# *Web Application Firewall* pada Situs *Web* Institut Bisnis Nusantara www.ibn.ac.id

Ariawan Aryapranata

*Program Studi Sistem Informasi Institut Bisnis Nusantara*
*Jl. D.I. Pandjaitan kav 24 by pass Jaktim INDONESIA*
*ariawan@ibn.ac.id*

*Intisari*— **Situs *Web* institusi pendidikan sering menjadi target serangan para *Hacker*. Serangan dengan cara khusus dan tidak terdeteksi dengan tujuan mengeksploitasi kelemahan Situs Web. Tujuan peretasan Situs-Situs diantaranya : distribusikan malware, curi data, posting iklan atau informasi terlarang, penipuan, atau tembus jaringan internal. Keamanan yang baik pada tingkat *web application* diperlukan bagi Institut Bisnis Nusantara www.ibn.ac.id, guna menangkal serangan *hacker* yang mentargetkan Situs tersebut.**
*Kata kunci— Web, Application, Firewall, Eksploitasi, Malware*

*Abstract*— ***Educational institution websites are often the target of attacks by hackers. Attacks in a special way and not detected with the aim of exploiting the weaknesses of the Website. The purpose of hacking sites includes : distributing malware, stealing data, posting advertisements or prohibited information, fraud, or penetrating internal networks. Good security at the web application level is needed for the* Institut Bisnis Nusantara, *www.ibn.ac.id, to ward off hacker attacks targeting the site.***
*Keywords— Web, Application, Firewall, Expolitation, Malware*

## I. PENDAHULUAN

Situs *Web* Institusi Pendidikan sering menjadi target serangan para *Hacker*. Dengan cara khusus dan tidak terdeteksi dengan tujuan mengeksploitasi kelemahan Situs *Web*. Serangan seperti SQL *injection*, *cross-site scripting* atau *session hijacking* ditujukan pada kerentanan dalam aplikasi *web* dan bukan pada tingkat jaringan. Karena alasan ini, sistem keamanan Teknologi Informasi tradisional seperti *firewall* atau *Intrusion Detection System/ Intrusion Prevention System* (IDS/IPS) diperlukan adanya tambahan pengamanan guna memberikan perlindungan yang komprehensif.

Situs yang diretas dapat digunakan untuk banyak hal, diantaranya : mendistribusikan *malware*, mencuri data, mem*post*ing iklan atau informasi terlarang, melakukan penipuan, atau menembus jaringan internal.

## II. BACKGROUNG/LATAR BELAKANG

Diperlukan keamanan yang baik pada tingkat *web application* Institut Bisnis Nusantara www.ibn.ac.id, guna menangkal serangan *hacker* yang mentargetkan Situs tersebut.

### *Web Application Firewall*

*Web Application Firewall* (WAF) berfungsi untuk mensaring, memantau, dan memblokir lalu lintas HTTP ke dan dari aplikasi *web*. WAF dibedakan dari *firewall* biasa karena WAF mampu menyaring konten aplikasi *web* tertentu sementara *firewall* biasa berfungsi sebagai gerbang pengaman antar *server*. Dengan memeriksa lalu lintas HTTP, ini dapat mencegah serangan yang berasal dari kelemahan keamanan aplikasi *web*, seperti SQL *Injection*, *cross-site scripting* (XSS), *file inclusion*, dan kesalahan konfigurasi keamanan [1].

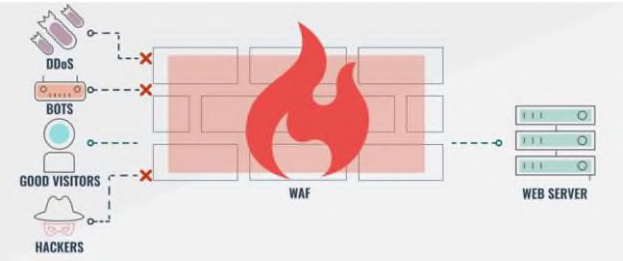
Manfaat utama WAF adalah perlindungan aplikasi *web* yang lengkap dan produktif pada tingkat aplikasi tanpa harus mengubah aplikasi itu sendiri. WAF juga menyediakan mekanisme keamanan proaktif seperti enkripsi URL atau *site usage enforcement*, untuk meminimalkan area serangan dengan upaya sesedikit mungkin. Selain itu, penggunaan WAF meningkatkan keamanan aplikasi *web* terhadap serangan eksternal [2].

