukan pengelompokkan jenis serangannya, langkah ketiga melakukan pengecekan kembali pada array yang sudah dikelompokkan sebelumnya, apakah ada script yang sebenarnya tidak rentan terhadap serangan XSS dan SQL Injection menggunakan Regular

Expression. Langkah terakhir adalah melakukan evaluasi dengan menggunakan rumus dan disajikan kedalam tabel.

Topik dan Batasannya

Berdasarkan latar belakang diatas pada tugas akhir ini membangun pendeteksian pada skrip PHP menggunakan metode Forward Taint Data Analisis. Agar tugas akhir ini dapat dilakukan lebih fokus dan mendalam maka kami memandang permasalahan penelitian yang diangkat perlu dibatasi;

- Dataset diperoleh dari aplikasi open source PHPiCalendar [13].
- Serangan yang akan diuji dan dianalisa adalah Cross-Site Scripting dan SQL Injection;
- Parameter pengujian adalah variabel pendukung akurasi, yaitu True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN).

Tujuan

Berdasarkan permasalahan yang telah dikemukakan diatas berikut adalah rincian tujuan penulisan tugas akhir ini yaitu Meningkatkan akurasi pendeteksian PHP Vulnerability menggunakan metode Forward Taint Data Analisis.

Organisasi Tulisan

Penelitian ini disusun dengan struktur sebagai berikut: Setelah dijelaskan pendahuluan pada bagian pertama, dijelaskan studi terkait pada bagian kedua. Selanjutnya, dijelaskan pemodelan sistem pada bagian ketiga. Selanjutnya evaluasi performansi sistem terhadap sistem yang dibagun pada bagian ketiga dan bagian keempat, dijelaskan kesimpulan dan saran untuk penelitian selanjutnya.