JURNAL INFORMATIKA, Vol.6 No. 2 September 2019, pp. 212~218
ISSN: 2355-6579
E-ISSN**:** 2528-2247

Uji *Vulnerability* pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS

Feri Wibowo[1], Harjono[2], Agung Purwo Wicaksono[3]

[1]Teknik Informatika, Universitas Muhammadiyah Purwokerto
e-mail: feriwibowo@ump.ac.id

[2]Teknik Informatika, Universitas Muhammadiyah Purwokerto
e-mail: harjono@ump.ac.id

[3]Teknik Informatika, Universitas Muhammadiyah Purwokerto
e-mail: agungpurwowicaksono@ump.ac.id

Abstract

Website jurnal Ilmiah merupakan salah satu aset sistem informasi penting yang dimiliki oleh instansi pendidikan tinggi, maka diperlukan kesadaran tinggi terkait faktor keamanan sistem informasi. Salah satu cara yang dapat dilakukan adalah *Vulnerability Assessment* (VA) sebagai kontrol preventif yang akan mencegah terjadi insiden terhadap sistem yang bebasis teknologi informasi. Metode yang digunakan adalah penelitian terapan yang berfokus pada analisis hasil evaluasi sehingga diharapkan dapat menghasilkan berupa informasi yang dijadikan masukan atau pengambilan keputusan tertentu sesuai urgensi sasaran. Secara teknis penelitian ini akan dilaksanakan menggunakan 3 tahapan inti dari proses *VA* yaitu penentuan batasan proyek, implementasi VA, dan analisis hasil VA. VA dilakukan menggunakan *software* OpenVAS dan AcunetixWVS. Proses VA terhadap website jurnal ilmiah UMP berbasis OJS versi 2.4.8.0 berjalan dengan baik dan menghasilkan temuan kelemahan atau kerentanan. OpenVAS menemukan celah kelemahan sejumlah 9 data, sedangkan Acunetix WVS menemukan celah kelemahan sejumlah 166 data. Data kelemahan ini bisa dijadikan masukan untuk tim sistem informasi UMP untuk segera menutup atau memperbaikai celah keamanan yang ada.

Keywords*: Vulnerability Assessment, jurnal, OpenVAS, Acunetix WVS*

Abstract

The scientific journal website is one of the important information system assets owned by higher education institutions, so high awareness is needed regarding information system security factors. One way that can be done is a Vulnerability Assessment (VA) as a preventive control that will prevent incidents of systems based on information technology. The method used is applied research that focuses on the analysis of evaluation results so that it is expected to produce in the form of information that is used as input or decision making according to the urgency of the target. Technically, this research will be carried out using three core stages of the VA process, the determination of project boundaries, VA implementation, and VA results analysis. VA is done using OpenVAS and AcunetixWVS software. The VA process for the OJS-based UMP scientific journal website version 2.4.8.0 runs well and results in findings of weaknesses or vulnerabilities. OpenVAS found 9 data weaknesses, while Acunetix WVS found 166 data loopholes. This weakness data can be used as input for the UMP information system team to close or correct existing security gaps immediately.

Keywords*: Vulnerability Assessment, jurnal, OpenVAS, Acunetix WVS*

1. Pendahuluan

Jurnal ilmiah merupakan salah tempat publikasi karya ilmiah hasil penelitian, dan selaras dengan peraturan Menristekdikti nomo 9 tahun 2018 bahwa jurnal ilmiah yang akan diajukan akreditasi harus sudah dikelola secara elektronik (daring/on-line). Sejalan dengan itu,

Universitas Muhammadiyah Purwokerto (UMP) sudah menerapkan junal ilmiah berbasis elektronik. Jurnal ilmiah berbasis elektronik atau dalam hal ini jurnal berbasis *open journal system* (OJS) yang dimiliki UMP berjumlah 24 jurnal yang semuanya dapat diakses secara daring. Website jurnal ilmiah UMP disimpan dan dijalankan pada server yang dikelola sendiri oleh Tim IT yang dimilik UMP. Hal ini menuntut pihak IT UMP untuk melakukan majamen server atau dalam hal ini *webserver* sendiri. Manajamen ini meliputi manajemen pengalokasian ruang penyimpanan, manajemen user, dan manajemen keamanan. Jurnal Ilmiah UMP merupakan salah satu aset penting bagi instansi karena jurnal ilmiah ini bisa dijadikan sebagai salah satu tolak ukur keberhasilan dari sisi akademik dan juga sebagai wajah kemajuan publikasi ilmiah di UMP. Seiring dengan kemajuan teknologi informasi, faktor kemanan merupakan bagian yang perlu ditingkatkan. Manajemen keamanan yang baik salah satunya yaitu dengan cara pembaruan berkala sistem keamanan, selain itu dapat digunakan untuk meminimalisir kerugian akibat celah kemanan yang dimanfaatkan oleh orang yang tidak bertanggung jawab atau biasa disebut hacker.

