

# IMPLEMENTASI FRAMEWORK LARAVEL DAN ENKRIPSI IONCUBE ENCODE UNTUK MENINGKATKAN KEAMANAN PADA PERPUSTAKAN DIGITAL

Hasirun<sup>1\*</sup>, Ari Budi Riyanto<sup>2</sup>

<sup>1,2</sup> Universitas Perwira Purbalingga, Purbalingga, Jawa Tengah, 533133, Indonesia

e-mail: <sup>\*</sup>hasirun@unperba.ac.id, <sup>2</sup>aribudiriyanto@unperba.ac.id

---

Diterima  
24-11-2024

Direvisi  
30-11-2024

Disetujui  
31-12-2024

---

**Abstract:** Information system is one of the things needed for an agency or company. In developing an information system, it is necessary to analyze the needs and risks that will be faced. One of the system developments is the digital library "Edu-Media" which is a website-based system that contains learning content such as videos, ebooks, music and assignments. The library development process uses Laravel because this framework can facilitate the development process and has a high level of security. Based on testing with the OWASP ZAP 2 application, there are no threats that have a high risk. The digital library is a website that is distributed along with server devices, therefore it is necessary to protect the PHP program code so that it cannot be duplicated or modified. The method used to protect the program code is by encrypting the program code using PHP ioncube encoder. The results of this ioncube encryption can be used to protect program code because it can be program code into bytecode which is not easy for humans to understand.

**Keywords:** Laravel; Framework; Encryption; Ioncube; Encoder

**Abstrak:** Sistem informasi merupakan salah satu hal yang diperlukan bagi sebuah instansi atau perusahaan. Dalam pengembangan sistem informasi diperlukan analisis kebutuhan dan resiko yang akan dihadapi. Salah satu pengembangan sistem yaitu pada perpustakaan digital "Edu-Media" yang merupakan sistem berbasis website yang berisi konten mengenai pembelajaran seperti video, ebook, musik dan tugas. Proses pengembangan perpustakaan menggunakan laravel karena *framework* ini dapat mempermudah dalam proses pengembangan serta memiliki tingkat keamanan yang tinggi. Berdasarkan pengujian dengan aplikasi OWASP ZAP 2 tidak ditemukan ancaman yang memiliki resiko tinggi. Perpustakaan digital merupakan website yang didistribusikan beserta perangkat *server*, oleh karena itu perlu adanya perlindungan pada kode program PHP agar tidak bisa diduplikasi maupun dimodifikasi. Metode yang digunakan untuk melindungi kode program yaitu dengan cara melakukan enkripsi kode program dengan menggunakan PHP ioncube encoder. Hasil dari enkripsi ioncube ini dapat digunakan melindungi kode program karena dapat kode program menjadi *bytecode* yang tidak mudah untuk dipahami oleh manusia.

**Kata kunci:** Laravel; Framework; Enkripsi; Ioncube; Encoder

## I. PENDAHULUAN

Sistem informasi merupakan salah satu hal yang menjadi perhatian pada suatu instansi atau perusahaan. Dengan perkembangan teknologi saat ini setiap instansi berlomba untuk mengembangkan sistem informasi agar dapat membantu untuk menyelesaikan pekerjaan yang ada. Dalam melakukan pengembangan sistem informasi tidak hanya sekedar bisa dipakai oleh pengguna akan tetapi harus diperhatikan dari hal keamanan dan kenyamanan bagi pengguna sistem. Sistem informasi ini bisa saja dalam bentuk website ataupun berbasis mobile tergantung dengan kebutuhan dari perusahaan itu sendiri. Website dapat diartikan sebagai kumpulan halaman informasi yang dapat

diakses oleh siapapun dan dimanapun selama bisa terhubung ke jaringan internet (Romadhon & Yudhistira, 2021).

Dalam melakukan pengembangan sistem informasi berbasis website ada beberapa hal yang perlu diperhatikan seperti bahasa pemrograman yang digunakan, perkembangan bahasa pemrograman, dan komunitas pengembang atau pengguna. Bahasa pemrograman yang cukup populer yaitu Hypertext Preprocessor (PHP) yang merupakan suatu bahasa pemrograman yang bersifat server-side (Endra et al., 2021). Sedangkan yang dimaksud dengan server-side yaitu script yang hanya dapat berjalan disisi server dan dapat diartikan bahwa bahasa pemrograman PHP ini terhubung langsung ke kumpulan data atau database. Bahasa pemrograman PHP juga merupakan bahasa yang open-source yang berarti bahwa pengguna dapat mengubah sesuai dengan keinginannya (Nur Ahzan et al., 2023). Hal ini dikarenakan source-code PHP tidak bisa dcompile menjadi executable file melainkan hanya diunggah pada suatu server (Eka Pratama, 2020).

PHP merupakan bahasa pemrograman yang bersifat open-source yang memiliki beberapa kelemahan seperti source-code mudah diduplikasi, dimodifikasi atau dapat digunakan kembali di sistem lain tanpa diketahui oleh pembuat kode. Disamping itu tingkat keamanan PHP ini masih rendah karena memiliki celah kerentanan seperti SQL Injection (Edy Listartha et al., 2022). Kurangnya dokumentasi juga menjadi salah satu kelemahan yang membuat developer mengalami kesulitan dalam pengembangan sistem. Akan tetapi dengan banyaknya komunitas dan ekosistem pengguna, bahasa pemrograman ini terus mengalami perkembangan seperti terbentuknya kerangka kerja atau framework. Framework itu sendiri diartikan sebagai kerangka kerja yang terdiri dari kumpulan library yang memiliki peran yang berbeda-beda akan tetapi terbagi digabung oleh komunitas developer dengan tujuan agar dapat mempermudah dalam pengembangan website dan mengurangi aktivitas menulis kode program yang berulang sehingga pekerjaan dapat diselesaikan dengan cepat.

