ISSN: 2808-7771 online

Prosiding Seminar Nasional Universitas Ma Chung
pp. 40-49, 2022

Analisis Resiko Celah Keamanan *Website* E-Commerce Berbasis *Content Management System* (CMS) Wordpress Menggunakan *Vulnerability Scanning* (Studi Kasus: beekella.com)

Putu Bayu Baskara*, I Made Widiartha, I Gede Santi Astawa

Program Studi Informatika, Universitas Udayana, Jl. Raya Kampus Unud, Jimbaran
Kuta Selatan, Badung, Bali, Indonesia 80361

Correspondence: Putu Bayu Baskara (bayu.baskara@student.unud.ac.id)

Received: *29 07 22* – Revised: *02 08 22* - Accepted: *04 08 22* - Published: *09 09 22*

Abstrak. Dengan adanya perkembangan teknologi didunia bisnis, saat ini *e-commerce* telah menjadi media dalam membantu pelaku bisnis menjalankan usahanya. Salah satunya adalah beekella.com yang merupakan *e-commerce* berbasis *website* yang menyediakan produk-produk bebahan *natural*. Dengan adanya e-commerce webiste proses promosi dan penjualan dapat menjadi lebih praktis. Website *e-commerce* ini dibuat dengan memanfaatkan Content Management System (CMS) Wordpress yang memudahkan dalam mengelola serta memfasilitasi pembuatan, pembaharuan, dan publikasi konten. Namun dibalik kemudahannya, tidak bisa dipungkiri bahwa cara ini juga memiliki celah keamanan (*vulnerabilities*) yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Sehingga perlu adanya analisis kerentanan keamanan dengan metode *vulnerability scanning* yang dalam penelitian ini terdiri dari tahapan ruang lingkup (*scope*), *vulnerability scanning*, *vulnerability analysis*, dan *reporting*. Analisis akan dilakukan dengan menggunakan *tool* Acunetix *Web Vulnerability Scanner*. Hasil *vulnerability scanning* dan *vulnerability analysis* menggunakan *tool* Acunetix *Web Vulnerability Scanner* menunjukkan bahwa *website e-commerce* beekella.com memiliki celah keamanan dengan *threat level* 3 yang memungkinkan adanya ekploitasi dan manipulasi pada *website* dan memiliki total 10 *vulnerability type* yang mana terdiri dari 1 *type risk severity high*, 4 *type dengan risk severity medium*, dan 5 *type dengan risk severity low*. Kerentanan yang berhasil terdeteksi memerlukan perhatian khusus, baik yang dengan status risk severity high, medium, maupun low karena tidak menutup kemungkinan dapat dimanfaatkan sebagai media untuk melakukan penyerangan terhadap *website*. Hasil dari analisis ini bukan menggaransi sistem akan bebas dari resiko keamanan, tetapi untuk meminimalisir serangan yang dapat disalahgunakan dan menjadi bahan pertimbangan bagi *developer* untuk mengambil tindakan pencegahan dari serangan.

Kata kunci: *Vurnerability, Security, Content Management System, Wordpress, Acunetix Web Vulnerability Scanner*

Citation Format: Baskara, P.B., I Made Widhiarta & I Gede Santi Atawa. (2022). Analisis resiko celah keamanan website e-commerce berbasis content management system (CMS) Wordpress menggunakan vulnerability scanning (studi kasus: beekella.com). *Prosiding Seminar Nasional Universitas Ma Chung*, 40-49.

ISSN 2808-7771 online

PENDAHULUAN

Perkembangan teknologi membawa perubahan besar dalam dunia bisnis saat ini. Teknologi yang memungkinkan untuk melakukan kegiatan transaksi barang dan jasa tersebut dikenal dengan istilah e-*commerce*. *E-commerce* adalah teknologi *internet* yang berfokus pada kegiatan transaksi barang atau jasa secara jarak jauh tanpa harus bertemu secara langsung. Para pelaku bisnis menggunakan teknologi *e-commerce* karena teknologi ini telah meningkatkan reliabilitas pelaku bisnis dalam kegiatan transaksi, tidak hanya karena kemudahannya, tetapi juga karena teknologi *e-commerce* sudah mulai terjangkau oleh semua pengguna *internet* sehingga memungkinkan para pelaku bisnis untuk memperluas jaringan pemasarannya (Saputra et al., 2017).