Kelemahan *(Vulnerability)* sebuah sistem infromasi bisa disebabkan oleh faktor internal dan faktor eksternal. *Vulnerability Assessment* (VA) juga dapat dikatakan sebagai suatu bentuk kontrol preventif seperti halnya antivirus yang akan mencegah terjadi insiden terhadap sistem yang bebasis teknologi informasi, maka tujuan VA sebenarnya adalah untuk meningkatkan kesadaran akan pentingnya keamanan informasi, yang seringkali menjadi prioritas kesekian dalam sebuah institusi (Priandono, 2006). Menurut (Greg & Kim, 2005) *vulnerability assessment* merupakan bagian dari *risk assessment* yang terdiri dari *risk analysis, policy development, training and implementation*, dan *vulnerability assessment and penetration testing.*

Penelitian dengan bahan kajian utama *vulnerabily* sudah banyak dilakukan, seperti penelitian oleh (Pangalila, Noertjahyana, & Andjarwirawan, 2015) menunjukan bahwa analisis *vulnerability* pada website http://sim.pertra.ac.id masih terdapat celah keamanan yang berada di level tinggi dan sedang, ini artinya masih mungkin website tersebut dapat diserang oleh hacker. Pengujian kerentanan terhadap web ojs versi 3.0 ditemukan masih ada celah untuk memanimpulasi file lokal bahkan dapat mengunggah file dengan melakukan serangan *Cross – Site Scripting* (XSS) (Yunanri, Riadi, & Yudhana, 2018). Teknik pelaksanaan *vulnerability assessment* merupakan proses yang cukup beresiko karena ada peluang untuk mengganggu sistem yang sedang dilakukan *assessment*. Menurut (Priandono, 2006) proses *vulnerability assessment* dibagi dalam tiga tahapan yaitu tahap penentuan batasan proyek, pelaksanaan assessment, dan pelaporan akhir. Proses ini dilakukan secara hati – hati dan terkendali urut dimana tahapan yang satu tidak dapat mendahului tahap yang lain.

Maka untuk melindungi website jurnal ilmiah UMP tentunya perlu peningkatan sistem keamanannya. Langkah awal yang dapat dilakukan adalah dengan evaluasi sistem keamanan server jurnal ilmiah UMP agar didapatkan data kelemahan (vulnerability) atau celah – celah keamanan yang dapat merugikan atau bahkan dapat dimanfaatkan untuk merusak sistem. Data kelemahan ini dapat dijadikan sebagai bahan masukan untuk tenaga IT UMP selaku pengelola server sehingga perbaikan – perbaikan kemanan server akan terus meningkat.

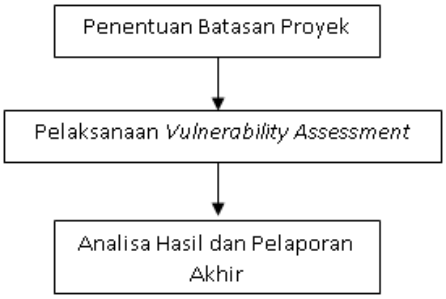
Tindakan yang dapat dilakukan adalah dengan mencoba menganalisis *vulnerability* menggunakan OpenVAS dan Acunetix WVS terhadap web jurnal ilmiah Universitas Muhammadiyah Purwokerto berbasis OJS versi 2.4.8.0. Tindakan ini akan menghasilkan data kelemahan yang ada di website jurnal ilmiah Universitas Muhammadiyah Purwokerto dan kemudian akan dianalisis sebagai bahan masukan bagian teknologi informasi UMP selaku pengelola server agar dapat meningkatkan sistem keamanannya.

2. Metode Penelitian

Open Vulnarebaliay Assessment System (OpenVAS) dan *Acunetix Web Vulnerability Scanner* (Acunetix WVS) merupakan software yang digunakan untuk *vulnerability assessment.* OpenVAS merupakan salah satu software yang mempunyai kemampuan untuk melakukan *scanning* secara komprehensif dalam menangani *vulnerability* sistem terhadap

gangguan yang sering atau pernah terjadi berdasarkan *signature* atau *anomaly* (statistik). (Subuh, 2008). *Acunetix WVS* merupakan alat penguji keamanan aplikasi web otomatis yang dapat mengaudit aplikasi web dengan memeriksa kerentanan seperti *SQL Injection, cross site scripting* dan kerentanan yang lainnya (Ortega, 2014).

