KAMI MENGABDI
VOLUME 4 NOMOR 2 NOPEMBER 2024

Jurnal Artikel

Sosialisasi Pencegahan Serangan Peretasan Pada Server Web Untuk Pelajar SMK

Parlindungan Tampubolon[1], Satria Firmansyah[2], Muhammad Akbar Firdaus[3], Nayandra Akbar Pratama[4], Raihan Putra Pratama[5,] Muhammad Zulfikor[6], Aura Sandi Yudha[7] EE Lailatul Putri[8]
Prodi Informatika Universitas 17 Agustus 1945 Jakarta
Email: parlindungan.tampubolon@uta45jakarta.ac.id

Artkel Info - : Received : ; Revised : ; Accepted:

Abstrak

Dalam beberapa tahun terakhir, kemajuan teknologi informasi telah berkembang pesat, memudahkan berbagai aktivitas dan pekerjaan, termasuk akses berita dan informasi. Salah satu media yang sering digunakan untuk mencari informasi adalah website, yaitu kumpulan halaman dalam satu domain atau subdomain yang memuat data seperti teks, gambar, dan suara yang dapat diakses secara daring. Kemajuan teknologi internet menjadikannya media utama untuk bertukar data, meskipun tidak semua informasi tersedia untuk umum. Penggunaan layanan jaringan interconnection networking (internet) dan komputer berkembang pesat di berbagai bidang, memudahkan akses informasi. Di era Internet dan World Wide Web, keamanan sistem menjadi isu penting dalam sistem informasi berbasis web global, dengan komitmen kuat dari para profesional keamanan sistem, komunitas riset, dan vendor perangkat lunak. Keamanan jaringan merupakan aspek penting dalam sistem informasi organisasi dan perusahaan; kelemahannya dapat meningkatkan serangan hacker.Seiring perkembangan zaman, website juga berkembang dan menjadi populer, sering menjadi sasaran serangan. Kegiatan pengabdian masyarakat berjudul "Sosialisasi Pencegahan Serangan Peretasan Pada Server Web Untuk Pelajar SMK" bertujuan memberikan pemahaman lebih baik tentang pencegahan serangan web server kepada peserta. Hasil kegiatan menunjukkan peningkatan signifikan dalam pemahaman partisipan tentang pencegahan serangan web server. Pembahasan kegiatan ini menyoroti pentingnya pencegahan serangan web server sebagai landasan partisipasi aktif dalam pendidikan berbasis teknologi. Dengan pemahaman yang lebih baik, pelajar lebih siap menghadapi tuntutan dunia kerja yang semakin terhubung secara digital dan menerapkan pengetahuan ini untuk meningkatkan kualitas hidup mereka.

Kata kunci: *Web Server, Serangan, Keamanan*

Abstract

In recent years, advancements in information technology have developed rapidly, facilitating various activities and tasks, including accessing news and information. One of the most frequently used media for finding information is the website, which is a collection of pages within a domain or subdomain containing data such as text, images, and audio that can be accessed online. The progress of internet technology has made it a primary medium for data exchange, although not all information is available to the public. The use of interconnection networking (internet) and computer services has grown rapidly across various fields, making information access easier. In the era of the Internet and the World Wide Web, system security has become a critical issue in global web-based information systems, with strong commitment from system security professionals, the research community, and software vendors. Network security is a crucial aspect of organizational and corporate information systems; its weakness can increase hacker attacks. As time progresses, websites have also evolved and become popular, often becoming targets of attacks. The community service activity titled "Socialization of Web Server Hacking Prevention for Vocational High School Students" aims to provide participants with a better understanding of web server attack prevention. The results of this activity showed a significant increase in participants' understanding of web server attack prevention. The discussion in this activity highlights the importance of preventing web server attacks as a foundation for active participation in technology-based education. With better understanding, students can be more prepared to face the demands of an increasingly digitally connected workforce and apply this knowledge to improve their quality of life.

Keywords: *Web Server, Attacks, Security*

1. PENDAHULUAN

Selama beberapa tahun terakhir, kemajuan teknologi informasi telah berkembang dengan cepat. Perkembangan ini telah membuat berbagai aktivitas dan pekerjaan menjadi lebih mudah, termasuk dalam mengakses berita dan informasi. Salah satu media yang sering digunakan untuk mencari berbagai jenis informasi saat ini adalah website [1]. Website adalah sekumpulan halaman yang tergabung dalam satu domain atau subdomain, dan dapat diartikan sebagai halaman yang memuat data seperti teks, gambar, suara, dan lainnya yang bisa diakses secara daring atau online [2].

Kemajuan teknologi internet telah menjadikannya sebagai media utama untuk bertukar data. Tidak semua informasi tersedia untuk khalayak umum [3]. Penggunaan layanan jaringan interconnection networking (internet) dan komputer berkembang dengan pesat di berbagai bidang, sehingga memudahkan akses ke berbagai jenis informasi [4] .

