ANASLISIS KERENTANAN TERHADAP ANCAMAN SERANGAN PADA *WEBSITE* PDAM TIRTA MUSI PALEMBANG

Doda Saputra Ahad[1], Muhamad.Akbar[2], Maria Ulfa[3]

[1,2,3] Fakultas Ilmu Komputer Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12 Palembang
dodasaputra@gmail.com, muhamad.akbar@binadarma.ac.id, maria.ulfa@binadarma.ac.id,

Abstrak. Pada saat ini *website* merupakan salah satu media informasi yang berkembang sangat cepat. Di dalam sebuah *website* tidak hanya desain dan informasi yang dipentingkan tetapi aspek keamanan serta celah kerentanan mempunyai peranan penting dalam sebuah website. Kebutuhan untuk mengetahui kerentanan sebuah *website* diperlukan untuk melindungi data dari kerusakan dan kehilangan data dan dari pihak yang tidak bertanggung jawab yang hendak mengakses dan merubah data. Permasalahan yang lain adalah mencakup perlindungan dari berbagai serangan dan gangguan dari luar maupun dalam. Metode yang digunakan pada penelitian tindakan yaitu *Action Research.* Untuk melakukan analisis keamanan *website*, *software* yang digunakan adalah *Acunetix website vulnerability scanner, Netsparker* dan *Nessus*. Penulis mengetahui celah kerentanan/vulnerability apa saja yang terdapat pada w*ebsite www.tirtamusi.com* mengkategorikannya sesuai dengan standar CVSS v3.

Keyword : Website, kerentanan website, Vulnerability, Acunetix, Netsparker, Nessus.

1. Pendahuluan

1.1 Latar Belakang

Web/Website merupakan sumber daya internet yang sangat populer dan dapat diguakan untuk memperoleh informasi, transaksi pembelian barang, diskusi, ataupun untuk keperluan lainnya. Sedangkan Hacking (Hack) merupakan suatu aktifitas mempelajari, menganalisis, memodifikasi, dan menyusup ke dalam sebuah sistem komputer baik untuk keuntungan maupun dimotivasi oleh tantangan. Jika kedua pengertian tersebut digabungkan, maka bisa ditarik kesimpulan bahwa Web-Hacking adalah suatu aktivitas mempelajari, menganalisis, memodifikasi, ataupun menyusup kedalam sebuah sistem komputer yang menggunakan protocol HTTP, yang mana file-file diletakkan kedalam sebuah kompter yang memiliki protocol tersebut (HTTP) yang disebut dengan istilah web server. Dari hasil wawancara dengan kepala unit bagian PDR (pengolahan data dan rekening) menyebutkan bahwa seringnya terjadi serangan terhadap situs web, dalam hal

ini banyak attacker yang mencoba menyerang server dengan cara menyisipkan file Sql Injection setelah sebelumnya melakukan serangan Ddos (Distributed Denial of Services) agar website tersebut down untuk beberapa waktu. Untuk menjaga situs web www.tirtamusi.com agar tetap berjalan sebagaimana mestinya serta mencegah gangguan dari pihak yang tidak bertanggung jawab, peneliti merasa perlu melakukan analisa pada situs web www.tirtamusi.com, untuk metode penelitian menggunakan metode action research dan dibantu tools analisis celah kerentanan dengan menggunakan Accunetic Web Vulnerability, Netsparker dan Nessus. Oleh karena itu peneliti tertarik untuk melakukan penelitian dengan judul "Analisis Kerentanan Terhadap Ancaman Serangan Pada Website PDAM Tirta Musi Palembang" terhadap sistem keamanan untuk melihat kerentanan atau Vulnerability yang ada.

