Analisis Vulnerability Sistem Informasi di Universitas Udayana Menggunakan Tool Acunetix Web Vulnerability Scanner

I Putu Adi Yuda[1], I Gusti Ngurah Anom Cahyadi Putra[2]

Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
adiyuda418@gmail.com[1]
anom.cp@unud.ac.id[2]

Abstract

Now, information technology is developing rapidly. Information systems provide convenience, especially in the field of education such as information systems at Udayana University. In addition, in universities, information systems are also used in elementary schools and high schools. Information systems must have good security. The requirements that must be met are privacy, integrity, authentication, and availability. However, no information system is completely secure. Like the information system at Udayana University has a vulnerability where it is still possible to be attacked by unauthorized parties. System vulnerability has three levels, namely low level, medium level, and high level. This can disrupt a system, and information can be changed by unauthorized parties. Therefore, it is necessary to scan the Udayana University information system to find out system vulnerabilities. The author uses the Acunetix Web Vulnerability Scanner tool. The results of the scanning can be used as a reference for evaluating system vulnerabilities so that further system security can be improved better than before.

Keywords: *information system, vulnerability, system security*

1. Pendahuluan

Sistem informasi memiliki peran yang penting untuk organisasi. Seperti halnya sistem informasi Universitas Udayana yang dapat memberi kemudahan untuk dapat menjalankan kegiatan dibidang pendidikan. Selain itu, dengan adanya sistem informasi dapat meningkatkan daya kompetitif suatu universitas di era perkembangan teknologi seperti sekarang ini. Di bidang pendidikan, selain universitas bahkan menggunakan juga sebagai sarana peningkatan pelayanan pendidikan seperti sekolah dasar sampai sekolah menengah atas.

Universitas Udayana sebagai perguruan tinggi yang menerapkan penggunaan sistem informasi yang digunakan untuk pendaftaran mahasiswa baru, registrasi KRS, melihat KHS, perpustakaan, dan lain sebagainya. Namun, suatu sistem informasi yang ada pastilah belum bisa sempurna. Masih terdapat suatu kerentanan (*vulnerability*) terhadap bermacam serangan seperti *DDoS*, *SQL Injection*, *ClickJacking*, *Cross Site Scripting (XSS)*, dan lain sebagainya [1]. Hal tersebut dapat menyebabkan ancaman untuk keamanan server yang ada. Kurangnya pemahaman terhadap evaluasi kerentanan suatu sistem informasi membuat ancaman dapat dengan mudah memasuki sistem. Oleh karena itu, perlu dilakukan pengujian penetrasi (*Penetration Testing*) untuk mengetahui apa saja kerentanan yang ada dalam sistem. Untuk melakukan pengujian menggunakan *Penetration Testing Tool* seperti *Acunetix Web Vulnerability Scanner [2]*. Pada *tool* tersebut dapat dideteksi apakah kerentanan tersebut termasuk *level low, medium,* atau *high*. Tujuan dari pengujian penetrasi adalah untuk menemukan kerentanan sistem sehingga dapat dilakukan evaluasi.

2. Metode Penelitian

Metode penelitian ini dilakukan secara sistematik sebagai acuan untuk melakukan penelitian agar memperoleh hasil yang dapat menjadi suatu solusi untuk menyelesaikan permasalah yang akan diteliti.

2.1. Kerangka Kerja Penelitian

Kerangka kerja penelitian adalah langkah-langkah yang digunakan dalam penelitian sampai mendapatkan suatu kesimpulan. Berikut ini merupakan alur dari penelitian yang dilakukan:

Gambar 1. Kerangka Kerja Penelitian

Berdasarkan kerangka kerja penelitian pada gambar 1 dapat dideskripsikan langkah-langkah penelitian sebagai berikut:

- Mengumpulkan Data: Pengumpulan data merupakan suatu hal yang penting sebagai penunjang penelitian. Penunjang tersebut dapat berupa jurnal, buku, media internet, maupun dokumen-dokumen.
- Membuat Skenario Pengujian: Skenario pengujian perlu dibuat agar dapat melakukan tindakan yang tepat dalam melakukan pengujian.
- Melakukan Pengujian: Pengujian dilakukan untuk mengetahui kelemahan dalam suatu sistem sebelum dapat melakukan evaluasi.
- Evaluasi: Evaluasi dilakukan setelah menemukan hasil yang berupa suatu data kerentanan apa saja yang terdapat pada sistem sehingga dapat ditarik suatu kesimpulan.