Di era Internet dan World Wide Web, keamanan sistem telah menjadi isu penting dalam sistem informasi berbasis web global. Hal ini dapat dilihat dari komitmen yang kuat dari para profesional keamanan sistem, komunitas riset, dan vendor perangkat lunak [5]. Salah satu aspek penting dalam sistem informasi organisasi dan perusahaan adalah keamanan jaringan. Lemahnya keamanan jaringan dapat meningkatkan serangan hacker pada sistem[6].

Seiring dengan berkembangnya zaman website pun juga turut ikut berkembang dan menjadi populer dikalangan masyarakat, banyaknya website yang ada pada saat ini membuat ia sering dijadikan sasaran [1].

Pencegahan serangan peretasan pada server web dapat dilakukan dengan berbagai langkah keamanan. Berikut adalah beberapa strategi penting untuk melindungi server web dari serangan peretasan:

1. Perbarui Perangkat Lunak Secara Berkala: Selalu pastikan bahwa sistem operasi, server web, dan semua aplikasi terkait diperbarui dengan patch keamanan terbaru.
2. Gunakan Firewall dan Sistem Deteksi Intrusi: Menggunakan firewall untuk memantau dan mengontrol lalu lintas jaringan serta sistem deteksi intrusi (IDS) untuk mendeteksi aktivitas mencurigakan dapat mencegah akses yang tidak sah.
3. Amankan Konfigurasi Server: Pastikan konfigurasi server web aman dengan menonaktifkan layanan yang tidak perlu, membatasi akses ke file dan direktori penting, dan menggunakan izin yang tepat.
4. Enkripsi Data: Gunakan HTTPS untuk mengenkripsi data yang dikirim antara server dan pengguna. Ini membantu mencegah penyadapan dan manipulasi data.
5. Implementasi Otentikasi dan Otorisasi yang Kuat: Gunakan kata sandi yang kuat dan multifaktor otentikasi (MFA) untuk melindungi akun pengguna dan administrator.
6. Monitor dan Audit Log: Pantau log server secara rutin untuk mendeteksi aktivitas yang mencurigakan. Audit log dapat membantu mengidentifikasi pola serangan dan merespons dengan cepat.
7. Proteksi Terhadap Serangan SQL Injection dan Cross-Site Scripting (XSS): Gunakan validasi input yang ketat dan teknik penyusunan kode

yang aman untuk mencegah serangan SQL Injection dan XSS.

8. Backup Data Secara Berkala: Lakukan backup data secara rutin dan simpan backup di lokasi yang aman untuk memastikan data dapat dipulihkan jika terjadi serangan.
9. Gunakan Alat Keamanan Tambahan: Pertimbangkan penggunaan alat keamanan tambahan seperti WAF (Web Application Firewall) untuk melindungi aplikasi web dari serangan.
10. Pelatihan Keamanan untuk Staf: Berikan pelatihan keamanan kepada staf untuk meningkatkan kesadaran mereka terhadap praktik keamanan terbaik dan ancaman terbaru.

Dengan menerapkan langkah-langkah ini, server web dapat terlindungi dari berbagai serangan peretasan dan ancaman keamanan lainnya.

2. METODE

2.1 Tempat dan waktu

Pengabdian masyarakat ini dilaksanakan pada tanggal 30 Januari 2024 dilakukan di SMK Perguruan Cikini Alur Laut pada pukul 10.00 WIB – 12.00WIB.

2.2 Khalayak Sasaran

Sasaran utama pada pengabdian masyarakat adalah siswa/i SMK Perguruan Cikini Alur Laut dengan memberikan pamahaman yang komprehensif tentang pencegahan serangan peretasan pada server web. Diharapkan dapat memberikan pemahaman mengenai mitigasi serangan pada web server.

2.3 Metode Pengabdian

Metode pengabdian ini dilakukan di SMK Cikini Alur Laut, kemudian menyampaikan materi tentang pencegahan terhadap serangan web server oleh bapak Parlindungan Tampubolon, S.Kom., M.Kom.

2.4 Indikator Keberhasilan

Keaktifan siswa dalam kegiatan pengabdian masyarakat diukur untuk mengetahui sejauh mana mereka berpartisipasi. Siswa dapat berkontribusi dalam pengembangan materi, mengajukan pertanyaan setelah materi disampaikan, serta memberikan pendapat atau saran terkait materi atau kekurangan selama pengenalan kegiatan..

3. HASIL DAN PEMBAHASAN

Kegiatan pengabdian masyarakat berjudul "Sosialisasi Pencegahan Serangan Peretasan Pada Server Web Untuk Pelajar SMK" bertujuan untuk memberikan pemahaman yang lebih baik kepada peserta mengenai cara pencegahan terhadap serangan web server.

Hasil dari kegiatan ini menunjukkan bahwa partisipan mengalami peningkatan signifikan dalam pemahaman mereka tentang pencegahan serangan terhadap web server. Pembahasan dalam kegiatan ini menyoroti pentingnya pencegahan terhadap serangan web server sebagai landasan untuk berpartisipasi aktif dalam pendidikan berbasis teknologi. Dengan meningkatkan pemahaman tersebut, pelajar dapat lebih siap menghadapi tuntutan dunia kerja yang semakin terhubung secara digital dan juga menerapkan pengetahuan ini dalam meningkatkan kualitas hidup mereka.