2. Metodologi dan Perancangan

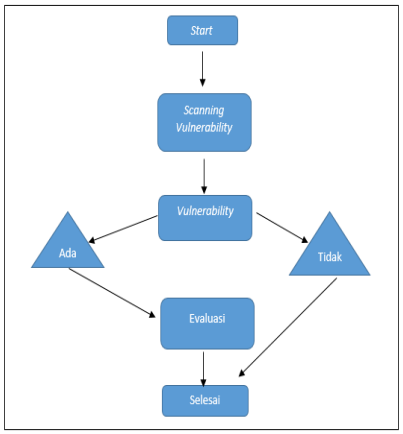
2.1 Metode

Dalam melakukan analisis disini peneliti mrnggunakan metode penelitian tindakan yaitu Action Research Menurut Jean Mcniff dan Jack WhiteHead (1988) ada lima tahapan dalam penelitian yang merupakan siklus dari action research, yaitu : Melakukan diagnosa (Diagnosing), Membuat rencana tindakan (Action Planning), Melakukan tindakan (Action Taking), Melakukan evaluasi (Evaluating), dan Pembelajaran (Learning).

2.2 Perancangan

(Diagnosing) > (Action Planning) > (Action Taking) > (Evaluating) > (Learning).

2.3 Diagram Alur Kerja



2.4 Kebutuhan Perangkat Keras

Kebutuhan perangkat keras dalam melakukan penelitian yakni melibatkan Satu unit komputer/laptop berfungsi sebagai *scanner* denegan spesifikasi :

1. Laptop : Acer 4740
2. Sistem Operasi : *Windows* 7 Ultimate 32bit
3. RAM : 3GB
4. Processor : Intel I3
5. Modem : BOLD *Huawei* E5372s

2.5 Kebutuhan Perangkat Lunak

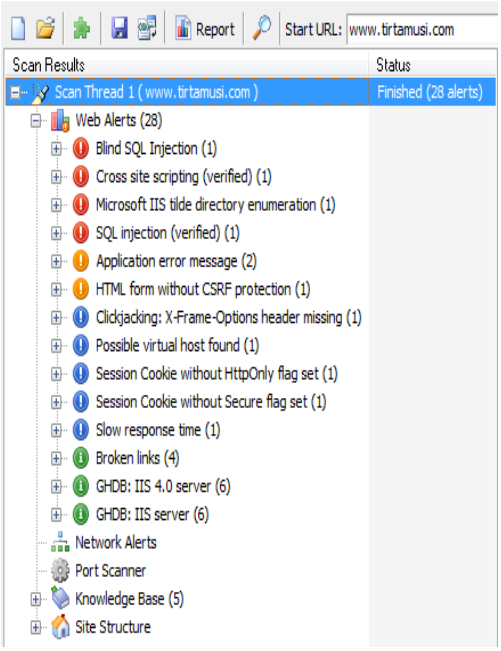
Dalam melakukan diagnosa, penulis dibantu dengan bebrapa *tools* bantuan untuk melakukan tes kerentanan pada *situsweb*

www.tirtamusi.com, perangkat lunak yang digunakan pada penelitian ini antara lain :

1. Sistem Operasi berbasis *Windows* (*Windows 7 Ultimate*)
2. *Acunetic Web Vulnerability Scanner 9.5*
3. *Netsparker 4.1.0.1*
4. *Nessus*

2.6 Level Kerentanan/*Vulnerability*

Dari hasil analisis maka dikategorikan level kerentanan berdasarkan *Common Vulnerability Scoring System (CVSS)* yang diambil dari bab 2 dengan 4 level antara lain :



