Keamanan *Website* Menggunakan *Vulnerability Assessment*

Ari Marta Tania [1], Didik Setiyadi [1], Fata Nidaul Khasanah [1,*]

[1] Teknik Informatika; STMIK Bina Insani; Jalan Raya Siliwangi No. 6 Rawa Panjang Kota Bekasi, 021-82436886; e-mail: arimarta21@gmail.com, didiksetiyadi@yahoo.com, fatanidaul@gmail.com

* Korespondensi: e-mail: fatanidaul@gmail.com

Diterima: 4 Mei 2018; Review: 11 Mei 2018; Disetujui: 29 Mei 2018

Cara sitasi: Tania AM, Setiyadi D, Khasanah FN. 2018. Keamanan *Website* Menggunakan *Vulnerability Assessment*. Informatics For Educators and Professionals. 2 (2): 171 – 180.

Abstrak: Penggunaan sebuah *website* sebagai sarana informasi semakin berkembang dalam berbagai bidang. Perkembangan ini harus diikuti dengan keamanan informasi yang terdapat pada sebuah *website* menyangkut akan kemungkinan resiko yang dihadapi bagi suatu organisasi. Analisa keamanan *website* dapat diketahui dengan melakukan evaluasi keamanan yang bertujuan untuk menemukan adanya celah-celah kerentanan dan resiko pada sebuah *website* serta menyadarkan pentingnya keamanan informasi. Dalam melakukan evaluasi keamanan diterapkanlah metode *Vulnerability Assessment* guna mengidentifikasi *asset-asset website* lalu menganalisa kerentanan yang ditemukan, memperhitungkan resiko yang direpresentasikan dalam bentuk angka serta memberikan solusi perbaikan.

Kata kunci: CVSS, Kali Linux, Keamanan Website

Abstract: *The use of a website as a means of information is growing in various fields. This development must be followed by information security that contains on a website concerning about the possible risks that is faced by an organization. The analysis of the security website can be identified by conducting a security evaluation that is aim at finding vulnerability and risk vulnerabilities on a website and awareness of the importance of information security. In conducting a security evaluation, the Vulnerability Assessment method is used to identify the website assets, afterwards analyze the vulnerability , counting the risks that is represented in the form of numbers and providing solutions for improvement.*

Keywords*: CVSS, Kali Linux, Website Security*

1. Pendahuluan

Media informasi semakin berkembang termasuk penggunaan *website, website* menjadi sumber informasi yang besar dan penggunaannya pun sudah banyak diterapkan dalam berbagai bidang. *Website* itu sendiri adalah halaman informasi yang dapat diakses oleh khalayak umum melalui internet tanpa batasan ruang dan waktu, halaman informasi ini dapat berupa teks, gambar, video dan lain-lain.

Web identik dengan Internet, karena kepopulerannya saat ini, web sudah menjadi interface aplikasi untuk melakukan transaksi dan sajian informasi yang lengkap dari seluruh dunia [Sidik & Pohan, 2014].

Penggunaan *website* yang terus berkembang ini harus diikuti dengan adanya kesadaran akan aspek keamanan informasi, keamanan informasi sebuah *website* dapat diartikan sebagai suatu kebutuhan akan adanya perlindungan terhadap informasi sebagai sebuat aset yang ada didalam sebuah *website* seperti mengatur akses informasi, mengatur identitas penguuna dan lain-lain. Dalam sebuah *website* terdapat data yang menjadi hal penting bagi suatu organisasi karena menyangkut akan kemungkinan resiko yang dihadapi, kurangnya

E-ISSN: 2548-3412 ; 171 – 180

perhatian dari pihak pengelola website terhadap aspek tersebut akan membawa kerugian bagi organisasi dikarenakan celah kerentanan yang ada pada *website* digunakan oleh seorang *attacker* untuk mengambil keuntungan. Celah kerentanan yang ada pada sebuah website dapat diketahui melalui evaluasi keamanan *website,* evaluasi keamanan berguna untuk menemukan celah-celah kerentanan yang menjadi kelemahan website tersebut. Kelemahan dalam sebuah sistem baik program, design, ataupun implementasi dinamakan sebagai Vulnerability [S'to, 2009].

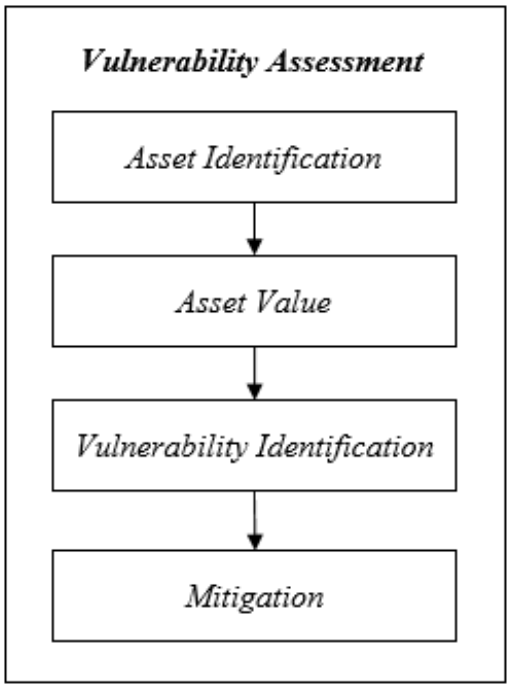
Evaluasi keamanan dilakukan guna menemukan celah-celah kerentanan pada *website* dan memberikan solusi terhadap kerentanan yang ditemukan.Evaluasi keamanan ini mencegah adanya resiko kehilangan data penting serta pengeluaran anggaran tambahan jika *website* terjadi *malfunction* ataupun *crash*

