

PROYEK AKHIR

**IMPLEMENTASI SISTEM PROTEKSI *CROSS SITE REQUEST FORGERY*
PADA WEBSITE TENDERPLUS.ID MENGGUNAKAN FRAMEWORK
CODEIGNITER 3**

**(Magang Bersertifikat Kampus Merdeka Studi Kasus: PT Baracipta Esa
Engineering)**



GIGIH RAGASAJIWO

NIM: 213310016

**PROGRAM STUDI TEKNOLOGI KOMPUTER
PROGRAM DIPLOMA TIGA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA**

2024

PROYEK AKHIR

**IMPLEMENTASI SISTEM PROTEKSI *CROSS SITE REQUEST FORGERY*
PADA WEBSITE TENDERPLUS.ID MENGGUNAKAN FRAMEWORK
CODEIGNITER 3**

**(Magang Bersertifikat Kampus Merdeka Studi Kasus: PT Baracipta Esa
Engineering)**

Diajukan sebagai salah satu syarat untuk menyelesaikan studi

Program Diploma

Program Studi Teknologi Komputer

Universitas Teknologi Digital Indonesia

Yogyakarta

Disusun Oleh :

GIGIH RAGASAJIWO

NIM: 213310016

**PROGRAM STUDI TEKNOLOGI KOMPUTER
PROGRAM DIPLOMA TIGA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA**

2024

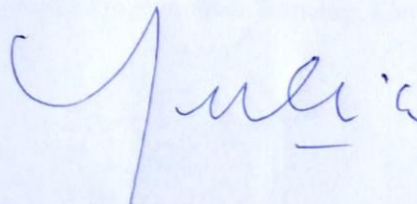
HALAMAN PERSETUJUAN
PROYEK AKHIR

Judul : Implementasi Sistem Proteksi *Cross Site Request Forgery* pada Website *Tenderplus.id* menggunakan Framework Codeigniter 3
Nama : Gigih Ragasajiwo
Nomor Mahasiswa : 213310016
Program Studi : Teknologi Komputer
Jenjang : Diploma III (D-3)
Tahun : 2024

Telah diperiksa dan disetujui untuk diujikan di hadapan Dewan Penguji
Proyek Akhir

Yogyakarta, 18 Juli 2024

Dosen Pembimbing,



Yudhi Kusnanto, S.T., M.T.

NIDN: 0531127002

HALAMAN PENGESAHAN
PROYEK AKHIR

IMPLEMENTASI SISTEM PROTEKSI *CROSS SITE REQUEST FORGERY*
PADA WEBSITE TENDERPLUS.ID MENGGUNAKAN FRAMEWORK
CODEIGNITER 3

(Magang Bersertifikat Kampus Merdeka Studi Kasus: PT Baracipta Esa
Engineering)

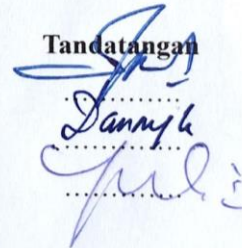
Telah dipertahankan di depan Dewan Penguji Proyek Akhir dan dinyatakan
diterima untuk memenuhi sebagian persyaratan guna memperoleh Gelar
Ahli Madya Komputer
Program Studi Teknologi Komputer
Universitas Teknologi Digital Indonesia
Yogyakarta

Yogyakarta, 5 Agustus 2024

Dewan Penguji

- | | NIDN |
|-------------------------------------|-------------|
| 1. Ir. M. Guntara, S.T., M.T. | 0509066101 |
| 2. Danny Kriestanto, S.Kom., M.Eng. | 0503068002 |
| 3. Yudhi Kusnanto, S.T., M.T. | 0531127002 |

Tandatangan



Mengetahui

Ketua Program Studi Teknologi Komputer



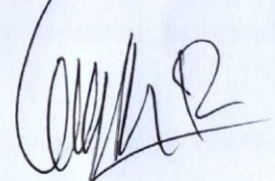
Adi Kusjani, S.T., M.Eng.