Perkembangan framework PHP yang dapat menarik perhatian pengembang website karena dengan menggunakan framework ini pengembangan web akan lebih sederhana dan lebih mudah karena sudah terdapat dokumentasi yang lengkap serta banyaknya komunitas pengguna sehingga akan mudah untuk melakukan kolaborasi maupun diskusi. Adapun beberapa framework yang cukup populer yaitu yii, codeigniter, laravel, symfony dan lain-lain. Secara umum framework yang dikembangkan menggunakan pola MVC (Model View Controller) yang membuat penulisan kode program lebih mudah dipahami karena sintak yang bersih dan fungsional yang dapat mengurangi banyak waktu pengembangan (Sari et al., 2022).

Laravel merupakan salah satu framework PHP yang paling populer dan kuat dalam pengembangan aplikasi web. Dirilis pada tahun 2011, Laravel dengan cepat menjadi favorit di kalangan pengembang berkat desain yang elegan, sintaksis yang ekspresif, dan berbagai fitur canggih yang disediakan. Framework ini mengadopsi pola desain Model-View-Controller (MVC), yang memisahkan logika aplikasi, tampilan, dan pengelolaan data secara terstruktur. Salah satu daya tarik utama Laravel adalah fitur Eloquent ORM, yang memudahkan interaksi dengan basis data dan menghilangkan kerumitan dalam mengelola model data. Framework ini menyediakan berbagai cara untuk menghindari kerentanan umum dan melindungi aplikasi dari serangan keamanan seperti pengamanan sql injection, perlindungan dari cross-site scripting (XSS), perlindungan CSRF (Cross-Site Request Forgery), enkripsi hashing dan pengamanan authorization. Sedangkan kelebihan lain ketika menggunakan framework laravel yaitu terdapat komunitas yang luas sehingga banyak library yang telah dikembangkan dan dapat digunakan untuk menyelesaikan proyek pengembangan baik dari skala rendah hingga menengah (Endra et al., 2021).

Pada proses pengembangan website tidak hanya memperhatikan bahasanya pemrograman yang digunakan akan tetapi harus memperhatikan bagaimana cara mengamankan data baik dalam mengelola maupun dalam penyimpanannya. Salah satu cara untuk mengamankan data yaitu dengan enkripsi yaitu dengan cara mengubah informasi atau data agar tidak dapat dipahami oleh pihak yang tidak berwenang. Tujuan dari enkripsi adalah untuk menjaga keamanan dan kerahasiaan data terutama apabila data diakses oleh pihak yang tidak sah. Adapun cara yang dapat dilakukan dalam menggunakan enkripsi yaitu melakukan enkripsi pada setiap data yang ada di database atau

melakukan enkripsi pada kode program yang ada pada sistem itu sendiri. Proses enkripsi yang dilakukan langsung pada data biasanya pada penyimpanan kata sandi (password) karena data ini merupakan data yang cukup beresiko apabila dapat dibaca oleh pihak yang tidak berwenang. Adapun metode yang sering digunakan dalam melakukan enkripsi data seperti MD5, Hash, SHA1. Sedangkan untuk melakukan enkripsi kode program bisa menggunakan php encoder seperti zend guard atau ioncube dan reverse cipher 4. Tujuan melakukan enkripsi kode program ini tidak hanya untuk melindungi data akan tetapi juga dapat melindungi kode program agar tidak mudah dipahami serta susah untuk dimodifikasi.

Enkripsi dapat dilakukan dengan berbagai metode salah satunya yaitu dengan mengubah kode program menjadi kode yang tidak dapat dimengerti oleh manusia seperti yang dilakukan oleh (Arisandi, 2017) dengan menggunakan algoritma AES dimana semua kode program dienkripsi dengan tujuan agar source code sulit untuk dibaca dan untuk menghindari pencurian kode program, walaupun semua kode tidak bisa dipahami akan tetapi masih bisa di eksekusi seperti sebelum dienkripsi. Metode lain yang dapat digunakan untuk melakukan enkripsi PHP yaitu dengan zend guard atau ioncube encoder. Dengan menggunakan aplikasi ini kode program PHP dienkripsi menjadi bytecode dan menggunakan fitur dynamic keys yang unik yang dapat meningkatkan lapisan keamanan (PHP Encoder 12, 2023). Untuk menjalankan file yang telah dienkripsi pada server perlu dilakukan instalasi library loader sesuai dengan aplikasi yang sudah dipilih. Penambahan library loader agar server mengenali jenis enkripsi yang digunakan serta dapat membaca dan menjalankan kode program.

Beberapa kelemahan yang ada pada bahasa pemrograman PHP membuat peneliti tertarik untuk menemukan sebuah metode yang dapat meningkatkan keamanan baik pada sumber kode atau dalam keamanan data. Salah satu cara untuk meningkatkan keamanan ketika menggunakan bahasa pemrograman PHP yaitu dengan menggunakan framework laravel karena memiliki tingkat keamanan yang lebih baik dibandingkan PHP native (Endra et al., 2021). Peningkatan keamanan kode program juga dilakukan oleh (Artono Dwi Ramadhan et al., 2020) yang membahas tentang implementasi teknik obfuscation dengan algoritma reverse cipher 4 pada source code PHP, hasil dari penelitian ini bahwa dengan menggunakan algoritma reverse cipher 4 dapat melakukan enkripsi pada source code asli (plaintext) menjadi source code obfuscated(chipertext) dengan tujuan agar tidak mudah untuk duplikasi dan dimodifikasi. Adapun penelitian (Rahmatulloh & Munir, 2015) yang membahas tentang ancaman Reverse Engineering Source Code PHP dimana dalam penelitian ini menghasilkan bahwa teknik obfuscation code dengan menggunakan algoritma RC4 dan encoding 85 karakter ASCII dapat memberikan perlindungan pada source code php sehingga dapat menjaga hak kekayaan intelektual.