WAF memiliki keunggulan dibandingkan *firewall* tradisional biasa karena menawarkan *visibilitas* yang lebih besar ke dalam data aplikasi sensitif yang dikomunikasikan dengan menggunakan lapisan aplikasi HTTP. Dan dapat mencegah serangan di lapisan aplikasi yang biasanya memotong *firewall* jaringan, diantaranya :

- Serangan *Cross-site scripting* (XSS), memungkinkan penyerang menyuntikkan dan mengeksekusi *skrip* berbahaya di *browser* pengguna lain.
- Serangan *Structured Query Language* (SQL) *Injection*, Penyerang mengakses dan mengubah data-data sensitif di aplikasi yang menggunakan *Database* SQL.
- *Web Session Hacking*, memungkinkan penyerang membajak ID dan menyamar sebagai pengguna yang berwenang. ID sesi biasanya disimpan dalam *cookie* atau *Uniform Resource Locator* (URL).
- Serangan *Distributed Denial of Service* (DDoS), Membanjiri lalu-lintas jaringan sehingga *server* lumpuh dan tidak dapat melayani.
- Serangan DoS *Layer* 7, membanjiri *server web* dengan aktivitas aplikasi rekursif.

- *Buffer Overflow*, input pengguna yang menimpa kode dalam memori.
- *Cookie Poisoning*, mengubah nilai parameter yang disimpan dalam *cookie* untuk merusak data yang dikirimkan di antara halaman *web*.

Beberapa jenis serangan DDoS menggunakan HTTP, sebagian besar menggunakan *lower-level methods*. WAF akan melindungi dari serangan DDoS tingkat *application-level/ layer* 7 (HTTP/ FTP).




Gambar 1. *Web Application Firewall*.

**PLESK WAF**

Plesk merupakan salah satu jenis *control panel hosting* yang digunakan untuk mengelola segala fasilitas *hosting*. Pada saat pertama kali dirilis, Plesk berada di bawah naungan sebuah perusahaan dari Amerika Serikat, yaitu Plesk Inc dan didesain di Rusia. Plesk saat ini bisa dijalankan dalam sistem operasi Windows dan Linux. Dengan memilih Plesk sebagai *control panel hosting*, dapat melakukan berbagai aktivitas di Situs *Web*, sama halnya menggunakan *control panel hosting* lainnya yang tidak asing di Indonesia yaitu cPanel. Plesk ataupun cPanel keduanya merupakan *control panel hosting* yang memiliki reputasi yang baik saat ini.

Untuk mendeteksi dan mencegah serangan, *Web Application Firewall* (ModSecurity) memeriksa semua permintaan ke *server web* dan respon terkait dari *server* terhadap sekumpulan aturannya. Jika pemeriksaan berhasil, permintaan HTTP diteruskan ke Situs untuk mengambil konten. Jika pemeriksaan gagal, tindakan yang telah ditentukan dilakukan. ModSecurity didukung di Plesk untuk Linux dan untuk Windows. Ini berfungsi sebagai modul *server web* (Apache atau IIS)[3].

**ModSecurity**

ModSecurity adalah *firewall* aplikasi *web open-source* (WAF). Awalnya dirancang sebagai modul untuk Apache HTTP *server*, telah berevolusi untuk menyediakan berbagai permintaan Protokol Transfer *Hipertext* dan kemampuan penyaringan respons bersama dengan fitur keamanan lainnya di sejumlah platform yang berbeda termasuk Apache HTTP *server*, Microsoft IIS dan Nginx. Ini adalah perangkat lunak gratis yang dirilis di bawah lisensi Apache 2.0. *Platform* ini menyediakan konfigurasi aturan yang dikenal sebagai 'SecRules' untuk pemantauan, pencatatan, dan penyaringan waktu nyata komunikasi Protokol Transfer Hipertext berdasarkan aturan yang ditetapkan pengguna.