3.1 Kegiatan

Berikut dokumentasi kegiatan:

Gambar 1. Pemaparan Materi

Gambar 2. Sharing Session

Gambar 3. Pemaparan Materi

Gambar 4. Foto Bersama

3.2 Keberhasilan

Indikator keberhasilan dilihat berdasarkan hasil kegiatan pengabdian masyarakat mengenai Sosialisasi Pencegahan Serangan Peretasan Pada Server Web Untuk Pelajar SMK di SMK Perguruan Cikini Alur Laut. Berikut adalah beberapa capaian yang telah dicapai melalui kegiatan pengabdian masyarakat ini:

1. Memberikan pemahaman dan peningkatan kepada para siswa tentang Pencegahan Serangan Peretasan Pada Server Web siswi di SMK Perguruan Cikini Alur Laut.
2. Siswa dapat mengetahui teknologi Pencegahan Serangan Peretasan Pada Server Web.
3. Kegiatan ini dapat meningkatkan motivasi dan minat siswa/i terhadap Keamanan Komputer.
4. Kegiatan ini juga membantu memperkuat hubungan antara SMK Perguruan Cikini Alur Laut dan Universitas 17 Agustus 1945 Jakarta. Kerja sama antara sekolah, siswa/i, dan pihak kampus atau dosen memperluas akses terhadap sumber daya dan peluang dalam bidang Pencegahan Serangan Peretasan Pada Server Web.

4. KESIMPULAN

Kegiatan pengabdian masyarakat yang bertujuan untuk sosialisasi tentang pencegahan serangan peretasan pada server web untuk siswa SMK di SMK Perguruan Cikini Alur Laut berhasil mencapai beberapa tujuan penting. Pertama, kegiatan ini berhasil meningkatkan pemahaman siswa tentang keamanan server web dan strategi pencegahannya. Siswa dapat memahami teknologi yang digunakan untuk melindungi informasi dan infrastruktur digital. Selain itu, kegiatan ini juga berhasil meningkatkan motivasi serta minat siswa terhadap bidang keamanan komputer, membantu mereka mempersiapkan diri untuk tantangan dunia digital yang semakin kompleks.

Kegiatan tersebut juga membawa manfaat dalam memperkuat hubungan antara SMK Perguruan Cikini Alur Laut dengan Universitas 17 Agustus 1945 Jakarta. Melalui kerjasama antara sekolah, siswa, dan pihak kampus atau dosen, tercipta kolaborasi yang produktif dalam bidang teknologi informasi. Ini tidak hanya memperluas akses terhadap sumber daya dan peluang dalam pencegahan serangan peretasan pada server web, tetapi juga mempromosikan pendidikan yang lebih terintegrasi dan aman dalam penggunaan teknologi di kalangan siswa SMK.

DAFTAR PUSTAKA

[1] Wiguna, B., Prabowo, W. A., Ananda, R., Informatika, T., Informatika, F., Tekbologi, I., Purwokerto, T., Pandjaitan, J. D. I., 128, N., Selatan, P., & Tengah Indonesia, J. (n.d.). *Wiguna, Implementasi Web Application Firewall dalam Mencegah Serangan SQL Injection pada Website Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website*. https://doi.org/10.31849/digitalzone.v11i2.4867ICCS

[2] Rosyida Zain, A., Muhamad, I., Matin, M., & Kautsar, D. K. (2023). Analisis Implementasi Modsecurity dan Reverse Proxy Untuk Pencegahan Serangan Keamanan DDoS pada Web Server. *SNIV: Seminar Nasional Inovasi Vokasi*, *2*(1), 118–127.

[3]Alfidzar, H., & Zen, B. P. (2022). Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif Guna Untuk Mendeteksi Serangan DDOS Pada Server. *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, *4*(2), 32–45. https://doi.org/10.20895/inista.v4i2.534

[4] Rizal, R., & Sumaryana, Y. (2021). Peningkatan Keamanan Aplikasi Web Menggunakan Web Application Firewall (WAF) Pada Sistem Informasi Manajemen Kampus Terintegrasi. *Jurnal ICT : Information Communication & Technology*, *20*(2), 323–330. https://doi.org/10.36054/jict-ikmi.v20i2.416

[5] Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, *18*(1), 77–86. https://doi.org/10.33364/algoritma/v.18-1.827

[6] Faatihah, atul, Dewi Zulaikha, A., Satrio Wicaksono, G., Teknologi Yogyakarta Jl Siliwangi, U., Lor, J., Mlati, K., Sleman, K., & Istimewa Yogyakarta, D. (2024). Analisis dan Evaluasi Terkait Keamanan pada Web Server. In *Jurnal Ilmiah Sains dan Teknologi* (Vol. 2, Issue 7).