Security Testing Dengan Menggunakan Metode OSSTMM Pada Web Institut Teknologi Telkom Purwokerto

Edy Surmana Putra Tarigan[1], Muhammad Fajar Sidiq[2], Ipam Fuaddina Adam[3], Rifki Adhitama[4]
[1,2,3]Program Studi S1 Informatika, Fakultas Teknologi Industri dan Informatika
[4]Program Studi S1 Rekayasa Perangkat Lunak, Fakultas Teknologi Industri dan Informatika
[1,2,3]Institut Teknologi Telkom Purwokerto
Jl. D. I. Panjaitan No. 128, Purwokerto Selatan, Banyumas, Jawa Tengah 53147
14102058@ittelkom-pwt.ac.id

Abstrak – Keamanan data pada web server merupakan tugas utama yang perlu untuk diperhatikan. Salah satu bidang yang sangat membutuhkan website adalah bidang Pendidikan seperti IT Telkom Purwokerto. IT Telkom Purwokerto menggunakan website resmi dengan domain yaitu http://ittelkom-pwt.ac.id. Website ini dipergunakan sebagai media informasi yang akan memberikan informasi mengenai akademik, penerimaan mahasiswa baru dan juga mengenai informasi alumni. Penggunaan website yang tidak berjalan dengan baik akan menimbulkan dampak yang sangat berpengaruh pada nilai bisnis dan juga kegiatan operasional kampus seperti pemberitahuan informasi yang terdapat pada website. Untuk mencegah hal ini dibutuhkan sebuah pengidentifikasian mengenai kondisi dan keadaan sebuah website dengan melakukan proses pengetesan keamaanan maka diperlukan adanya pengecekan kerentanan dan celah kerawanan pada suatu web. Metode yang digunakan penelitian ini adalah metode OSSTMM karena mampu menguji seberapa tinggi tingkat keamanan suatu aplikaksi web melalui diketahuinya nilai dan tingkat keamanan dan rekomendasi yang berguna Hasil dari metode ini adalah Actual Security yang bernilai 79,5937 yang menunjukkan bahwa keamanan yang belum dapat menyeimbangkan dengan interaksi ataupun dengan layanan yang ada. Oleh karena itu untuk dapat mencapai nilai 100 harus ditingkatkan lagi sebanyak 20,99. dengan membuat nilai Limitation yaitu Vulnerability, Weakness dan Concern bernilai 0.

Kata kunci – Website, OSSTMM, Actual Security

Abstract—Data security on the web server is the main task that needs to be considered. One area that really needs a website is the field of education such as IT Telkom Purwokerto. Purwokerto IT Telkom uses an official website with a domain, http://ittelkom-pwt.ac.id. This website is used as an information medium that will provide information about the academic, admission of new students and also about alumni information. The use of websites that do not work well will have an impact that has a profound effect on the value of the business as well as campus operations such as notification of information contained on the website. To prevent this, an identification is needed regarding the condition and condition of a website by conducting a security testing process, so it is necessary to check for vulnerabilities and vulnerabilities on a web. The method used in this study is the OSSTMM method because it is able to test how high the security level of a web application is through knowing the value and level of security and useful recommendations. or with existing services. Therefore to be able to reach a value of 100 must be increased again by 20.99. by making the Limitation value, Vulnerability, Weakness and Concern is 0

Keywords- Website, OSSTMM, Actual Security

I. PENDAHULUAN

Server digunakan sebagai media penyimpanan data yang terdapat pada website, keamanan data pada web server menjadi tugas utama yang perlu untuk diperhatikan. Web server sangat dibutuhkan oleh setiap bidang seperti pendidikan, kesehatan, dan juga kegiatan bisnis. Salah satu bidang yang sangat membutuhkan website adalah bidang pendidikan dikarenakan banyaknya kebutuhan dalam bidang pendidikan yang mendorong untuk melakukan kinerja yang cepat dan efisien seperti akademik, promosi dan PMB. [3]

IT Telkom Purwokerto merupakan salah satu perguruan tinggi yang terdapat di Indonesia yang bergerak di bidang pendidikan. IT Telkom Purwokerto menggunakan website resmi dengan domain yaitu http://ittelkom-pwt.ac.id. Website ini dipergunakan sebagai media informasi yang akan memberikan informasi mengenai akademik, penerimaan mahasiswa baru dan juga mengenai informasi alumni. Penggunaan website yang tidak berjalan dengan baik

akan menimbulkan dampak yang sangat berpengaruh pada nilai bisnis dan juga kegiatan operasional kampus seperti pemberitahuan informasi yang terdapat pada website. Untuk mencegah hal ini dibutuhkan sebuah pengidentifikasian mengenai kondisi dan keadaan sebuah website. Pengidentifikasian kondisi dapat dilakukan dengan melakukan proses mengetes keamanan suatu web. Dalam melakukan proses pengetesan keamaanan maka diperlukan adanya pengecekan kerentanan dan celah kerawanan pada suatu web.