ModSecurity paling umum digunakan untuk memberikan perlindungan terhadap kelas kerentanan umum menggunakan OWASP ModSecurity *Core Rule Set* (CRS). Ini adalah seperangkat aturan sumber terbuka yang ditulis dalam bahasa SecRules ModSecurity.

Untuk mendeteksi ancaman, ModSecurity perlu dipasang pada *server web* atau sebagai s*erver proxy* di depan aplikasi *web*. Ini memungkinkan mesin memindai komunikasi HTTP masuk dan keluar ke titik akhir. Bergantung pada konfigurasi aturan, mesin akan memutuskan bagaimana komunikasi harus ditangani yang mencakup kemampuan untuk meneruskan, menjatuhkan, mengalihkan, mengembalikan kode status yang diberikan, menjalankan *skrip* pengguna, dan lainnya.

**Fail2ban**

Fail2ban tersedia di hampir setiap *repositori* distribusi sekarang ini, dan ini merupakan *extensible Swiss-army knife* dalam pencegahan otentikasi *brute-force*, *fail2ban* dilengkapi dengan sejumlah filter untuk mendeteksi upaya lain yang dapat melakukan hal-hal buruk pada sistem, Yang perlu dilakukan hanya menginstalnya, jalankan, perbarui dan nyalakan *filter*nya untuk layanan apa pun yang dijalankan, terutama SSH. Konfigurasi lainnya juga bisa dilakukan untuk berapa lama pencekalan berdasarkan berapa banyak pencocokan *filter* (seperti upaya login yang gagal dari berbagai jenis) dan juga menentukan larangan lebih lama untuk pelaku "*residivist*" yang terus kembali [4].

## III. Metodologi Penelitian

Metode penelitian yang dilakukan adalah Penelitian Tindakan (*Action Research)* dengan mengamati (observasi) lingkungan Teknologi Informasi Institut Bisnis Nusantara, menganalisa kebutuhan yang diperlukan dalam pengembangan Situs *Web* www.ibn.ac.id, serta mempelajari teori-teori terkait pengembangan Situs *Web* dan keamanan nya dengan menerapkan *Web Application Firewall* pada Situs *Web* www.ibn.ac.id. Peninjauan ulang dalam pengembangan Situs *Web* dan keamanan nya ini perlu dilakukan untuk memastikan sudah optimalnya penerapan *Web Application Firewall* dan *IP Address Banning (Fail2ban)* pada situs *web* www.ibn.ac.id Institut Bisnis Nusantara.

## IV. Hasil dan Pembahasan

**Observasi**

Observasi pada teknologi yang digunakan Situs *Web* Institut Bisnis Nusantara adalah sebagai berikut.

TABEL I
TEKNOLOGI WEB SERVER INSTITUT BISNIS NUSANTARA

| Software / Version | Category |
|---|---|
| IIS 5.0 | Web Servers |
| Microsoft ASP.NET | Web Frameworks |

Teknologi *Web Server* yang digunakan pada Situs *Web* Institut Bisnis Nusantara adalah dengan menggunaan *webserver* IIS versi 5.0 dan ASP.Net pada *web framework* nya.

Tampilan Situs *Web* Institut Bisnis Nusantara adalah seperti pada gambar berikut :


Gambar 3. Tampilan Situs *Web* Institut Bisnis Nusantara

Situs *Web* Institut Bisnis Nusantara menggunakan HTML versi 4.0 dengan desain yang belum *responsive* pada perangkat *Mobile.*

**Analisa**

Hasil observasi yang telah dilakukan dapat dianalisa bahwa teknologi Situs *Web* yang digunakan pada Institut Bisnis Nusantara perlu ada pembaruan versi atau menggunakan teknologi terkini. Teknologi yang digunakan memiliki beberapa celah keamanan yang terdapat pada *web server* IIS versi 5.0 yang tercantum pada daftar *Common Vulnerabilities and Exposures* (CVE) berikut [5].