Metode penelitan yang digunakan adalah metode penelitian terapan yang berfokus pada analisis hasil evaluasi sehingga diharapkan dapat menghasilkan berupa informasi yang dijadikan masukan atau pengambilan keputusan tertentu sesuai urgensi sasaran. Secara teknis penelitian ini akan dilaksanakan menggunakan 3 tahapan inti dari proses *vulnerability assessment* (Priandono, 2006). 3 tahapan tersebut seperti yang terlihat pada Gambar 1.



Gambar 2. Garis Besar Proses *Vulnerability Assessment*

Proses vulanerability assessment dilaksanakan secara detail, terukur dan terkendali, maka proses yang satu tidak bisa mendahului proses yang lain. Setiap tahap harus dilakukan dengan didasari kerjamasa antar pihak – pihak yang terkait baik dari level manajer sampai level pelaksana teknologi informasi.

1. Batasan proyek diperlukan agar *vulnerability assessment* tidak terlalu luas, sehingga melibatkan hal – hal lain yang tidak perlu dan tidak terlampau sempit sehingga melewatkan hal – hal yang penting. Untuk menentukan batasan sistem, ada 3 hal yang perlu dijadikan sebagai pertimbangan yaitu pemahaman terhadap proses bisnis sistem yang akan diuji, pemahaman kompleksitas sistem dan penentuan waktu dan biaya.

2. Pelaksanaan *Vulnerability Assessment* tentunya mengacu dari batasan proyek yang telah didefinisikan sebelumnya dan dari standar keamanan sistem yang telah diterapkan dilapangan. Tahap pelaksanaan meliputi tahap pengumpulan data yang dilakukan wawancara langsung dengan tim tenaga teknologi informasi yang menerapkan kemanaan. Data yang dikumpulkan berupa data standar keamanan yang diterapkan di sistem web junral OJS Universitas Muhammadiyah Purwokerto, seperti data konfigursasi jaringan dan konfirgusi keamanan pada sistem server. Di tahap ini *tools* yang akan digunakan adalah *OpenVAS* dan *Acunetix WVS.*

3. Tahap analisa hasil dan laporan akhir berisi analisa temuan di lapangan yang merupakan hasil dari *scanning* menggunakan *OpenVAS* dan *Acunetix WVS.* Temuan ini tidak serta merta langsung ditindaklanjuti oleh pemilih sistem yang diuji atau *client,* akan tetapi temuan ini perlu dievaluasi kembali untuk melihat sejauh mana temuan gangguan atau kelamahan ini akan berdampak terhadap sistem. Selain dievaluasi juga dilakukan pengelompokan terhadap hasil temuannya. Laporan akhir ini sebaiknya dibuat menjadi dua versi, yaitu versi lengkap dan detail yang akan diberikan kepada tim pelaksana IT atau administrator sistem, kemudian versi ringkas yang lebih informatif akan diberikan kepada pimpinan perusahaan.

3. Hasil dan Pembahasan

Tahap penentuan batasan proyek diperlukan agar *vulnerability assessment* tidak terlalu luas, sehingga melibatkan hal – hal lain yang tidak perlu dan tidak terlampau sempit sehingga melewatkan hal – hal yang penting. Untuk menentukan batasan sistem, ada 3 hal yang perlu dijadikan sebagai pertimbangan yaitu pemahaman terhadap proses bisnis sistem yang akan diuji, pemahaman kompleksitas sistem dan penentuan waktu dan biaya. Proses bisnis sistem yang ada pada website jurnal Universitas Muhammadiyah Purwokerto (UMP) terdiri dari 2 (dua) hal yaitu yang pertama software yang digunakan untuk membangun jurnal di UMP yaitu software *Open Journal System* (OJS). Kemudian yang kedua yaitu mempertimbangkan kompleksitas server

dimana jurnal UMP berada, server yang digunakan merupakan server yang dibagi *resource*-nya dengan aplikasi lain yang ada di UMP, sehingga lalulintas data yang terjadi pada server jurnal termasuk padat. Maka yang akan dilakukan proses *vulnerability assesment* hanya pada sistem jurnal UMP walapun di server yang sama terdapat sistem lain yang ada di UMP.

