Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF

Stefanus Eko Prasetyo [a], *Nurul Hassanah* [b]

[a] *Universitas Internasional Batam, Jl. Gajah Mada Baloi – Sei Ladi, Batam, 29442, Indonesia*
[b] *Universitas Internasional Batam, Jl. Gajah Mada Baloi – Sei Ladi, Batam, 29442, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 02 Juli 2021
Revisi Akhir: 07 Juli 2021
Diterbitkan *Online*: 10 September 2021

KATA KUNCI

Keamanan Website
ISSAF
Penetration Testing
Hacker

KORESPONDENSI

E-mail: stefanus.eko.p@gmail.com

A B S T R A C T

With the support of various types of media for delivering information, technological developments change over time. To facilitate access to information, one of them can use the media website. With the development of website technology, more and more parties are using it as a supporting medium for information transmission, including educational institutions in Indonesia. However, many administrators do not understand the security of the website created but pay more attention to the appearance and function of the website. As a result, there were cases of hacker attacks on websites that resulted in data leaks and changes in website appearance. Therefore, it is important to realize the importance of website security to prevent leakage of important data. Because there have been cases of hacker attacks that have occurred several times, the researchers conducted a security analysis of the main website of the Universitas Internasional Batam Institute using the ISSAF method.

1. PENDAHULUAN

Dengan pertumbuhan teknologi yang semakin inovatif dalam menciptakan media baru dalam penyampaian informasi ialah website. Teknologi yang terdapat pada website saat ini sangat dibutuhkan dalam penyampaian informasi secara luas tanpa batas. Sistem penggunaan website yang gampang dan bisa diakses oleh siapa saja asal terkoneksi jaringan internet dan dapat dibuka pada perangkat komputer dan smartphone [1]. Tidak ketinggalan institusi Pendidikan menjadikan teknologi website sebagai media untuk memberikan informasi terbaru serta mempromosikan kepada masyarakat umum terkait informasi gelombang penerimaan mahasiswa baru ataupun informasi beasiswa yang tersedia. Melalui situs website institusi tersebut masyarakat dapat memberikan feedback seperti saran, kritik ataupun pertanyaan terkait dengan institusi secara bebas [2].

Sebanding dengan tingkat penggunaan website yang tinggi juga diimbangi dengan munculnya kerentanan dari teknologi website yang berisiko diserang oleh para hacker dari berbagai celah keamanan website yang kurang diperhatikan administrator sehingga terjadilah peretasan website. Dengan tingkat keamanan website yang rendah menjadikan para hacker dapat dengan mudah mengakses data penting [3]. Dengan semakin canggihnya teknologi yang tersedia sekarang menjadikan hacker makin pintar dalam melakukan teknik hacking untuk mendapatkan keuntungan pribadi dari pembobolan tersebut. Maka penting melakukan self-pentest secara teratur untuk menguji kerentanan website. Agar tingkat keamanan website dapat terus di-update secara berkala untuk mencegah terjadinya serangan hacker [4]. Dalam melakukan pentest terdapat beberapa framework yang dapat digunakan. Dalam penelitian ini peneliti menggunakan metode ISSAF (Information Systems Security Assessment Framework) yaitu merupakan framework yang terstruktur penggunaannya yang terdiri dari beberapa tahap dalam pengelompokan informasi dalam rencana, penilaian serta laporan pengujian sistem keamanan ke dalam domain yang diuji dan menganalisa secara jelas [5].

Melalui penelitian ini, peneliti ingin melakukan analisis keamanan pada website utama Institusi Universitas Internasional Batam untuk mengetahui kerentanan serta celah keamanan yang kurang diperhatikan oleh administrator menggunakan metode ISSAF. Dikarenakan website utama Universitas Internasional Batam sudah beberapa kali diserang hacker maka perlu tindak lanjut dalam meningkatkan keamanan website dan mencegah terjadinya serangan hacker lainnya.