NIDN: 0515067501

PERNYATAAN KEASLIAN PROYEK AKHIR

Dengan ini Saya menyatakan bahwa naskah Proyek Akhir ini belum pernah diajukan untuk memperoleh gelar Ahli Madya Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan Saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 1 Juli 2024



Gigih Ragasajiwo

NIM: 213310016

HALAMAN PERSEMBAHAN

Puji syukur kehadiran Tuhan Yang Maha Esa atas segala rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penulisan Proyek Akhir ini dengan baik dan tepat waktu. Proyek Akhir ini penulis persembahkan kepada:

1. Allah SWT atas segala limpahan nikmat dan rezeki serta kemudahan dalam menyelesaikan Proyek Akhir ini.
2. Kedua orang tua dan keluarga yang selalu memberikan doa, semangat, serta dukungan, sehingga penulis dapat menyelesaikan proses perkuliahan dari awal sampai menyelesaikan Proyek Akhir.
3. Bapak Adi Kusjani, S.T., M.Eng., Kaprodi Teknologi Komputer Universitas Teknologi Digital Indonesia.
4. Bapak Yudhi Kusnanto, S.T., M.T. selaku dosen Pembimbing Akademik Universitas Teknologi Digital Indonesia yang telah membimbing dalam penyelesaian Tugas Akhir.
5. Seluruh rekan mahasiswa Program Studi Teknologi Komputer angkatan 2021 yang telah keluh kesah serta memberikan saran dan kritik kepada penulis selama perkuliahan.
6. Peserta Magang PT Baracipta Esa Engineering khususnya Divisi Full Stack Developer.
7. Teman dekat yang selalu memberi dukungan dan semangat kepada penulis dalam segala situasi dan kondisi.
8. Seluruh pihak yang tidak dapat disebutkan satu-persatu.

HALAMAN MOTO

“Orang yang hebat adalah orang yang memiliki kemampuan menyembunyikan kesusahan, sehingga orang lain mengira bahwa ia selalu senang.”

-Imam Syafi’i-

“Ohayo! Konnichiwa! Oyasumi! Aku ingin ada di setiap harimu..”

-Gabriela Abigail-

KATA PENGANTAR

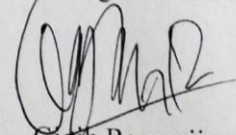
Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas limpahan rahmat dan karunia-Nya, Proyek Akhir dengan judul “Implementasi Sistem Proteksi *Cross Site Request Forgery* pada Website Tenderplus.id menggunakan Framework Codeigniter 3” ini dapat selesai dengan baik dan tepat waktu.

Penulis menyadari banyak pihak yang memberikan dukungan serta bantuan dalam penyelesaian Proyek Akhir ini. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Ibu Sri Redjeki, S.Si., M.Kom., Ph.D., selaku Rektor Universitas Teknologi Digital Indonesia.
2. Ibu Dr. L.N. Harnaningrum, S.Si., M.T., selaku Wakil Rektor 1 Universitas Teknologi Digital Indonesia.
3. Bapak Dr. Bambang Purnomosidi Dwi Putranto, S.E., Akt., S.Kom., MMSI selaku Dekan Fakultas Teknologi Informasi Universitas Teknologi Digital Indonesia.
4. Bapak Adi Kusjani, S.T., M.Eng., selaku Ketua Program Studi Teknologi Komputer Diploma 3 Universitas Teknologi Digital Indonesia.
5. Keluarga Besar penulis yang selalu memberikan doa, dukungan serta motivasi selama menjalani aktivitas perkuliahan.

Akhir kata, penulis menyadari bahwa Proyek Akhir ini masih banyak terdapat kekurangan. Oleh karena itu, penulis sangat berharap mendapatkan kritik dan saran yang membangun. Semoga Proyek Akhir ini bermanfaat bagi semua pihak.

Yogyakarta, 5 Agustus 2024



Gigin Ragasajiwo

NIM: 213310016

DAFTAR ISI

| | Hal |
|--|------|
| PROYEK AKHIR | i |
| HALAMAN PERSETUJUAN PROYEK AKHIR | ii |
| HALAMAN PENGESAHAN PROYEK AKHIR | iii |
| PERNYATAAN KEASLIAN PROYEK AKHIR | iii |
| HALAMAN PERSEMBAHAN | v |
| HALAMAN MOTO..... | vi |
| KATA PENGANTAR..... | vii |
| DAFTAR ISI | vii |
| DAFTAR GAMBAR | xi |
| DAFTAR TABEL..... | xiii |
| DAFTAR LISTING PROGRAM..... | xiv |
| DAFTAR LAMPIRAN | xv |
| INTISARI..... | xvi |
| ABSTRACT..... | xvii |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Tujuan..... | 2 |
| 1.4 Batasan Masalah..... | 2 |
| BAB 2 DASAR TEORI DAN TINJAUAN PUSTAKA | 3 |
| 2.1 Tinjauan Pustaka..... | 3 |
| 2.2 Dasar Teori | 4 |
| 2.2.1 CSRF | 4 |
| 2.2.2 <i>Full Stack Developer</i> | 5 |