Mencari celah kerentanan pada sebuah *website* dapat diketahui dengan menggunakan *software* secara otomatis, yang kemudian *software* tersebut akan mencari kelemahan yang ada pada website yang bisa jadi merupakan jalan masuk bagi *attacker*. Kerentanan yang ditemukan pada *website* dapat direpresentasikan kedalam bentuk angka sehingga mudah untuk dipahami. Dalam menyajikan nilai kerentanan dapat menggunakan *CVSS versi 2. Common Vulnerability Scoring System* (CVSS) merupakan sebuah kerangka (*framework*) terbuka yang digunakan untuk mengkomunikasikan karakteristik dan dampak yang ditimbulkan oleh sebuah kerentanan aplikasi [Afrih Juhad et al., 2016].

Penurunan nilai kerentanan setelah perbaikan menjadi penanda bahwa evaluasi keamanan yang dilakukan telah dapat mengurangi resiko yang sebelumnya ada dan dapat dikatakan bahwa *website* menjadi relatif aman.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode *Vulnerability Assessment,* metode ini terbagi menjadi empat tahapan. Metode *Vulnerability Assessment,* mengidentifikasi celah-celah kerentanan dan potensi ancaman terhadap setiap sumber daya yang ada pada sebuah *website*. Gambaran mengenai tahapan dari metode *Vulnerability Assessment* dipaparkan pada Gambar 1.



Sumber: Hasil Penelitian (2018)

Gambar 1. Metode *Vulnerability Assessment*

Berdasarkan gambar diatas, dapat dijelaskan bahwa metode tersebut memiliki empat tahapan, yaitu tahap *asset identification*, tahap *asset value*, tahap *vulnerability identification* dan tahap *mitigation*. Tahap *Asset Identification*, pada tahap ini yang dilakukan adalah menentukan aset-aset yang ada pada *website*, menganalisa kerentanan untuk memastikan agar keamanan informasi aset tersebut memiliki tingkat keamanan yang baik contohnya seperti *web server, application server* dan *database server.* Tahap *Asset Value,* pada tahap ini mengidentifikasi aset-aset yang telah ditemukan dari *website* untuk memberikan peringkat terhadap aset yang paling berharga. Memberikan nilai terhadap kerentanan yang ada sesuai dengan kategori dan resiko yang dimiliki. Tahap *Vulnerability Identification,* pada tahap ini dilakukan identifikasi mengenai celah-celah kerentanan yang ada pada *website.* Kegiatan *vulnerability identification* ini dilakukan dengan menggunakan aplikasi yang ada pada sistem operasi Kali Linux. Tahap *Mitigation,* pada tahap ini membahas mengenai proteksi terhadap celah-celah kerentanan yang berada pada kategori *high* yang ditemukan pada *website,* kerentanan yang ditemukan akan diberikan solusi perbaikan untuk mengatasi kerentanan tersebut guna meningkatkan performa *website* menjadi lebih baik.