1. *None*
2. *Low*
3. *Medium*
4. *High*
5. *Critical*

3 Hasil dan Pembahasan

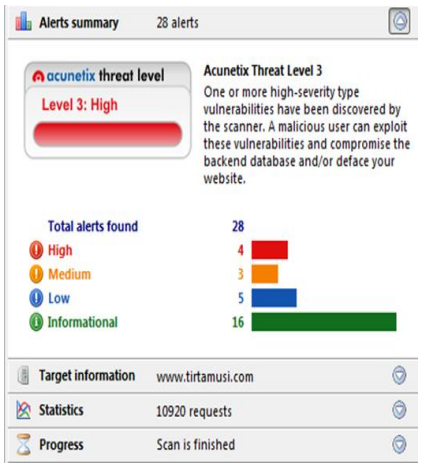
3.1 Hasil

Dari hasil penelitian yang dilakukan pada website PDAM Tirtamusi Palembang menggunakan 3 tools, yang pertama menggunakan Acunetic. Dari hasil scanning tersebut di dapatkanlah hasil bahwa Acunetic menemukan 28 jenis total alert yang terdiri dari 4 dengan jenis yang bertipe high, 3 medium, 5 low dan 16 informasi dengan kategori threat level High. Sedangkan tools yang kedua yaitu menggunakan Netsparker. Scanning yang dilakukan menggunakan tools tersebut maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi. Dan untuk tools ketiga yaitu menggunakan Nessus, dari hasil scanning yang dilakukan maka didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.

3.2 Pembahasan

3.2.1 Scanning www.tirtamusi.com Dengan Acunetic

Dari hasil *scanning* menggunakan *Acunetic*, didapatkan 28 total *alert* yang terdiri dari 4 dengan jenis yang bertipe *high*, 3 *medium*, 5 *low* dan 16 informasi dengan kategori *threat level High*.



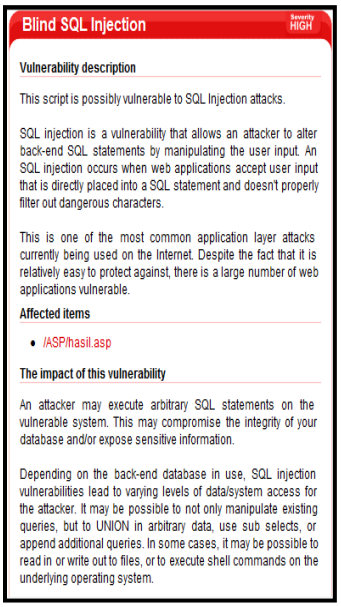
Report hasil *scanning* menggunakan *Acunetic* :

1. Kategori *High*

   Kategori *critical* adalah mulai dari skor 7.0 sampai dengan 8.9, dari hasil *scanning* menggunakan *Acunetic* terdapat 4 jenis kerentanan yang didapatkan dengan kategori *critical* ini antara lain :

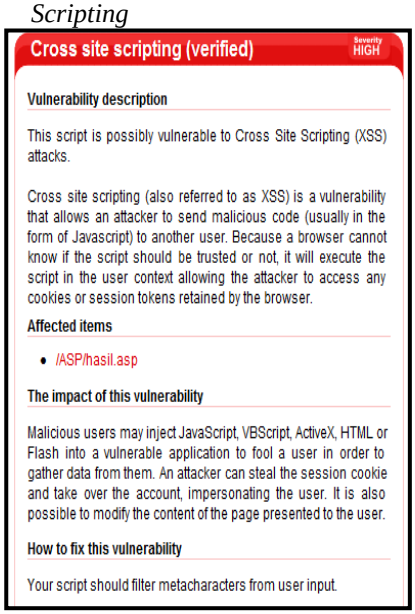
1. *Blind SQL Injection*

   Berikut penjelasan dari *tools Acunetic* tentang *Blind Sql Injection* :



2. *Cross Site Scripting*

   Berikut penjelasan dari *tools Acunetic* tentang *Cross Site Scripting*



3. *Miscrosoft IIS tilde directiory enumeration*

   Berikut penjelasan dari *tools Acunetic* tentang *Miscrosoft IIS tilde directiory enumeration* :

Microsoft IIS tilde directory enumeration Severity HIGH

Vulnerability description

It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access as an attacker can find important files and folders that they are not normally visible.

Affected items

- /

The impact of this vulnerability

Possible sensitive information disclosure.

How to fix this vulnerability

Consult the "Prevention Technique(s)" section from Soroush Dalili's paper on this subject. A link to this paper is listed in the Web references section below.