| | | |
|-------------------------------------|---|-----------|
| 2.2.3 | PHP | 7 |
| 2.2.4 | MySQL..... | 7 |
| 2.2.5 | Codeigniter..... | 8 |
| 2.2.6 | Figma | 8 |
| 2.2.7 | Visual Studio Code..... | 8 |
| 2.2.8 | NPM..... | 9 |
| 2.2.9 | Composer | 9 |
| 2.2.10 | Bootstrap | 9 |
| 2.2.11 | JavaScript | 10 |
| 2.2.12 | jQuery..... | 10 |
| BAB 3 RANCANGAN SISTEM | | 11 |
| 3.1 | Analisa Kebutuhan Perancangan..... | 11 |
| 3.1.1 | Perangkat Keras | 11 |
| 3.1.2 | Perangkat Lunak..... | 11 |
| 3.2 | Alur Kerja Proteksi CSRF | 11 |
| 3.2.1 | Inisialisasi CSRF Protection di CodeIgniter 3 | 12 |
| 3.2.2 | Generate Token CSRF..... | 12 |
| 3.2.3 | Penyertaan Token CSRF pada Form | 13 |
| 3.2.4 | Penyertaan Token CSRF pada AJAX Request..... | 14 |
| 3.3 | Rancangan Basis Data | 14 |
| 3.3.1 | Tabel Pengguna | 15 |
| 3.3.2 | Tabel Data Leads..... | 16 |
| 3.3.3 | Tabel Pemenang | 16 |
| 3.3.4 | Tabel Plot Tim | 17 |
| 3.3.5 | Tabel Kontak Lead | 18 |
| 3.3.6 | Tabel Tim Marketing..... | 18 |

| | | |
|-------|---|----|
| 3.4 | Rancangan Diagram | 19 |
| BAB 4 | IMPLEMENTASI DAN PEMBAHASAN | 21 |
| 4.1 | Implementasi | 21 |
| 4.1.1 | Konfigurasi CSRF | 21 |
| 4.1.2 | Halaman <i>Login</i> | 22 |
| 4.1.3 | Halaman <i>Manage Marketing</i> | 26 |
| 4.1.4 | Halaman Plot Tim | 32 |
| 4.1.5 | Halaman <i>CRM</i> | 36 |
| 4.2 | Hasil Pengujian..... | 42 |
| 4.2.1 | Hasil Pengujian Halaman <i>Login</i> | 42 |
| 4.2.2 | Hasil Pengujian Halaman <i>Manage Marketing</i> | 47 |
| 4.2.3 | Hasil Pengujian Halaman Plot Tim..... | 48 |
| 4.2.4 | Hasil Pengujian Halaman <i>CRM</i> | 50 |
| BAB 5 | KESIMPULAN DAN SARAN | 53 |
| 5.1 | Kesimpulan..... | 53 |
| 5.2 | Saran..... | 53 |
| | DAFTAR PUSTAKA | 54 |
| | LAMPIRAN..... | 56 |