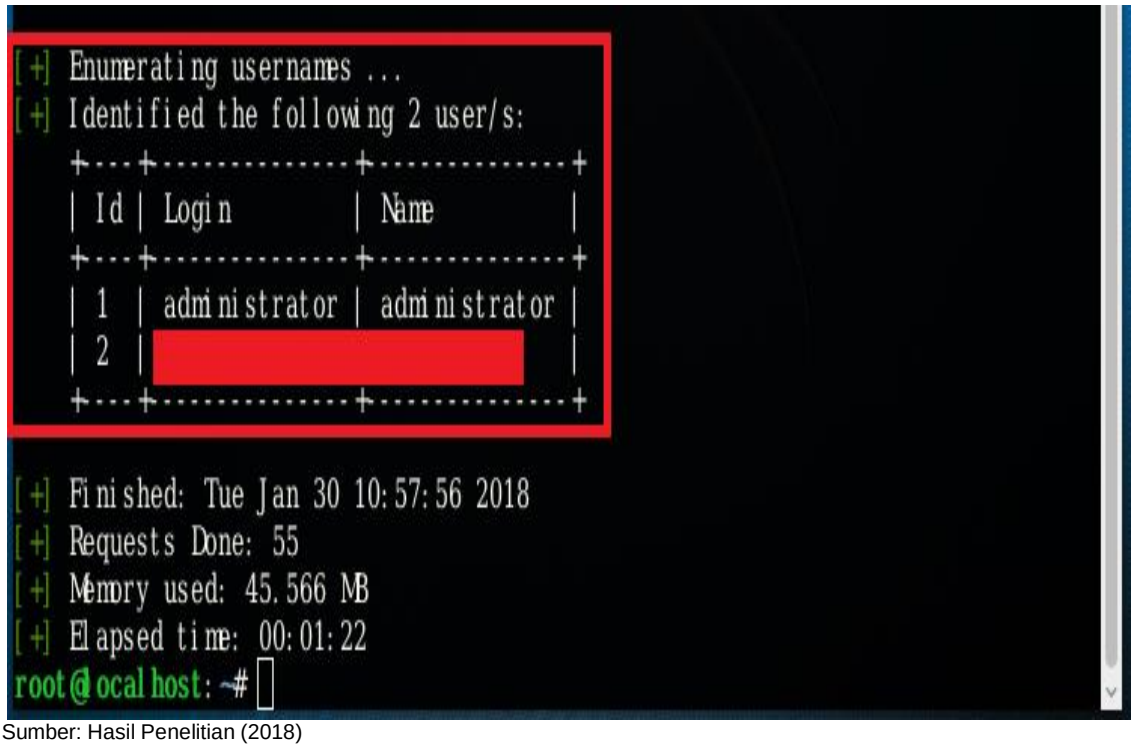
3. Hasil dan Pembahasan

Dalam pengujian kerentanan yang dilakukan, penelitian ini menggunakan *tool* yang ada pada sistem operasi Kali Linux. Berikut beberapa tahapan yang dilakukan, yaitu pengujian kerentanan dan penilaian kerentanan.

3.1. Pengujian Kerentanan

XML RPC adalah sebuah protokol *Remote Procedure Call* (RPC) yang menangani data antar aplikasi yang menggunakan protokol HTTP dalam transportnya dan XML sebagai *encoding*. Kemampuan untuk mengirim sejumlah data yang besar tersebut menjadi celah bagi seorang *attacker* untuk membawa data yang besar berisikan daftar kata kunci yang akan dicoba satu persatu atau dapat disebut juga *brute force attack.*

Untuk menguji apakah *website* tersebut rentan terhadap teknik *brute force attack* atau tidak, maka dilakukan pengujian menggunakan *Wpscan* untuk mendapatkan *username* nya terlebih dahulu. Hasil eksekusi *syntax* pada *tool Wpscan* terlihat pada gambar 2.



Sumber: Hasil Penelitian (2018)

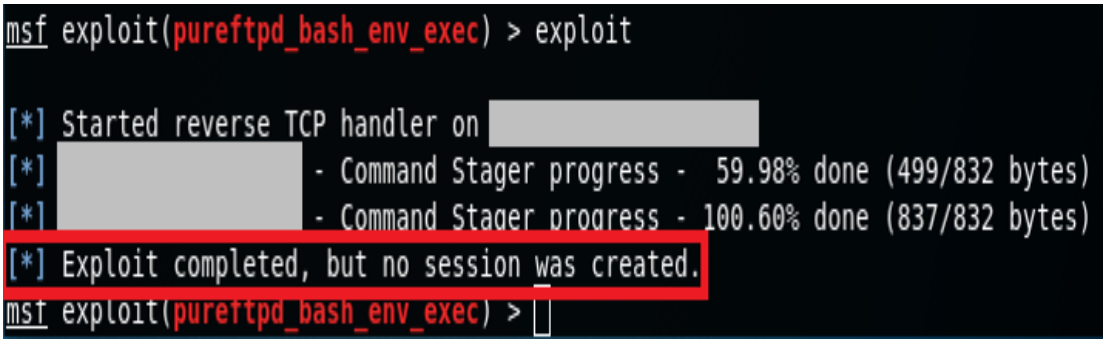
Gambar 2. Pencarian *Username* Menggunakan *Tool Wpscan*

E-ISSN: 2548-3412 ; 171 – 180

Selanjutnya Pengujian *brute force attack* untuk mencari password yang cocok dengan menggunakan *exploit* dengan nama *wp_find_password*, *exploit* ini ditulis menggunakan bahasa pemrograman *ruby* dan menggunakan metode *wp.getUsersBlogs* untuk mengambil blog para pengguna.