4. *Sql Injection* (*Verified*)

Berikut penjelasan dari *tools Acunetic* tentang *Sql inejction* (*verified*) :

SQL injection (verified) Severity HIGH

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Affected items

- /ASP/hasil.asp

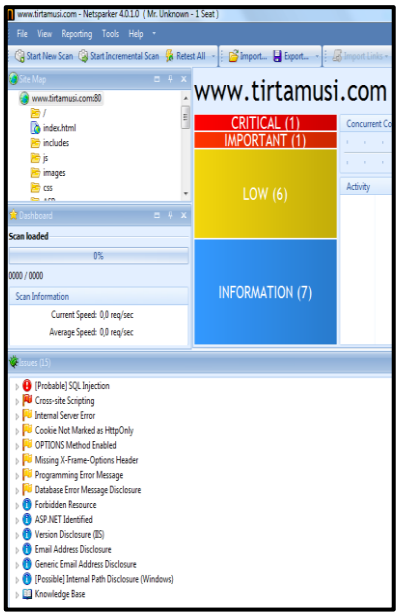
The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to

3.2.2 Scanning menggunakan *Netsparker*

Dari hasil scanning menggunakan Netsparker maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi.



a. *Sql Injection* (probably)

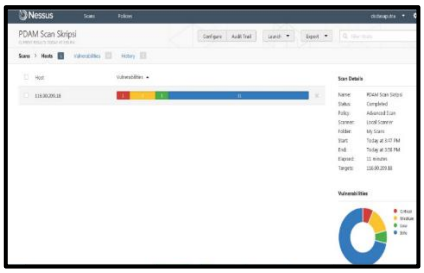
Sql Injection adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan *string* yang diimbuhkan dalam pernyataan *SQL* atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Berikut hasil yang menunjukkan adanya celah *Sql Injection* :

b. *Cross Site Scripting*

Cross Site Scripting/XSS merupakan salah satu jenis serangan injeksi code (code injection attack). *XSS* dilakukan oleh penyerang dengan cara memasukkan kode *HTML* atau *client script code* lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya. Berikut hasil dari *scanning Netsparker* yang menunjukkan adanya *XSS* ditunjukkan dengan gambar 4.24 :

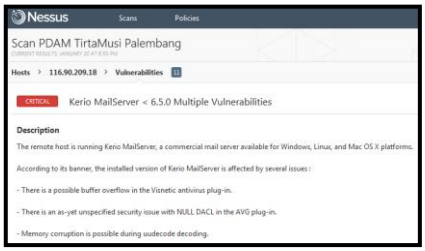
3.2.3 Scanning Menggunakan Nessus

Dari hasil scanning menggunakan Nessus maka didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.



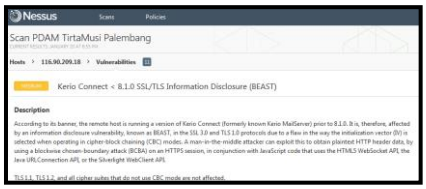
a. *Kerio Mailserver*

Dalam hal ini ditemukan jenis mail*server* yang digunakan pada situs *www.tirtamusi.com* yang mana menggunakan *kerio mailserver* 6.4.1 yang mana hal ini memudahkan *attacker* untuk menyusup masuk kedalam sistem. Berikut hasil tampilan dari *kerio mail server* yang didapatkan dari hasil *scanning* menggunakan *Nessus* :



b. *Kerio Connect 8.1.0 SSL/TLS Information Disclosure (BEAST).*

Kerio Connect adalah mail dan groupware *server* yang komersial yang dikembangkan oleh *Kerio Technologies*. Ini berjalan pada *Windows*, *Linux* dan *OS X*. Berikut hasil dari kerentanan yang didapat dari hasil *scanning* menggunakan *Nessus* :



3.2.4 Evaluasi Hasil Pembahasan

Setelah melakukan *scanning* menggunakan 3 *tools* yang berbeda yaitu *Acunetic*, *Netsparker* dan *Nessus*, penulis mendapatkan beberapa kerentanan yang teridentifikasi seperti *Blind Sql Injection*, *Sql injection*, *Cros site scripting*, *application error*, *broken link* dan lain lain, maka didapatkanlah hasil yaitu terdapat banyak sekali celah kerentanan yang perlu di evaluasi oleh seorang *administrator* dan pengelola situs*web www.tirtamusi.com* yang sangat rentan terhadap serangan agar segera menutup celah dan memperbaiki sistem yang *error* seperti yang telah disebutkan sebelum terjadi serangan yang dapat mengakibatkan kerugian dari pihak perusahaan.

