



**PENERAPAN SISTEM KEAMANAN WEBSITE MENGGUNAKAN WAF (WEB
APPLICATION FIREWALL) DENGAN FRAMEWORK OWASP (OPEN WEB
APPLICATION SECURITY PROJECT)**

LAPORAN PENELITIAN

MUHAMMAD DANDI PERMANA

191420058

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS TEKNOLOGI

UNIVERSITAS BINA DARMA

PALEMBANG

2023



PENERAPAN SISTEM KEAMANAN WEBSITE MENGGUNAKAN WAF (WEB APPLICATION FIREWALL) DENGAN FRAMEWORK OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

MUHAMMAD DANDI PERMANA

191420058

Laporan Penelitian ini diajukan sebagai syarat memperoleh gelar Sarjana Komputer

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BINA DARMA

PALEMBANG

2023

HALAMAN PENGESAHAN

**PENERAPAN SISTEM KEAMANAN WEBSITE MENGGUNAKAN
WAF (WEB APPLICATION FIREWALL) DENGAN
FRAMEWORK OWASP (OPEN WEB APPLICATION SECURITY
PROJECT)**

**MUHAMMAD DANDI PERMANA
191420058**

Telah diterima sebagai salah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Teknik Informatika

Palembang, 07 September 2023
Fakultas Sains Teknologi
Universitas Bina Darma
Dekan,

Pembimbing



Syahril Rizal R I, S.T., M.M., M.Kom.


Universitas Bina Darma
Fakultas Sains Teknologi

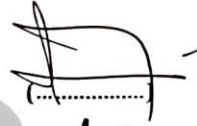
Dr. Tata Sutabri, S.Kom., MMSI., MKM.

HALAMAN PERSETUJUAN

Laporan Penelitian Berjudul "PENERAPAN SISTEM KEAMANAN WEBSITE MENGGUNAKAN WAF (WEB APPLICATION FIREWALL) DENGAN FRAMEWORK OWASP (OPEN WEB APPLICATION SECURITY PROJECT)" Oleh "Muhammad Dandi Permana", telah dipertahankan di depan komisi pengujian pada hari Kamis tanggal 07 September 2023.

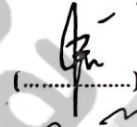
Komisi Penguji

1. Ketua : Syahril Rizal R I, S.T., M.M., M.Kom.



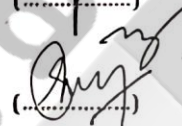
(.....)

2. Anggota : Febriyanti Panjaitan, M.Kom.



(.....)

3. Anggota : Suryayusra, M.Kom.



(.....)

Mengetahui,
Program Studi Teknik Informatika
Fakultas Sains Teknologi
Universitas Bina Darma
Ketua,



Universitas Bina Darma
Fakultas Sains Teknologi

Alek Wijaya, S.Kom., M.I.T.

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Muhammad Dandi Permana
NIM : 191420058

Dengan ini menyatakan bahwa :

1. Karya akhir saya adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana) di Universitas Bina Darma atau perguruan tinggi lainnya ;
2. Karya tulis ini murni gagasan, rumusan dan penelitian saya dengan arahan dari tim pembimbing ;
3. Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah di tulis atau di publikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar rujukan ;
4. Saya bersedia karya tulis ini di cek keasliannya menggunakan plagiarism checker serta di unggah di internet, sehingga dapat diakses secara daring ;
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi dengan peraturan dan perundang-undangan yang berlaku;

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 07 September 2023
Yang membuat pernyataan



MUHAMMAD DANDI PERMANA

NIM : 191420058

ABSTRAK

Website adalah salah satu bentuk media promosi paling populer saat ini. Website digunakan untuk memberikan informasi kepada pelanggan. Selain itu, data-data pada situs web haruslah dijaga dari hal-hal yang tidak diinginkan seperti XSS Attack. Demi menjaga keamanan website BOOM STORE dari serangan itu maka penulis membuat peningkatan keamanan website. Penelitian ini menerapkan keamanan aplikasi berbasis Web Application Firewall (WAF) dengan menggunakan ModeSecurity sebagai keamanannya dan ZAP (Zed Attck Proxy) sebagai Web Application Penetration Testing Tool yang bertujuan untuk meningkatkan sistem keamanan website tersebut dengan pemanfaatan firewall. Pada penelitian ini menggunakan metode eksperimen dengan mengimplementasikan Web Application Firewall (WAF) sebagai sistem proteksi berbasis web, kemudian proses analisis dan ujicoba untuk memperoleh saran yang akurat dalam implementasi firewall. Hasil penelitian ini menunjukkan bahwa firewall yang digunakan dengan ModeSecurity berbasis Web Application Firewall (WAF) telah berhasil menghentikan serangan dari attacker dengan metode Cross Site Scripting (XSS).

Kata Kunci : Website, Web Application Firewall, OWASP, Modsecurity, ZAP

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah Swt. Yang telah melimpahkan rahmat dan karunia-Nya sehingga Karya Akhir ini dapat diselesaikan guna memenuhi salah satu syarat untuk menyelesaikan studi untuk program Sarjana, Teknik Informatika di Universitas Bina Darma.