Dalam pengimplementasiannya terdapat berbagai cara untuk mengetes keamanan suatu web, yaitu adanya beberapa metode seperti NIST, ISSAF dan OSSTMM [4]. Namun metode yang lebih baik, efisien dan lebih mampu mencakup penyelesaian dalam Security testing secara menyeluruh adalah OSSTMM [5][6]. OSSTMM merupakan metode global komprehensif untuk security testing dan merupakan metode yang mampu menguji seberapa tinggi tingkat keamanan suatu aplikaksi web melalui diketahuinya nilai dan tingkat keamanan dan rekomendasi yang berguna [4].

Berdasarkan latar belakang diatas maka dilakukan penelitian security testing pada website IT Telkom Purwokerto dengan domain http:ittelkom-pwt.ac.id dengan menggunakan metode OSSTMM. Dari penelitian ini diharapkan untuk mengetahui tingkat keamanan suatu website sebagai bahan pengevaluasian kepada pihak pengembang.

II. METODE PENELITIAN

A. Study Literature

Pada tahap ini dilakukan Study Literature untuk mencari informasi atau referensi penelitian sebelumnya yang berkaitan dengan penelitian yang dilakukan. Adapun informasi yang dicari yaitu berupa metode atau objek yang akan diteliti.

B. Pengumpulan Data

Pengumpulan data dilakukan wawancara dengan pihak Akademik Institut Telkom Purwokerto untuk mengali informasi seputar sistem yang akan dilakukan penelitian.

C. Analisis Data

Pada tahap ini data akan dianalisis untuk mengetahui data mana yang akan digunakan dan yang akan di terapkan metode OSSTMM.

D. Perancangan Metode OSSTMM

Perancangan metode OSSTMM diawali dengan:

a) Wawancara

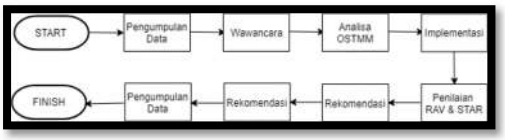
Wawancara dilakukan untuk mencari informasi seputar website IT Telkom Purwokerto yang akan diuji.

b) Study Literature

Study Literature dilakukan untuk mengetahui tahapan yang harus dilakukan pada saat penelitian seperti web penetration testing, web vulnerability, dan security testing.

c) Analisa OSSTMM

Pada tahap ini terlebih dahulu perlu dilakukan analisa tentang hal yang diperlukan sebelum dilakukannya Security testing. Dan juga memiliki hasil informasi-informasi yang didapatkan dari hasil wawancara untuk digunakan dalam menentukan suatu web yang akan di lindungi. Beberapa tahapan yang dilakukan pada OSSTMM seperti Gambar 2.1



Gambar 1 Tahapan metode OSSTMM

Berikut ini tahapan metode OSSTMM

1. Mendefinisikan apa yang akan diproteksi yang disebut dengan Aset.
2. Mengetahui lingkungan sekitar Aset yang dapat berupa mekanisme proteksi, proses atau service yang berada disekitar Aset. Disini akan terjadi interaksi dengan Aset. Ini disebut dengan Zona Engagement.
3. Mengetahui segala sesuatu yang berada diluar Zona Engagement yang diperlukan untuk menjaga Aset. Semua ini disebut dengan Skop.
4. Bagaimana skop berinteraksi dengan dirinya sendiri dan dunia luar. Aset yang berada dalam skop dikelompokkan melalui arah interaksi. Bisa dipahami sebagai arah darimana dilakukan security testing (pengetesan keamanan) pada penelitian. Hal ini disebut dengan Vektor. Masing-masing vektor harus dites secara terpisah.
5. Identifikasi perlengkapan yang diperlukan untuk melakukan tes. Pada Vektor, interaksi bisa terjadi pada berbagai level. Level-level ini bisa dibagi dalam banyak jalan, semuanya dibagi berdasarkan fungsi dan disebut dengan Channel yakni Human, Physical, Wireless, Telecommunication dan Data Network. Masing-masing channel harus dites terpisah untuk masing-masing vektor. Setiap Channel memiliki 17 modul yang sama. Setiap modul memiliki tugas yang berbeda-beda tergantung channel masing-masing.
6. Menentukan Tipe Tes. Tentukan informasi apa yang ingin dihasilkan dari sebuah tes. Apakah hanya sekedar melakukan tes pada interaksi dengan Aset atau jangkauan yang lebih seperti mendapatkan respon dari penanganan keamanan.