Dari hasil eksekusi *syntax* diatas didapatkan informasi mengenai *website* bahwa ditemukan *password* yang cocok untuk *username* administrator. Hal ini membuktikan bahwa *website* tersebut rentan terhadap serangan *brute force attack.*

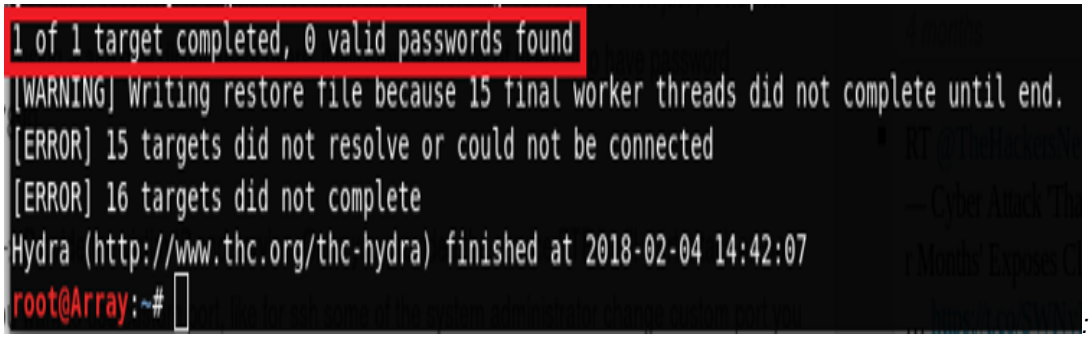
Port 21 Service FTP (File Transport Protocol), digunakan untuk transfer file komputer seperti docs, multimedia dan lain-lain antara *client* dan *server* pada jaringan komputer yang memerlukan *username* dan *password* untuk mengaksesnya. Untuk menguji apakah *port 21 service FTP* rentan terhadap teknik *brute force* atau tidak, maka dilakukan pengujian menggunakan dua *tool* yaitu *Metasploit-Framework* dan *THC-Hydra* untuk mendapatkan *username* dan *password FTP Server.* Berikut ini pengujian kerentanan terhadap serangan *Brute Force Attack* menggunakan *tool Metasploit-Framework:*



Sumber: Hasil Penelitian (2018)

Gambar 3. Uji *Port FTP* Menggunakan *Metasploit-Framework*

Berikut ini pengujian kerentanan terhadap serangan *Brute Force Attack* menggunakan *tool THC-Hydra:*

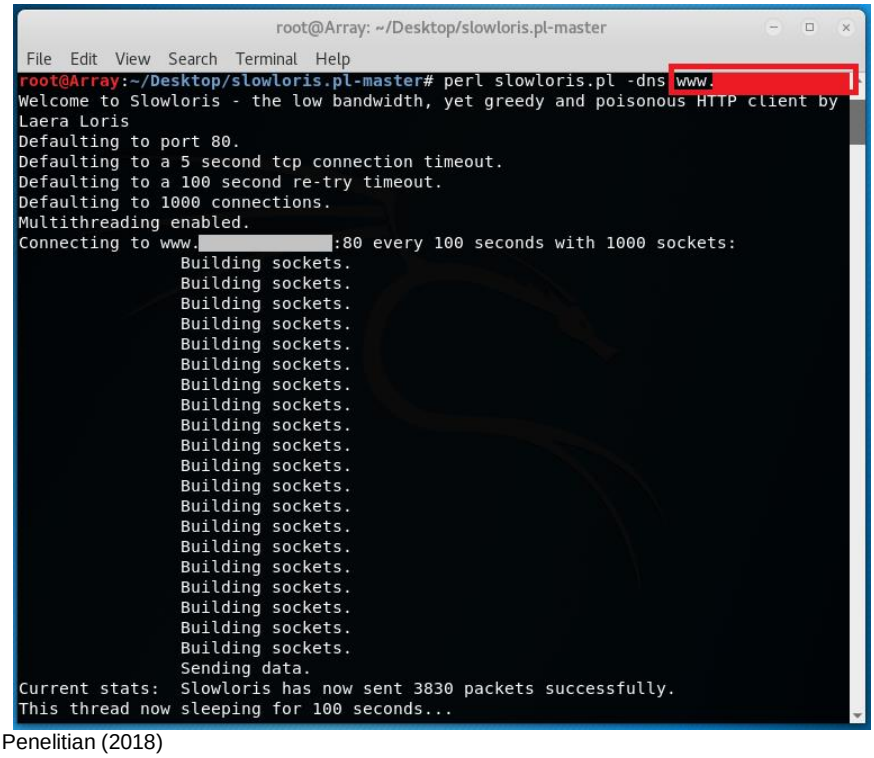


Sumber: Hasil Penelitian (2018)

Gambar 4. Uji *Port FTP* Menggunakan *THC-Hydra*

Berdasarkan hasil proses diatas menggunakan dua *tool* yaitu *Metasploit-Framework* dan *THC-Hydra* tidak didapatkan *username* dan *password* yang cocok. Hal ini membuktikan bahwa *port 21 Service FTP* berstatus aman.