Pada Kesempatan yang baik ini, tak lupa penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bimbingan, arahan, nasehat, dan pemikiran dalam penulisan karya akhir ini terutama kepada:

1. Prof. Dr. Sunda Ariana, M.Pd., M.M selaku Rektor Universitas Bina Darma Palembang.
2. Dr. Tata Sutabri, S.Kom., M.MSI., M.KM selaku Dekan Fakultas Sains Teknologi Universitas Bina Darma Palembang.
3. Alek Wijaya, S.Kom., M.I.T selaku Ketua Program Studi Teknik Informatika Universitas Bina Darma.
4. Syahril Rizal, ST, M.M., M.Kom selaku Dosen Pembimbing yang telah memberikan bimbingan dan arahan dalam penulisan Laporan Karya Akhir ini.
5. Febriyanti Panjaitan, M.Kom selaku dosen penguji yang telah memberikan bimbingan dan arahan dalam penulisan Laporan Karya Akhir ini.
6. Suryayusra, M.Kom selaku dosen penguji yang telah memberikan bimbingan dan arahan dalam penulisan Laporan Karya Akhir ini.

DAFTAR ISI

HALAMAN PENGESAHAN.....	Error! Bookmark not defined.
HALAMAN PERSETUJUAN	ii
SURAT PERNYATAAN	iii
ABSTRAK.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL.....	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah.....	2
1.5 Manfaat Penelitian	3
BAB II TINJAUAN PUSTAKA	4
2.1 Penelitian Terdahulu	4
2.2 Keamanan Website.....	4
2.3 Website	5
2.4 Web Appliacion Firewall (WAF).....	5
2.5 Open Web Application Security Project (OWASP).....	5
2.6 ModSecurity	6
BAB III METODOLOGI PENELITIAN	7
3.1 Observasi.....	7
3.2 Alat dan Bahan Sistem WAF.....	8
3.2.1 Web Application Firewall (WAF)	8
3.2.2 Sistem Operasi	8
3.2.3 Virtual Machines	9
3.2.4 Server Web.....	9
3.2.5 Framework OWASP	9
3.2.6 Data Uji Coba	9
3.2.7 Dokumentasi OWASP	9
3.2.8 Lingkungan Pengujian Terpisah (Sandbox)	9

3.3	Implementasi WAF	10
3.3.1	Implementasi ModSecurity	12
3.3.2	Instalasi OWASP ZAP	14
3.4	Pengujian Sistem Keamanan.....	15
3.4.1	Percobaan XSS Attack.....	15
3.4.2	Penetration Testing Tool menggunakan OWASP ZAP.....	17
BAB IV	HASIL DAN PEMBAHASAN	23
4.1	Analisis Hasil Penelitian	23
4.1.1	Analisis Hasil Serangan XSS Pada Website	23
4.1.2	Analisis Hasil Penetration menggunakan OWASP ZAP.....	23
4.2	Pembahasan	25
4.2.1	Mengidentifikasi Kerentanan Keamanan Website	25
4.2.2	Menganalisis Tingkat Keamanan Website	26
4.2.3	Rekomendasi Perbaikan Keamanan.....	26
BAB V	KESIMPULAN DAN SARAN	27
5.1	Kesimpulan.....	27
5.2	Saran	27
DAFTAR PUSTAKA	29
LAMPIRAN	

DAFTAR GAMBAR

Gambar 3.1 Flowchart Tahapan Penelitian	7
Gambar 3.2 Website Boom Store	7
Gambar 3.2 Diagram Alur Web Application Firewall	10
Gambar 3.3 Instalasi Web Applications Firewall (WAF)	13
Gambar 3.4 Ubah nama modsecurity.conf	13
Gambar 3.5 Isi folder /usr/share/modsecurity-crs/	13
Gambar 3.6 Include konfigurasi modsecurity	14
Gambar 3.7 Rule yang digunakan	14
Gambar 3.8 Unduh ZAP	14
Gambar 3.9 Instalasi OWASP ZAP	15
Gambar 3.10 Menjalankan OWASP ZAP di ubuntu	15
Gambar 3.11 Berhasil melakukan percobaan XSS attack	16
Gambar 3.12 Akses ditolak oleh WAF	16
Gambar 3.13 Hasil log ModSecurity	16
Gambar 3.14 Pengujian menggunakan OWASP ZAP	20
Gambar 3.15 Hasil pengujian setelah menerapkan Modsecurity	20
Gambar 3.16 Masih bisa di attack	22
Gambar 3.17 Test attack gagal menggunakan OWASP ZAP	22

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....	4
Tabel 3.1 klasifikasi pada OWASP ZAP	20
Tabel 4.1 Identifikasi Celah Serangan.....	24
Tabel 4.2 Sebelum menggunakan WAF.....	25
Tabel 4.3 Sesudah menggunakan WAF.....	25