DAFTAR GAMBAR

| | Hal |
|---|-----|
| Gambar 2.1 Skema <i>Web Development</i> dengan <i>Design Pattern</i> MVC | 6 |
| Gambar 3.1 <i>Flowchart</i> Implementasi proteksi CSRF | 12 |
| Gambar 3.2 Fitur <i>built-in</i> untuk CSRF di <i>file config.php</i> | 12 |
| Gambar 3.3 Mekanisme token Ketika login pada <i>website</i> | 13 |
| Gambar 3.4 Penyertaan Token CSRF pada Form Login..... | 13 |
| Gambar 3.5 Penyertaan Token CSRF pada AJAX..... | 14 |
| Gambar 3.6 Relasi Antar Tabel | 15 |
| Gambar 3.7 <i>Sequence Diagram</i> <i>input form</i> | 19 |
| Gambar 3.8 <i>Sequence Diagram</i> <i>Validation form</i> | 19 |
| Gambar 3.9 <i>Sequence Diagram</i> <i>Request AJAX</i> | 20 |
| Gambar 4.1 Halaman <i>Login</i> | 22 |
| Gambar 4.2 <i>Cookie</i> CSRF ketika mengakses Halaman <i>Login</i> | 23 |
| Gambar 4.3 Halaman <i>Dashboard Supplier</i> | 26 |
| Gambar 4.4 Halaman <i>Manage Marketing</i> | 26 |
| Gambar 4.5 <i>Modal</i> aksi detail | 27 |
| Gambar 4.6 <i>Modal</i> Edit Marketing | 29 |
| Gambar 4.7 <i>Modal Delete</i> Tim Marketing..... | 31 |
| Gambar 4.8 Halaman Plot Tim..... | 32 |
| Gambar 4.9 <i>Modal</i> Tambahkan Anggota | 33 |
| Gambar 4.10 Halaman CRM | 36 |
| Gambar 4.11 <i>Modal</i> Edit Lead | 37 |
| Gambar 4.12 Halaman Login dengan Proteksi CSRF | 45 |
| Gambar 4.13 Halaman Login sebagai <i>Attacker</i> | 45 |
| Gambar 4.14 Tampilan setelah <i>Login</i> dengan Proteksi CSRF..... | 46 |
| Gambar 4.15 Tampilan setelah <i>Login</i> tanpa proteksi CSRF | 46 |
| Gambar 4.16 <i>URL AJAX POST</i> Manage Marketing ke <i>URL</i> Target..... | 47 |
| Gambar 4.17 Hasil ketika <i>attacker</i> mencoba memasukkan data | 48 |
| Gambar 4.18 <i>URL AJAX POST</i> Plot Tim yang mengarah ke <i>URL</i> Target..... | 48 |

| | |
|--|----|
| Gambar 4.19 Hasil ketika <i>attacker</i> mencoba memasukkan data tim marketing.. | 49 |
| Gambar 4.20 Hasil <i>attacker</i> menambahkan perusahaan ke tim marketing..... | 50 |
| Gambar 4.21 <i>URL AJAX POST</i> CRM yang mengarah ke <i>URL</i> Target..... | 51 |
| Gambar 4.22 Hasil ketika <i>attacker</i> menambahkan data CRM..... | 51 |
| Gambar 4.23 Hasil ketika <i>attacker</i> mengedit data CRM..... | 52 |

DAFTAR TABEL

| | Hal |
|-------------------------------------|-----|
| Tabel 2.1 Tinjauan Pustaka | 3 |
| Tabel 3.1 Tabel Pengguna | 15 |
| Tabel 3.2 Tabel Data Leads | 16 |
| Tabel 3.3 Tabel Pemenang | 16 |
| Tabel 3.4 Tabel Plot Tim | 17 |
| Tabel 3.5 Tabel Kontak Lead | 18 |
| Tabel 3.6 Tabel Tim Marketing | 18 |

DAFTAR LISTING PROGRAM

| | Hal |
|---|-----|
| Listing 4.1 Konfigurasi CSRF | 21 |
| Listing 4.2 Kerangka Halaman <i>Login</i> | 25 |
| Listing 4.3 Listing <i>Function</i> Detail <i>Manage Marketing</i> | 28 |
| Listing 4.4 <i>Function</i> Edit Tim Marketing | 31 |
| Listing 4.6 <i>Function</i> Tambahkan Anggota | 34 |
| Listing 4.7 <i>Function</i> Menambahkan Perusahaan ke Tim Marketing | 35 |
| Listing 4.8 <i>Function</i> Edit CRM | 39 |
| Listing 4.9 <i>Function</i> Tambah CRM | 41 |
| Listing 4.10 Kerangka Halaman <i>Login Attacker</i> | 44 |