s

2.2. Pengertian Keamanan Jaringan

Keamanan jaringan merupakan tindakan yang dilakukan sebagai kontrol terhadap jaringan sehingga hanya dapat digunakan oleh orang yang memiliki hak untuk mengaksesnya. Suatu sistem dikatakan aman jika memiliki empat aspek, yaitu kerahasiaan (*privacy*), integritas(*integrity*), *authentication*, dan *availability* [3].

a. *Privacy*
   Privacy merupakan suatu aspek dimana suatu sistem informasi hanya dapat dilihat atau diakses oleh pihak yang memiliki hak akses tanpa diketahui pihak siapapun yang tidak memiliki hak akses.

b. *Integrity*
   Integritas berkaitan dengan keutuhan suatu informasi. Suatu informasi tersebut jangan sampai diubah oleh pihak yang tidak memiliki hak akses kecuali mendapatkan izin dari pihak yang berwenang.

c. *Authentication*
   Authentication adalah mensyaratkan ketika pengiriman suatu informasi bisa untuk diidentifikasi dengan baik dan benar serta memberikan jaminan bahwa identitas yang diperoleh adalah benar atau tidak palsu.

d. *Availability*
   Availability berkaitan dengan ketersediaan informasi. Sesuatu yang dibutuhkan oleh pengguna layanan teknologi informasi haruslah dapat dipenuhi sehingga tingkat ketersediaan informasi dapat.

Selain itu, Menurut John D. Howard dalam bukunya "*An Analysis of security incidents on the internet*" menyatakan bahwa: "Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab." [4].

2.3. Pengujian Penetrasi (*Penetration Testing*)

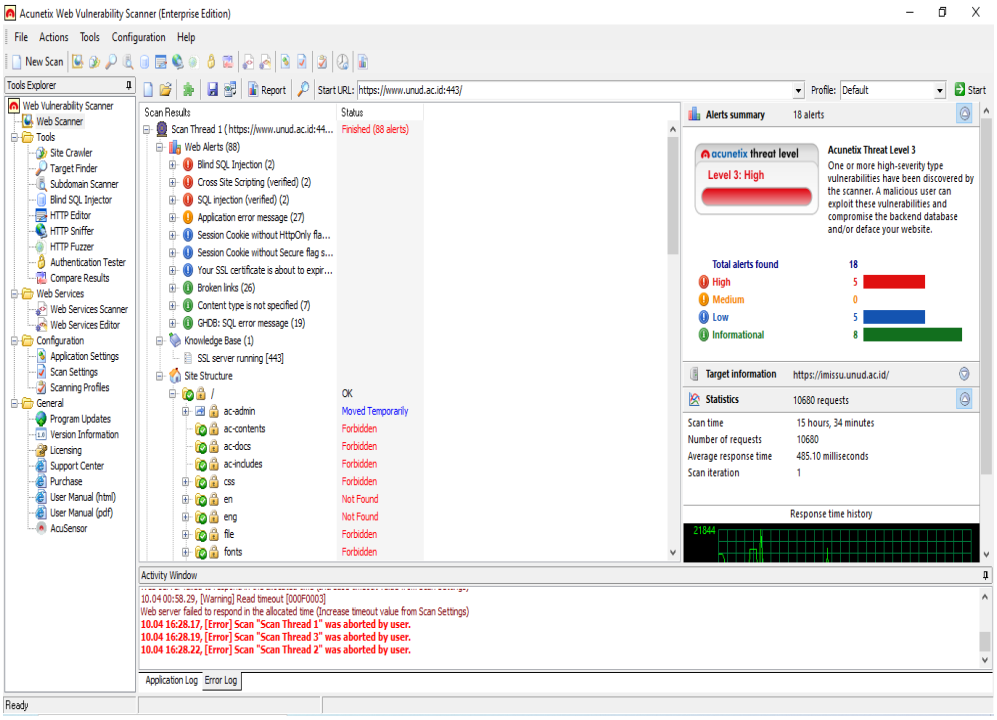
Menurut Georgia Weidman, pengujian penetrasi, atau *pentesting* melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan [5]. Pada *pentest* (sebagai lawan untuk penilaian kerentanan), penguji tidak hanya menemukan kerentanan yang dapat digunakan oleh penyerang tetapi juga mengeksploitasi kerentanan, jika memungkinkan, untuk menilai apa yang mungkin diperoleh penyerang setelah sukses eksploitasi. Tujuan melakukan pengujian penetrasi adalah untuk menemukan kerentanan yang memungkinkan dapat diserang oleh pihak yang tidak memiliki hak akses terhadap suatu sistem. Dengan memperoleh hasil dari pengujian penetrasi sistem dapat dilakukan evaluasi sehingga dapat digunakan untuk meningkatkan keamanan sistem [6].