2. TINJAUAN PUSTAKA

2.1 Website

Website merupakan sebuah teknologi sebagai media penyampaian informasi yang dapat berisi informasi seperti berita terkini tapi juga dapat berisi video maupun lagu [6]. Penggunaan website yang mudah karena dapat diakses dimanapun dan kapanpun dengan syarat memiliki akses internet menjadikan website sebagai media penyampai informasi yang dapat diandalkan. Dalam pengaksesan website pengguna hanya perlu menggunakan smartphone ataupun perangkat komputer dalam mengakses.

2.3 *Information System Security Assessment Framework*

Information System Security Assessment Framework (ISSAF) Adalah metode yang digunakan untuk mengevaluasi keamanan sistem, jaringan komputer ataupun kelemahan program aplikasi. Dalam framework metode ISSAF terdapat 3 tahap dalam evaluasi penilaian yaitu *Planning and Preparation, Assessment, dan Reporting, Clean Up and Destroy Artifacts* [7].

2.3 Penetration Testing

Penetration Testing Adalah metode penilaian dengan cara menguji kelemahan dari keamanan sistem, jaringan komputer ataupun kelemahan program aplikasi web. Dengan melakukan serangan langsung terhadap target atau sistem yang akan diuji. Hasil dari pengujian ini dapat menjadi masukan untuk memperbaiki kelemahan sistem yang terdeteksi, sehingga dapat meningkatkan keamanan dan guna menghindari serangan cyber yang dapat terjadi kapan saja [8]. Metode ini memiliki 3 metode yang berbeda berdasarkan jangkauan lingkungan dan jenis target yaitu *black box testing*, *white box* testing dan *grey box testing*. Berikut penjelasan 3 metode pentest sebagai berikut:

1. *Black Box Testing*

Dalam metode ini, penguji melakukan serangan tanpa mengetahui infrastruktur yang digunakan oleh target. Penguji harus mencari tahu semua kerentanan dalam keamanan sistem berdasarkan kemampuan serta pengetahuan mereka. Metode *black box* ini digunakan untuk mengaudit keamanan sistem dengan penyerang eksternal untuk melakukan serangan pada celah kerentanan yang ditemukan. Dari 3 metode pentest yang ada peneliti menggunakan metode *black box* dalam pengujian penelitian ini.

2. *White Box Testing*

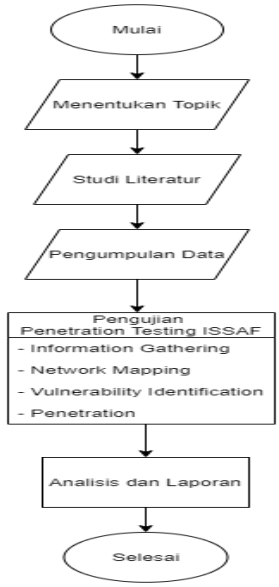
Dalam metode ini, penguji diberikan semua informasi terkait infrastruktur keamanan sistem target yang akan diuji dan dilakukannya audit keamanan sistem dari internal. Serangan yang dilakukan dengan mensimulasikan jika bahaya terjadi dalam lingkungan internal.

3. *Grey Box Testing*

Dalam metode ini, metode *grey box* merupakan gabungan dari 2 metode yaitu *black box* dan *white box.* Penguji diberikan informasi terkait infrastruktur keamanan sistem tapi juga harus mencari informasi sendiri untuk menemukan celah kerentanan sistem.

3. METODOLOGI

Dalam penelitian ini digunakan framework ISSAF sebagai metode penelitian dan menggunakan metode *black box* testing dalam pengujian pentest. Dan dalam penulisan penelitian ini agar sesuai dengan tahapan yang diperlukan maka menggunakan alur penelitian. Berikut bagan alur penelitian dapat dilihat pada Gambar 1 sebagai berikut.



Gambar 1. Alur Penelitian

1. Menentukan Topik

Pada tahap ini, peneliti mencari topik yang akan diangkat menjadi judul penelitian.

2. Studi Literatur

Setelah menemukan topik dilanjutkan mencari referensi jurnal, informasi terkait ataupun teori yang sudah dikemukakan untuk mendukung topik ini.

3. Pengumpulan Data

Pada tahap ini peneliti melakukan pengumpulan informasi terhadap topik yang dipilih untuk memperjelas penelitian.