Berdasarkan penelitian yang telah dilakukan terhadap peningkatan keamanan dalam bahasa pemrograman PHP maka dalam penelitian ini akan melakukan implementasi framework laravel serta melakukan perlindungan source code dengan menggunakan enkripsi ioncube encoder. Implementasi dari framework laravel ini karena jika menggunakan php native masih terdapat beberapa kelemahan seperti SQL injection oleh karena itu untuk meningkatkan keamanan website diperlukan kerangka kerja atau framework yang lebih baik. Penelitian ini dilakukan pada salah satu produk dalam bentuk website yang pengembangannya menggunakan framework laravel. Produk yang dimaksud merupakan sebuah web perpustakaan digital dengan nama "Edu-Media" dimana pada produk ini dijual dengan paket beserta dengan perangkat kerasnya yaitu dalam bentuk server lokal yang sudah terinstall website perpustakaan digital. Adapun konten yang ada pada perpustakaan digital ini yaitu terdiri dari ebook, musik dan video. Dengan adanya distribusi penjualan ini perlu dilakukan keamanan khusus untuk melindungi data atau konten yang ada pada web perpustakaan digital. Selain itu untuk menjaga kode program perlu dilakukan enkripsi dengan menggunakan ioncube encoder dengan tujuan untuk menjaga keaslian kode program sehingga tidak mudah untuk diduplikasi, dimodifikasi, serta menjaga hak cipta dari produk perpustakaan digital.

Agar penelitian ini dapat berjalan secara terarah maka perlu ditentukan beberapa hal seperti rumusan masalah, batasan penelitian, tujuan penelitian dan manfaat dari penelitian. Hal yang pertama dilakukan yaitu menentukan rumusan masalah dari penelitian ini, adapun rumusan dari

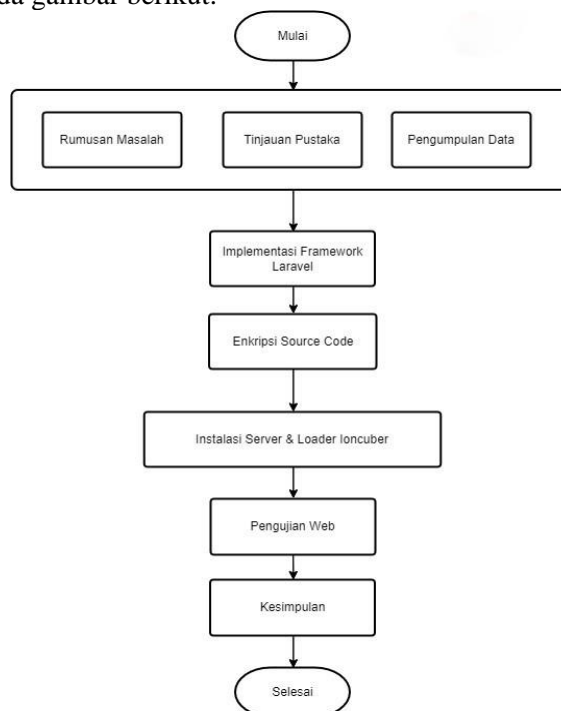
penelitian ini yaitu bagaimana cara untuk meningkatkan keamanan dalam pengembangan sistem berbasis website pada perpustakaan digital “Edu-media” dan cara untuk mengimplementasi enkripsi ioncube encode untuk melindungi kode program agar tidak mudah untuk diduplikasi dan dimodifikasi oleh pihak yang tidak berwenang. Selain itu untuk melakukan evaluasi terhadap penelitian ini juga diperlukan sebuah pengujian yang nantinya dapat dijadikan sebagai kesimpulan untuk menentukan tingkat kewanaman dalam pengembangan sebuah sistem berbasis website.

Batasan pada penelitian ini ditentukan agar kegiatan penelitian lebih fokus untuk membahas permasalahan yang ditangani, ada beberapa batasan pada penelitian ini yaitu membahas tentang implementasi framework laravel pada pengembangan web perpustakaan digital “Edu-media” untuk meningkatkan kewanaman data, objek penelitian yaitu web perpustakaan digital dengan nama “Edu-Media”, Enkripsi yang digunakan dalam penelitian ini dengan menggunakan ioncube encoder yang berfungsi untuk melakukan enkripsi source code PHP. Proses enkripsi yang dilakukan hanya dari bahasa pemrograman saja yaitu php dengan framework laravel.

Adapun tujuan dari penelitian yang akan dilakukan yaitu dapat memberikan kontribusi dalam melakukan implementasi enkripsi ioncube encoder pada framework laravel, dapat meningkatkan keamanan data dalam pengembangan website terutama pada objek penelitian yaitu perpustakaan digital “Edu-media”, dapat mengetahui tingkat kewanaman enkripsi dengan menggunakan ioncube serta dapat mengetahui bagaimana cara untuk melindungi source code agar tidak mudah untuk dipahami oleh manusia sehingga tidak dapat diduplikasi maupun dimodifikasi. Sedangkan manfaat dari penelitian ini adalah dapat meningkatkan kewanaman website dengan melakukan implementasi framework laravel dan melindungi kode program PHP agar tidak terjadi duplikasi dan dimanfaatkan oleh orang lain tanpa diketahui oleh pembuat kode program.

## II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini dengan menerapkan metode research and development (R & D) pada web perpustakaan digital untuk meningkatkan keamanan baik pada data maupun dari kode program yang telah dibuat. Berikut ini merupakan tahapan yang dilakukan dalam penelitian seperti pada gambar berikut:



Gambar 1. Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini dimulai dari menentukan rumusan masalah, tinjauan pustaka dan pengumpulan data yang diperlukan untuk penelitian ini. Kemudian tahapan selanjutnya yaitu melakukan implementasi framework laravel yang merupakan kerangka kerja yang digunakan untuk pengembangan website perpustakaan digital. Setelah proses pengembangan selesai maka langkah selanjutnya yaitu melakukan enkripsi source code dengan tujuan agar tidak mudah dimengerti oleh manusia sehingga tidak dapat diduplikasi maupun modifikasi. Tahapan selanjutnya yaitu melakukan instalasi server beserta dengan paket loader yang berfungsi untuk mengenali enkripsi agar dapat dijalankan pada server. Ketika proses enkripsi berhasil dan bisa berjalan pada sisi server maka tahapan yang terakhir yaitu melakukan pengujian web dan menarik kesimpulan dari kegiatan penelitian ini. Adapun tahapan yang dilakukan bertujuan untuk mengetahui tingkat keamanan baik pada data perpustakaan maupun kode program website.