TABEL II
CVE MICROSOFT IIS 5.0

CVE-2011-5279
CVE-2009-4444
CVE-2009-3023
CVE-2009-2521
CVE-2009-1535
CVE-2009-1122
CVE-2008-1446

Belum terpasangnya *Secure Socket Layer* (SSL *Certificate*) pada *domain* ibn.ac.id yang menjadikan tidak terenkripsi komunikasi antara *browser client* dan *Web Server* sehingga informasi *username*, *password* dan data sensitif lain dapat terbaca secara *plain text.*

Kebutuhan *server* baru untuk meningkatkan keamanan dan penggunaan teknologi *web* yang terbaru diperlukan bagi situs *web* ibn.ac.id, analisa kebutuhan *server* Institut Bisnis Nusantara yaitu sebagai berikut :

| Software / Version | Category |
|---|---|
| Nginx | Web Servers |
| PHP 7.3.19 | Programming Languages |
| WordPress | CMS, Blogs |
| Plesk | Hosting Panels |
| Google Font API | Font Scripts |
| Lightbox | JavaScript Frameworks |
| Twitter Emoji (Twemoji) | JavaScript Graphics |
| jQuery | JavaScript Frameworks |

Gambar 4. Teknologi Server IBN terbaru

*Web server* IBN perlu menggunakan Nginx yang baik kecepatannya, dan menggunakan *programming language* PHP versi 7.3, desain *web* menggunakan wordpress untuk kemudahan pengelolaan konten serta perlu dukungan spesifikasi *server* dengan 4 CPU dan 8 GB RAM serta 160 GB SSD pada media penyimpanannya.

**Konfigurasi**

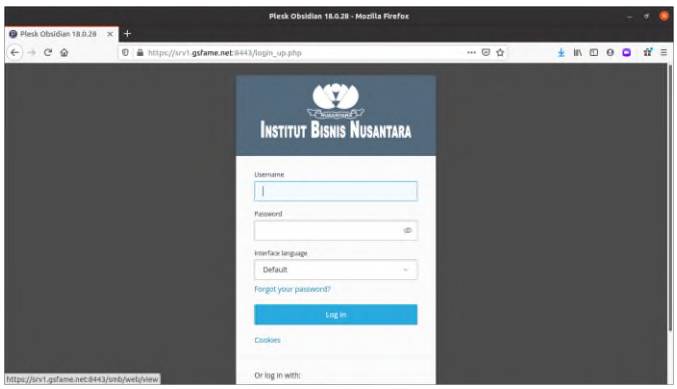
Konfigurasi *server* baru diperlukan bagi Situs *Web* Institut Bisnis Nusantara untuk mendukung keamanan yang baik.

Plesk sebagai *control panel web server* digunakan dengan tujuan kemudahan pengelolaan bagi *administrator server* situs *web* ibn.ac.id. Situs *Web* ibn.ac.id terbaru menggunakan *Content Management Systems* wordpress dengan desain yang *responsive* terhadap perangkat *Mobile*.

Pada penelitian ini pembuatan situs *web* dengan menggunakan *content management systems wordpress* tidak dibahas secara detail, pembahasan secara detail dapat dibahas pada penelitian berikutnya.

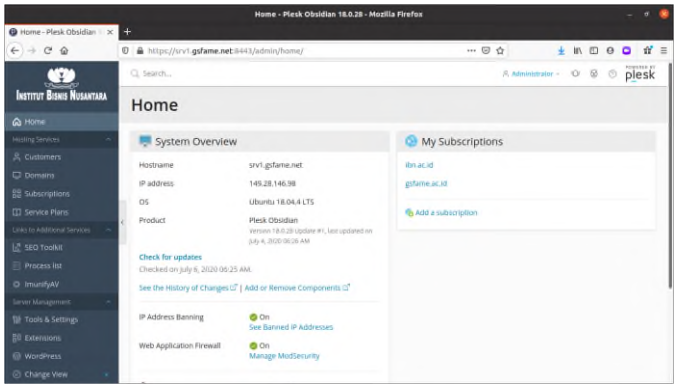
Gambar 5. Situs *Web* IBN Terbaru

Tampilan *Login* pada Plesk *Control Panel* seperti pada gambar berikut.