Beekella.com adalah *e-commerce* berbasis website yang menyediakan produk-produk *natural* berbahan dasar propolis dan madu *Trigona* (*Stingless Bee*) yang disebut juga lebah klanceng/kelulut, serta *Virgin Coconut Oil* (VCO). Website ini menjadi sarana untuk mempromosikan produk-produk yang dijual, karena memiliki jangkauan ke semua orang yang rata-rata saat ini merupakan pengguna aktif internet. Selain itu konsumen dapat melihat produk yang diinginkan tanpa harus bertatap muka dan proses jual beli menjadi lebih praktis. Website *e-commerce* ini dikembangkan dengan memanfaatkan *Content Management System* (CMS) Wordpress, yang memudahkan dalam mengelola serta memfasilitasi pembuatan, pembaharuan, dan publikasi konten (Risnaputra & Triyono, 2020). Namun, dibalik kemudahannya tidak bisa dipungkiri bahwa terdapat ancaman terkait dengan celah keamanan (*vulnerability*) pada *website e-commerce* berbasis *Content Management System* (CMS) Wordpress ini. Adanya celah keamanan ini, tentunya memerlukan perhatian serius agar tidak dieksploitasi oleh pihak yang tidak bertanggung jawab hingga menimbulkan kerugian (Andria, 2020).

Berdasarkan paparan diatas, perlu dilakukannya analisis resiko celah keamanan *Website e-commerce beekella.com* menggunakan metode *vulnerability scanning*. Proses *scanning* ini akan dilakukan dengan *software* Acunetix Web Vulnerability Scanner yang kemudian dianalisis, hasil dari analisis ini nantinya bukan untuk menggaransi sistem akan bebas dari resiko keamanan, tetapi untuk meminimalisir serangan yang dapat disalahgunakan dan menjadi bahan pertimbangan bagi *developer* untuk mengambil tindakan pencegahan dari serangan (Zirwan, 2022).

LANDASAN TEORI

Berikut adalah beberapa landasan teori mengenai beberapa vulnerability type yang biasanya berhasil dideteksi menggunakan *tool* Acunetix Web *Vulnerability Scanner:*

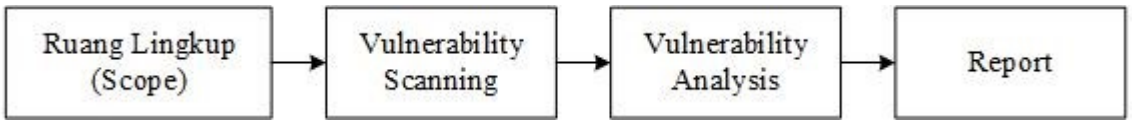
1. ***Session fixation*** adalah serangan yang memungkinkan penyerang untuk membajak sesi pengguna yang valid. Serangan tersebut mengeksplorasi batasan dalam cara aplikasi web mengelola ID sesi, lebih khusus lagi aplikasi web yang rentan. Saat mengautentikasi pengguna, itu tidak menetapkan ID sesi baru, sehingga memungkinkan untuk menggunakan ID sesi yang ada. Serangan tersebut terdiri dari membujuk pengguna untuk mengautentikasi dirinya dengan ID sesi yang diketahui, dan kemudian membajak sesi yang divalidasi pengguna dengan mengetahui ID sesi yang digunakan. Penyerang harus memberikan ID sesi aplikasi Web yang sah dan mencoba membuat browser korban menggunakannya.
2. ***Application error message*** adalah kerentanan yang memungkinkan sebuah halaman berisi pesan kesalahan/peringatan yang dapat mengungkapkan informasi sensitif. Pesan juga dapat berisi lokasi file yang menghasilkan pengecualian yang tidak ditangani.
3. ***Error message on page*** adalah kerentanan pada halaman yang berisi pesan kesalahan/peringatan yang dapat mengungkapkan informasi sensitif. Pesan juga dapat berisi lokasi file yang menghasilkan pengecualian yang tidak ditangani.
4. ***HTML form without CSRF protection*** adalah jenis kerentatan yang memungkinkan eksploitasi berbahaya situs web di mana perintah tidak sah dikirimkan dari pengguna yang dipercaya situs web.
5. ***Same site scripting Seorang*** adalah kesalahan konfigurasi DNS umum yang dapat mengakibatkan masalah keamanan kecil dengan aplikasi web dan memungkinkan penyerang dapat membajak RFC2109 (HTTP State Management Mechanism).
6. ***Clickjacking: X-Frame-Options header missing*** adalah kerentanan dengan teknik berbahaya untuk menipu pengguna web agar mengklik sesuatu yang berbeda dari apa yang pengguna anggap sedang mereka klik, sehingga berpotensi mengungkapkan informasi rahasia atau mengambil kendali komputer mereka saat mengklik halaman web yang tampaknya tidak berbahaya.
7. ***Cookie without HttpOnly flag set*** adalah kerentanan yang memungkinkan menginstruksikan browser bahwa cookie dapat diakses oleh script sisi klien.