DAFTAR LAMPIRAN

| | Hal |
|---|-----|
| Lampiran A. Dokumentasi Teknis..... | 56 |
| Lampiran A. 1 Pengerjaan Project | 56 |
| Lampiran A. 2 Foto Bersama Divisi Full Stack Developer dan Mentor | 56 |
| Lampiran A. 3 Zoom Meeting dengan PT KAI | 57 |
| Lampiran B. Source Code Program | 57 |
| Lampiran B. 1 <i>Source Code View Login</i> | 59 |
| Lampiran B. 2 <i>Source Code Views Manage Marketing</i> | 71 |
| Lampiran B. 3 <i>Source Code Views Plot Tim</i> | 77 |
| Lampiran B. 4 <i>Source Code View CRM</i> | 91 |
| Lampiran C. Keputusan Hasil Ujian Pendadaran | 92 |
| Lampiran C. 1 Keputusan Hasil Ujian Pendadaran | 92 |
| Lampiran D. Catatan Ujian Pendadaran..... | 93 |
| Lampiran D. 1 Catatan Ujian Pendadaran..... | 93 |
| Lampiran D. 2 Bukti ACC Revisi Dosen Penguji 1 | 94 |
| Lampiran D. 3 Bukti ACC Revisi Dosen Penguji 2..... | 95 |
| Lampiran E. Logbook Bimbingan Proyek Akhir | 96 |

INTISARI

Keamanan web merupakan aspek penting dalam pengembangan aplikasi web. Salah satu ancaman dari keamanan web tersebut adalah Cross-Site Request Forgery (CSRF), yang memungkinkan penyerang dapat memanipulasi browser korban untuk melakukan tindakan yang tidak diinginkan pada situs web. Dalam konteks ini, seorang pengguna yang sah dapat tanpa sadar mengirimkan permintaan berbahaya kepada server, yang kemudian dieksekusi sebagai tindakan yang sah oleh server.

Pada proyek akhir ini, fokus utama adalah mengimplementasikan sistem proteksi CSRF pada website TenderPlus.id. Implementasi ini bertujuan untuk meningkatkan keamanan website dari ancaman CSRF dengan memastikan bahwa setiap permintaan HTTP yang berpotensi membahayakan dilindungi oleh token CSRF. Token ini berfungsi sebagai verifikasi tambahan yang memastikan bahwa permintaan yang dikirimkan ke server berasal dari sumber yang sah dan bukan dari sumber yang berbahaya. Proses implementasi ini menggunakan framework CodeIgniter 3 dimana menggunakan teknik proteksi CSRF yang telah disediakan oleh framework tersebut.

Hasil dari proyek ini diharapkan dapat meningkatkan keamanan website TenderPlus.id dari ancaman CSRF, memberikan pengalaman pengguna yang lebih aman, dan menjadi referensi bagi pengembang lain yang ingin mengimplementasikan proteksi serupa. Selain itu, dokumentasi dan best practice yang dihasilkan dari proyek ini diharapkan dapat membantu komunitas pengembang dalam memahami dan mengadopsi teknik proteksi CSRF dalam aplikasi mereka, sehingga meningkatkan standar keamanan web secara keseluruhan.

Kata Kunci: Keamanan web, CSRF, Cross-Site Request Forgery, CodeIgniter 3, proteksi CSRF, token CSRF, TenderPlus.id, pengembangan aplikasi web.

ABSTRACT

Web security is an important aspect of web application development. One such web security threat is Cross-Site Request Forgery (CSRF), which allows an attacker to manipulate a victim's browser to perform unwanted actions on a website. In this context, a legitimate user can unknowingly send a malicious request to the server, which is then executed as a legitimate action by the server.

In this final project, the main focus is to implement a CSRF protection system on the TenderPlus.id website. This implementation aims to increase the security of the website from CSRF threats by ensuring that every potentially malicious HTTP request is protected by a CSRF token. This token serves as an additional verification that ensures that requests sent to the server come from legitimate sources and not from malicious sources. This implementation process uses the CodeIgniter 3 framework which uses CSRF protection techniques that have been provided by the framework.

The results of this project are expected to improve the security of the TenderPlus.id website from CSRF threats, provide a safer user experience, and become a reference for other developers who want to implement similar protections. In addition, the documentation and best practices generated from this project are expected to help the developer community in understanding and adopting CSRF protection techniques in their applications, thus improving overall web security standards.

Keywords: Web security, CSRF, Cross-Site Request Forgery, CodeIgniter 3, CSRF protection, CSRF token, TenderPlus.id, web application development.