Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 2, Nomor : 1, Januari 2023 : 57-71 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Analisis Implementasi Laravel 9 Pada Website E-Book Dalam Mengatasi N+1 Problem Serta Penyerangan Csrf dan Xss

Analysis of Laravel 9 Implementation on E-Book Websites in Overcoming N+1 Problems and Csrf and Xss Attacks

M. Mahdi Maulana Lubis*[1], Tommy[2], Divi Handoko[3], Nur Wulan[4]
[1,2,3] Prodi Teknik Informatika Universitas Harapan Medan , Jl. HM. Joni No.70 C, Teladan Bar Kota Medan, Sumatera Utara, Indonesia.

[1]mmahdi6870@gmail.com*, [2]tomshirakawa@gmail.com, [3]divihandoko@gmail.com, [4]nurwulanstth@gmail.com

Abstrak

Di era digital saat ini penggunaan website sangat meningkat pesat masyarakat menyukai segala hal yang instan bahkan dalam hal membaca buku, mereka lebih memilih membaca e-book dari pada membaca buku secara konvensional. Oleh karena itu dibitihkan sebuah website yang mampu mengolah data secara cepat sehingga pembaca tidak akan menunggu lama saat ingin mencari buku ataupun jurnal yang mereka ingikan. Selain itu website juga menyimpan data para pembaca dan menyimpannya, namun banyak sekali oknum-oknum yang tidak bertanggung jawab yang menggunakan data mereka secara illegal maka dibutuhkan pengamanan lebih lanjut bagi kenyamanan para pembaca, oleh karena itu peneliti akan menganalisa penyelesaian permasalahan keamanan website dari penyerangan xss dan csrf serta N+1 problem menggunakan Laravel apakah memiliki pengaruh terhadap website e-book ataukah tidak sama sekali

Kata kunci : *Website, E-book, XSS, CSRF, N+1 Problem*

Abstract

In the current digital era, the use of websites is increasing rapidly, people like everything that is instant, even in terms of reading books, they prefer to read e-books rather than reading books conventionally. Therefore we need a website that is able to process data quickly so that readers will not wait long when they want to find the book or journal they want. In addition, the website also stores data for readers and stores it, but there are lots of irresponsible people who use their data illegally, so further security is needed for the convenience of readers, therefore researchers will analyze the solution to website security problems from xss attacks. and csrf and N+1 problems using Laravel whether it has an effect on the e-book website or not at all

Keywords*: Website, E-book, XSS, CSRF, N+1 Problem*

1. Pendahuluan

Dunia informasi saat ini seakan tidak bisa terlepas dari teknologi. Penggunaan teknologi oleh masyarakat menjadikan dunia teknologi semakin lama semakin canggih. Dengan kemajuan teknologi yang begitu pesat ini disebabkan oleh semakin cepatnya akses informasi dalam kehidupan sehari-hari. Internet sebagai jaringan terbesar sebagai sumber informasi yang telah menjadi kebutuhan banyak orang. Internet menyimpan berbagai jenis informasi yang tidak terbatas. Internet berperan sebagai sarana komunikasi, publikasi, serta sarana untuk mendapatkan berbagai informasi yang dibutuhkan. Menurut [1] ”internet merupakan sebuah jaringan yang saling berhubungan antar satu sama lainnya untuk keperluan komunikasi dan menyebarkan informasi dengan perangkat komputer. Bahkan untuk saat ini internet tidak saja terhubung pada perangkat komputer saja tapi juga pada handphone / android.” Munculnya internet ternyata dapat mempengaruhi penggunaan komputer yang semula komputer hanya dijadikan sebagai alat mesin tik, sekarang komputer sudah dijadikan sebagai alat untuk mengakses informasi dan juga alat pembaca e-Book. E-Book sendiri merupakan buku atau dokumen / artikel dalam format elektronik yang mempunyai banyak manfaat. Hampir setiap peralatan elektronik saat ini dilengkapi oleh *web browser*, mulai dari komputer, handphone ataupun *gadget* telah dilengkapi *web browser* yang biasa digunakan untuk menjelajah internet. *Web browser* dapat diartikan sebagai *tools* atau aplikasi yang digunakan untuk mencari informasi, membuka atau menjelajah halaman internet melalui *web*. *Web Browser* adalah sebuah *software* aplikasi yang digunukan untuk menerima, menampilkan, dan menerjemahkan informasi dari *world wide web* (WWW*)* [2]. Dan salah satu informasi itu dibuat dalam format HTML. Kode HTML yang kita buat akan diterjemahkan oleh *web browser* agar tampil seperti yang dirancang. Pada dasarnya seluruh *web browser* dapat menampilkan kode HTML sama baiknya, namun jika sudah berbicara mengenai desain halaman, tiap-tiap *browser* memiliki beberapa perbedaan.”