Kegiatan penelitian ini dilakukan pada saat pengembangan web perpustakaan digital dengan nama "Edumedia" yang merupakan salah satu produk dari perusahaan CV. Braling Komputer yang berlokasi di Purbalingga, Jawa Tengah. Sedangkan waktu yang digunakan untuk penelitian ini yaitu pada bulan juni-juli 2023 mulai dari tahapan pengembangan sampai dengan pengujian dari produk perpustakaan digital Edumedia. Sedangkan untuk mendukung penelitian ini diperlukan beberapa data yang berkaitan dengan pengembangan website dan jenis enkripsi. Metode pengumpulan data yang dilakukan dengan cara menggunakan studi pustaka dari jurnal atau artikel yang membahas tentang implementasi laravel dan enkripsi data. Alat dan bahan yang digunakan dalam penelitian ini adalah sebagai berikut:

Tabel 1. Alat dan Bahan

No	Nama	Keterangan
1	CPU Mini Server	Mini Server dengan spesifikasi core i3-7200, 8 GB RAM, SSD 512 GB yang terinstall sistem operasi ubuntu 20.04 yang berfungsi sebagai server lokal perpustakaan digital
2	Web Perpustakaan Digital	Web yang digunakan sebagai objek penelitian
3	PHP Ioncube Encoder	Enkripsi Source Code Perpustakaan Digital
4	OWASP ZAP	Berfungsi untuk pengujian kerentanan website
5	Laptop	Untuk menjalankan web dan aplikasi OWASP ZAP

Analisa yang dilakukan dalam penelitian ini yaitu berkaitan dengan proses pengembangan sebuah sistem berbasis website dan bagaimana cara untuk melindungi kode program agar tidak bisa ditiru oleh orang lain. Dalam pengembangan sebuah website diperlukan sebuah bahasa pemrograman yang digunakan untuk menghubungkan antara database dengan user interface website. akan tetapi dalam pengembangan website jika hanya menggunakan PHP saja masih terdapat beberapa kelemahan terutama dalam keamanan data. Kelemahan pada PHP native yang tidak bisa dihindari yaitu SQL injection, Cross Site Scripting dan Brute Force. Untuk mengatasi hal tersebut diperlukan sebuah kerangka kerja atau framewok php yang dapat meningkatkan keamanan seperti yang dilakukan oleh (Aryanti et al., 2021) yang melakukan analisis pada web yang menggunakan php native dan juga web dengan menggunakan framework codeigniter, hasil dari penelitian tersebut menjelaskan bahwa php native memiliki celah keamanan yang lebih banyak dibandingkan dengan web yang menggunakan framework codeigniter. Penelitian juga dilakukan oleh (Lapatta, 2022) yang membahas tentang implementasi framework laravel yang digunakan untuk pengembangan sistem manajemen data dosen, alasan utama dalam implementasi laravel karena framework ini dapat mempermudah dalam pengembangan website serta memiliki tingkat keamanan data yang tinggi. Disisi lain untuk menjaga hak cipta dalam suatu website perlu dilakukan keamanan tambahan terutama pada objek penelitian ini yaitu perpustakaan digital edumedia karena kode program ini didistribusikan langsung ke pelanggan dengan tujuan agar tidak bisa ditiru oleh pihak yang tidak berwenang. Adapun cara yang dapat dilakukan yaitu dengan melakukan enkripsi

kode program dengan menggunakan algoritma tertentu, sedangkan dalam penelitian ini untuk melindungi kode program perpustakaan digital edumedia dengan menggunakan PHP ioncube encoder.

### III. HASIL DAN PEMBAHASAN

#### 1. Implementasi Laravel

Implementasi laravel merupakan tahapan pertama yang dilakukan dalam penelitian ini. Versi framework laravel yang digunakan dalam penelitian adalah versi 6 dan menggunakan php versi 7.2. Penggunaan framework laravel ini karena dapat mempermudah dalam proses pengembangan website serta memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan menggunakan *php native*. Dalam implementasinya ada beberapa *library* dan konfigurasi seperti pada gambar 2 berikut ini:

```

1  {
2      "name": "laravel/laravel",
3      "type": "project",
4      "description": "The Laravel Framework.",
5      "keywords": [
6          "framework",
7          "laravel"
8      ],
9      "license": "MIT",
10     "require": {
11         "php": "^7.2.5|^8.0",
12         "barryvdh/laravel-dumpdf": "^2.0",
13         "dompdf/dompdf": "^2.0",
14         "fideloper/proxy": "^4.4",
15         "laravel/framework": "^6.20.26",
16         "laravel/tinker": "^2.5",
17         "laravel/ui": "1.*",
18         "spatie/laravel-permission": "3.18"
19     },
20     "require-dev": {
21         "facade/ignition": "^1.16.15",
22         "fakerphp/faker": "^1.9.1",
23         "mockery/mockery": "^1.0",
24         "nunomaduro/collision": "^3.0",
25         "phpunit/phpunit": "^8.5.8|^9.3.3"
26     },
27     "config": {
28         "optimize-autoloader": true,
29         "preferred-install": "dist",
30         "sort-packages": true
31     },
32     "extra": {
33         "laravel": {
34             "dont-discover": []
35         }
36     }

```

Gambar 2. Implementasi Laravel

#### 2. Enkripsi Ioncube

Tahapan yang kedua dalam penelitian ini adalah melakukan enkripsi terhadap kode program PHP yang ada pada framework laravel. Proses enkripsi menggunakan aplikasi PHP encoder dengan nama ioncube. Tujuan proses enkripsi agar kode program yang telah dibuat tidak mudah untuk dipahami oleh manusia sehingga dapat mengurangi tingkat resiko pencurian kode program yang dapat dilakukan dengan cara duplikasi atau modifikasi tanpa diketahui oleh pembuat kode program. Web perpustakaan digital nantinya akan dijual beserta perangkat servernya, oleh karena itu perlu adanya perlindungan khusus untuk kode program tersebut. Adapun versi ioncube encoder yang dipakai dalam penelitian ini versi 10.2 dan melakukan enkripsi PHP pada versi 7.2. Kode program asli atau yang belum dilakukan enkripsi dapat dilihat pada gambar 3 sedangkan hasil dari enkripsi dapat dilihat pada gambar 4 seperti berikut ini:

```

LoginController.php X CatatanController.php Login.php
app > Http > Controllers > Auth > LoginController.php
1 <?php
2
3 namespace App\Http\Controllers\Auth;
4
5 use App\Http\Controllers\Controller;
6 use App\Providers\RouteServiceProvider;
7 use Illuminate\Foundation\Auth\AuthenticatesUsers;
8 use Illuminate\Support\Facades\DB;
9 use Illuminate\Http\Request;
10 use Illuminate\Http\Response;
11 use App\Models\UserModel;
12 use Session;
13 use Auth;
14
15
16 class LoginController extends Controller
17 {
18     /**
19      *
20      * Login Controller
21      *
22      *
23      * This controller handles authenticating users for the application and
24      * redirecting them to your home screen. The controller uses a trait
25      * to conveniently provide its functionality to your applications.
26      *
27      */
28     private $user;
29     use AuthenticatesUsers;
30
31
32     /**
33      * Where to redirect users after login.
34      *
35      * @var string
36      */
37     protected $redirectTo = RouteServiceProvider::HOME;
38
39     /**
40      * Create a new controller instance.

```

Gambar 3. Kode Program

```

LoginController.php X
app > Http > Controllers > Auth > LoginController.php
1 <?php //004fb
2 if(!extension_loaded('ionCube Loader')){$_oc=strtolower(substr(PHP_UNAME(),0,3));$_ln='ioncube_loader_'.$_oc.'_'.substr(PHP_VERSION(),0,3).('$_oc=='win'
3 ?)
4 HR+cPu1FOHA6/bacNwFqCKZhgZtiJQcCKTICS30TqjBhJPGHpk0xmVd/g3hBo+Hvh4uLejC81Q
5 MthpDGNahbXysAQuajLi.feqMwlrWddZehevGohr0JHOZX8q1BFZsV0akSrjIhdZrKbrIdLcPo
6 qIeowc-vhxfgqrRiZA5dV4Q5Fob1Cox0qamK2IkDjhtRVnxfwQASWuG1Vr:j7nzjZNF++[Y0YITdX
7 G0P17K+YM8i+vJg29o3k0AHAvu1GK28LSY/yvR9kdxADirDpMmEfhCldtMqNzo3NarqxY0R3p
8 me3hwQzYHVQ0dAogv5yPkt5ea0de33i8ZJLxRw90v+fg1o9NX529302Arndrq+6W0kK6c/
9 jclRrRjkh9m8zCnTvjt9b1V1AC0TLvjDQ73QQ9PHfx1yufdyvJ6RHgMM81sUz71DtQMw2e4E
10 QUpHzBz3Jh1h7g1zXw/7i8uV803fdHBEbt9Ni2fFzPhnFGBF52zIVF1sJtyCfAKWDC/Of9NY0IE
11 Hn4SMFp6L8eD8o27wn40Dz09vuTXPGqhpT36Q0Vdmm4w9aUXVjyEZ0bHXNg5+ixJ4p878F/KeU
12 Np8brnPKwPL7H9u127wga+vzZaW0c+kbCubVtCfRUBjJaR8Jng3SUHg/nJ01zxDB0smwAX0W16K
13 ZpuBE09DxkKulNv131vK7XV5QrTD06DQZ6b5/7RCBa31VIA6nKHrpI2ukoy3k2qk+csbApTebm1
14 DKrZNSn3ZbTr1s8hVoZckrV8j+nUe/1pL0G01YIXV31cCsHswdiCwMknB+r7XbLYMg36EDk2F+pT
15 3xrsYaE6wTGjH0J2GXJzTBG2+R0b2TSYswkxH40xR96Pj4911J4Ic2fQ7mUa50//e00r-jo15GqB
16 tVg+dJMwQF61vpSY41iBxbjU5s1tSKY+ny/wyMCEBGG30My2t52s3HJpnpXewQE5jI01hGsrVD
17 wU0VhyhAx2/2wHdkmn0DX0bivZLNDFGmKXPD193e3sCheTZ0YVvNqEp330MketHEE3KxuYbvj0x
18 1YyTr0BG37vapcCr11U/hkg5aFWG1D8rCmoKgy1vcZbH185v61NjK6x+zXhqqpA1pu/bu4eXig
19 AJMg5hVwMp2Vlc+no1qc0bNkFcrH9y2KA1/ciaEKCL88F5URKpLuTIvbeoGYCZuk+th0yXbFiJf
20 fR9v0AKIpscFZb/ArD7/Fly+Z6e+jnBva50QTRFPMTCisT0YTFIUI3RTSapZdrAK+HzGIDTFVEUG
21 hwpV3Q7/36Z6aK1Cw0+9F+zj5eTbnksyM6fNY81d3wAwqjElu6w4EMCCTHwvSCYBjfx9D6FR7J
22 qQj+9p1U0pbse5670uogTasiEG7Cabyz1VTPJTRcr1hiCz3R0McTtrqnv8AeYjcnKwgsMM
23 qWkjZndOqEPQ055RmBBPHMFAEk1R0rBe3o+rVIEKELj8hcMQKkRqTHkOge8v2wkhY0A0CMTI2ASg
24 4dLSQJz7H0t+8pMBJ2kdR2Bk/Dbdt/t1Pmaq9ySHeedHURGrFwffEdouY7Pc-jf1KjgdLbsWFFP1
25 WyskPOMTztnDoe3laQFkuBXC3MroZ1dp87j+HavwF0QY4m4Uafn9yA+B3UJ9XU1wozIYp/77Pc
26 JnA3qjKYkBmtfjiddt3zhnaACSONt1EhZ4RjZp4s40SAu0SYBPUeXBtQmmQLcVaobXL3xUNVdudv
27 pCL4yz9AyQvm+6x1ndVt7R+54uJ+XC70Dv+crb0XoInidgIGHBPFWw60T5kykSM115vg1Bcdqk
28 0GmTgT12Wvj2isAn4kPchheNwjiuL7H4FtpPPdLWmq1AaZERxzW2h1UohX53QjJcUgck5JNkU
29 7FpUjzFRg8HNNvyQn8LWmTmFWpHb8DeQAGEdaqjT7yF0rBUmFDHvPCJAF3CLawOjgBBRbzRG1wn
30 Tqxt28w3Wt9FRDFcvPsg5UWkdsuuVJciVgkD0gGRcJ8op0foqzJFa17JMBFyHNIRED7RPAvRPF
31 oJAKm//fj56/c05SnTes031cPVJX/VJxuq1Vt3F53BKw9/xnp/MjMZEPEPyn7hhgFqLWimKJSL
32 +0BqDvLmUsX0967mqR342aMIUn88J0WwSXP645EB4yuVjIRwMFS7WYKoyguMI-FpuHTJ/UsaJu
33 Y99YMDvIwb311+1N9xphz0+biSanP/3Z7Sshh2hDPV+o2aHsMB6hKNhkr4m51Cp67Apstz06P2
34 ISUX/2qnlcxd2XTYVY0bmla3fPuyLUduDesTbFbTmmsH+nDocjw7vZaesig4/vf1sn9ShgRVLk
35 q0TmDk3FYdQZ4YUa74/4s91IwUyrtzCbZot3+h4bs1hi5kiVFRtmPXTBUnrz3mChLGBRKF/1
36 fMgTmg2wAe7hBozSKF11ZaMHd1p4H+F5adLa1z9nm/a3BnEp20x20+buAX7bgY/SSAQy2jazxq
37 5v4q0SGhhHCuW5g5/s1whn5K/7490L7dUe84xw0s1Us9NoBAY3I07Cjwy4Bb3DyYsVTrE1SCLo
38 DBjG8jpa0B1us2gUucU7kYKY6vLbher9fdeYxT3hoxyFGAabqHKPDCI0//Svo10DFe+XcTJG/et
39 TrW76buXL8NgsDMnqaODRr11G1aE78XtLrSnclwyEE0z3vnmWq92pk8x21GGBDTP9yp7dw21vX
40 IUxGc5owdjuV/XEjxwmGCZUZf1k5Xg08ceV0+HDMHCq0KEmD1VQugTRnO/j/X5SWZvfkur14xDM

```

Gambar 3. Kode Program Terenkripsi

### 3. Instalasi Loader Pada Server

Untuk menjalankan *source code* yang sudah dienkripsi dengan *ioncube* diperlukan library loader yang dapat diinstall pada server. Library loader harus disesuaikan dengan versi php yang digunakan. Dalam penelitian ini menggunakan PHP versi 7.2 dan ioncube loader harus



menyesuaikan yaitu dengan versi 7.2. Sistem operasi server yang digunakan dalam penelitian ini menggunakan Ubuntu 20.04 dan diperlukan konfigurasi tambahan seperti pada baris terakhir pada Gambar 4 seperti berikut ini:

```

GNU nano 4.8 /etc/php/7.2/apache2/php.ini Modified
; If openssl.cafile is not specified or if the CA file is not found, the
; directory pointed to by openssl.capath is searched for a suitable
; certificate. This value must be a correctly hashed certificate directory.
; Most users should not specify a value for this directive as PHP will
; attempt to use the OS-managed cert stores in its absence. If specified,
; this value may still be overridden on a per-stream basis via the "capath"
; SSL stream context option.
;openssl.capath=

; Local Variables:
; tab-width: 4
; End:

zend_extension = /usr/local/ioncube/ioncube_loader_lin_7.2.so

^G Get Help ^O Write Out ^W Where Is ^R Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
    
```

Gambar 4. Instalasi Loader Ioncube

#### 4. Perbandingan Enkripsi dan Tanpa Enkripsi

##### a. Perbandingan Ukuran File

Dalam melakukan enkripsi *source code* dilakukan analisis perbandingan ukuran file dengan tujuan untuk melihat perbedaan antara ukuran file asli dengan file yang sudah terenkripsi. Pada percobaan enkripsi dengan menggunakan aplikasi ioncube menghasilkan file enkripsi dengan rata-rata kenaikan ukuran file sebesar 184 %. Kenaikan ukuran file ini nantinya akan dilihat proses kecepatannya apakah akan mempengaruhi waktu kecepatan akses atau tidak. Hasil perbandingan file dapat dilihat pada tabel 2 berikut ini:

Tabel 2. Perbandingan Ukuran File

No	File	Ukuran File		Presentase Perubahan
		File Asli	File Terenkripsi	
1	HomeController.php	4 KB	9 KB	125%
2	ShowController.php	6 KB	13 KB	117%
3	DashboardController.php	2 KB	7 KB	250%
4	EbookController.php	8 KB	17 KB	113%
5	ClassworkController.php	8 KB	16 KB	100%
6	VideoController.php	7 KB	16 KB	129%
7	MusikController.php	7 KB	16 KB	129%
8	UserControllerr.php	4 KB	11 KB	175%
9	KelasController.php	2 KB	8 KB	300%
10	LoginController.php	1 KB	5 KB	400%
Rata-rata				184%



### b. Perbandingan Kecepatan file

Pengujian terhadap kecepatan file perlu dilakukan karena seperti pada penjelasan sebelumnya bahwa proses enkripsi dengan *ioncube* menghasilkan ukuran file yang lebih besar. Perbandingan kecepatan akses berfungsi untuk melihat apakah ada perbedaan waktu eksekusi file sebelum dan setelah dilakukan proses enkripsi. Adapun hasil dari perbandingan menggambarkan bahwa adanya kenaikan kecepatan akses data sebesar 0,11 % antara file asli dengan file hasil enkripsi. Hasil perbandingan kecepatan akses dapat dilihat pada tabel 3 berikut ini.

Tabel 3. Perbandingan Kecepatan Akses

Percobaan	Ukuran File		Presentase Perubahan
	File Asli	File Terenkripsi	
1	281 ms	246 ms	-12,46%
2	275 ms	206 ms	-25,09%
3	242 ms	398 ms	64,46%
4	262 ms	219 ms	-16,41%
5	261 ms	208 ms	-20,31%
6	276 ms	214 ms	-22,46%
7	231 ms	255 ms	10,39%
8	142 ms	202 ms	42,25%
9	254 ms	207 ms	-18,50%
10	247 ms	245 ms	-0,81%
	Rata-rata		0,11%

### 5. Perbandingan Enkripsi dan Tanpa Enkripsi

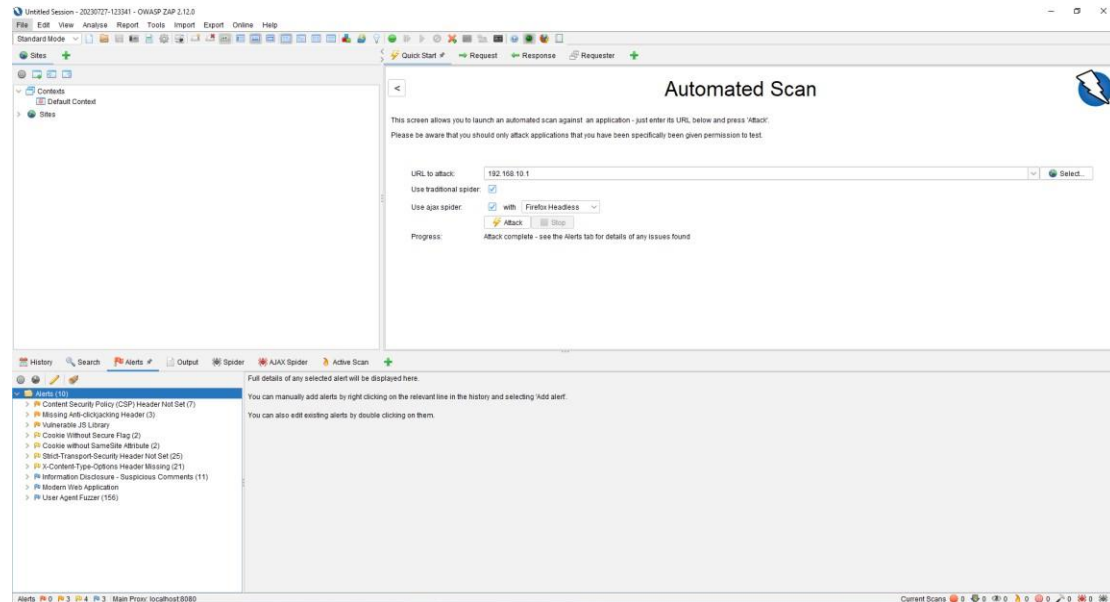
Pada gambar 5 berikut ini merupakan tampilan dari website perpustakaan digital dengan nama edumedia. Gambar tersebut merupakan hasil dari enkripsi dengan menggunakan enkripsi *ioncube*. Tampilan website tidak mengalami perubahan setelah dilakukan enkripsi sehingga dapat diartikan dengan melakukan *enkripsi ioncube* tidak akan merubah tampilan atau fungsi dari website perpustakaan digital. Tampilan website setelah dilakukan enkripsi kode program dapat dilihat seperti pada gambar 5 berikut ini:



Gambar 5. Tampilan Web Perpustakaan Digital setelah dienkripsi

## 6. Pengujian keamanan web perpustakaan digital

Proses pengujian website tidak hanya dari fungsi dan tampilan dari website akan tetapi diperlukan pengujian terhadap keamanan web. Pengujian keamaan web dilakukan menggunakan aplikasi Owasp Zap 2.12.0. Aplikasi ini berfungsi untuk mengetahui kerentanan yang ada pada website perpustakaan digital. berikut hasil dari pengujian kerentanan website dengan menggunakan aplikasi Owasp Zap 2.



Gambar 5. Pengujian Kerentanan Website

Gambar 5 menunjukkan bahwa dengan menggunakan framework laravel dapat meningkatkan keamanan karena tidak menghasilkan resiko *Sql injection* dan *Cross Site Scripting*. Jika dibandingkan hasil penelitian sebelumnya bahwa dengan menggunakan php native masih terdapat ancaman *Cross Site Scripting* seperti yang dilakukan dalam penelitian (Ghozali et al., 2019). Sedangkan dalam penelitian ini hanya menghasilkan ancaman yang masih tergolong medium dan tidak berbahaya. Berikut ini adalah tingkat ancaman yang dihasilkan pada penelitian ini:

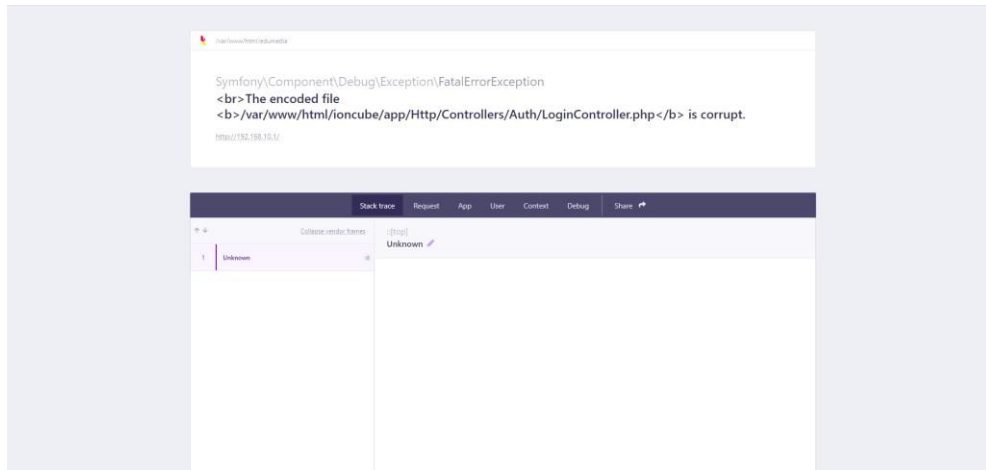
Tabel 4. Hasil Scan Kerentanan Website

No	Jenis Ancaman	Tingkat Resiko
1	Content Security Policy (CSP) Header Not Set	Medium
2	Missing Anti-clickjacking Header	Medium
3	Vulnerable JS Library	Medium
4	Cookie Without Secure Flag	Low
5	Cookie without SameSite Attribute	Low
6	Strict-Transport-Security Header Not Set	Low
7	X-Content-Type-Options Header Missing	Low
8	Information Disclosure - Suspicious Comments	Low
9	Modern Web Application	Low
10	User Agent Fuzzer	Low

## 7. Pengujian Enkripsi Ioncube

Pengujian terhadap enkripsi juga dilakukan dengan tujuan enkripsi yang dilakukan dapat melindungi kode program dan tidak mudah untuk diduplikasi maupun modifikasi. Adapun pengujian yang dilakukan adalah menambahkan kode program PHP pada file yang telah

dienkripsi. Hasil dari pengujian ini bahwa apabila file enkripsi dimodifikasi maka akan menghasilkan keterangan “*The encode file is corrupt*” yang berarti bahwa dengan adanya modifikasi pada file maka akan merusak file dan tidak dapat dijalankan. Hasil tampilan dari



modifikasi file dapat dilihat pada gambar seperti berikut :

Gambar 6. Pengujian Enkripsi

#### IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan pada objek web perpustakaan digital edumedia bahwa dengan menerapkan framework laravel dapat meningkatkan keamanan website karena tidak menghasilkan resiko ancaman Sql Injection dan Cross Site Scripting serta ancaman yang dihasilkan dari pengujian kerentanan website dengan menggunakan aplikasi Owasp Zap 2.12.0 menghasilkan ancaman yang tidak berbahaya atau dengan kategori medium. Sedangkan hasil enkripsi pada source code PHP pada framework laravel dengan menggunakan ioncube encode dapat meningkatkan ukuran file akan tetapi tidak berpengaruh pada kecepatan dan kinerja dari web perpustakaan digital. Dengan adanya proses enkripsi juga dapat meningkatkan keamanan pada source code PHP karena menghasilkan file enkripsi yang tidak mudah untuk dipahami oleh manusia sehingga dapat mengurangi resiko terjadinya pencurian data serta tidak mudah untuk diduplikasi maupun dimodifikasi

Saran untuk penelitian selanjutnya sebaiknya melakukan perbandingan analisis kewanaman antara framework PHP maupun pada Enkripsi PHP. Dengan adanya penelitian pada framework lain maka dapat digunakan sebagai alternatif pengembang website untuk meningkatkan keamanan baik pada data atau kode program.

#### REFERENSI

- Arisandi, D. (2017). *Rancang Bangun Aplikasi Enkripsi Coding Berbasis Php Program Menggunakan Algoritma AeS. 2.*
- Artono Dwi Ramadhan, Bambang Pramono, & Sutardi. (2020). *Implementasi Teknik Obfuscation Pada Source Code Php Dengan Algoritma Rivest Cipher 4.* <https://doi.org/10.5281/ZENODO.4394557>
- Aryanti, D., Nurholis, & Nashar Utamajaya, J. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode Owasp (Open Web Application Security Project) Pada Dinas Tenaga Kerja. *Jurnal Syntax Fusion, 1*(03), 15–25. <https://doi.org/10.54543/fusion.v1i03.53>
- Edy Listartha, I. M., Premana Mitha, I. M. A., Aditya Arta, M. W., & Yuda Arimika, I. Km. W.

- (2022). Analisis Kerentanan Website SMA Negeri 2 Amlapura Menggunakan Metode OWASP (Open Web Application Security Project). *SIMKOM*, 7(1), 23–27. <https://doi.org/10.51717/simkom.v7i1.63>
- Eka Pratama, I. P. A. (2020). Pengujian dan Analisa Reverse Engineering Pada Platform Android (Studi Kasus: Tebak\_Gambar.apk). *JTT (Jurnal Teknologi Terpadu)*, 8(2), 69–76. <https://doi.org/10.32487/jtt.v8i2.834>
- Endra, R. Y., Aprilinda, Y., Dharmawan, Y. Y., & Ramadhan, W. (2021). Analisis Perbandingan Bahasa Pemrograman PHP Laravel dengan PHP Native pada Pengembangan Website. *Expert: Jurnal Manajemen Sistem Informasi dan Teknologi*, 11(1), 48. <https://doi.org/10.36448/expert.v11i1.2012>
- Ghozali, B., Kusriani, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. *Creative Information Technology Journal*, 4(4), 264. <https://doi.org/10.24076/citec.2017v4i4.119>
- Lapatta, N. T. (2022). Pengembangan Sistem Manajemen Data Dosen Universitas Xyz Menggunakan Framework Laravel. *Naratif : Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, 4(2), 161–169. <https://doi.org/10.53580/naratif.v4i2.164>
- Nur Ahzan, Z., Wua Laja, Y. P., & Hijriani, L. (2023). Efektivitas Pengembangan Media Bahasa Pemrograman Open-Source dalam Penerapan Computational Thinking Mahasiswa. *Jurnal Cendekia : Jurnal Pendidikan Matematika*, 7(2), 1519–1532. <https://doi.org/10.31004/cendekia.v7i2.2282>
- PHP Encoder* 12. (2023, July 23). *PHP Encoder* 12. [https://www.ioncube.com/php\\_encoder.php](https://www.ioncube.com/php_encoder.php)
- Rahmatulloh, A., & Munir, R. (n.d.). *Pencegahan Ancaman Reverse Engineering Source Code PHP dengan Teknik Obfuscation Code pada Extension PHP*.
- Romadhon, M. H., & Yudhistira, Y. (2021). *Sistem Informasi Rental Mobil Berbasis Android Dan Website Menggunakan Framework Codeigniter 3 Studi Kasus: CV Kopja Mandiri*. 2(1).
- Sari, L. I., Probonegoro, W. A., & Romadiana, P. (2022). Penggunaan Framework Laravel Pelayanan Reservasi Kamar Berbasis Web di Renz Hotel Pangkalpinang. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, 9(2), 1507–1519. <https://doi.org/10.35957/jatisi.v9i2.1505>