Kerentanan terhadap serangan *Denial of Services* (DoS) dapat di eksploitasi menggunakan *Slowloris.* DoS (*Denial of Service*) yang dilakukan bekerja dengan cara memenuhi permintaan atau melakukan *flooding* dengan mengirimkan paket sebanyak mungkin secara terus menerus hingga server target tidak dapat melayani permintaan tersebut atau *down*. Berikut ini pengujian kerentanan terhadap serangan *Denial of Services* (DoS) menggunakan *Slowloris*:

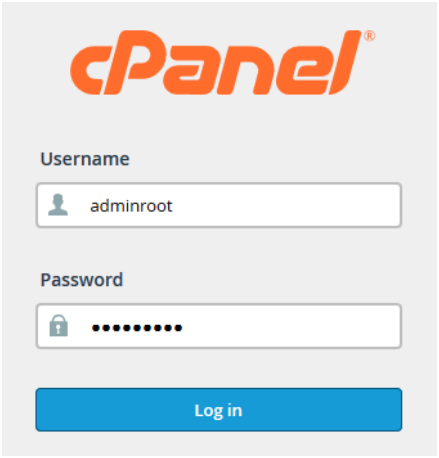


Sumber: Hasil Penelitian (2018)

Gambar 5. Eksekusi *Syntax Slowloris*

Dari hasil pengecekan yang dilakukan pada situs *issup.me,* didapatkan kesimpulan bahwa *website* yang diserang masih dapat menangani permintaan *client* setelah dilakukan serangan DoS (*Denial of Service*) atau masih dalam kondisi *up*. Hal ini membuktikan bahwa *website* tersebut tidak bereaksi terhadap serangan DoS (*Denial of Service*) atau sudah berstatus aman.

Port 80 *Service* HTTP (*Hyper Text Transfer Protocol*), *port* ini rentan terhadap kegiatan *sniffing* yang dilakukan oleh *attacker* dikarenakan tidak dilakukannya enkripsi terhadap data yang ditransmisikan antara *client* dan *server.* Kegiatan *sniffing* dapat dilakukan dengan menggunakan *tool Webscarab* yang memungkinkan kita untuk dapat melihat *username* dan *password* pada *website* target pada saat melakukan aktivitas *login.* Berikut ini adalah tampilan halaman *login cpanel:*

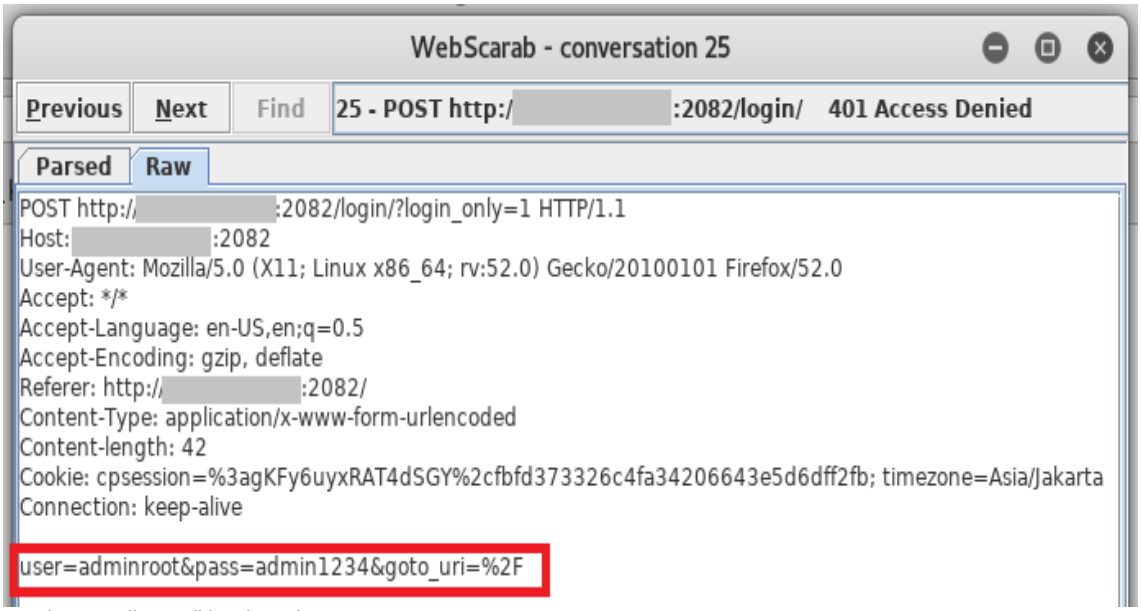


Sumber: Hasil Penelitian (2018)

Gambar 6. *Login Cpanel*

E-ISSN: 2548-3412 ; 171 – 180

Hasil aktivitas *sniffing* yang dilakukan menggunakan *tool Webscarab* pada *website* dapat dilihat pada gambar 7.