Framework adalah struktur konseptual dasar yang berisi 7 kumpulan fungsi untuk tujuan tertentu yang sudah siap untuk digunakan, sehingga pembuatan aplikasi dapat dilakukan dengan lebih cepat karena kode programnya tidak di buat dari awal. Laravel adalah *framework* bahasa pemrograman *Hypertext Preprocessor* (PHP) yang ditujukan untuk pengembangan aplikasi berbasis *web* dengan menerapkan konsep *Model View Controller* (MVC). *Framework* ini dibuat oleh Taylor Otwell dan pertama kali dirilis pada tanggal 9 Juni 2011. Laravel berlisensi *open source* yang artinya bebas digunakan tanpa harus melakukan pembayaran. Fitur-fitur modern Laravel yang sangat membantu *developer* dalam membuat aplikasi adalah *Bundles*, *Eloquent Object-Relational Mapping* (ORM), *Query Builder, Application Logic, Reverse Routing, Resource Controller, Class Auto Loading, View Composers, Blade, IoC Containers, Migration, Database Seeding, Unit Testing, Automatic Pagination, Form request, dan Middleware.* Pada saat sekarang *Hypertext Preprocessor* lebih lebih dikenal dengan singkatan *Hypertext Preprocessor* (PHP).

Sesuai dengan namanya, *Hypertext Preprocessor* digunakan untuk membuat *website* pribadi. *Hypertext Preprocessor* merupakan suatu bahasa pemograman yang digunakan *user* untuk membangun sebuah *web* saat ini dan dapat digunakan secara gratis. Menurut [3] menyimpulkan bahwa: Bahasa pemrograman *Hypertext Preprocessor* adalah bahasa pemrograman untuk membuat *web* yang *server-side scripting*. *Hypertext Preprocessor* digunakan untuk membuat halaman *web* dinamis. Sistem manajemen *database* yang sering digunakan dengan *Hypertext Preprocessor* adalah MySQL. Namun *Hypertext Preprocessor* juga mendukung Pengelolaan sistem *Database Oracle, Microsoft Access, Interbase, d-base, PostgreSQL*, dan sebagainya.

Menurut [4] *Cross Site Request Forgery* (CSRF) adalah serangan pada website yang dieksekusi atas wewenang korban, tanpa dikehendakinya. Sebuah serangan CSRF memaksa *browser log-on* korban untuk mengirim permintaan HTTP, termasuk *cookie* sesi dan informasi otentikasi, untuk aplikasi *web* yang rentan. *Cross Site Scripting* dikenal sebagai salah satu jenis serangan (*attack*) terampuh pada aplikasi *web*. Serangan ini disebabkan kegagalan dalam melakukan *validasi input user/client. Website* yang menyimpan *cookies* mengizinkan pengguna untuk datang kembali tanpa mengetikkan *username* dan *password*, akan menarik perhatian penyerang untuk lebih mengekplorasi fitur-fitur yang terdapat pada *website* setelah *login*. Cross site scripting atau serangan XSS adalah serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman *website* atau *web* aplikasi. Peretas akan mengeksekusi skrip berbahaya di *browser* korban dengan cara memasukkan kode berbahaya ke halaman *web* atau *web* aplikasi yang sah. Serangan ini dapat dilakukan menggunakan JavaScript, VBScript, ActiveX, Flash, dan bahasa sisi *client* lainnya. Meskipun *cross site scripting* termasuk jenis serangan *cyber* berbahaya, namun sebagian besar korban tidak menyadari bahwa mereka sedang diserang.

Di tahun 2016, Tanjila Farah, dkk "mengimplementasikan pengujian metodologi black-box dan menguji serangan XSS dan CSRF. Metodologi ini mendapatkan hampir 30% dari aplikasi web rentan terhadap serangan XSS dan CSRF. Hasilnya mereka telah menilai kerentanan XSS dan CSRF pada 500 aplikasi web di Bangladesh. Semua pengujian selesai secara manual. Fokus mereka adalah pada kerentanan XSS dan CSRF karena peringkat tinggi mereka di daftar OWASP" [5]. Di tahun 2018, Putra dan Wijaya "Melakukan bentuk penelitian dengan studi kasus. studi kasus merupakan strategi penelitian yang berusaha memahami kedinamisan dalam konteks tunggal yang dalam hal ini mengacu pada variabel tunggal pada Toko Mahkota Sport Sanggau serta objek penelitian berupa Membangun Keamanan Website e-commerce dari serangan *Cross Site Request Forgery* (CSRF). Metode penelitian yang digunakan penulis adalah metode penelitian dan pengembangan atau yang lebih dikenal dengan Research and Development"[4].

N+1 *Query* adalah suatu masalah yang terjadi ketika kita memerlukan untuk *load data child* dari relasi *parent-child* dimana kita melakukan banyak *query* select

pada *child data*. N+1 disini artinya adalah 1 *query* untuk parent dan N adalah jumlah *record* pada *table child*. Berdasarkan dari latar belakang masalah di atas, penulis ingin membuat sebuah analisis implementasi laravel 9 pada sebuah *website e-book* dalam mengatasi N+1 *Problem* serta mengatasi penyerangan CSRF dan XSS. Dimana dalam analisa ini akan membahas apakah N+1 *problem* serta penyerangan CSRF dan XSS dapat mempengaruhi kinerja *website e-book* dan keamanan *website* tersebut dengan menggunakan *Framework* Laravel 9.