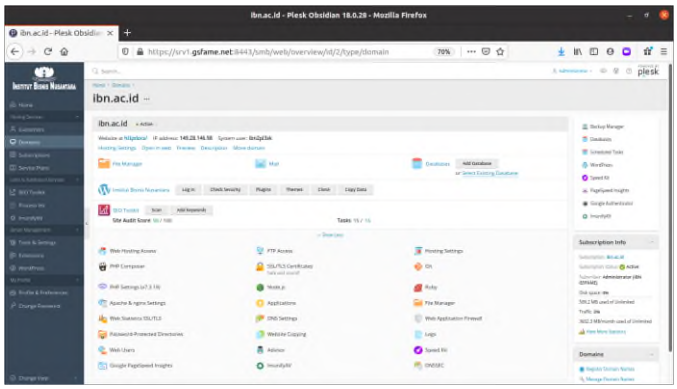

Gambar 6. Login PLESK IBN

Plesk memiliki tampilan *dashboard* yang berisikan informasi tentang *IP Address Server*, Sistem Operasi yang digunakan, *Hostname*, versi dari Plesk dan informasi tentang konfigurasi keamanan seperti : *IP Address Banning* dan *Web Application Firewall*, dan juga beberapa menu lain yang dapat digunakan dengan mudah.




Gambar 7. *Dashboard* PLESK

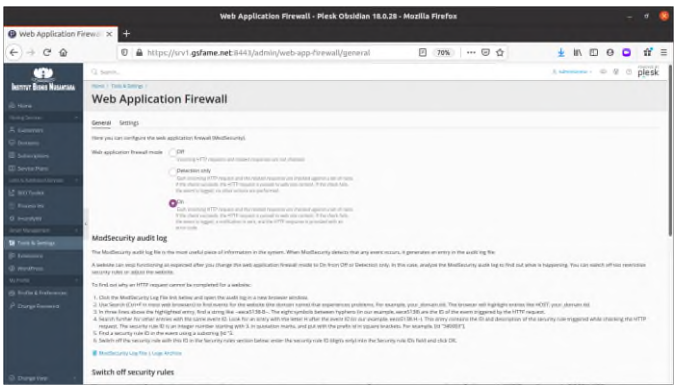
Plesk menyediakan *dashboard* khusus dalam pengelolaan situs *web* ibn.ac.id, seperti : instalasi wordpress, SSL *Certificate*, dan juga konfigurasi untuk PHP, Apache atau Nginx *web server*, dan lain-lain.




Gambar 8. *Dashboard* PLESK ibn.ac.id

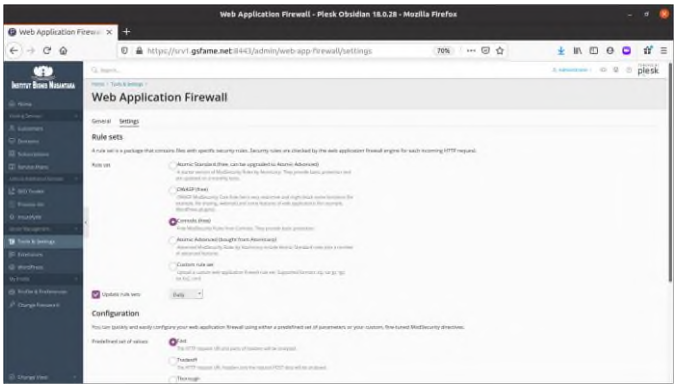
**ModSecurity WAF**

Untuk dapat bekerjanya *Web Application Firewall* pada PLESK, yaitu dengan mengaktifkan ModSecurity yang terdapat pada PLESK.




Gambar 9. WAF ModSecurity PLESK

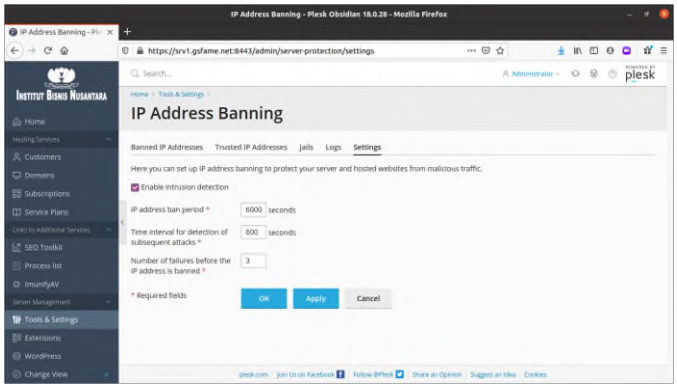
Konfigurasi *Rule set* berisikan *file-file* dengan spesifik *security rules*, konfigurasi *rule set* yang dipilih adalah dari Comodo *Rule set*.