ISSN 2808-7771 online

8. ***Cookie without secure flag set*** adalah kerentanan yang memungkinkan menginstruksikan browser bahwa cookie dapat diakses oleh saluran SSL yang tidak aman.
9. ***Possible virtual host found*** adalah metode untuk menghosting beberapa nama domain (dengan penanganan terpisah untuk setiap nama) pada satu server (atau kumpulan server). Hal ini memungkinkan satu server untuk berbagi sumber dayanya, seperti siklus memori dan prosesor, tanpa mengharuskan semua layanan yang disediakan untuk menggunakan nama host yang sama.
10. ***Wordpress admin accessible without HTTP authentication*** adalah kerentanan yang memungkinkan akses ke dasbord administrasi.

METODE PELAKSANAAN

Pada penelitian ini, analisis resiko celah keamanan akan dilakukan dengan menggunakan *vulnerability scanning*. Adapun objek pada penelitian ini adalah *Website E-Commerce* beekella.com. Tahapan yang akan dilakukan pada penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Metode *Vulnerability Scanning*.

1. Ruang Lingkup (*Scope*): pada tahapan ini akan ditentukan batasan-batasan (*scope*) terhadap target yaitu *Website e-commerce beekella.com* yang akan dianalisis *vulnerability* nya.
2. *Vulnerability Scanning*: pada tahapan ini akan dilakukan proses *scanning vulnerability* terhadap target. Proses *scanning* pada penelitian ini akan menggunakan *tool* Acunetix Web *Vulnerability Scanner* yang merupakan salah satu *tool* populer untuk analisis *vulnerability*.
3. *Vulnerability Analysis*: pada tahapan ini informasi-informasi dari hasil proses *vulnerability scanning* menggunakan *tool* scanner akan analisis, sehingga dapat diperoleh apa saja yang menjadi *vulnerability* dari target serta cara untuk memperbaiki atau mengatasinya. Analisis ini akan dilakukan secara otomatis pada Acunetix Web Vulnerability Scanner saat proses *scanning* telah selesai.

4. *Reporting*: pada tahapan ini hasil *vulnerability analysis* akan didokumentasikan agar dapat menjadi sumber referensi dan bahan pertimbangan bagi *developer* target kedepannya (Alwi et al., 2020).

HASIL DAN PEMBAHASAN

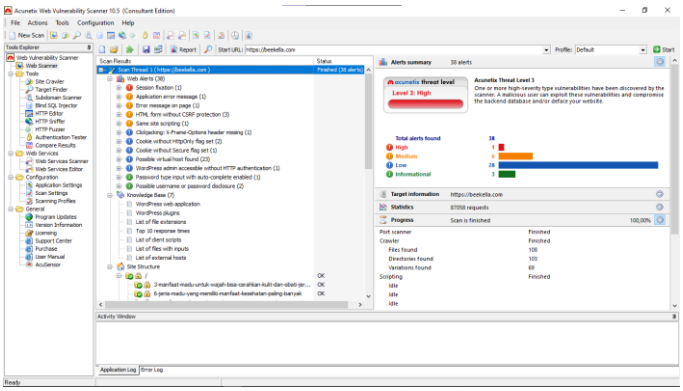
Hasil dari penelitian ini terdiri dari hasil proses ruang lingkup (*scope*) yang berisi batasan apa saja yang akan dilakukan pada penelitian, *vulnerability scanning* dengan menggunakan tool Acunetix *Web Vulnerability Scanner* yang berisi hasil *scanning* berupa tingkatan kerentanan (*threat level*), *vulnerability analysis* yang berisi hasil analisa jenis kerentanan, dampak serta solusi yang direkomendasikan.

Ruang Lingkup (*Scope*)

Pada penelitian ini, analisis akan dilakukan berdasarkan pengujian secara *passive attack* terhadap target yaitu *Website E-Commerce* beekella.com, tanpa melakukan eksploitasi terhadap target seperti melakukan DDOS, merubah tampilan, dan lain-lain. Pengujian ini akan menggunakan bantuan tool untuk melakukan scanning vulnerability pada website.

Vulnerability Scanning

Berikut adalah hasil dari proses vulnerability scanning dengan menggunakan tool Acunetix Web Vulnerability Scanner. Proses scanning dilakukan dengan menginputkan URL dari *Website E-Commerce* beekella.com, kemudian tool akan melakukan scanning secara otomatis terhadap target tersebut. Setelah proses scanning selesai akan ditampilkan informasi berupa threat level (tingkatan ancaman) serta alerts (peringatan) yang berhasil teridentifikasi. Hasil vulnerability scanning pada *Webesite E-Commerce* beekella.com dapat dilihat pada Gambar 2.



Gambar 2. Hasil Vulnerability Scanning menggunakan Acunetix WVS.

ISSN 2808-7771 online

Pada Gambar 2, dapat dilihat hasil proses vulnerability scanning menunjukkan adanya celah keamanan pada *Website e-commerce beekella.com* dengan *threat level* 3: High yang berpotensi timbulnya ekploitasi serta manipulasi pada sistem. Proses *scanning* ini dilakukan selama 2 jam 6 menit yang berhasil mengidentifikasi sejumlah alerts (peringatan) yang memiliki beberapa risk severity yaitu, *high*, *medium*, *low* yang dapat dilihat pada Tabel 1.

Tabel 1. Hasil *Vulnerability Scanning Website E-Commerce* beekella.com

No	Vulnerability Type	Risk Severity		
		High	Medium	Low
1	*Session fixation*	1		
2	*Application error message*		1	
3	*Error message on page*		1	
4	*HTML form without CSRF protection*		3	
5	*Same site scripting*		1	
6	*Clickjacking: X-Frame-Options header missing*			1
7	*Cookie without HttpOnly flag set*			2
8	*Cookie without secure flag set*			1
9	*Possible virtual host found*			23
10	*Wordpress admin accessible without HTTP authentication*			1

Berdasarkan Tabel 1, dapat dilihat hasil *scanning Vulnerability Website e-commerce beekella.com* menunjukkan terdapat 10 *vulnerability type*. Setiap *vulnerability type* ini memiliki *risk severity* yang terdiri dari 1 *type risk severity high*, 4 *type* dengan *risk severity medium*, dan 5 *type* dengan *risk severity low*.

Vulnerability Analysis

Berikut adalah hasil analisis berdasarkan *vulnerability type* yang berhasil diidentifikasi pada proses *scanning* menggunakan Acunetix Web Vulnerability Scanner. Hasil analisis ini berupa dampak yang dapat ditimbulkan serta rekomendasi solusi yang dapat dilakukan untuk memperbaikinya setiap *vulnerability type*.

1. High Risk Severity

Berikut adalah dampak dan solusi dari *vulnerability type* dengan *risk severity high* yang berhasil di*scanning*:

No	Vulnerability Type	Analysis Result
1	*Session Fixation*	**Dampak**: seorang penyerang dapat memfiksasi (mengatur) pengidentifikasi sesi korban (membajak session valid) untuk dapat masuk ke website.
		Solusi: aplikasi web harus mengabaikan ID sesi apa pun yang disediakan oleh browser pengguna saat login dan harus selalu menghasilkan sesi baru yang akan digunakan pengguna untuk login jika berhasil diautentikasi.

2. Medium Risk Severity

Berikut adalah dampak dan solusi dari *vulnerability type* dengan *risk severity medium* yang berhasil di*scanning*:

No	Vulnerability Type	Analysis Result
1	*Application Error Message*	**Dampak:** pesan kesalahan dapat mengungkapkan informasi sensitif. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut.
		Solusi: mereview kembali *source code* pada *website* dan memperbaiki *error* yang terjadi.
2	*Error message on page*	**Dampak:** pesan kesalahan dapat mengungkapkan informasi sensitif. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut.
		Solusi: mereview kembali source code pada website dan memperbaiki error yang terjadi.
3	*HTML form without CSRF protection*	**Dampak:** penyerang dapat memaksa pengguna aplikasi web untuk melakukan tindakan yang dipilih penyerang. Eksploitasi CSRF yang berhasil dapat membahayakan data dan operasi pengguna akhir dalam kasus pengguna normal. Jika pengguna akhir yang ditargetkan adalah akun administrator, ini

ISSN 2808-7771 online

		dapat membahayakan seluruh aplikasi web.
		Solusi: periksa apakah formulir ini memerlukan perlindungan CSRF dan terapkan tindakan penanggulangan CSRF jika perlu.
4	*Same site scripting*	**Dampak:** seorang penyerang dapat membajak RFC2109 (HTTP State Management Mechanism).
		Solusi: disarankan bahwa entri localhost non-FQ dihapus dari konfigurasi server nama untuk domain yang menghosting situs web yang mengandalkan manajemen status HTTP.

3. Low Risk Severity

Berikut adalah dampak dan solusi dari *vulnerability type* dengan *risk severity low* yang berhasil di*scanning*:

No	Vulnerability Type	Analysis Result
1	*Clickjacking: X-Frame-Options header missing*	**Dampak:** dampaknya tergantung pada aplikasi web yang terpengaruh seperti menipu pengguna web agar mengklik sesuatu yang berbeda dari apa yang pengguna anggap sedang mereka klik, sehingga berpotensi mengungkapkan informasi rahasia atau mengambil kendali komputer mereka saat mengklik halaman web yang tampaknya tidak berbahaya.
		Solusi: konfigurasikan server web untuk menyertakan header X-Frame-Options.
2	*Cookie without HttpOnly flag set*	**Dampak:** akses cookie oleh script sisi klien melalui instruksi browser.
		Solusi: menyetel flag HTTPOnly untuk cookie ini.
3	*Cookie without secure flag set*	**Dampak**: akses cookie oleh saluran SSL yang tidak aman melalui instruksi browser.

		Solusi: menyetel flag HTTPOnly untuk cookie ini.
4	*Possible virtual host found*	**Dampak:** direktori dapat mengekspos informasi sensitif yang dapat membantu pengguna jahat untuk mempersiapkan serangan lebih lanjut.
		Solusi: konsultasikan konfigurasi host virtual dan periksa apakah host virtual ini harus dapat diakses publik.
5	*Wordpress admin accessible without HTTP authentication*	**Dampak:** pengungkapan informasi dan akses masuk pada dashbord admin wordpress
		Solusi: membatasi akses ke dasbor administrasi WordPress menggunakan otentikasi HTTP. Kata sandi yang melindungi dasbor admin WordPress melalui lapisan otentikasi HTTP adalah langkah efektif untuk menggagalkan penyerang yang mencoba menebak kata sandi pengguna. Selain itu, jika penyerang berhasil mencuri kata sandi pengguna, maka harus melewati otentikasi HTTP untuk mendapatkan akses ke formulir login WordPress.

KESIMPULAN

Berdasarkan hasil dan pembahasan yang telah diuraikan sebelumnya maka dapat disimpulkan:

1. Hasil *vulnerability scanning* dan *vulnerability analysis* menggunakan tool Acunetix Web Vulnerability Scanner menunjukkan bahwa *website e-commerce beekella.com* memiliki celah keamanan dengan *threat level* 3 yang memungkinkan adanya ekploitasi dan manipulasi pada website dan memiliki total 10 *vulnerability type* yang mana terdiri dari 1 *type risk severity high*, 4 *type* dengan *risk severity medium*, dan 5 *type* dengan *risk severity low.*
2. Kerentanan pada situs *website e-commerce beekella.com* memerlukan perhatian khusus, baik yang dengan status *risk severity high*, *medium* maupun *low* karena tidak

ISSN 2808-7771 online

menutup kemungkinan dapat dimanfaatkan sebagai media untuk melakukan penyerangan terhadap *website*.

DAFTAR PUSTAKA

Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning. *INFORMAL: Informatics Journal*, *5*(2), 43. https://doi.org/10.19184/isj.v5i2.18941

Andria. (2020). Analisis celah keamanan website menggunakan tools WEBPWN3R di Kali Linux. *Generation Journal*, *4*(2), 69–76.

Risnaputra, I., & Triyono, G. (2020). Implementasi cms wordpress pada e-commerce untuk pelayanan katering CV. Alam Jaya. *IDEALIS : InDonEsiA JournaL Information System*, *3*(1), 481–485. https://doi.org/10.36080/idealis.v3i1.2151

Saputra, I. G. N. I., Sasmita, G. M. A., & Wiranatha, A. A. K. A. C. (2017). Pengembangan sistem keamanan untuk e-commerce. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *5*(1), 17. https://doi.org/10.24843/jim.2017.v05.i01.p03

Zirwan, A. (2022). Pengujian dan analisis kemanan website menggunakan acunetix vulnerability scanner. *Jurnal Informasi Dan Teknologi*, *4*(1), 70–75. https://doi.org/10.37034/jidt.v4i1.190

© 2022 by authors. Content on this article is licensed under a Creative Commons Attribution 4.0 International license. (http://creativecommons.org/licenses/by/4.0/).