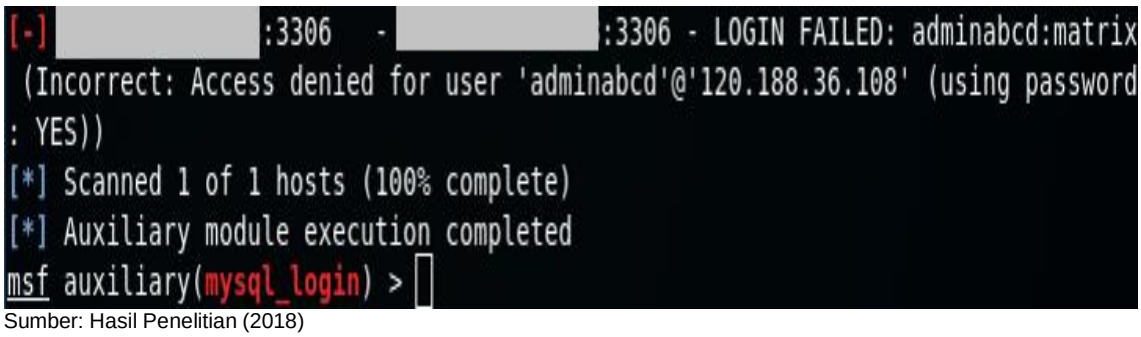
Sumber: Hasil Penelitian (2018)

Gambar 7. *Sniffing* Menggunakan *Tool Webscarab*

Berdasarkan hasil kegiatan *sniffing* yang dilakukan menggunakan *tool Webscarab* pada gambar diatas menunjukan bahwa pada saat terjadi aktivitas *login* melalui *cpanel, username* dan *password* dapat terdeteksi sehingga dikategorikan tidak aman.

Port 3306 *Service MySQL*, *port 3306/tcp Service MySQL* terbuka, *port 3306* rentan terhadap serangan *brute force attack* dengan memanfaatkan kredensial yang lemah, untuk menguji apakah *port 3306 service MySQL* rentan terhadap teknik *brute force attack* atau tidak, maka dilakukan pengujian menggunakan *tool Metasploit-Framework* untuk mendapatkan *username* dan *password port 3306 Service MySQL.*

Berikut ini pengujian kerentanan terhadap serangan *Brute Force Attack* menggunakan *tool Metasploit-Framework*.



Sumber: Hasil Penelitian (2018)

Gambar 8. Pengujian Menggunakan *Tool Metasploit-Framework*

Berdasarkan hasil proses diatas menggunakan *tool Metasploit-Framework* tidak didapatkan *username* dan *password* yang cocok. Hal ini membuktikan bahwa *port 3306 Service MySQL* pada *website* berstatus aman.

Pengujian yang telah dilakukan berdasarkan *Vulnerability Identification* menggunakan *tool* yang ada pada sistem operasi Kali Linux dapat dilihat lebih jelas pada tabel 1 hasil pengujian.