Pengumpulan informasi terkait server website jurnal Universitas Muhammadiyah Purwokerto (UMP) (jurnalnasional.ump.ac.id) yang digunakan oleh Biro Teknologi Informasi dan Komunikasi (BTIK) UMP didapatkan no *IP address* dari server dan alamat domain jurnal UMP.

Sebelum proses *vulnerability assesment* maka disiapkan sebuah komputer yang memiliki spesifikasi minimal menurut *Greenbone Network* sebagai berikut:

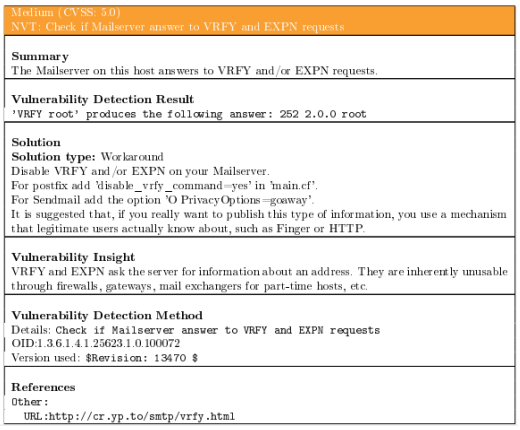
- Type: Linux
- Version: Other Linux (64bit)
- Memory: 2048M
- Harddisk: 9Gb
- CPUs: 2

Tahap selanjutnya adalah proses *Vulnerability Assessment* menggunakan OpenVAS dan AcunetixWVS. Proses *scanning* yang pertama menggunakan OpenVAS menghasilkan data-data kelemahan pada website jurnal ilmiah UMP. Data kelemahan yang didapat berjumlah 9 data kelemahan dengan rincian 7 data berada di level *medium* dan 2 data berada di level *low,* sedangkan di level *high* tidak ditemukan kelemahan seperti terlihat pada Tabel 1.

Tabel 1. Hasil *Scanning* Menggunakan OpenVAS

Host	High	Medium	Low
Server Website Jurnal	0	7	2

Gambar 2 menunjukan salah satu kelemahan di level *medium* yang dideteksi oleh *software* OpenVAS yaitu pada bagian *Mailserver.*


Medium (CVSS: 5.0)
NVT: Check if Mailserver answer to VRFY and EXPN requests

Summary
The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result
'VRFY root' produces the following answer: 252 2.0.0 root

Solution
Solution type: Workaround
Disable VRFY and/or EXPN on your Mailserver.
For postfix add 'disable_vrfy_command=yes' in 'main.cf'.
For Sendmail add the option 'O PrivacyOptions=goaway'.
It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

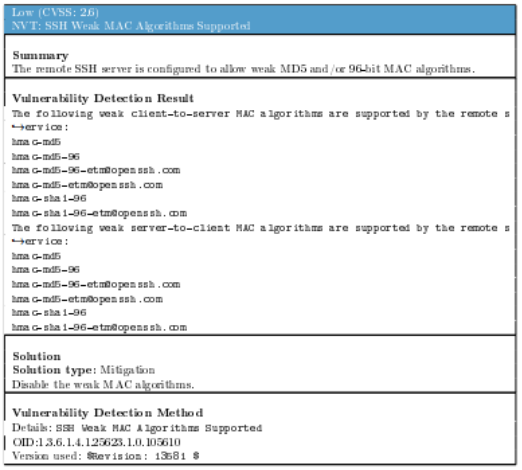
Vulnerability Insight
VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method
Details: Check if Mailserver answer to VRFY and EXPN requests
OID:1.3.6.1.4.1.25623.1.0.100072
Version used: $Revision: 13470 $

References
Other:
URL:http://cr.yp.to/smtp/vrfy.html

Gambar 2. *Sample* Data Kelemahan pada Level *Medium* OpenVAS

Kelemahan pada level *Low* juga ditemukan sejumlah 2 data, Gambar 3 menunjukan salah satu kelemahan di level *Low* yang dideteksi oleh *software* AcunetixWVS yaitu pada bagian konfigurasi *remote SSH server* yang lemah.


Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96
hmac-md5-96-etm@openssh.com
hmac-md5-etm@openssh.com
hmac-sha1-96
hmac-sha1-96-etm@openssh.com

Solution
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: $Revision: 13581 $

Gambar 3. *Sample* Data Kelemahan pada Level *Low* OpenVAS

Proses *scanning* yang kedua menggunakan AcunetixWVS menghasilkan data-data kelemahan pada website jurnal ilmiah UMP. Data kelemahan yang ditemukan berjumlah 166 data kelemahan dengan rincian 149 data berada di level *medium* dan 17 data berada di level *low,* sedangkan di level *high* tidak ditemukan kelemahan seperti terlihat pada Tabel 2.

