ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE SCANNING DAN PERHITUNGAN SECURITY METRIKS

ANALYSIS WEBSITE SECURITY USING SCANNING METHOD AND CALCULATION OF SECURITY METRICS

Mia Zattu Maharani[1,1], Henry Rossi Andrian S.T., M.T.[1,2], Setia Juli Irzal Ismail S.T., M.T.[1,3]

[1] Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
[1]miazattum.student@telkomuniversity.ac.id, [2]rossi@tass.telkomuniveristy.ac.id, jul@tass.telkomuniversity.ac.id

Abstrak

Komputer sebagai media komunikasi data hingga saat ini berkembang semakin pesat. Salah satu bentuk nyata evolusi teknologi itu adalah perkembangan media informasi *online* seperti *website* yang dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu. Keamanan *website* saat ini sangat dibutuhkan untuk menjaga informasi-informasi yang terdapat pada *website*. Oleh karena itu perlu diterapkan suatu keamanan yang lebih baik, pada proyek akhir ini dilakukan analisis keamanan website dengan metode scanning dan perhitungan security metriks. Pengujian dilakukan dengan cara *vulnerability assessments* menggunakan aplikasi *acunetix* untuk menganalisis keamanan pada suatu *website* setelah itu dilakukan perhitungan *security metrics.* Hasil yang didapat pada perhitungan *security metrics* dengan menggunakan formula *base score* menunjukkan nilai *high* yang berarti tingkat keparahan paling berbahaya yang menempatkan target *scan* pada resiko maksimum untuk *hacking* dan pencurian data dalam *web* igracias.telkomuniversity.ac.id

Kata kunci : ***scanning, acunetix,* keamanan *website, security metrics***

Abstract

Computers as a medium of data communication to date is growing more rapidly. One of the real forms of technological evolution is the development of online information media such as websites that can be accessed around the world as long as connected to the internet network without limited space and time. Website security is currently needed to maintain the information contained on the website. Therefore it is necessary to apply a better security, in this final project conducted a security analysis website with the method of scanning and calculation of security metrics. Testing is done by way of vulnerability assessments using an acunetix application to analyze the security on a website after that do the calculation of security metrics. The results obtained in the calculation of security metrics by using the base score formula shows the high value which means the most dangerous severity that places the target scan at the maximum risk for hacking and data theft in the web igracias.telkomuniversity.ac.id..

Keywords: ***scanning , acunetix, website security , security metrics***

1. Pendahuluan

Website adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu [1]. Banyak ancaman keamanan terjadi dalam bentuk pencurian virtual di Internet. Dalam hitungan detik, seorang pencuri virtual dapat mengakses sistem dan mencuri informasi penting, seperti *password* dan informasi pribadi. Kerusakan juga bisa dilakukan dengan infiltrasi sistem dan informasi tentang itu dengan melewatkan virus dan *worm* oleh karena itu dibutuhkan pengetahuan tentang celah keamanan *web* agar *web* tersebut dapat segera diperbaiki.

Vulnerability Assessment (VA) adalah analisa keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil scanning jaringan, konfigurasi pada sistem, cara pengelolaan, kesadaran keamanan orang-orang yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada [1]. Jauh berbeda dengan pentest *blackbox* dan *greybox*. Kedua jenis pentest ini tidak mampu memberikan hasil yang komprehensif karena tidak seluruh potensi kerentanan kritis akan teridentifikasi. Bahkan ditemukan dalam banyak kasus, hasil pentest *blackbox* melaporkan tidak adanya kelemahan kritis, namun saat dilakukan *Vulnerability Assessment (VA)* terdapat beberapa kelemahan kritis

Pada proyek akhir ini dilakukan pengujian celah keamanan dengan metode scanning pada web igracias.telkomuniversity.ac.id, ppdu.telkomuniversity.ac.id. Hasil *scan* berupa perhitungan *security metrics* yang akan menampilkan *score* akhir dari hasil *Vulnerability Assessments*

2. Dasar Teori /Material dan Metodologi/perancangan

2.1 Website

Website adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu [1]. *Website* merupakan sebuah komponen yang terdiri dari teks, gambar, suara animasi sehingga menjadi media informasi yang menarik untuk dikunjungi oleh banyak orang.

2.2 Acunetix

Acunetix website application scanner merupakan perangkat lunak yang dikembangkan untuk melakukan *scanning*. Kelebihan dari *tools* ini adalah kemampuannya untuk memberikan solusi dari kelemahan yang ditemukan dan mengelola *traceability* dari setiap *vulnerabilities* tersebut. Selain itu, *acunetix* menyediakan fungsi-fungsi tambahan yang dapat digunakan untuk melakukan pengujian lebih lanjut terhadap *website* yang diuji. [1]

2.3 Security Metrics

Security metrics merupakan pengukuran kuantitatif untuk menilai operasi keamanan di organisasi membantu organisasi untuk membuat keputusan tentang berbagai aspek keamanan yang meliputi arsitektur keamanan dan kontrol untuk efektivitas dan efisiensi operasi keamanan [2]. *Security metrics* dapat diukur dengan skala 1-10 dimana 10 adalah sistem sangat tidak aman dan bisa ditembus penyerang selain itu, *security metrics* berharga untuk tingkat manajerial TI dan stakeholder yang mempertanyakan dampak keamanan terhadap bisnis proses dan kegiatan. *NIST (National Institute of Standards and Technology)* mengkategorikan *security metrics* menjadi 3 tipe sebagai berikut [3] :

a. *implementation metrics* yaitu dimaksudkan untuk menunjukkan kemajuan dalam mengimplementasikan informasi program keamanan, kontrol keamanan, dan kebijakan prosedur yang terkait [3]

b. *effectiveness/efficiency metrics* yaitu dimaksudkan untuk memantau apakah program tingkat proses dan sistem tingkat kontrol keamanan diterapkan dengan benar, operasi sebagaimana yang dimaksud serta memperoleh hasil yang diinginkan [3]

b. *impact metrics* yaitu dimaksudkan untuk mengartikulasikan dampak keamanan informasi pada misi organisasi [3]

security metrics pada Proyek Akhir ini dinilai dengan parameter yaitu *vulnerability assessments y*ang dimaksud dengan *vulnerability* adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi sistem. Kerentanan*(vulnerability)*. Selanjutnya dilakukan perhitungan *Common Vulnerability Scoring System* menggunakan metode sebagai berikut [4].

1. Base score/overall score mewakili karakteristik intrinsik dan mendasar dari kerentanan yang konstan seiring waktu dan lingkungan pengguna.

2. Temporal score mewakili karakteristik kerentanan yang berubah dari waktu ke waktu namun tidak diantara lingkungan pengguna.

3. Environmental score mewakili karakteristik kerentanan yang relevan dan unik bagi lingkungan pengguna tertentu.

2.4 Topologi Sistem Usulan

Perancangan dari topologi sistem usulan yang akan dibangun dapat dilihat pada gambar dibawah ini :

Gambar 1 Topologi Sistem Usulan

Pada Gambar 3.2 adalah rancangan desain dari gambar sistem yang akan dibangun pada Proyek Akhir ini. Pada gambar di atas terdapat website yang akan diuji menggunakan aplikasi *acunetix* untuk mengetahui celah keamanan pada *web* tersebut, setelah dilakukan pengujian akan dilakukan perhitungan *security metrics* untuk mendapatkan hasil akhir dari pengujian tersebut.

2.5 Perancangan dan Rencana pengerjaan

Adapun langkah-langkah pengerjaan Proyek Akhir ini adalah sebagai berikut:

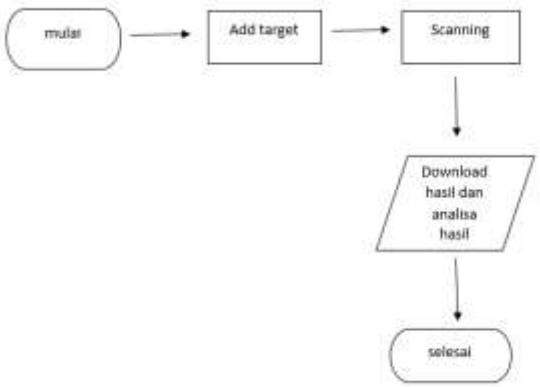
1. Melakukan proses instalasi *acunetix*.
2. Melakukan vulnerability assessments.
3. Menganalisa hasil dari *scanning.*
4. Menghitung *security metrics* dari hasil yang telah didapatkan dari proses *scanning*.
5. Melakukan dokumentasi terhadap proses instalasi, dan perhitungan *security metrics*.

2.6 Rencana Pengujian

1. *Scanning*
   Akan dilakukan *scanning vulnerability* untuk mengetahui beberapa celah pada suatu *web*
2. Perhitungan *security metrics*
   Setelah dilakukan proses *scanning vulnerability* dan mendapat data dari beberapa celah akan dilakukan perhitungan *security metrics* untuk mendapatkan hasil akhir dari pengujian yang telah dilakukan.

2.7 Skenario Pengujian

1. Vulnerability Assessments



Gambar 2 proses vulnerability assessments

3. Pembahasan

3.1 implementasi

Gambar 3 Hasil Scanning

Pada gambar 3 dapat dilihat hasil dari scanning web https://igracias.telkomuniversity.ac.id tertulis bahwa *"Acunetix Threat Level 3"* yang berarti kerentanan dikategorikan sebagai yang paling berbahaya yang menempatkan target *scan* pada resiko maksimum untuk *hacking* dan pencurian data.

Tabel 1 hasil scanning

Celah	Jumlah
Cross site scripting	7
jQuery cross site scripting	4
Vulnerable javascript library	2
HTML Form without CSRF protection	22

1. *Cross site scripting(XSS)* merupakan salah satu jenis serangan injeksi yang memungkinkan penyerang untuk mengirim kode berbahaya(biasanya dalam bentuk javascript) ke pengguna lain agar dapat mengumpulkan cookie sesi dan mengambil alih akun dan meniru identitas pengguna dan memodifikasi isi halaman yang disajikan kepada pengguna.

   solusi yang disarankan adalah dengan membuat karakter-karakter yang memiiki makna di dalam *HTML(HyperText Markup Language)* dan *JavaScript* untuk diubah menjadi *named entity* atau cara lainnya dengan menghilangkan sama sekali seluruh tag *HTML* atau *script* dari inputan *user*.

2. *Jquery cross site scripting* Pada igracias ini menggunakan *jquery* versi lama yang rentan terhadap *cross site scripting*

   Solusi yang disarankan adalah dengan memperbaharui menjadi *jquery* 1.6.3.

3. *Vulnerable javascript library Javascript* yang digunakan pada *web* ini adalah *javascript* yang rentan terkena serangan

   Solusi yang disarankan adalah dengan memperbaharui ke versi terakhir

4. *HTML form without CSRF protection*

   CSRF (Cross Site Request Forgery) adalah sebuah serangan pada *website* yang dieksekusi atas wewenang korban, tanpa dikehendakinya. *CSRF* merupakan pemalsuan *request* yang berasal dari site yang berbeda, tetapi dari sisi *client* tidak mengubah alamat IP karena dieksekusi oleh korban. Penyerang mengirimkan link atau halaman berisi *request* tersembunyi pada pengguna(korban), yang dieksekusi oleh pengguna tersebut ke *website* target. Dalam menyusun serangan, penyusun akan mempelajari terlebih dahulu kelemahan-kelemahan *website* target yang dapat dimanfaatkan dengan teknik *CSRF*. *Website* yang menyimpan *cookies* sehingga mengizinkan pengguna untuk datang kembali tanpa mengetikkan *username* dan *password*, akan menarik perhatian penyerang untuk lebih mengeksplorasi fitur-fitur yang terdapat pada *website* setelah *login*.

3.2 *Base score*

mewakili karakteristik intrinsik dan mendasar dari kerentanan yang konstan seiring waktu dan lingkungan pengguna

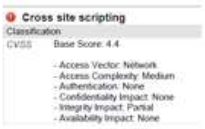
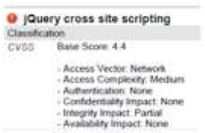
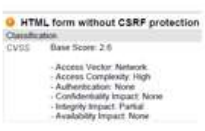
BaseScore = (0.6*Impact +0.4*Exploitability-1.5)*f(Impact)

*Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))*

*Exploitability = 20 * AccessComplexity * Authentication * AccessVector*

f(Impact) = 0 if Impact=0; 1.176 otherwise

Tabel 2 *base score*

Celah	*Base score*	Kategori
Cross site scripting 	4.4	Sedang
Jquery cross site scripting 	4.4	Sedang
Vulnerable javascript library 	6.4	Tinggi
HTML form without CSRF Protection 	2.6	Rendah

4. Kesimpulan

Dari hasil pengujian sistem dapat diambil kesimpulan sebagai berikut :

1. Pengujian keamanan website dapat dilakukan dengan cara *Vulnerability Assessment* menggunakan aplikasi *acunetix.*
2. Menentukan keamanan sebuah *website* dapat ditentukan dengan menggunakan *security metrics* yang dapat menampilkan hasil berlabel *High, Medium* atau *Low* yang ditentukan dengan menggunakan rumus *BaseScore* yang menghasilkan jumlah hasil 1-10.
3. Hasil vulnerability assessments pada igracias.telkomuniversity.ac.id adalah bernilai high.

Daftar Pustaka :

[1] Suryayusra, "Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang menggunakan Acunetix Vulnerability," *Thesis,* 2014.

[2] M. Khan, "Security Metrics Based Network Risk Asessment," *Thesis* , 2013.

[3] s. Radack, "Performance Measurement Guide For Information Security," *report,* 2008.

[4] first, "www.first.org," first, 2017. [Online]. Available: https://www.first.org. [Diakses 24 july 2017].