4. Pengujian Penetration Testing ISSAF

Tahap ini dilakukan 4 proses pengujian serangan menggunakan metode ISSAF meliputi: Information Gathering, Network Mapping, Vulnerability Scanning, dan Penetration.

5. Analisis dan Laporan

Pada tahap ini dilakukan analisis terhadap pengujian yang sudah dilakukan dan merangkumnya ke dalam laporan.

Dalam proses pengujian pentest dengan framework ISSAF dapat disimpulkan berikut tahapan yang akan dilaksanakan, tools yang digunakan dan fungsi tools dapat dilihat pada Tabel 1.

Tabel 1. Metode ISSAF

Nama Tahapan	Tools	Keterangan
Information Gathering	Whois, SSL Scan	Mencari Informasi Website
Network Mapping	Nmap	Scan Port
Vulnerability Identification	Acunetix Web Vulnerability Scanner	Scan Kerentanan
Penetration	1. Low Orbit Ion Canon 2. SQLMap	1. DDOS Attack 2. SQL Injection

4. HASIL DAN PEMBAHASAN

Pada tahapan pengujian *pentest* keamanan website Universitas Internasional Batam menggunakan metode ISSAF dengan 4 tahap dijelaskan sebagai berikut:

4.1. Pengujian

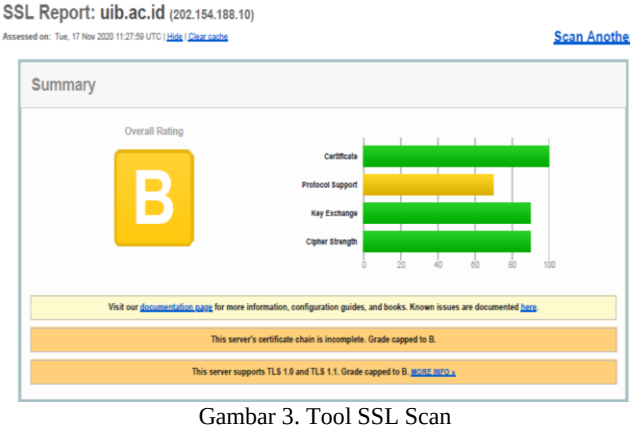
1. Information Gathering

Pada tahap ini dilakukannya pencarian informasi terkait target website menggunakan 2 tools online yaitu *Whois Domain* dan *SSL Scan*. Berikut hasil domain website uib.ac.id menggunakan tool Whois pada Gambar 2. dan tool SSL Scan pada Gambar 3.

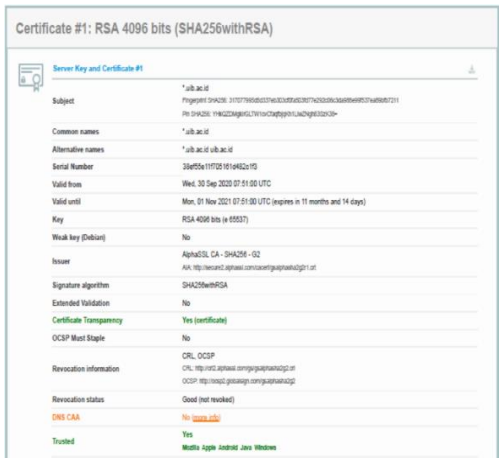
```
Domain ID: PANDI-DO151821
Domain Name:uib.ac.id
Created On:2002-09-28 13:32:26
Last Updated On:2020-11-01 02:43:55
Expiration Date:2021-10-31 23:59:59
Status:clientTransferProhibited
Status:serverTransferProhibited
Status:autoRenewPeriod
==========================================================
Sponsoring Registrar Organization:Digital Registra
Sponsoring Registrar City:Sleman
Sponsoring Registrar State/Province:Yogyakarta
Sponsoring Registrar Postal Code:55281
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:0274882257
Sponsoring Registrar Contact Email:info@digitalregistra.co.id
Name Server:nsid1.rumahweb.com
Name Server:nsid2.rumahweb.net
Name Server:nsid3.rumahweb.biz
Name Server:nsid4.rumahweb.org
DNSSEC:Unsigned

Information Updated: 2020-11-17 11:04:07
```

Gambar 2. Tool Whois

Dari Gambar 2. hasil *tool Whois* didapati informasi terkait website uib.ac.id seperti tanggal pembuatan hingga waktu kadaluarsa website serta layanan web hosting yang digunakan.



Gambar 3. Tool SSL Scan



Gambar 4. Hasil SSL Scan

Dan dari Gambar 3. Dan Gambar 4. hasil tool SSL Scan didapati bahwa website target sudah menggunakan *protokol* keamanan SSL dengan *rating* B. Dan terdapat masalah yang perlu diperbaiki yaitu protokol support server masih menggunakan versi lama yaitu TLS 1.0 dan TLS 1.1.

2. Network Mapping

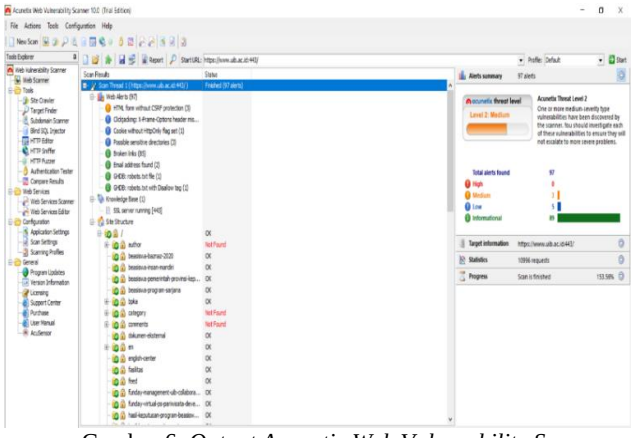
Pada tahap ini dilakukan *scanning port* menggunakan aplikasi Nmap. Dari output pengujian terdapat 6 port yang berstatus open. Berikut hasil *scanning* dengan Nmap pada Gambar 5.

Port		State (toggle closed [0] | filtered [5])	Service	Reason	Product
22	tcp	open	tcpwrapped	syn-ack	
25	tcp	filtered	smtp	no-response	
53	tcp	filtered	domain	no-response	
80	tcp	open	http	syn-ack	nginx
139	tcp	filtered	netbios-ssn	no-response	
443	tcp	open	http	syn-ack	nginx
445	tcp	filtered	microsoft-ds	no-response	
1723	tcp	open	pptp	syn-ack	MikroTik
2000	tcp	open	bandwidth-test	syn-ack	MikroTik bandwidth-test server
5678	tcp	filtered	rrac	no-response	
8291	tcp	open	tcpwrapped	syn-ack	

Gambar 5. Output Nmap Scan

3. Vulnerability Identification

Pada tahap ini dilakukannya scanning kerentanan pada website uib.ac.id menggunakan aplikasi *Acunetix Web Vulnerability Scanner*. Didapati hasil pengujian kerentanan website pada level 2: Medium masih dalam tahap aman. Berikut hasil scanning dengan aplikasi Acunetix pada Gambar 6.

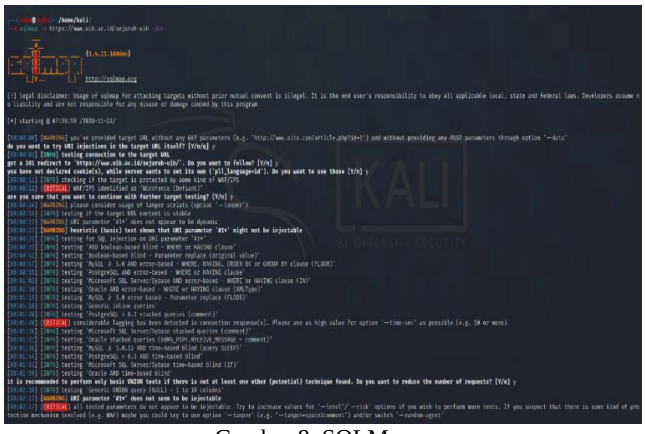


Gambar 6. *Output Acunetix Web Vulnerability Scanner*

Penetration

Pada tahap ini dilakukan dengan 2 jenis serangan yaitu serangan DDOS Attack dan SQL Injection menggunakan OS Kali Linux. Berikut hasil dari DDOS Attack dengan LOIC pada Gambar 7. dan SQL Injection dengan SQLMap pada Gambar 8.

Gambar 7. LOIC



Gambar 8. SQLMap

Pada Gambar 8. dilakukan serangan berbeda jumlah treads mulai dari 10, 40, dan 50 thread. Dan pada 50 threads berhasil mengakibatkan server down sementara. Tapi berikutnya IP peneliti sudah terblokir dengan pengamanan firewall server. Sedangkan pada Gambar 8. serangan SQL Injection gagal ditembus.

5. KESIMPULAN DAN SARAN

Dari penelitian yang telah dilakukan dapat disimpulkan bahwa keamanan website utama Institusi Universitas Internasional Batam www.uib.ac.id tergolong cukup aman dari serangan hacker. Dari 4 tahap pengujian menggunakan metode ISSAF didapati pada tahap penetration DDOS *Attack* website utama masih bisa ditembus dan mengakibatkan server down sementara. Tapi dengan adanya backup keamanan firewall yang aktif cukup membantu server untuk menghindari serangan hacker terhadap serangan berikutnya. Secara keseluruhan keamanan sistem website utama masih tergolong relatif aman dari serangan hacker.

Berikut saran berdasarkan hasil pengujian yang yang perlu dilakukan perbaikan ataupun diterapkan dalam memperbaiki keamanan website agar lebih aman terhindar dari serangan hacker:

1. *Upgrade* sertifikat *protocol support* SSL dari TLS 1.0 dan TLS 1.1 ke TLS 1.3.
2. Menerapkan keamanan CSRF dalam HTML website untuk mencegah hacker melakukan serangan dengan menemukan kelemahan lain yang tidak terdeteksi.

DAFTAR PUSTAKA

[1] A. Manik, I. Salamah, and E. Susanti, "PENGGUNA WEBSITE POLITEKNIK NEGERI SRIWIJAYA THE IMPACT OF WEBQUAL 4 . 0 METHOD TOWARDS USER," *J. Elektro Telekomun. Terap.*, pp. 477–484, 2017.

[2] D. R. Chandranegara, C. Sri, K. Aditya, and F. D. Setiawan, "Implementasi Website Profile Madrasah Muhammadiya Al-Munawarroh Malang Sebagai Media Informasi Bagi Masyarakat," vol. 4, no. 2, pp. 305–309, 2020.

[3] I. Riadi and A. Y. Y. W, "Analisis Keamanan Website Open Journal System Menggunakan Security Analysis Open Journal System Website Using," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 4, pp. 853–860, 2020, doi: 10.25126/jtiik.202071928.

[4] E. I. Alwi, H. Herdianti, and F. Umar, "Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning," *INFORMAL Informatics J.*, vol. 5, no. 2, p. 43, 2020, doi: 10.19184/isj.v5i2.18941.

[5] M. Rusdan, D. T. H Manurung, and F. Kharisma Genta, "Evaluation of Wireless Network Security Using Information System Security Assessment Framework (ISSAF) (Case Study: PT. Keberlanjutan Strategis Indonesia)," *TEST Eng. Manag.*, vol. 83, no. June, pp. 15714 – 15719, 2020.

[6] W. S. Fatmala, Suprapto, and A. Rachmadi, "Analisis Kualitas Layanan Website E-Commerce Berrybenka Terhadap Kepuasan Pengunjung Menggunakan Metode WebQual 4.0 dan Importance Performance Analysis (IPA)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 175–183, 2018.

[7] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020, doi: 10.29100/jipi.v5i1.1565.

[8] L. D. Samsumar, K. Gunawan, D. Program, S. Manajemen, D. Program, and S. Komputerisasi, "Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi," *Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, pp. 73–82, 2017.

BIODATA PENULIS

Stefanus Eko Prasetyo, S.Kom., MMSI
Dosen Tetap Pada Universitas Internasional Batam.

Nurul Hassanah
Mahasiswa Universitas Internasional Batam Program Studi Sistem Informasi sejak 2017.