Ini disebut dengan Tipe Tes. Tipe Tes ditentukan setiap kali ingin melakukan tes.

d) Implementasi

Setelah didapatkan informasi yang telah dibutuhkan maka tahap selanjutnya yaitu tahap implementasi keamanan. Pada tahap implementasi keamanan digunakan Sistem Operasi Kali Linux dengan kumpulan aplikasi yang tersedia dan bersifat opensource yang sudah di install Nmap, Zenmap, Nikto, Whois dan sebagainya.

e) Penilaian RAV dan STAR

Setelah tahap implementasi dilakukan maka selanjutnya dilakukan penilaian keamanan sistem dengan menggunakan penilaian Risk Assessment Value (RAV) dan Securtity Testing Audit Report (STAR). RAV digunakan untuk menghasilkan nilai keamanan sedangkan STAR digunakan untuk mengetahui hasil keamanan sistem berupa komentar tentang security testing yang dilakukan dan juga dapat berbentuk status.

f) Rekomendasi

Hasil dari penilain RAV dan STAR akan dijadikan rekomendasi untuk pengambilan keputusan.

g) Kesimpulan

Pada tahap ini akan ditarik kesimpulan berdasarkan hasil nilai akhir dari penelitian yang telah dilakukan

E. Pengujian Metode

Pada tahap pengujian dilakukan untuk mengetahui hasil dari metode dan apakah metode berjalan sesuai dengan yang diharapkan.

F. Analisis Hasil

Hasil yang didapatkan dari pengujian metode akan dianalisis. Jika terdapat kendala pada proses ini maka akan dilakukan proses pengujian kembali.

G. Penulisan Laporan

Selanjutnya hasil akan dilaporkan dalam bentuk penulisan laporan untuk memenuhi persyaratan tugas akhir..

III. HASIL PENELITIAN

Untuk mendapatkan hasil penelitian ini dapat dilakukan pengujian. Berikut ini hasil dari pengujian dari setiap tahap penelitian.

A. Wawancara

Wawancara yang dilakukan kepada pihak SISFO untuk mengetahui informasi seputar sistem web ittelkom-pwt.ac.id yang akan digunakan untuk penelitian ini.

B. Analisis OSSTMM

Adapun yang dianalisis pada OSSTMM yaitu:

1. Aset

Objek penelitian pada penelitian ini adalah sistem jaringan website ittelkom-pwt.ac.id.

2. Zona Engangement

Zona Engangement adalah sekitaran lingkungan yang menyangkut mekanisme proteksi, proses/layanan yaitu sebagai berikut:

a) Mekanisme Proteksi

Mekanisme proteksi yang digunakan oleh website kampus menggunakan proteksi DMZ. Proteksi DMZ yang dimaksud masih belum menggunakan sistem aktif tapi masih dengan menggunakan sistem pasif. Terkait dengan evaluasi website belum tertata dengan baik cuma ada anomali jaringan, traffic nya dapat diketahui dan dapat di cek lalu di evaluasi. Kemudian untuk hal akses untuk masuk kedalam website hanya dapat digunakan oleh team IT saja. Lalu untuk traffic di jaringan website tergolong masih kecil karena masih institusi.

b) Proses/Layanan

Proses/layanan yang diberikan seperti untuk menarik calon mahasiswa baru untuk dapat melihat masa pendaftaran untuk masuk ke kampus Institut Teknologi Telkom Purwokerto.

3. Skop

Beberapa hal yang dapat mempengaruhi secara langsung. Diantaranya adalah sebagai berikut:

a) Energi Listrik

Energi listrik yang digunakan untuk beroperasi jika mati listrik dengan menggunakan DBS.

b) Kebijakan/Legislasi/Regulasi

Kebijakan untuk melindungi website dengan menggunakan DMZ

c) Hosting dan Bandwith Internet

Hosting dan Bandwith Internet menggunakan 2 jalur, ada yang untuk jalur internet dan ada jalur untuk website.

4. Vektor

Ruang lingkup dalam berinteraksi dengan dirinya sendiri dan dengan dunia luar. Pengetesan security testing yang dilakukan dari dua arah, yaitu dari luar dan dari dalam. Dikarenakan pengetesan keamanan dilakukan dengan menggunakan jaringan internet luar

dan jaringan internet lokal, sehingga di tetapkan pada penelitian ini menggunakan dua arah interaksi.

5. Channel

Setelah dilakukan penelitian pada objek sistem web ittelkom-pwt.ac.id maka channel yang tepat untuk untuk membahas penelitian tersebut adalah dengan menggunakan Data Network Channel.

6. Tipe Tes

Tipe tes yang dilakukan harus tepat dan di sesuaikan dengan kondisi analis dalam melakukan penelitian ini. Tipe tes dipilih dari salah satu tipe tes yang ada. Maka dari itu ditentukan tipe tes yang paling tepat untuk penelitian ini adalah Double Blind (Black Box Test).

Berikut ini hasil dari penilaian RAV.

Gambar 2. Nilai RAV

Nilai yang telah didapatkan berasal dari rumus perhitungan RAV, yang memiliki Actual Security yang bernilai 79,5937. Jika dilihat dari penilaian RAV tersebut maka menunjukkan keamanan yang belum dapat menyeimbangkan dengan interaksi ataupun dengan layanan yang ada. Oleh karena itu untuk dapat mencapai nilai 100 harus ditingkatkan lagi sebanyak 20,99.

Cara yang digunakan untuk mendapatkan nilai 100 adalah dengan membuat nilai Limitation yaitu Vulnerability, Weakness dan Concern bernilai 0, karena itu nilai Limitation harus diperbaiki, sedangkan untuk menaikkan nilai yaitu dengan cara membuat nilai kontrol tinggi. Ketika nilai Limitation bernilai 0 maka nilai kontrol akan membuat nilai Actual Security menjadi diatas 100. Berikut ini pelaporan dari STAR.

Gambar 3. Laporan dari STAR

Beberapa rekomendasi solusi yang disarankan untuk penelitian ini adalah:

A. Rekomendasi Umum

1. Membuat kebijakan pemeliharaan secara berskala untuk aset sistem website ittelkom-pwt.ac.id.
2. Mempunyai sistem cadangan untuk mem-backup data dan jalur alternatif jikalau sistem website ittelkom-pwt.ac.id rusak ataupun mati.

B. Rekomendasi solusi untuk Vulnerability

1. Membuat anti-clicjacking x-frame option header
2. Menyembunyikan file yang berisi informasi yang penting.
3. Menyembunyikan folder file License.txt yang dapat mengidentifikasi sistem
4. Pastikan filter xss browser web diaktifkan.
5. Pastikan bahwa flag httponly diatur untuk semua cookie.

C. Rekomendasi untuk mengatasi Weakness dan Concern

1. Pada sistem belum ada pemberitahuan(notification) yang diberikan ketika ada serangan ke arah aset.
2. Membuat sertifikat lisensi SSL agar data lebih aman.

IV. PENUTUP

A. Kesimpulan

Beberapa kesimpulan yang dapat diambil dari penelitian ini adalah:

1. Ada beberapa tes yang tidak dilakukan karena dapat mengganggu kinerja dari web tersebut.
2. Hasil penilaian RAV pada sistem web ittelkom-pwt.ac.id adalah 79,5937 berarti masih kurang 20.99 untuk dapat memiliki nilai yang sempurna.
3. Metode OSSTMM masih memiliki kekurangan untuk penentuan hasil analisa, oleh karena itu hasil analisa yang didapatkan dapat berbeda beda dari setiap analis.
4. Beberapa tahapan yang ada di metode OSSTMM masih ada yang perlu ditambahkan dengan lebih rinci dan jelas

DAFTAR PUSTAKA

[1] Cenzic,Application Vulnerability Trends Report,2014.
[2] Erdogan, Gencer, Security Testing of Web Based Applications. Norwegia: University of Science and Technology, 2009.
[3] E.M,Angela," Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website,"no.22, vol.VII, 2013.
[4] Y. I. Fernando and R. Abdillah, “Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Manual (OSSTMM),” vol. 2, no. 1, pp. 33–40, 2016.
[5] F. Masykur, “Analisis Vulnerability Web Based Application Menggunakan Nessus,” no. 1, pp. 320–326, 2015.
[6] A. Boham and S. A. Rondonuwu, “e-journal ‘Acta Diurna’ Volume VI. No. 2. Tahun 2017,” vol. VI, no. 2, 2017