2. Metodologi Penelitian

Bentuk penelitian yang penulis gunakan dalam penelitian ini adalah studi kasus. Studi kasus pada penelitian ini yaitu melakukan analisis implementasi laravel 9 pada website e-book dalam mengatasi n+1 problem serta mengatasi penyerangan csrf dan xss. metode penelitian yang digunakan penulis adalah metode penelitian dan pengembangan atau yang lebih dikenal dengan Research and Development. Sebagaimana dikemukakan oleh Sugiyono dalam [4], bahwa metode penelitian dan pengembangan adalah "metode yang digunakan untuk menghasilkan produk tertentu dan menguji keefektivan produk tersebut". Metode pengumpulan data merupakan bagian paling penting dalam sebuah penelitian. Ketersediaan data akan sangat menentukan dalam proses pengolahan dan analisa selanjutnya. Karenanya, dalam pengumpulan data harus dilakukan dengan teknik yang dapat menjamin bahwa data yang diperoleh adalah benar, akurat dan bisa dipertanggungjawabkan sehingga hasil pengolahan dan analisa data tidak bias. Adapun jenis data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder merupakan data yang berhubungan secara langsung dengan penelitian yang dilaksanakan dan bersumber dari youtube serta data lain yang diperlukan hasil searching di internet mengenai artikel-artikel, jurnal, dan adanya hasil dari penelitian sebelumnya yang dapat digunakan oleh peneliti sebagai bahan perbandingan dengan penelitian yang dilakukan.

Teknik pengumpulan data adalah cara-cara yang dilakukan untuk mencari, mengumpulkan dan memperoleh data untuk digunakan dalam melakukan penelitian, baik itu data yang diperoleh dengan survei langsung maupun dengan penggalian informasi. Untuk memperoleh data dan informasi dalam penelitian ini, penulis menggunakan teknik pengambilan data sebagai berikut :

1. Studi Dokumentasi

Dimaksudkan disini adalah untuk memperoleh data dan informasi dengan mempelajari dokumen-dokumen yang berhubungan dengan permasalahan yang penulis angkat sesuai dengan dokumen yang ada pada Mahkota Sport Sanggau. sumber-sumber berupa data, catatan, maupun laporan yang berhubungan dengan Mahkota Sport Sanggau untuk mendapatkan kelengkapan informasi yang mendukung penelitian sesuai permasalahan dan topik yang dibahas.

2. Akses *internet*

Akses *internet* digunakan untuk mencari data pendukung dari berbagai buku, *ebook*, maupun jurnal-jurnal yang disediakan di *internet*.

3. Hasil dan Pembahasan

Perkembangan website membaca *online* sangat berkembang pesat begitu pula seperti dalam hal pembuatannya, sangat banyak *framework* yang memudahkan para developer untuk membuat website pada bagian backend dan frontend pada website, biasanya ada banyak masalah yang akan dihadapi oleh developer. Contohnya keamanaan data pada website, keamanaan data sangat penting karena sangat sering dilakukannya pencurian data yang cukup *sensitive* dan masalah yang sering dihadapi adalah lambatnya data yang akan ditampilkan pada *website* saat melakukan *load* pada *database* saat dibuka oleh *user* yang biasanya dihadapi *website e-book* karena memiliki data yang sangat banyak. Dalam penelitian ini beberapa permasalahan yang akan dianalisis adalah kecepatan penampilan data pada saat *load* data ke *database* dan performa Laravel dalam mengatasi CSRF dan XSS Berdasarkan uraian diatas maka diperlukan cara untuk melindungi data pada *website* dan masalah yang terjadi ketika kita memerlukan untuk *load data child* dari relasi *parent child* dimana kita melakukan banyak *query select* pada *child data* atau disebut dengan N+1 Problem, maka digunakan lah Laravel dalam mengatasi keamaanan *website* menggunakan token_csrf yang ketat juga *blade engine* yang dimiliki oleh laravel yang dapat mengatasi serangan XSS dan dapat mengatasi N+1 Problem dengan melakukan *Eager Load* untuk meload data relasi ketika pertama kali digunakan. Dengan kata lain, ketika melakukan sebuah *query* parent model yang digunakan pada aktivitas tersebut merupakan model relasi yang belum diload.

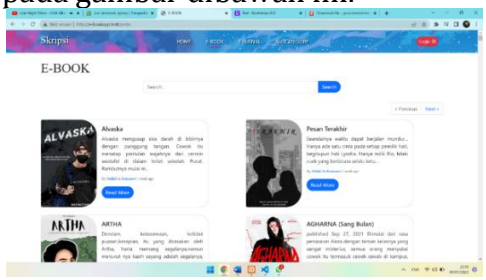
3.1 E-Book

Seiring dengan pesatnya berkembang e-learning, maka dibutuhkan buku yang dapat dikirim melalui teknologi internet dan dibaca dengan menggunakan *couter* atau perangkat lain yang disebut *ebook reader* dan karena buku tersebut bersifat elektronik, maka orang menyebutnya *ebook* atau buku eletronik. Buku elektronik adalah salah satu bentuk teknologi yang memanfaatkan komputer untuk menayangkan informasi multimedia dalam bentuk dinamis dan ringkas. Bermacam-macam jenis *e-book*, mulai dari yang paling sederhana yang sekedar memindahkan buku konvensional menjadi bentuk *softcopy* atau juga elektronik dan dapat dibaca melalui komputer. Dengan teknologi ini ratusan buku dapat disimpan dalam sekeping CD maupun flashdisk, karena umumnya ebook seperti ini berukuran kurang dari 5 Megabyte. Selain ebook dalam bentuk sederhana, ada juga ebook yang lebih kompleks yang mengintegrasikan tayangan video, efek animasi, audio, gambar, dan unsur multimedia lainnya. Dan biasanya ebook jenis ini memiliki ukuran yang lebih besar dibanding ebook yang hanya berisikan teks dan gambar saja [6].