3. Hasil dan Pembahasan

Pada bagian ini berisikan tentang hasil dari proses *scanning website* Universitas Udayana untuk menguji kerentanan yang ada dan pembahasan mengenai kerentanan yang terdeteksi oleh *tool Acunetix Web Vulnerability Scanner*.

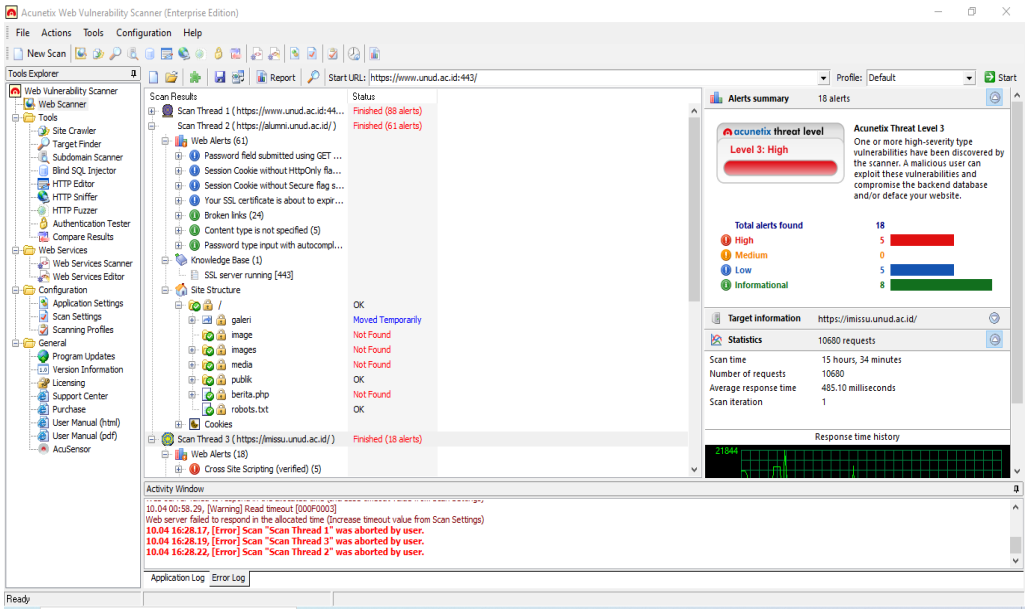
3.1. Vulnerability Scanning

Bagian ini memuat pembahasan dari data hasil penelitian dari kerentanan sistem informasi di Universitas Udayana.Pengujian yang dilakukan penulis adalah *vulnerability scanning*. Untuk melakukan *vulnerability scanning* menggunakan *tool acunetix web vulnerability scanner* untuk mengetahui celah yang terdapat pada sistem informasi di Universitas Udayana.



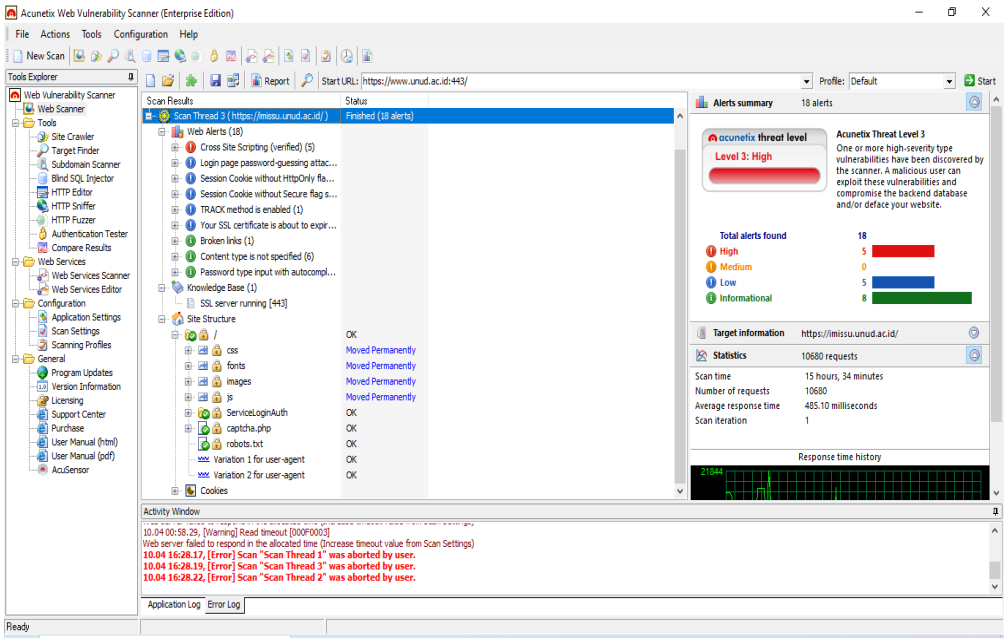
Gambar 2. Hasil *Scanning* dengan *Tool Acunetix Web Vulnerability Scanner* pada *https://unud.ac.id*