Tabel 2. Hasil *Scanning* Menggunakan AcunetixWVS

Host	High	Medium	Low
Server Website Jurnal	0	149	17

Data kelemahan yang dihasilkan dari hasil *scanning* menggunakan AcunetixWVS dapat digrupkan menjadi beberapa grup peringatan yang ditemukan, hal ini untuk mempermudah menyimpulkan bagian mana yang paling banyak kelemahanya dan perlu perhatian lebih untuk diperbaiki. Grup data kelemahan ditunjukan pada Tabel 3.

Tabel 3. Grup Data Kelemahan hasil Scanning Menggunakan Acunetix WVS

Alert group	Severity	Alert count
HTML form without CSRF protection	Medium	74
User credentials are sent in clear text	Medium	65
Backup files	Medium	9
Host header attack	Medium	1
Possible sensitive directories	Low	16
Clickjacking: X-Frame-Options header missing	Low	1

Dari Tabel 3 dapat disimpulkan yang paling banyak ditemukan adalah pada grup "*User credentials are sent in clear text"* yang artinya user ketika mengirim pesan akan melalui *port* atau saluran yang tidak terenkripsi. Gambar 4 menunjukan salah satu data kelemahan di level *medium* yang dideteksi oleh *software* Acunetix WVS yaitu pada grup *User credentials are sent in clear text.*

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.

Gambar 4. *Sample* Data Kelemahan Pada Level *Medium* Acunetix WVS

Hasil *scanning* antara OpenVAS dan Acunetix WVS menunjukan perbedaan yang cukup lebar. Dengan target *scanning* yang sama yaitu website jurnal ilmiah UMP, pertama dari segi waktu jika menggunakan OpenVAS jauh lebih singkat yaitu kurang lebih hanya 60 menit, sedangkan menggunakan Acunetix membutuhkan waktu 954 minutes. Kemudian dari sisi *report scanning* yang dihasilkan juga sangat berbeda, OpenVAS menghasilkan data kelemahan yang terdeteksi sejumlah 9 data, sedangkan Acunetix menemukan data kelemahan sejumlah 166 data. Gambaran data perbandingan hasil *scan* ditunjukan pada Tabel 4.

Tabel 4. Perbandingan Hasil *Scanning*

Software	Scan Time (minutes)	Result		
		High	Medium	Low
OpenVAS	60	0	7	2
Acunetix WVS	954	0	149	17

4. Kesimpulan

Proses *Vulnerability Assessment* terhadap website jurnal ilmiah UMP berbasis OJS versi 2.4.8.0 berjalan dengan baik dan menghasilkan temuan kelemahan atau kerentanan. OpenVAS menemukan celah kelemahan sejumlah 9 data, sedangkan Acunetix WVS menemukan celah kelemahan sejumlah 166 data. Dengan perbandingan waktu *scanning* yang cukup jauh yaitu OpenVAS membutuhkan waktu 60 menit sedangkan Acunetix WVS membutuhkan waktu 954 menit. Data kelemahan ini bisa dijadikan masukan untuk tim sistem informasi UMP untuk segera menutup atau memperbaikai celah keamanan yang ada.

Referensi

Greg, M., & Kim, D. (2005). *Inside Network Security Assessment Guarding your IT Infrastructure*. dd: Sams Publishing.

Ortega, M. (2014). Acunetix Web Vulnerability Scanner. Retrieved October 28, 2018, from https://hakin9.org/acunetix-web-vulnerability-scanner/

Pangalila, R., Noertjahyana, A., & Andjarwirawan, J. (2015). Penetration Testing Server Sistem Informasi Manajemen Dan Website Universitas Kristen Petra. *Jurnal Infra*, *3*(2), pp.271-p.276. Retrieved from http://publication.petra.ac.id/index.php/teknik-informatika/article/view/3145

Priandono, A. (2006). Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi. *Jurnal Teknik Informatika Dan Sistem Informasi*, *1*(2), 73–83.

Subuh, M. (2008). *Desain dan Implementasi Vulnerability Assessment untuk Penelusuran Celah Keamanan Jaringan Komputer pada Sekretariat DPRD Banyuasin*. STMIK PalComTech Palembang.

Yunanri, W., Riadi, I., & Yudhana, A. (2018). Analisis Deteksi Vulnerability pada Webserver Open Jurnal System menggunakan OWASP Scanner. *Jurti*, Vol. 2, pp. 1–8.