Menurut [7] "Secara sederhana e-book dapat diartikan sebagai buku elektronik atau buku digital. E-book merupakan versi digital dari buku yang pada umumnya terdiri dari sekumpulan kertas yang memuat teks atau gambar. E-book merupakan sebuah bentuk perubahan dari buku cetak". Berikut adalah implementasi sistem dilakukan dengan membuat *website e-book* dengan menggunakan Laravel *9* yang nanti akan diujicoba untuk mengatasi *N+1 problem* , CSRF dan XSS. Adapun saat *website e-book* pertama kali dibuka akan menampilkan halaman *landing page*, hasil implementasi dari halaman *landing page* yang dapat dilihat pada gambar dibawah ini.

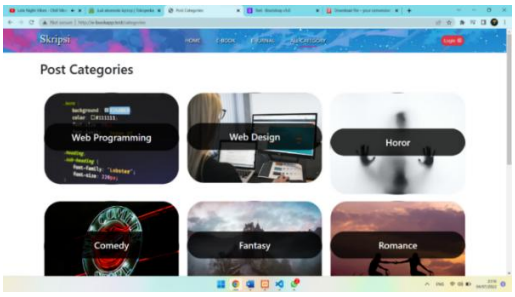
Gambar 1. Halaman Landing Page

Pada halaman *landing page* terdapat halaman *E-book, e-jurnal, serta all category* yang saling terhubung dan mengambil data-data dari *database*. Adapun halaman *E-book* yang berfungsi menampung semua buku yang ditulis oleh *user* agar dapat dilihat oleh *guest* ataupun *user* lainnya berikut merupakan tampilan halaman *E-book page* yang dapat dilihat pada gambar dibawah ini.



Gambar 2. Halaman E-book page

Pada halaman selanjutnya adalah halaman *all category* yang berfungsi mengambil data semua kategori yang dibuat oleh admin untuk para *user* agar lebih memiliki variasi dalam menulis cerita baru. Berikut merupakan tampilan halaman *all category page* yang dapat dilihat pada gambar dibawah ini.

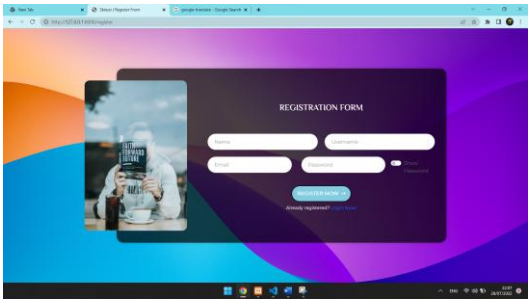


Gambar 3. Halaman All Categories

Website e-book memiliki halamn *login* yang berfungsi untuk para *user* agar dapat *login* untuk membuat cerita baru dan admin untuk membuat *category* ataupun mengubah akses para *user* tersebut. Berikut merupakan tampilan halaman *login page*.

Gambar 4. Halaman Login Form

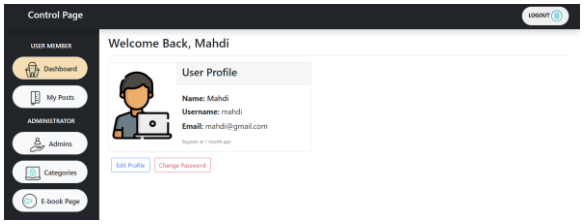
WebsiteE-book juga memiliki halaman *register* untuk mendaftarkan para *guest* yang hanya bisa melihat buku jadi dapat membuat buku pada *website e-book* dengan mendaftar pada halaman *register* agar para *guest* menjadi *user* yang memiliki akses yang lebih banyak dari para *guest*. Berikut merupakan tampilan halaman *register* yang dapat dilihat pada gambar di bawah ini.



Gambar 5. Halaman Registration Form

Setelah halaman *login* dan *register* para *user* akan masuk kedalam halaman control *page* atau halaman *dashboard* setelah *login* pada *website e-book*, halaman *dashboard* menampilkan semua data *profile user* ataupun admin yang *login* yang memiliki 2 tombol yaitu tombol edit *profile* dan change password yang memiliki fungsi untuk mengubah *profile* data *user* ataupun admin yang *login* dan tombol change password

memiliki fungsi merubah password *user* ataupun admin. Pada halaman *dashboard* ada 2 tipe berbeda yaitu admin dan *user* yang memiliki akses yang berbeda pada *website e-book*. Berikut merupakan tampilan halaman *dashboard* Admin yang dapat dilihat pada gambar berikut .

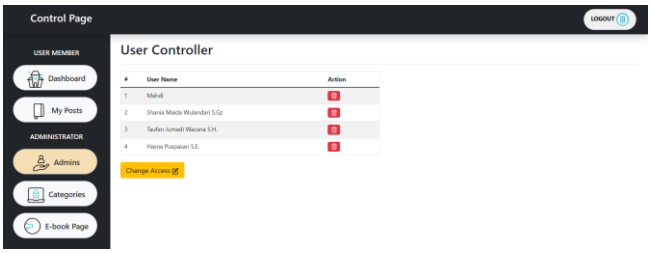


Gambar 6. Halaman Dashboard Page Admin

Dan berikut merupakan tampilan halaman *dashboard user* yang dapat dilihat pada gambar berikut .