3.2.5 Dokumentasi dan Pelaporan (*Documentation and Reporting*)

Pada tahap ini peneliti membuat laporan mengenai celah keamanan yang ditemukan serta hasil dari penelitian yang telah dilakukan. Dari hasil *scanning* yang telah dilakukan sebelumnya maka didapatkan hasil sebagai berikut :

Tabel 4.1 Celah keamanan dan level kerentanan

No	Tools	Celah Keamanan	Level
1	*Acunetic*	*a. Blind SQL Injection* *b. Cross Site Scripting* *c. Miscrosoft IIS tilde* *d. directiory enumeration* *e. Sql Injection (Verified)*	*High*
		f. Application Error Messagess *g. HTML form without CSRF protection*	*Low*
		h. Clickjacking X-frame option header missing *i. Possible virtual host found*	*Information*
		j. Session cookie without secure flag set *k. Session cookie without secure flag set* *l. Slow response time* *m. Broken link* *n. GHDB (google hacking database (IIS 4.0 server))* o. *GHDB IIS server*	
2	*Netsparker*	*a. Sql Injection* *b. Cross site scriping*	*Critical*
		a. *Internal Server Error* *b. Cookie not marked as HTTP only* *c. Option method enable*	*Low*

		d. missing x-frame option header e. *programming error message* f. *Database error messagess disclosure*	
3	*Nessus*	a. *Kerio Connect 8.1.0 SSL/TLS Information Disclosure (BEAST).* b. *Kerio MailServer < 6.6.2 Multiple XSS (KSEC-2008-12-16-01)*	*Medium*

4 Kesimpulan

hasil simpulan sebagai berikut :

1. Dari hasil scanning yang dilakukan dengan menggunakan tools Acunetic di dapatkanlah hasil bahwa Acunetic menemukan 28 jenis total alert yang terdiri dari 4 dengan jenis yang bertipe high, 3 medium, 5 low dan 16 informasi dengan kategori threat level High.

2. Untuk hasil scanning yang telah dilakukan sebelumya dengan mengguanakan tools kedua yaitu Netsparker maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi.

3. Sementara untuk tools yang terakhir dengan menggunakan aplikasi Nessus didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.

4. Hasil penelitian ini menunjukan bahwa masih banyak terdapat celah yang ada pada website www.tirtamusi.com yang bertipe High ataupun Critical yang memerlukan perhatian khusus, sementara untuk kerentanan lainnya dengan kategori low dan informasi juga tidak dapat dikesampingkan karena dapat mempermudah hacker untuk menembus sistem dari server itu sendiri.

Daftar Pustaka

1 FAIR-ISO/IEC 27005 COOKBOOK. (2010). Implementing a vulnerability management process. SANS Institute InfoSec Reading Room.

2 Jasman (2015). Panduan Praktis WEB Hacking dari Subkultural Programmer. Yogyakarta : ANDI.

3 Matthew B. Miles & A. Michael Huberman (1994). Qulitative Data Anlysis. : Sage Publication : United Staten of America.

4 McNiff Jean & Jack Whitehead (1988). Action Research : Principles and Practice. London and New York : RoutledgeFalmer.
5 Sofana, Iwan (2013). Membangun Jaringan Komputer. Bandung : Informatika Bandung
6 Wikipedia. CVSS (Common Vulnerability Scoring System). Diakses pada 25 November 2015 Dari : https://en.wikipedia.org/wiki/CVSS
7 Wikipedia. Web Bacon. Diakses pada 10 November 2015 dari : https://en.wikipedia.org/wiki/Web_beacon.
8 Wikipedia. Web server. Diakses pada 27 November 2015 Dari : https://id.wikipedia.org/wiki/Server_web
9 Wikipedia. Analysis. Diakses pada 29 November 2015 Dari : https://en.wikipedia.org/wiki/Analysis