Analisis *Vulnerability* pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability

[1]Rini Mayasari, [2]Azhari Ali Ridha, [3]Didi Juardi, [4]Kiki Ahmad Baihaqi
[1,3]Program Studi Teknik Informatika, Universitas Singaperbangsa Karawang
[2]Program Studi Sistem Informasi, Universitas Singaperbangsa Karawang
[4]Program Studi Teknik Informatika, Universitas Buana Perjuangan
Email: rini.mayasari@staff.unsika.ac.id

Abstract

The issue of website security is very crucial at the present time, so that security issues and website vulnerabilities become very important in developing website applications. In detecting vulnerabilities in this study used a qualitative method using the Acunetix Vulnerability Scanner software, which starts from the initiation, investigation, testing and verification stages. The results of this study, the vulnerability level of Universitas Singaperbangsa Karawang is at level 2, namely Medium, so it is possible to access and collect sensitive information because with this information an intruder can easily exploit the existing weaknesses.

Keywords: *vulnerability, website, qualitative methods*

Abstraksi

Isu keamanan website merupakan hal yang sangat krusial pada masa sekarang, sehingga masalah keamanan dan kerentanan website menjadi sangat penting dalam mengembangkan aplikasi website. Dalam mendeteksi kerentanan dalam penelitian ini digunakan metode kualitatif dengan memanfaatkan perangkat lunak *Acunetix Vulnerability Scanner*, yang dimulai dari tahap inisiasi, investigasi, pengujian dan verifikasi. Hasil dari penelitian ini, tingkt kerentanan website Universitas Singaperbangsa berada pada level 2 yaitu Medium, sehingga kemungkinan untuk mengakses dan mengumpulkan informasi sensitif, karena dengan infromasi tersebut penyusup bisa dengan mudah mengeksploitasi kelemahan yang ada.

Kata kunci: vulnerability, website, metode kualitatif

1. PENDAHULUAN

Seiring dengan perkembangan internet dan teknologi web membawa dampak besar bagi peradaban. Internet telah merubah tatanan hidup masyarakat dunia. Menurut data dari worldometer [1] terdapat lebih dari 4 milliar pengguna internet, dengan banyaknya jumlah pengguna internet maka akan semakin banyak pula pihak-pihak yang menyalahgunakan layanan internet untuk berbuat kejahatan, sehingga sering terjadi kebocoran-kebocoran data oleh peretas [2].

Isu yang sering terjadi adalah banyaknya akun-akun yang berisi username dan password bocor di dunia maya, kebocoran data ini sangat mengkhawatirkan dan harus jadi perhatian penting bagi setiap orang yang akan melakukan transaksi di internet. Selain itu juga data-data terkait informasi pribadi

juga sering tersebuar di dunia maya [3] hal tersebut sangat rentan dan jadi berbahaya jika disalahgunakan.

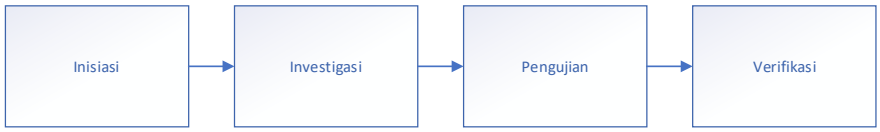
Kerentanan website menjadi perhatian penting bagi pengembang website agar website yang dikembangkan tidak mudah untuk dieksploitasi, hal ini menjadi focus dan prioritas utama jika mengembangkan website [4] sehingga bisa meminimalisir kerentanan dan keamanannya dari serangan hacker.

Kerentanan dari website bisa diketahui dengan cara melakukan evaluasi system [5] terhadap keamanan website tersebut. Salah satunya menggunakan perangkat lunak yang khusus dirancang untuk mengetahui kerentanan yang ada pada suatu sistem yaitu *Acunetix Vulnerability Scanner*.

Scanning yang dilakukan menggunakan perangkat lunak tersebut untuk mengetahui kerentanan (*vulnerability*) yang ada pada sebuah website yang nantinya diketahui hasil penilaian *risk rating* [6] dari website tersebut, sehingga hasil dari proses *scanning* dapat menjadi gambaran mengenai kondisi dan kerentanan apa saja yang ada pada website Universitas Singaperbangsa Karawang.

2. METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode kualitatif. Dalam menunjang penelitian ini digunakan beberapa perangkat lunak yang lazim digunakan untuk menguji keamanan web atau aplikasi salah satunya adalah *Acunetix Vulnerability Scanner*. Adapun untuk tahapannya seperti Gambar 1. dibawah ini:



Gambar 1. Tahapan Penelitian

3. HASIL DAN PEMBAHASAN

Tahap pertama, merupakan tahap inisiasi yang digunakan untuk mengkaji dan menelaah informasi-informasi terkait aspek-aspek apa saja yang terkait dengan keamanan website, untuk analisis keamanan pada website Universitas Singaperbangsa Karawang dalam penelitian ini. Analisis vulnerability dilakukan dengan menggunakan perangkat lunak Acunetix Vulnerability Scanner untuk mengetahui kerentanan apa saja yang ada di dalam website Universitas Singaperbangsa Karawang.

Tahapan kedua, merupakan tahapan investigasi yang dilakukan untuk mengetahui teknologi apa saja yang digunakan pada web server website Universitas Singaperbangsa Karawang serta perangkat lunak apa saja yang digunakan untuk membangun website Universitas Singaperbangsa Karawang. Pada tahapan ini digunakan perangkat lunak nmap untuk melakukan information gathering terkait informasi pada website Universitas Singaperbangsa Karawang, adapun untuk hasilnya adalah

a. Informasi Server

Pada tahapan ini didapatkan informasi web server yang digunakan pada website Universitas Singaperbangsa Karawang. Perangkat lunak yang digunakan untuk mendapatkan informasi server adalah browserspy, dengan aplikasi ini akan didapatkan informasi mengenai spesifikasi dan informasi mengenai server website Universitas Singaperbangsa Karawang. Adapun untuk hasil dari penelusuran informasi server Unsika terlihat pada tabel 1 dibawah ini:

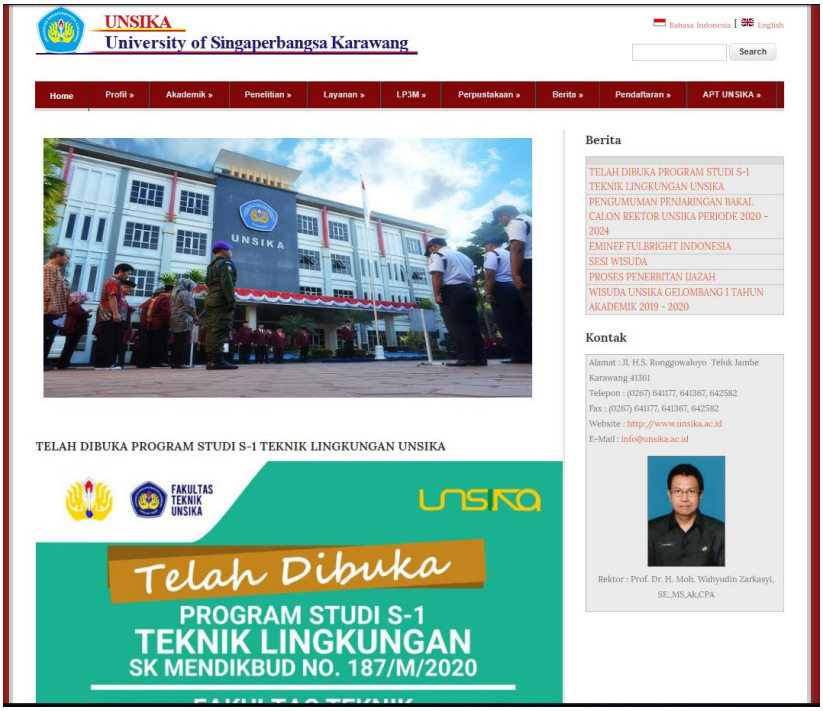
Tabel 1. Web Server Information

Header	Value
Web server	Apache/2.4.25 (Win32) OpenSSL/1.0.2j
HTTP response code	200
Server Address	https://unsika.ac.id/
cache-control	no-cache, must-revalidate, post-check=0, pre-check=0
connection	close
content-language	en
content-type	text/html; charset=utf-8
date	Tue, 02 Jun 2020 12:20:17 GMT
expires	Sun, 19 Nov 1978 05:00:00 GMT
server	Apache/2.4.25 (Win32) OpenSSL/1.0.2j
transfer-encoding	chunked
x-content-type-options	nosniff
x-generator	Drupal 7 (http://drupal.org)
Time to contact web server	2.632208 seconds
Web server	Apache/2.4.25 (Win32) OpenSSL/1.0.2j
HTTP response code	200
Server Address	https://unsika.ac.id/

Dari tabel 1 didapatakan informasi bahwa server Unsika menggunakan Apache versi 2.4.25 dengan menggunakan system operasi Microsoft Windows (Win32).

b. Informasi Perangkat Lunak

Websita Universitas Singaperbangsa Karawang dibangun dengan Content Management System (CMS) Drupal. Dalam pengembangannya website tersebut mnasih menggunakan Drupal Versi 7.17 yang terakhir update tanggal 11-07-2012. Sedangkan untuk versi terakhir untuk saat ini drupal adalah versi 8.86. jadi terlihat bahwa CMS yang digunakan sekarang masih menggunakan versi lama yaitu 7.17. Adapun untuk tampilan beranda dari website Universitas Singaperbangsa Karawang terlihat pada Gambar 2 dibawah ini:



Gambar 2. Tampilan Website Universitas Singaperbangsa Karawang

Tahapan ketiga, yaitu tahapan pengujian terhadap website Universitas Singaperbangsa Karawang dengan melakukan scanning dan pengumpulan informasi terkait keamanan dan kerentanan pada website Universitas Singaperbangsa Karawang. Adapun untuk hasil pengujian menggunakan acunetix vulnerability scanner adalah

a. Total Alert Found

Dari analisis yang dilakukan oleh acunetix maka terdapat 26 alert found, dengan sebaran yaitu 26 dalam level medium, 3 di level low dan 10 di level informational.

First scan		Second scan	
Total alerts found	14	Total alerts found	26
High	0	High	0
Medium	5	Medium	13
Low	0	Low	3
Informational	9	Informational	10

Dari analisis yang dilakukan oleh acunetix maka terdapat 26 alert found, dengan sebaran yaitu 26 dalam level medium, 3 di level low dan 10 di level informational.

b. Risk Vulnerability

Untuk vulnerability yang muncul terdapat resiko yang mungkin bisa dijadikan acuan bagi penulis kepada pengelola website unsika untuk memperhatikan hasil analisis yang dilakukan, adapaun risk vulnerability yang ditemukan adalah:

a. Medium Risk

Merupakan risiko vulnerability tingkat menengah atau sedang. Dari hasil analisis vulnerability terdapat risiko sebanyak 12 HTML form without CSRF Protection, 7

Application error message, 3 User credentials are sent in clear text dan 1 Slow HTTP Denial of Service Attack.

Vulnerabilty group	Instances
HTML form without CSRF protection	12
Application error message	7
User credentials are sent in clear text	3
Slow HTTP Denial of Service Attack	1

b. Low Risk Vulnerability

Merupakan risiko vulnerability tingkat rendah. Dari hasil analisis vulnerability terdapat risiko sebanyak 1 Clickjacking: X-Frame-Options header missing, 1 Session Cokkie without Secure flag set dan 1 TRACE method is enabled.

Vulnerabilty group	Instances
Clickjacking: X-Frame-Options header missing	1
Session Cookie without Secure flag set	1
TRACE method is enabled	1

c. Information Risk Vulnerability

Merupakan risiko vulnerability yang sifatnya informasi. Dari hasil analisis vulnerability yang dilakukan terdapat sebanyak 17 broken links dan 12 Password type input with auto-complete enabled.

Vulnerabilty group	Instances
Broken links	17
Password type input with auto-complete enabled	12

Untuk menentukan tingkat vulnerability pada suatu sistem Acunetix mebaginya menjadi 3 skala yang tediri dari skala 1 sampai 3. Dari hasil analisis yang dilakukan oleh Acunetix tingkat vulnerability yang dimiliki oleh website Universitas Singaperbangsa Karawang berada pada **level 2 (Medium).** Hasil ini menunjukkan bahwa website Universitas Singaperbangsa Karawang masih memiliki celah keamanan yang harus diperhatikan oleh pengelola website sehingga adanya ancaman dan pengaksesan informasi tanpan ijin yang berpotensi merusak sistem bisa diminimalisir.

Tahapan terakhir yaitu tahapan verifikasi yaitu tahapan dimana hasil dari analisis pada penelitian ini dilaporkan kepada pihak terkait yaitu pengelola website dan server untuk dilakukan tindaklanjut terhadap temuan-temuan tehadap vulnerability website Universitas Singaperbangsa Karawang.

4. KESIMPULAN

Berdasarkan dari hasil analisis dan penelaahan yang telah dilakukan terhadap website Universitas Singaperbangsa Karawang menggunakan acunetix vulnerability, maka dapat menarik kesimpulan bahwa penelitian ini menghasilkan analisis kerentanan keamanan sistem web Universitas Singaperbangsa Karawang, terdapat informasi error crlf injection/http response splitting pada input variabel id dan cross site scripting pada input variabel idjp pada website Universitas Singaperbangsa

Karawang dan proses scanning vulnerability pada website Universitas Singaperbangsa Karawang memakan waktu lebih dari 12 jam, sehingga menghasilkan beberapa informasi terkait keamanan dan kerentanan yang ada pada website Universitas Singaperbangsa Karawang.

DAFTAR PUSTAKA

[1] Number of Internet Users (2016) - Internet Live Stats. (2020, February 2).

[2] Juardi, D. (2017, November 28). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. Syntax: Jurnal Informatika.

[3] Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. Jatiswara, 34(3), 239-249.

[4] Purwantoro, P. (2017). Implementasi Metode Online Scanner Untuk Mencari Kerentanan Keamanan (Vulnerability) Server (Studi Kasus: Website www.unsika.ac.id). JURNAL REKAYASA INFORMASI, 6(1). Retrieved from https://ejournal.istn.ac.id/index.php/rekayasainformasi/article/view/34

[5] Tania, A. M., Setiyadi, D., & Khasanah, F. N. (2018, June 1). Keamanan Website Menggunakan Vulnerability Assessment. INFORMATICS FOR EDUCATORS AND PROFESSIONAL : Journal of Informatics.

[6] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264-275.