Gambar 7. Halaman Dashboard Page User

Terakhir admin memiliki 2 akses halaman tambahan yaitu adalah halaman admins *page*, halaman ini menampilkan seluruh *user* yang mendaftar pada *website e-book* halaman ini berfungsi untuk para admin dapat merubah *user* menjadi admin ataupun sebaliknya admin dapat menurunkan admin yang lain menjadi *user*, halaman admins *page* juga memiliki fungsi agar admin dapat menghapus *user* tersebut. Berikut merupakan tampilan halaman admins *page* yang dapat dilihat pada gambar dibawah ini .



Gambar 8. Halaman Admins Page

3.2 Framework

Menurut [8] "*Framework* merupakan sebuah *software* atau aplikasi yang bisa dibilang seperti kerangka kerja yang fungsinya untuk memudahkan *developer* dalam mengembangkan aplikasi *website* yang ada".

Adapun Bahasa *Framework* yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Laravel

Menurut [9] Laravel merupakan *framework* bahasa pemrograman *Hypertext Preprocessor* yang memiliki banyak fitur dan sangat membantu developer dalam membangun sebuah aplikasi berbasis web. Laravel adalah sebuah *web development framework* yang didesain untuk meningkatkan kualitas aplikasi dengan mengurangi beban biaya pengembangan dan memudahkan proses maintenance serta meningkatkan produktifitas pekerjaan dengan kode program yang rapi dan terstruktur. Laravel memiliki beberapa kelebihan diantaranya; menggunakan *Command Line Interface* (CLI) Artisan, dapat menggunakan package manager *Hypertext Preprocessor* Composer, penulisan kode program yang rapi, singkat dan terstruktur, dan mudah dimengerti developer. Laravel adalah *web framework* berbasis bahasa pemrograman *Hypertext Preprocessor* yang bersifat *free* dan *open source*, Laravel dirilis dibawah lisensi MIT dengan kode sumber yang sudah disediakan oleh Github, Laravel dibuat oleh Taylor Otwell dan ditujukan untuk pengembangan aplikasi web yang mengikuti pola arsitektur model-view-controller (MVC) [10].

b. Bootstrap

Bootstrap merupakan salah satu jenis *framework* gabungan dari CSS dan Java script yang ditawarkan sebagai alternatif diantaranya *framework* lainnya yang dimana awal *framework* ini dikembangkan oleh Mark Otto dan Jacob Thornton dikantor Twitter dengan maksud untuk menghadirkan konsistensi ketahapan *intrface development* dalam membangun sebuah website [11].

3.3 N+1 Query Problem

N+1 *Query* adalah suatu masalah yang terjadi ketika kita memerlukan untuk *load data child* dari relasi *parent-child* dimana kita melakukan banyak *query* select pada child data. N+1 artinya adalah 1 *query* untuk *parent* dan N adalah jumlah *record* pada table child. Biasanya N+1 *Query* terjadi bila menggunakan *Eloquent Object Relation Maping. Eloquent Object Relation Maping* (ORM) adalah sebuah fitur dari Lumen / Laravel yang di dalamnya terdapat fungsi-fungsi *active record* (*query* SQL) untuk mengelola data di *database*. Dengan menggunakan *Eloquent ORM*, *database* bisa kita bungkus ke dalam objek, sehingga operasi *Create, Read, Update, Delete* (CRUD) pada tabel *database* dapat dilakukan tanpa melibatkan perintah atau *query* SQL sama sekali, bahkan sampai relasi antar tabelnya juga. Saat mengakses hubungan *Eloquent* sebagai properti, model terkait adalah *lazy loaded*. Ini berarti data hubungan tidak benar-benar dimuat sampai pertama kali mengakses properti. Namun, Eloquent dapat melakukan *Eager load* pada saat Anda menanyakan model induk. Dan dapat mengatasi mengurangi masalah N+1 *Query* [12].

3.3.1 Analisa N+1 Query Problem

N+1 *Query* sering terjadi bila menggunakan *Eloquent ORM*, *Eloquent Object Relation Maping* (ORM) adalah sebuah fitur dari Lumen / Laravel yang di dalamnya terdapat fungsi-fungsi *active record* (*query* SQL) untuk mengelola data di *database*. Artinya dengan *Eloquent ORM* ini kita dapat melakukan relasi antar tabel tanpa *query* sql sama sekali. Relasi antar 2 / 3 tabel hanya dengan menambahkan fungsi pada model tabel tersebut yang kembaliannya berisi "*hasMany*" ataupun "*belongsTo*". Berikut merupakan pemakaian *eloquent ORM* pada *website* e-book yang diteliti.

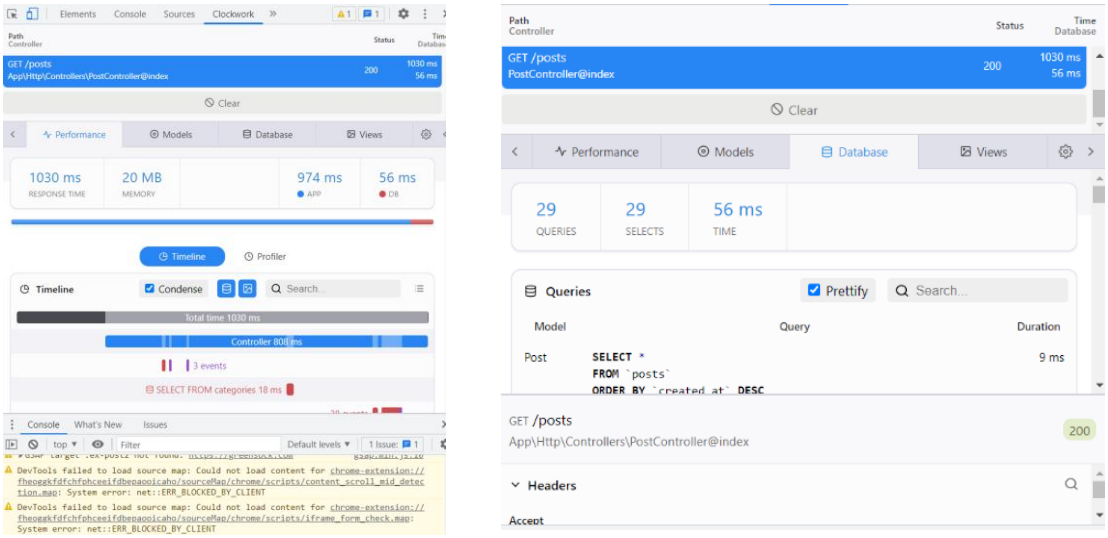
Gambar 9. Model User Menggunakan Eloquent ORM

Pada gambar 9 model *user* pada *website* e-book memiliki fungsi *posts* yang memiliki arti tabel *user* pada *database* berelasi dengan tabel *posts* pada *database*, fungsi diatas memiliki kembalian *hasMany* yang berarti 1 *user* boleh memiliki banyak *post* (buku). Pada gambar diatas merupakan penggunaan *Eloquent ORM* untuk melakukan relasi antar tabel tanpa menggunkan *query* sql sama sekali. Berikut merupakan gambar model post pada *website e-book.*

Gambar 10. Model Post Menggunakan Eloquent ORM

Pada gambar 10 model post pada *website e-book* memiliki fungsi *author* yang memiliki arti tabel posts pada *database* berelasi dengan tabel *user* pada *database*, fungsi diatas memiliki kembalian *belongsTo* yang berarti 1 post (buku) hanya milik 1 *user*. Pada gambar diatas merupakan penggunaan *Eloquent ORM* untuk melakukan relasi antar tabel tanpa menggunkan *query* sql sama sekali. Pada penjelasan diatas kita sudah cukup tau Permasalahan N+1 *query* problem, pada *website e-book* terjadinya N+1 *query problem* terjadi pada halaman e-book saat *load data* semua

buku yang ditulis oleh penulis yang dimana buku tersebut memiliki *category* dan *author* masing masing berelasi untuk mengetahui N+1 *query problem* ini kita dapat menggunakan *clockwork*. *Clockwork* adalah aplikasi yang dapat memberikan informasi tentang waktu proses aplikasi, termasuk data permintaan, metrik kinerja, *entri log, query basis data*, *query cache*, perintah *redis*, peristiwa yang dikirim, tugas yang diantrikan, tampilan yang dirender, dan lainnya - untuk permintaan HTTP dan ini hasil halaman *e-book* pada *website e-book* saat di *inspect* mengunakan *clockwork*.



Gambar 11. Perbandingan Hasil Clockwork Pada Halaman E-Book Sebelum dan Sesudah N+1 Terselesaikan

Dapat dilihat perbandingan hasil clockwork pada website sebelum dan sesudah menyelesaikan N+1 *query problemsI.* Pada gambar 11 dapat diketahui load data buku yang berjumlah 5000 data pada halaman *e-book* sebelum N+1 *query problem* memerlukan waktu 1030 ms dengan load data ke database 56 ms, dan setelah N+1 *query problem* tersebut 29 *query* dengan waktu 56 ms dengan *query* yang berulang ulang yang membuat *load data* menjadi lebih lama.

3.4 Cross-Site Scripting *(XSS)*

Menurut [5] XSS adalah serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman *website* atau *web* aplikasi. Peretas akan mengeksekusi skrip berbahaya di browser korban dengan cara memasukkan kode berbahaya ke halaman *web* atau *web* aplikasi yang sah. Serangan ini dapat dilakukan menggunakan JavaScript, VBScript, ActiveX, Flash, dan bahasa sisi klien lainnya. Kerentanan ini memungkinkan pencurian terhadap identitas pengguna, melewati batasan sistem, serangan malware dll. *reflected, stored* dan *DOM-based. Reflected* XSS dieksekusi melalui browser dan terjadi jika *website* menyediakan tempat bagi pengguna untuk melakukan masukan. Pada dasarnya terdapat tiga jenis serangan XSS yaitu:

3.2.1 *Stored XSS* (*Persistent XSS*)

Stored XSS merupakan jenis XSS yang paling merusak. Dalam *stored XSS*, skrip jahat yang disuntikkan akan disimpan secara permanen di server target, seperti *database*, forum pesan, *visitor log*, dan lain-lain.

3.2.2 *Reflected XSS* (*Non-persistent XSS*)

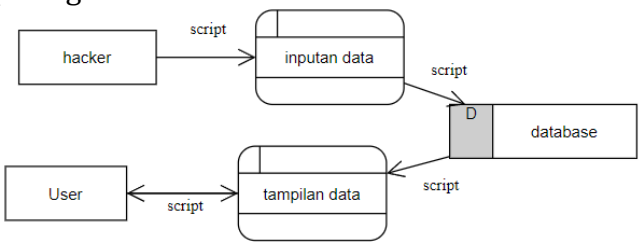
Reflected XSS terjadi ketika skrip berbahaya dipantulkan dari web aplikasi ke browser korban.

3.2.3 *DOM-based XSS*

Serangan ini terjadi jika *web* aplikasi menulis data ke *Document Object Model* (DOM) tanpa *sanitization* yang tepat. Penyerang dapat memanipulasi data ini untuk memasukkan konten XSS pada halaman *web* seperti kode Javascript yang berbahaya. [13].

3.4.1 Analisa Serangan XSS

Menurut [5] XSS adalah serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman *website* atau *web* aplikasi. Peretas akan mengeksekusi skrip berbahaya di *browser* korban dengan cara memasukkan kode berbahaya ke halaman *web* atau *web* aplikasi yang sah. Serangan ini dapat dilakukan menggunakan JavaScript, VBScript, ActiveX, Flash, dan bahasa sisi klien lainnya. Kerentanan ini memungkinkan pencurian terhadap identitas pengguna, melewati batasan sistem, serangan *malware* dll. *reflected, stored* dan *DOM-based. Reflected* XSS dieksekusi melalui *browser* dan terjadi jika *website* menyediakan tempat bagi pengguna untuk melakukan masukan. Adapun *data flow* diagram sistem serangan XSS dapat dilihat pada gambar dibawah ini.



Gambar 12. Data Flow Diagram XSS Attack

Berdasarkan gambar 3.5 diatas dapat diketahui serangan XSS dilakukan dengan memasukan script ke dalam inputan yang akan diolah oleh *website* untuk disimpan kedalam *database* yang akan ditampilkan pada *website* yang diakses oleh *user.*

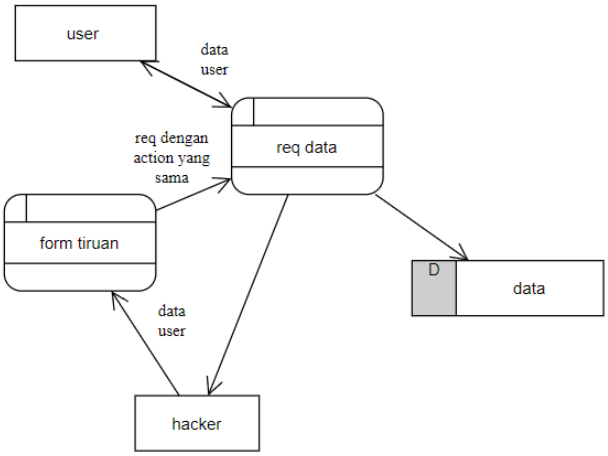
3.5 *Cross-site Request Forgery* (CSRF*)*

Menurut [3] '*Cross-site Request Forgery* (CSRF) adalah jenis serangan yang memanfaatkan otentikasi dan otorisasi target ketika permintaan palsu sedang dikirim ke *server web*. Oleh karena itu, kerentanan CSRF yang mempengaruhi pengguna seperti administrator, selama serangan *Cross-site Request Forgery* (CSRF), Serangan CSRF secara khusus menargetkan request data bukan pencurian data, karena penyerang tidak memiliki cara untuk melihat *respons*

terhadap permintaan yang dipalsukan. Dengan sedikit bantuan rekayasa sosial, penyerang dapat menipu pengguna aplikasi *web* untuk melakukan tindakan yang dipilih penyerang. Contoh akibat dari Serangan CSRF ini adalah mampu melakukan perubahan detail akun pada korban. Data pribadi seperti nama, alamat, bahkan sampai password korban bisa diubah dengan menggunakan teknik ini'.

3.5.1 Analisis Serangan CSRF

Menurut [3] '*Cross-site Request Forgery* (CSRF) adalah jenis serangan yang memanfaatkan otentikasi dan otorisasi target ketika permintaan palsu sedang dikirim ke *server web*. Adapun data flow diagram sistem serangan CSRF dapat dilihat pada gambar dibawah ini.



Gambar 13. Data Flow Diagram CSRF Attack

Berdasarkan data flow pada gambar di atas diketahui serangan CSRF dilakukan dengan hacker membuat form tiruan dengan *method* dan *action* yang sama dengan *website* yng ingin diserang setelah itu hacker melakukan req data ke *website* asli , website asli akan mengirim kan data *user* ke hacker.

4. Kesimpulan

Berdasarkan hasil analisis Implementasi laravel 9 pada sebuah *website e-book* dalam mengatasi N+1 *problem* serta mengatasi penyerangan CSRF dan XSS, maka didapakan kesimpulan sebagai berikut :

a. Pada *website e-book* yang telah di implentasikan Laravel 9 dalam pembuatan sistem nya yang memiliki halaman *e-book* yang bertugas untuk menampilkan seluruh data buku, *category* dan *author* masing masing buku, dalam hal ini digunakan lah *eloquent ORM* untuk pembuatan relasi antar 3 tabel tersebut dan menghasilkan 1 masalah yaitu N+1 *query problem* yang jika tidak diselesaikan maka akan menghasilkan *query* yang berulang-ulang dan sangat banyak yang membuat

load data halaman *e-book* sangat lambat dan jika diselesaikan menggunakan *eager load* maka hanya menghasilkan *query* yang diperlukan saja. Agar dapat membuat user menjadi nyaman dan efisiensi waktu untuk para *user* dan *guest* yang ingin membaca buku.

b. Analisis serangan CSRF dan XSS dalam *website e-book* yang telah di implementasi mengunakan Laravel 9 sangat efektif. Laravel 9 melidungi serangan dengan cukup baik dengan mengatasi XSS menggunakan *blade template* yang otomatis mengubah semua hasil yang dikeluarkan sudah melewati menggunakan htmlspecialchart yang berguna untuk membuat semua *script* ataupun *code* menjadi *text* biasa sedangkan CSRF sendiri Laravel 9 langsung melidungi tanpa perlu *mencoding* apapun karena bersifat otomatis yang semua form harus diberikan CSRF_Token agar Laravel 9 mau memproses form tersebut ke dalam *database*.

DAFTAR PUSTAKA

[1] A. Wibawanto, "Penggunaan Internet dalam Perpustakaan," *Pustakaloka*, vol. 10, no. 2, p. 191, 2018, doi: 10.21154/pustakaloka.v10i2.1472.

[2] M. K. Taryana Suryana, "Fungsi Web Browser Memilih Aplikasi Editor HTML Text Editor Notepad ++," *Repository.Unikom.Ac.Id*, pp. 1–9, 2020, [Online]. Available: https://repository.unikom.ac.id/68227/1/Materi 1 Pengenalan HTML.pdf

[3] M. Sitinjak Daniel Dido Jantce TJ and J. Suwita, "Analisa Dan Perancangan Sistem Informasi Administrasi Kursus Bahasa Inggris Pada Intensive English Course Di Ciledug Tangerang," *Ipsikom*, vol. 8, no. 1, pp. 1–19, 2020.

[4] H. P. Siregar and T. Wijaya, "Membangun Keamanan Dari Serangan Cross-Site Request Forgery (CSRF)," *Inf. Commun. Technol. Tour.*, vol. 1, no. 1, pp. 58–68, 2018, [Online]. Available: http://sisfotenika.stmikpontianak.ac.id/index.php/enter/article/view/795/559

[5] P. Kerentanan, D. A. N. Penetrasi, I. M. E. Listartha, G. Arna, J. Saskara, and S. Santyadiputra, "KEAMANAN PADA APLIKASI WEB MANAJEMEN SKRIPSI PRODI XYZ Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications," vol. 4, no. 2, pp. 1–14, 2021.

[6] I. F. Meutia, "Owned by Author(s), published by," no. May, 2021.

[7] Z. D. Martha, E. P. Adi, and Y. Soepriyanto, "E-book berbasis mobile learning," *J. Kaji. Teknol. Pendidik.*, vol. 1, no. 2, pp. 109–114, 2018, [Online]. Available: http://journal2.um.ac.id/index.php/jktp/article/view/3705/2775.

[8] K. Wijaya, R. Supariyanto, and E. Istiawan, "Implementasi Framework Bootstrap Dalam Perancangan Sistem Penerimaan Mahasiswa Baru Pada Sekolah Tinggi Ilmu Tarbiyah Al-Quran Al-Ittifaqiah," *J. Sist. Inf.*, vol. 04, no. 02, pp. 7–11, 2020.

[9] Moch Zawaruddin Abdullah, Mungki Astiningrum, Yuri Ariaynto, Dwi Puspitasari, and Atiqah Nurul Asri, "Rancang Bangun Sistem Informasi Akuntansi Berbasis Website menggunakan Framework Laravel," *J. Pengabdi. Polinema Kpd. Masy.*, vol. 8, no. 1, pp. 74–80, 2021, doi: 10.33795/jppkm.v8i1.64.

[10] D. Saputra, "Analisis Perbandingan Performa Web Service Rest Menggunakan Framework Laravel, Django Dan Ruby On Rails Untuk Akses Data Dengan," *J. Bangkit Indones.*, vol. 7, no. 2, p. 17, 2018, doi: 10.52771/bangkitindonesia.v7i2.90.

[11] J. Martin and A. R. Tanaamah, "Perancangan Dan Implementasi Sistem Informasi Penjualan Berbasis Desktop Website Menggunakan Framework Bootstrap Dengan Metode Rapid Application Development, Studi Kasus Toko Peralatan Bayi 'Eeng Baby Shop,'" *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 1, p. 57, 2018, doi: 10.25126/jtiik.201851547.

[12] A. Adithya, "Mengatasi Permasalahan N+1 Query di Laravel," *Lab Informatika*, 2019. https://www.lab-informatika.com/mengatasi-permasalahan-n1-query-di-laravel) (accessed Jun. 30, 2022).

[13] W. S. M. Faizal Kurniawan, "Optimasi Metode Otomatisasi Penghilangan Kerentanan Terhadap Serangan Xss Pada Aplikasi Web," *Tek. Inform.*, vol. XV, pp. 12–19, 2020, [Online]. Available: http://ejournal.stmik-wp.ac.id.