Gambar 10. Comodo *Rule Set* dan *Configuration Fast*

**Fail2ban**

Konfigurasi tambahan lainnnya yang ada pada PLESK dapat digunakan adalah mengaktifkan *IP Address Banning (Fail2ban)*, dengan tujuan untuk mencekal *(Block) IP Address* yang melakukan upaya *login* yang gagal atau juga serangan *Brute Force*[6].

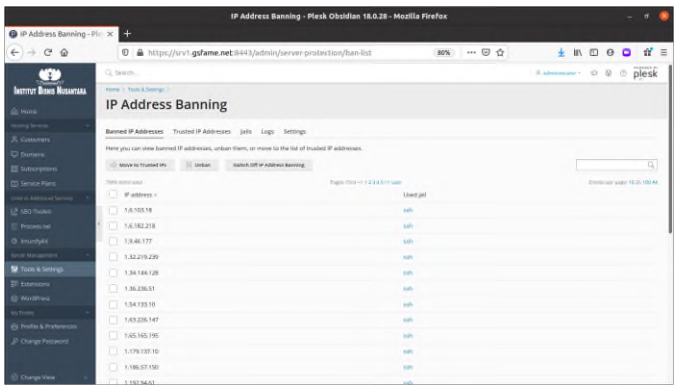



Gambar 11. *IP Address Banning (Fail2ban)*

**Tinjauan Ulang**

Konfigurasi *Web Application Firewall* dan *IP Address Banning (Fail2ban)* yang telah diterapkan dapat dilakukan pengujian.

Hasil pengujian keamanan dapat dilihat pada daftar dari *IP Address - IP Address* yang telah dicekal *(Banned)*, dapat dilihat pada menu *Banned IP Addresses.*




Gambar 12. Daftar *IP Address* yang dicekal

## V. KESIMPULAN

*Web Application Firewall* menganalisa lalu lintas HTTP untuk menentukan apakah *traffic* yang masuk *valid* dan berupaya untuk mencegah serangan *web* seperti serangan DDoS, *cross-site scripting* (XSS) dan SQL *Injection*. Dengan diterapkannya *Web Application Firewall* dapat mengamankan pada *application layer* Situs *Web* www.ibn.ac.id dan konfigurasi keamanan tambahan lain dengan menerapkan *IP Address Banning (fail2ban)* bisa mencekal (*block*) *IP Address-IP Address* yang gagal *login* dan upaya serangan *brute force*.

## UCAPAN TERIMA KASIH

Terima kasih Kepada Institut Bisnis Nusantara, Khususnya kepada Rektor, para Wakil Rektor, para Ketua Program Studi, dan pengurus Jurnal ESENSI Komputasi yang telah memberikan kesempatan dalam publikasi jurnal ini, Harapan jurnal ini dapat memberikan pengetahuan dan manfaat. Terima kasih.

## REFERENSI

[1] Margaret Rouse. Definition : Web Application Firewall (WAF), 2019.

[2] Maximilian Dermann, Mirko Dziadzka, Boris Hemkemeier, Achim Hoffmann, Alexander Meisel, Matthias Rohr, and Thomas Schreiber. Best Practices: "Use of web Application Firewalls." OWASP German Chapter, 2008.

[3] https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/web-application-firewall-modsecurity.73383/

[4] Bledsoe, Greg (2016-01-14). "Server Hardening | Linux Journal". Linux Journal. Retrieved 2018-09-22.

[5] https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-3436/version_id-63588/Microsoft-IIS-5.0.html

[6] https://docs.plesk.com/en-US/obsidian/administrator-guide/server-administration/protection-against-brute-force-attacks-fail2ban.73381/