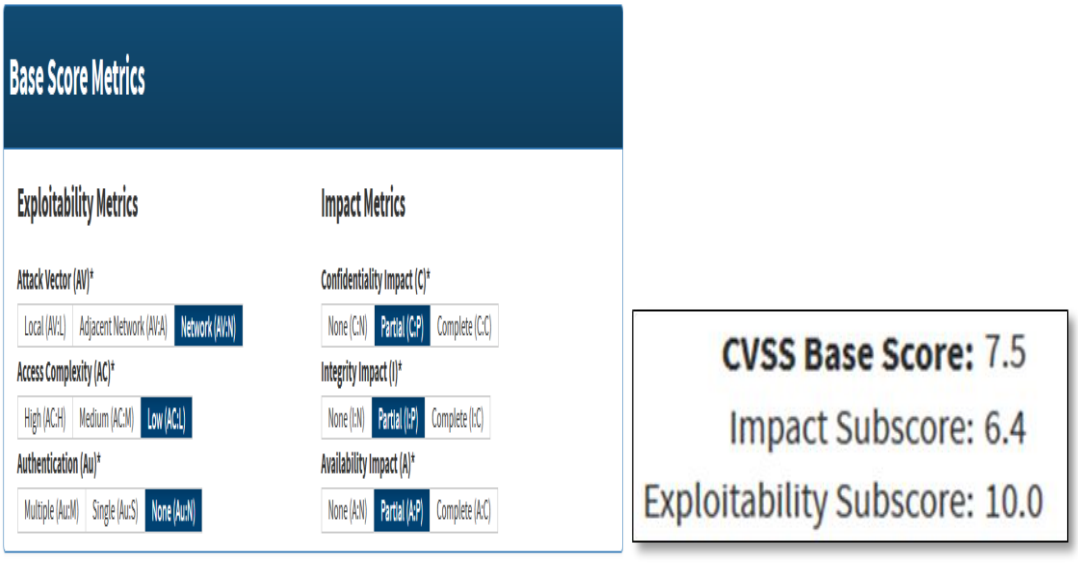
Tabel 1. Hasil Pengujian

No	Pengujian	Tool	Hasil Pengujian	Status
1	*XML-RPC*	WPScan dan Exploit *wp_find_password*	Pengujian yang dilakukan dengan menggunakan teknik serangan *brute force* menunjukan hasil bahwa adanya *username* dan *password* yang cocok.	Tidak Aman
2	*Port 21 Service FTP (File Transfer Protocol)*	*Metasploit-Framework* dan *THC-Hydra*	Pengujian yang dilakukan dengan menggunakan teknik *brute force* tidak menunjukan hasil adanya *username* dan *password FTP server* yang cocok.	Aman
3	*Web Server*	*Slowloris*	Hasil dari serangan *Denial of Service* (DoS) yang telah dilakukan menunjukan *website* masih dalam keadaan *up.*	Aman
4	*Port 80 Service HTTP (Hyper Text Transfer Protocol)*	*Webscarab*	Kegiatan *sniffing* yang dilakukan berhasil, *username* dan *password* dapat terlihat saat admin sedang melakukan kegiatan *login* pada *cpanel website.*	Tidak Aman
5	*Port 3306 Service MySQL*	*Metasploit Framework*	Pengujian yang dilakukan dengan menggunakan teknik *brute force* tidak menunjukan hasil adanya *username* dan *password* yang cocok.	Aman

Sumber: Hasil Pengolahan Data (2018)

3.2. Penilaian Kerentanan

Pengujian yang telah dilakukan, direpresentasikan ke dalam bentuk angka menggunakan *Common Vulnerability Scoring System* (CVSS). *XML-RPC*, berikut adalah hasil perhitungan nilai kerentanan menggunakan CVSS.



Sumber: Hasil Penelitian (2018)

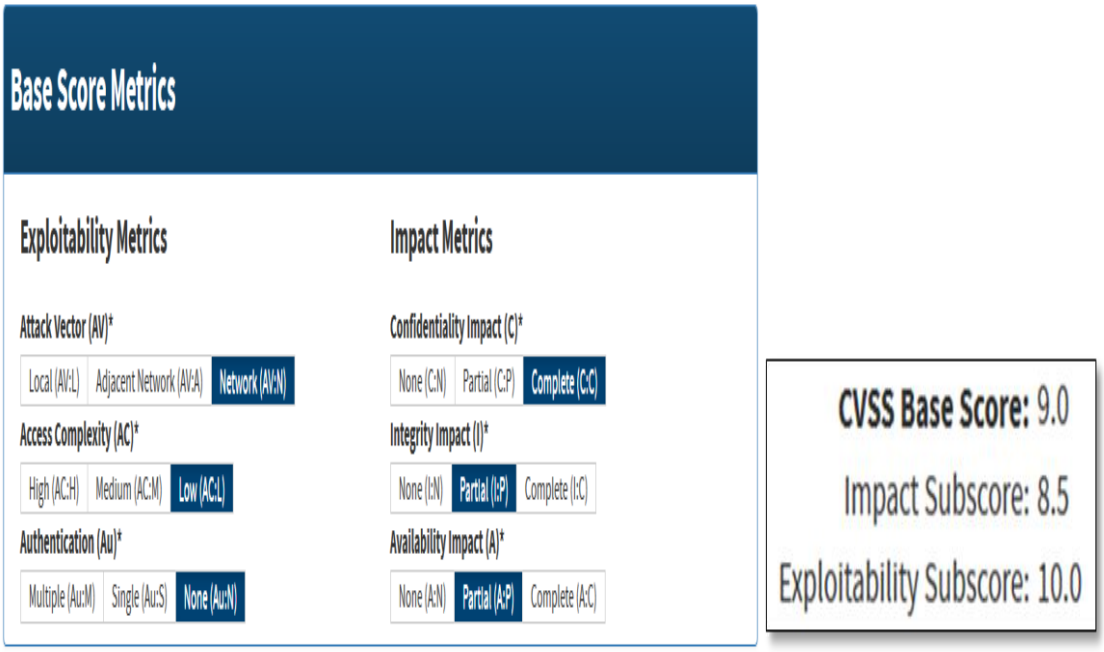
Gambar 9. Penilaian *Base Score Metrics-Brute Force Attack XML-RPC*

E-ISSN: 2548-3412 ; 171 – 180

Sumber: Hasil Penelitian (2018)

Gambar 10. Grafik *Base Score Metrics-Brute Force Attack XML-RPC*

Port 80/tcp *Service* HTTP (*Hyper Text Transfer Protocol*) berikut adalah hasil perhitungan nilai kerentanan menggunakan CVSS:



Sumber: Hasil Penelitian (2018)

Gambar 11. Penilaian *Base Score Metrics-Port 80 HTTP*

Sumber: Hasil Penelitian (2018)

Gambar 12. Grafik *Base Score Metrics-Port 80 HTTP*

Berdasarkan hasil pengujian diatas dan juga perhitungan nilai kerentanan yang dilakukan, kerentanan tersebut dapat diatasi dengan memberikan solusi agar nilai kerentanan dapat diturunkan. Penjelasan mengenai solusi yang diberikan, tersaji pada tabel dibawah ini:

Tabel 2. Solusi Perbaikan Kerentanan

No	Pengujian	Masalah/Kerentanan	Solusi Perbaikan Kerentanan
1	*XML-RPC*	Pengujian yang dilakukan dengan menggunakan teknik serangan *brute force* menunjukan hasil bahwa adanya *username* dan *password* yang cocok.	Serangan ini dapat diatasi dengan menon-aktifkan file *xmlrpc.php*
2	*Port 80 Service HTTP (Hyper Text Transfer Protocol)*	Kegiatan *sniffing* yang dilakukan berhasil, *username* dan *password* dapat terlihat saat admin sedang melakukan kegiatan *login* pada *Cpanel.*	Kegiatan *sniffing* yang dilakukan guna melihat aktivitas *login* dapat diatasi dengan menggunakan SSL (*Secure Socket Layer*) pada *website.*

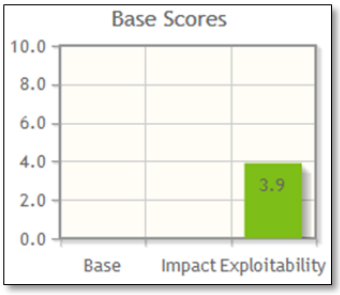
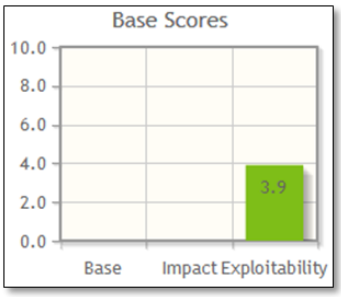
Sumber: Hasil Penelitian (2018)

Berdasarkan pada kerentanan yang ditemukan melalui serangkaian pengujian, diberikanlah solusi terhadap kerentanan tersebut. Setelah solusi yang disarankan selesai dilakukan, maka diadakanlah pengujian hasil perbaikan mengenai nilai kerentanan yang ada.

Guna melihat penurunan nilai kerentanan yang ditemukan setelah dilakukannya pengujian ulang atau *re-testing,* maka akan dilakukan kembali perhitungan nilai kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS) *Calculator* versi 2. Perhitungan nilai kerentanan sebelum dan sesudah perbaikan di tampilkan dalam tabel 3 perbandingan nilai kerentanan.

E-ISSN: 2548-3412 ; 171 – 180

Tabel 3. Tabel Perbandingan Nilai Kerentanan Sebelum dan Sesudah Perbaikan

No	Pengujian	Sebelum Perbaikan	Sesudah Perbaikan
1	*XML-RPC*		
2	*Port 80 Service HTTP (Hyper Text Transfer Protocol)*		

Sumber: Hasil Penelitian (2018)

Berdasarkan tabel diatas, nilai kerentanan sebelum dilakukan perbaikan menunjukkan bahwa jika kerentanan tersebut di lakukan eksploitasi maka akan memiliki dampak yang mempengaruhi sistem sedangkan nilai kerentanan setelah perbaikan menunjukkan bahwa kerentanan tersebut masih dapat di eksploitasi namun tidak memiliki dampak apapun.

4. Kesimpulan

Berdasarkan pengujian keamanan *website* menggunakan metode *Vulnerability Assessment* dapat disimpulkan bahwa setelah dilakukan serangkaian pengujian, terdapat dua pengujian yang memiliki status tidak aman diantaranya *XML-RPC* dan *Port 80 Service HTTP (Hyper Text Transfer Protocol).* Adanya kerentanan tersebut dapat mengancam keamanan *website* jika tidak dilakukan perbaikan, oleh karna itu peneliti telah merekomendasikan solusi perbaikan. Setelah solusi perbaikan yang disarankan sudah selesai dikerjakan lalu dilakukan pengujian ulang serta nilai kerentanan dihitung kembali. Pada tabel perbandingan nilai kerentanan sebelum dan sesudah perbaikan terlihat adanya penurunan nilai kerentanan sehingga dapat dikatakan bahwa *website* tersebut sudah melakukan perbaikan atas kerentanan yang ada dan resiko kerentanan dapat dikurangi. Penelitian yang dilakukan mengenai evaluasi kemanan *website* ini selanjutnya dapat dikembangkan berupa pengujian keamanan *website* menggunakan *Hacking Methodology.*

Referensi

Afrih Juhad H, Isnanto RR, Widianto ED. 2016. Analisis Keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro. J. Teknol. dan Sist. Komput. 4: 479.

Gupta A, Kaur K. 2013. Vulnerability Assessment and Penetration Testing. Int. J. Eng. Trends Technol. 4: 328–333.

Mardianto I, Sediyono A, Hafzan A. 2015. Analisa Kerentanan SIS.TRISAKTI.AC.ID Menggunakan Teknik Vulnerability Scan. JETri 13: 90–101.

Mantra IGN, Alaydrus M. 2015. Analisis Kerentanan Keamanan (Va) Web Perguruan Tinggi Swasta Jakarta. Pros. Senat. 2015: 1–6.

Masykur F. 2015. Analisis Vulnerability Web Based Application Menggunakan Nessus. 320–326.

Putu IG, Juliharta K. Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing. 149–158.

Sidik B, Husni Iskandar Pohan. 2012. Pemrograman web dengan HTML. Bandung: Informatika.