Pada gambar 2 merupakan hasil scanning yang dilakukan pada *https://unud.ac.id* yang terdapat suatu kerentanan *level high* yaitu *SQL Injection* dan *Cross Site Scripting (XSS)*. Selain itu, terdapat kerentanan *level medium* seperti *Application error message* dan kerentanan *level low* yaitu *session cookie without httpOnly flag set* dan *session cookie without secure flag set*. Selanjutnya hasil *scanning* gambar 3 akan ditampilkan pada gambar di bawah ini.



Gambar 3. Hasil *Scanning* dengan *Tool Acunetix Web Vulnerability Scanner* pada *https://alumni.unud.ac.id*

Pada gambar 3 hasil scanning pada *https://alumni.unud.ac.id* yang terdapat kerentanan *level low* yaitu *password field submitted,SSL certificate is about to expired, session cookie without httpOnly flag set* dan *session cookie without secure flag set*. Selanjutnya hasil *scanning* gambar 4 akan ditampilkan dibawah ini.



Gambar 4. Hasil *Scanning* dengan *Tool Acunetix Web Vulnerability Scanner* pada https://imissu.unud.ac.id

Pada gambar 4 hasil *scanning* menunjukan terdapat kerentanan *level high* yaitu *cross site scripting (XSS)*. Selain itu terdapat kerentanan *level low* yaitu *login page password- quession attack*, *SSL certificate is about to expired*, *session cookie without httpOnly flag set*, *session cookie without secure flag set*, dan *TRACK method is enable*. Berdasarkan hasil scanning yang telah dilakukan dapat diklasifikasikan tingkatan kerentanan yang terdapat pada website Universitas Udayana pada tabel di bawah.

Tabel 1. Klasifikasi Tingkat Kerentanan yang Ditemukan

Tingkat Kerentanan	Keterangan
Level High	*SQL Injection* *Cross Site Scripting (XSS)*
Level Medium	*Application error message*
Level Low	*login page password- quession attack* *SSL certificate is about to expired* *Session cookie without httpOnly flag set* *Session cookie without secure flag set* *TRACK method is enabled*

4. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa suatu informasi tidak ada yang sempurna. Seorang *web programmer* maupun *server administrator* hanya bisa melakukan pengurangan resiko-resiko kerentanan sistem semaksimal mungkin. Hasil pengujian menunjukan

terdapat kerentanan sistem dengan tiga tingkatan yaitu *level high*, *level medium*, dan *level low*. Pengujian penetrasi dapat dilakukan kembali setelah melakukan evaluasi terhadap kerentanan sistem dengan tujuan untuk meningkatkan keamanan sistem informasi Universitas Udayana.

Daftar Pustaka

[1] Sahren, Dalimuthe, R. A., & Amin, M. (2019). Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus, 994–1001.
[2] Al Fajar, F. (2020). Analisis Keamanan aplikasi web Prodi Teknik Informatika Uika Menggunakan ACUNETIX web vulnerability. INOVA-TIF, 3(2), 110. https://doi.org/10.32832/inova-tif.v3i2.4127
[3] Retna Mulya, B. W., & Tarigan, A. (2018). Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan CVSS Dan Fmea. ILKOM Jurnal Ilmiah, 10(2), 190–200. https://doi.org/10.33096/ilkom.v10i2.311.190-200
[4] Sirait, F., & Putra, S. (2018). Implementasi Metode Vulnerability Dan Hardening Pada Sistem Keamanan Jaringan, 9.
[5] Weidman, G. (2014). Penetration testing: A hands-on introduction to hacking. No Starch Press.
[6] Kamilah, I., Ritzkal, & Hendrawan, A. H. (2019). Analisis Keamanan Vulnerability Pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika.