



JURNAL INFORMATIKA DAN TEKNOLOGI KOMPUTER

Halaman Jurnal: <https://journal.amikveteran.ac.id/index.php/jitek>
Halaman UTAMA Jurnal : <https://journal.amikveteran.ac.id/index.php>



ANALISIS KEAMANAN WEB NEW KUTA GOLF MENGGUNAKAN METODE VULNERABILITY ASSESSMENTS DAN PERHITUNGAN SECURITY METRIKS

Rifky Lana Rahardian ^a

^a Sistem Komputer, rifky@stikom-bali.ac.id, Institut Teknologi Dan Bisnis STIKOM Bali

ABSTRACT

Various crimes that are security threats that can occur when we are socially networked, one of them is virtual theft. New Kuta Golf has tournament standard field and the first course with a layout model link. Large mobility companies also make data processing even bigger and more web sites that are concerned with transactions and promotional media. This is a reference to obtain information about the security of the New Kuta Golf website. The data that has been obtained are carried out for the project work step, are: (1) To conduct a Vulnerability assessment. (2) Analyze the results of the scan. (3) Calculate security metrics from the results obtained from the scanning process. (4) Documentation of the installation process, and calculating security metrics. The results of the research then analyzed and discussed with a review of the theory that was embraced. From the results of the tests, the following results are obtained: (1) In carrying out website security testing can be done by Vulnerability Assessment uses the acunetix application to find detailed results. (2) Determining the security of a website can be determined using security metrics. (3) The results of the vulnerability assessment on <http://newkutagolf.co.id> has a high value.

Keywords: Internet, Security, Vulnerability assessments

Abstrak

Berbagai kejahatan yang merupakan ancaman keamanan yang bisa saja terjadi saat kita beraktifitas di jejaring sosial, pencurian virtual di Internet dapat menjadi salah satu contoh ancaman. New Kuta Golf merupakan lapangan dengan standar tournament dan merupakan lapangan pertama dengan layout model links. Besarnya mobilitas perusahaan tentunya juga membuat data yang berproses semakin besar dan banyak, dikarenakan website berperan penting dalam transaksi dan media promosi. Hal tersebut menjadi acuan penulis yang berkeinginan mendapatkan informasi mengenai keamanan website New Kuta Golf, sebagai bahan penilaian untuk mengetahui seberapa besar ancaman dalam jaringan internet. Data yang telah didapat kemudia diproses untuk menjalankan langkah pengerjaan proyek, diantaranya: (1) Melakukan Vulnerability assessments. (2) Menganalisa hasil dari scanning. (3) Menghitung security metrics dari hasil yang telah didapatkan dari proses scanning. (4) Melakukan dokumentasi terhadap proses instalasi, dan perhitungan security metrics. Hasil penelitian kemudia dianalisis dan dilakukan pembahasan dengan telaah teori yang telah diterangkam. Pengujian didapatkan hasil, sebagai berikut: (1) Dalam melakukan pengujian keamanan website dapat dilakukan dengan cara Vulnerability. Assessment menggunakan aplikasi acunetix hingga menemukan hasil yang detail. (2) Menentukan keamanan sebuah website dapat ditentukan dengan menggunakan security metrics. (3) Hasil vulnerability assessments pada <http://newkutagolf.co.id> adalah bernilai high.

Kata Kunci: Internet, Keamanan, Vulnerability assessments

1. PENDAHULUAN

Website adalah kumpulan halaman yang didalamnya terdapat dokumen – dokumen multimedia (teks, gambar, suara, animasi, video) yang diakses menggunakan protocol HTTPS (hypertext, transfer protocol) [1] - [3]. Fungsi dari website antara lain media promosi, media pemasaran, media informasi, media pendidikan, serta media komunikasi [2]. Dalam menggunakan internet atau beraktifitas di jejaring sosial, banyak kejahatan yang merupakan ancaman keamanan yang bisa saja terjadi dalam bentuk apapun, pencurian virtual di Internet dapat menjadi salah satu contoh ancaman. Dengan sangat cepat, seorang hacker dapat mengakses sistem dan melakukan pencurian informasi penting, seperti mengambil data dan informasi pribadi. Kerusakan juga bisa dilakukan dengan infiltrasi sistem, kemudian informasi yang didapat

Received September 10, 2022; Revised September 30, 2022; Accepted November 1, 2022

tentang website dapat digunakan untuk menyisipkan virus dan *worm* oleh karna itu dibutuhkan pengetahuan tentang keamanan web agar web tersebut dapat segera lebih dipersiapkan keamanan yang lebih baik.

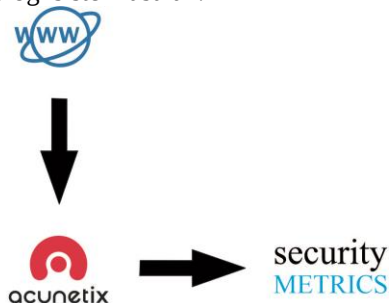
Vulnerability Assessment (VA) adalah keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi data, hasil scanning jaringan, konfigurasi pada sistem, cara pengelolaan, kesadaran keamanan orang – orang yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada [1]. Berbeda dengan pentest *blackbox* dan *greybox*. Dalam metode *blackbox*, penguji atau tester tidak dibekali dengan informasi apapun mengenai sistem yang akan diuji, baik itu infrastruktur atau *source code* yang digunakan. Mereka diposisikan seperti seorang *hacker* yang harus mengeksploitasi sistem untuk mencari celah keamanan yang dapat diretas. Penguji yang menggunakan metode *blackbox* harus familiar dengan alat pemindaian otomatis dan metodologi pentest manual. Mereka juga harus memiliki kemampuan untuk membuat map dari sistem yang diuji berdasarkan observasi yang telah dilakukan. Berbeda dengan pentest metode *blackbox* yang memposisikan penguji sebagai *hacker* atau orang luar, maka metode *greybox* memposisikan penguji sebagai pengguna. Dalam metode ini, penguji memiliki akses dan informasi hanya sebatas sebagai pengguna. Tujuan dari metode *greybox* adalah untuk memberikan penilaian keamanan yang lebih efisien dari pada *blackbox*. Dengan memiliki sejumlah informasi, mereka dapat menguji sistem keamanan dan mensimulasikan serangan. Metode *greybox* juga memungkinkan pengujian dapat melakukan pengujian secara lebih focus untuk mengeksploitasi kerentanan dengan resiko yang lebih besar [4]. Metode *blackbox* dan *greybox* ini kurang mampu memberikan hasil yang lebih lengkap dan akurat, karena tidak semua potensi kerentanan akan teridentifikasi. Sering ditemukan kejadian pentest *blackbox* melaporkan tidak adanya kelemahan kritis, namun saat dilakukan *Vulnerability Assessment (VA)* terdapat beberapa kelemahan kritis. Hal tersebut dapat membuktikan bahwa melakukan *Vulnerability Assessment (VA)* lebih baik dari pada melakukan pentest *blackbox* dan *greybox*.

New Kuta Golf merupakan lapangan dengan standar tournament dan merupakan lapangan pertama dengan layout model links. Hal ini memberikan tantangan tersendiri bagi pemain dengan handicap kecil maupun bagi pemula. Dalam sehari new Kuta Golf hampir dikunjungi pemain sekitar 200 orang. New Kuta Golf sudah menggunakan sistem reservasi lapangan berbasis web sebagai media transaksi yang dapat memudahkan pemain dalam melakukan booking lapangan sesuai keinginan, website juga digunakan untuk media promosi event yang akan diselenggarakan dan tentunya untuk media informasi perusahaan. Besarnya mobilitas perusahaan tentunya juga membuat data yang berproses juga semakin besar, dikarenakan website berperan penting dalam transaksi dan media promosi. Hal tersebut menjadi acuan penulis yang berkeinginan mendapatkan informasi mengenai keamanan website agar dapat memberikan *report* seberapa aman website new Kuta Golf. Data yang di dapat akan digunakan untuk menjadi acuan melakukan perbaikan keamanan, tentunya agar keamanan website beserta data bisa lebih terjamin. Maka dari itu dalam tugas proyek ini dilakukan pengujian celah keamanan dengan metode scanning *Vulnerability Assessment (VA)* pada website <http://newkutagolf.co.id>. Hasil *scan* berupa perhitungan *security metrics* yang akan menampilkan *score* akhir dari hasil *Vulnerability Assessment (VA)*.

2 METODOLOGI PENELITIAN

2.1 Topologi sistem usulan

Berikut merupakan gambar topologi sistem usulan:



Gambar 1. Topologi Sistem Usulan

Gambar 1 merupakan topologi sistem usulan yang akan dilakukan penulis dalam pengujian. Tentukan website yang akan diuji, kemudian jika sudah lakukan pengujian menggunakan aplikasi acunetix agar dapat mengetahui celah keamanan pada web tersebut, setelah dilakukan pengujian akan dilakukan perhitungan *security metrics* untuk mendapatkan hasil akhir.

Perancangan dan Rencana pengerjaan

Adapun langkah – langkah pengerjaan proyek ini sebagai berikut:

- 1) Melakukan *Vulnerability assessments*.
- 2) Menganalisa hasil dari *scanning*.
- 3) Menghitung *security metrics* dari hasil yang telah didapatkan dari proses *scanning*.
- 4) Melakukan dokumentasi terhadap proses instalasi, dan perhitungan *security metrics*.

Rencana Pengujian

1) Scanning

Akan dilakukan *scanning vulnerability assessments* menggunakan aplikasi acunetix untuk mengetahui beberapa celah pada suatu web. *Acunetix website application scanner* merupakan perangkat lunak yang dikembangkan untuk melakukan *scanning*. Kelebihan dari *tools* ini adalah kemampuan untuk memberikan solusi dari kelemahan yang ditemukan dan mengelola *traceability* dari setiap *vulnerabilities* tersebut. Selain itu, acunetix menyediakan fungsi – fungsi tambahan yang dapat digunakan untuk melakukan pengujian lebih lanjut terhadap *website* yang diuji [10].

2) Perhitungan *security metrics*.

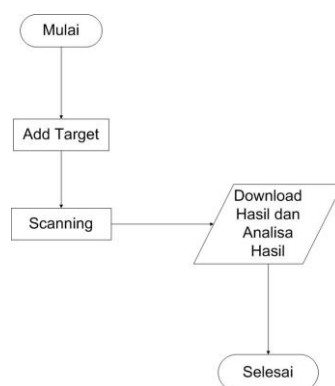
Setelah dilakukan proses *scanning vulnerability* dan mendapat data dari beberapa celah akan dilakukan perhitungan *security metrics* untuk mendapatkan hasil akhir dari pengujian yang telah dilakukan. *Security metrics* merupakan pengukuran kuantitatif untuk menilai operasi keamanan di organisasi membantu organisasi untuk membuat keputusan tentang berbagai aspek keamanan yang meliputi arsitektur keamanan dan kontrol untuk efektivitas dan efisiensi operasi keamanan [7]. *Security metrics* dapat diukur dengan skala 1-10 dimana 10 adalah sistem sangat tidak aman dan bisa ditembus penyerang selain itu, *security metrics* berharga untuk tingkat manajerial TI dan stakeholder yang mempertanyakan dampak keamanan terhadap bisnis proses dan kegiatan. NIST (*National Institute of Standards and Technology*) mengkategorikan *security metrics* menjadi 3 tipe sebagai berikut [6] :

- a. *Implementation metrics* yaitu memberikan informasi program keamanan, kontrol keamanan, dan kebijakan prosedur yang terkait [6].
- b. *Effectiveness/efficiency metrics* yaitu proses pemantauan apakah keamanan sudah diterapkan sesuai prosedur dan hasil yang baik [6].
- c. *Impact metrics* yaitu informasi terkait dampak keamanan yang perusahaan atau organisasi terima kedepannya [6].

Security metrics pada proyek ini dinilai dengan parameter yaitu *vulnerability assessments* yang dimaksud dengan *vulnerability* adalah suatu kelemahan program yang memungkinkan terjadinya pemanfaatan secara sewenang-wenang pada sistem. Selanjutnya dilakukan perhitungan *Common Vulnerability Scoring System* menggunakan metode sebagai berikut [8].

- a. *Base score/overall score* mewakili karakteristik intrinsik dan mendasar dari kerentanan yang konstan seiring waktu dan lingkungan pengguna.
- b. *Temporal score* mewakili karakteristik kerentanan yang berubah dari waktu ke waktu namun tidak diantara lingkungan pengguna.
- c. *Environmental score* mewakili karakteristik kerentanan yang relevan dan unik bagi lingkungan pengguna tertentu.

2.2 Topologi Tahapan Pengujian Vulnerability Assessments

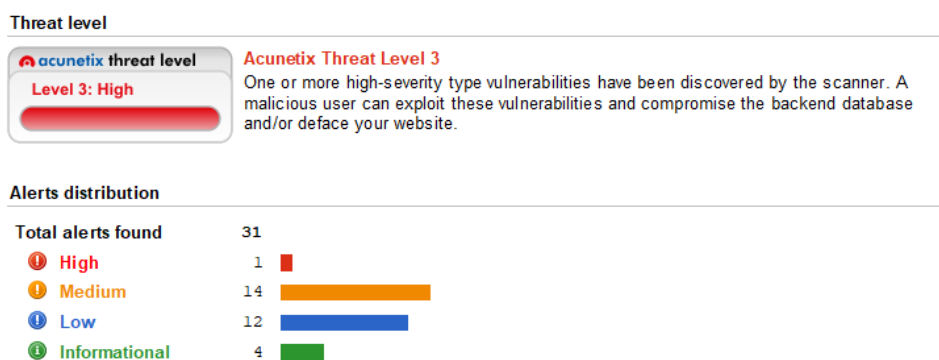


Gambar 2. Proses Vulnerability Assessments

Pada gambar 2 merupakan tahap – tahap pengerjaan pengujian dari proyek ini. Dari menentukan target, dalam hal ini proyek melakukan pengujian kepada <http://newkutagolf.co.id> yang merupakan *website* dari perusahaan New Kuta Golf. Lakukan *scanning* menggunakan aplikasi *acunetix* yang hasilnya akan didownload untuk dilakukan perhitungan hingga mencapai hasil yang seharusnya.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi



Gambar 3. Hasil Scanning

Pada gambar 3 dapat dilihat hasil dari scanning web <http://newkutagolf.co.id> tertulis bahwa “Acunetix Threat Level 3” yang masuk dalam kategori “High” yang berarti merupakan target paling rentan beresiko serangan hacking dan pencurian data. Kategori hasil dari scanning terbagi menjadi 4 yaitu high, medium, low, dan information. Berikut merupakan penjelasan dari masing-masing status yang ditemukan setelah melakukan proses scanning:

- **High** : Kerentanan yang paling berisiko untuk serangan hacking dan pencurian data.
- **Medium** : Kerentanan yang disebabkan misconfiguration server, skema jaringan dan sitecoding yang lemah.
- **Low** : Kerentanan yang disebabkan oleh kurangnya enkripsi pada jalur lalu lintas data.
- **Informational**: item yang memberikan informasi tentang layanan yang telah ditemukan selama scanning.

Tabel 1. Hasil Scanning

Celah	Jumlah
Blind SQL Injection	1  Blind SQL Injection • /welcome/getPrice - o idPrice
Application Error Message	1  Application error message • /welcome/getPrice - o idPrice
Direction Listing	7  Directory listing • /assets • /assets/css • /assets/fonts • /assets/gallery • /assets/images • /assets/images/thumb • /uploads
Error Message On Page	8  Error message on page • /booking • /newsevent/index/ • /programactivity/index/ • /subscribe/save_in • /Transaksi/getTime • /welcome/getPrice • /welcome/getSpace • /welcome/getTimeSel
HTML Form Without CSRF Protection	11  HTML form without CSRF protection • / • /forgot • /newsevent • /newsevent/index/2 • /play • /programactivity • /Transaksi/pay (d21edfc6c45cdb428e55ad3c6c48ada8)

Same Site Scripting	1  Same site scripting • Web Server
Clickjacking X-Frame-Option Header Missing	1  Clickjacking: X-Frame-Options header missing • Web Server
Cookie Without HttpOnly Flag Set	3  Cookie without HttpOnly flag set • /
Cookie Without Secure Flag Set	3  Cookie without Secure flag set • /
Hidden From Input Named Price Was Found	5  Hidden form input named price was found • / • /Transaksi • /Transaksi/pay (d21edfc6c45cdb428e55ad3c6c48ada8)
Broken Links	3  Broken links • /assets/css/fonts/frontglyphs.html • /assets/lightGallery/dist/js/lightgallery-all.min.js • /assets/lightGallery/lib/jquery.mousewheel.min.js
Password Type Input With Auto-Complete Enabled	1  Password type input with auto-complete enabled • /forgot

Pada tabel 1 dapat dilihat hasil scanning web <http://newkutagolf.co.id> terdapat beberapa celah dan jumlah bagian yang rentan diserang hacking atau bagian keamanan yang mudah untuk disusupi yang dapat digunakan untuk pencurian data. Dari hasil scanning tersebut dapat digunakan untuk memperkuat website itu sendiri dengan cara menutup atau melakukan perbaikan dibagian – bagian yang rentan, yang tentunya dilakukan untuk mengamankan website dari hacker – hacker yang ingin merusak atau mencuri data perusahaan melalui website.

Maka dari hasil scanning vulnerability menggunakan aplikasi acunetix web vulnerability scanner dapat disimpulkan bahwa website <http://newkutagolf.co.id> masuk dalam kategori “**High**” yang berpotensi menjadi target paling rentan beresiko terkena serangan hacking dan pencurian data.

3.2 Base Score

Mewakili karakteristik intrinsik dan mendasar dari kerentanan yang konstan seiring waktu dan lingkungan pengguna. Berikut merupakan rumus yang digunakan dalam mengetahui hasil base score yang diperoleh :

$$\begin{aligned} \text{BaseScore} &= (0.6 * \text{Impact} + 0.4 * \text{Exploitability} - 1.5) * f(\text{Impact}) \\ \text{Impact} &= 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact})) \\ \text{Exploitability} &= 20 * \text{AccessComplexity} * \text{Authentication} * \text{AccessVector} \\ f(\text{Impact}) &= 0 \text{ if Impact}=0; 1.176 \text{ otherwise.} \end{aligned}$$

Rumus tersebut sudah langsung terdapat dalam aplikasi yang digunakan penulis yaitu acunetix web vulnerability.

Tabel 2. Base Score

Celah	Base Score	Kategori
 Blind SQL Injection Classification CVSS Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial	6.8	Tinggi
 Application error message Classification CVSS Base Score: 5.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None	5.0	Sedang
 HTML form without CSRF protection Classification CVSS Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None	2.6	Rendah
 Same site scripting Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah

Clickjacking: X-Frame-Options header missing Classification CVSS Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial	6.8	Tinggi
Cookie without HttpOnly flag set Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah
Cookie without Secure flag set Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah
Hidden form input named price was found Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah
Broken links Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah

 Password type input with auto-complete enabled Classification CVSS Base Score: 0.0 - Access Vector: Network - Access Complexity: Low - Authentication: None - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: None	0.0	Rendah
--	-----	--------

Dalam tabel 2 telah dijelaskan celah – celah keamanan pada website <http://newkutagolf.co.id> yang dapat menjadi celah untuk merusak atau mencuri data yang ada. Celah yang terdapat pada tabel sudah dikategorikan langsung oleh aplikasi berdasarkan rumus base score. Dalam base score yang di peroleh pada website <http://newkutagolf.co.id> adalah 6.8 dengan tingkat kerentanan high, yang merupakan kerentanan paling berbahaya.

4. KESIMPULAN

Dari hasil pengujian yang penulis lakukan dapat diambil kesimpulan sebagai berikut :

- 1) Dalam melakukan pengujian keamanan website dapat dilakukan dengan cara *Vulnerability Assessment* menggunakan aplikasi acunetix hingga menemukan hasil yang detail.
- 2) Menentukan keamanan sebuah website dapat ditentukan dengan menggunakan security metrics yang dapat menampilkan hasil berlabel High, Medium atau Low yang ditentukan dengan menggunakan rumus BaseScore yang menghasilkan jumlah hasil 1-10.
- 3) Hasil vulnerability assessments pada <http://newkutagolf.co.id> adalah bernilai high.

DAFTAR PUSTAKA

- [1]. Suryayusra, “Analisis Web Vulnerability pada Portal Pemerintahan Kota Palembang menggunakan Acunetix Vulnerability,” Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom, Thesis, 2014.
- [2]. Penda Sudarto Hasugian, “Perancangan Website Sebagai Media Promosi Dan Informasi,” Journal Of Informatic Pelita Nusantara, Volume 3, No. 1, Maret 2018, e-ISSN 2541-3724.
- [3]. Imanuel Christian Mauko “Pengembangan Website Unit Penelitian Dan Pengabdian Kepada Masyarakat Dan Penerapan Jurnal Elektronik Berbasis Open Source Di Politeknik Negeri Kupang” Jurnal Ilmiah FLASH, Volume 3, Nomor 2, Desember 2017.
- [4]. Wahyu Nur Cholifah1, “Pengujian Black Box Testing Pada Aplikasi Action & Strategy Berbasis Android Dengan Teknologi Phonegap” Jurnal String, Vol. 3, No.2, Desember 2018, p-ISSN: 2527-9661 e-ISSN: 2549-2837
- [5]. Betta Wahyu Retna Mulya, “Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea” ILKOM Jurnal Ilmiah, Volume 10, Nomor 2, Agustus 2018.
- [6]. M. Khan, “Security Metrics Based Network Risk Asessment,” Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom, Thesis , 2013.
- [7]. s. Radack, “Performance Measurement Guide For Information Security,” report, 2008
- [8]. Yunanri. W, “Analisa Deteksi Vulnerability Pada Webserver Open Jurnal System Menggunakan OWASP Scanner” JURTI, Volume 2, Nomor 1, Juni 2018, ISSN: 2579-8790.
- [9]. Mia Zattu Maharani, “Analisis Keamanan Website Menggunakan Metode Scanning Dan Perhitungan Security Metriks” e-Proceeding of Applied Science, Vol.3, No.3 Desember 2017, ISSN : 2442-5826

- [10]. Chanchala Joshi, “Security Testing and Assessment of Vulnerability Scanners in Quest of Current Information Security Landscape,” *International Journal of Computer Applications* (0975-8887) Volume 145 –No.2, July 2016