5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 – ISSN 2962-8628 (*online*)

ANALISIS *VULNERABILITY* DAN *RISK ASSESMENT* TERHADAP *WEBSITE* PT. DAPUR COKELAT INDONESIA MENGGUNAKAN METODE *PENETRATION TESTING*

Fazrin Tri Wahyuni[1], Gunawan Pria Utama[2], Imelda Imelda[3], Painem Painem[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]2011510795@student.budiluhur.ac.id, [2]gunawan.priautama@budiluhur.ac.id, [3]imelda@budiluhur.ac.id, [4]painem@budiluhur.ac.id
(*: corresponding author)

Abstrak - Adanya keamanan jaringan bertujuan untuk melindungi sistem jaringan dari ancaman dan serangan yang dapat menyebabkan kerugian kecil maupun besar bagi perusahaan. Berdasarkan riset dan penelitian ini, PT. Dapur Cokelat Indonesia masih belum bisa maksimal dalam melakukan identifikasi atau mendeteksi celah kerentanan atau serangan yang ada pada *website* mereka. Lalu ada pun timbul keresahan yaitu adanya laporan pengaduan yang sering terjadi terkait gangguan sistem pada *website* mereka. Dengan masalah tersebut maka dari itu salah satu pencegahan yang dapat diterapkan dalam penelitian ini ialah dengan menganalisis atau meguji suatu kerentanan *(Vulnerability)* dengan metode pengujian penetrasi *(penetration testing)* dan mengidentifikasi risiko *(Risk Assesment)* pada *website* mereka sedini mungkin sehingga dapat dilakukan mitigasi risiko atau pencegahan risiko. Analisis ini menggunakan teknik wawancara (*Interview*), *Observation*, *information gathering*, dan metode *assessment* risiko. Tujuan Penelitian ini adalah sebagai identifikasi risiko dalam melakukan sistem *controlling* dari proses berjalannya suatu sistem. Melalui analisis dan pengujian penetrasi ini hasil yang diperoleh ialah ditemukan beberapa celah keretanan *(vulnerability)* pada *website* PT. Dapur Cokelat Indonesia dengan impact yang ditimbulkan tidak berpengaruh kepada jalannya operasional dan impact dapat diterima *(accept)*. Kontribusi dan Solusi yang dapat diterapkan yaitu dengan membuat suatu aplikasi yang dapat membantu menganalisis celah kerentanan *(Vulnerability)* serta dapat mengindentifikasi risiko dengan melakukan mitigasi risiko *(Risk Assessment)* pada *website* dengan maksud dan tujuan supaya dapat meningkatkan tingkat kontrol keamanan pada *website* PT. Dapur Cokelat Indonesia.

Kata Kunci: *Vulnerability, Risk Assesment, Pengujian Penetrasi*

VULNERABILITY ANALYSIS AND RISK ASSESMENT AGAINTS WEBSITE PT. DAPUR COKELAT INDONESIA USING PENETRATION TESTING METHODS

Abstract - *There is network security aimed at protecting network systems from threats and attacks that can cause small or large losses to the company. Based on this research and study, PT. Dapur Cokelat Indonesia is still not able to effectively identify or detect vulnerabilities or attacks present on their website. Then there arose a concern regarding frequent complaints related to system disturbances on their website. With that issue in mind, one of the preventive measures that can be applied in this research is to analyze or test a vulnerability using penetration testing methods and to identify risks in their website as early as possible, so that risk mitigation or prevention can be carried out. This analysis uses interview techniques, observation, information gathering, and Risk Assessment methods. The purpose of this research is to identify risks in implementing a controlling system for the operation of a system. Through this analysis and penetration testing, the results indicate that several vulnerabilities were found on the website of PT. Dapur Cokelat Indonesia, with the impact being significant on operational processes and deemed acceptable. The contributions and solution that can be implemented is to create an application that can help analyze vulnerabilities and identify risks by conducting risk assessments on the website, with the aim of enhancing the level of security control on the website of PT. Dapur Cokelat Indonesia.*

Keywords: *Vulnerability, Risk Assesment, Penetration testing*

1. PENDAHULUAN

Penerapan keamanan dalam menjaga suatu sistem informasi sangat diperlukan[1]. Oleh karena itu organisasi perlu melakukan asesmen pada aplikasi berbasis website agar oraganisasi mampu mendeteksi kerentanan dan memahami risiko yang dihadapi. Salah satu metode untuk penilaian tingkat risiko kerentanan keamanan aplikasi berbasis website adalah OWASP *Risk Rating Methodology*[3]. Dalam menerapkan suatu keamanan dalam sistem informasi, perusahaan atau organisasi perlu memperhatikan 3 aspek yaitu *Confidentiality* (kerahasiaan) yang merupakan kemampuan sistem menjaga kerahasiaan data dan informasi yang disimpan di dalamnya, *Integrity* (integritas) yang merupakan kemampuan sistem menjaga keutuhan dan keaslian data dan informasi, dan *Availability* (ketersediaan) yang merupakan kemampuan sistem selalu tersedia dan dapat diakses oleh pengguna terdaftar[8].

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya yang telah dikerjakan oleh Diah Priyawati, Siti Rokmah, dan Ihsan Cahyo Utomo dalam jurnal mereka yang berjudul "*Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP*" [7]. Perbedaan pertama yaitu jenis metode penetration testing yang dilakukan berbeda. Dalam jurnal melakukan penelitian dengan metode grey box, sedangkan peneliti menggunakan black box[4]. Perbedaan kedua yaitu tidak terdapat identifikasi port pada penelitian, sedangkan peneliti melakukan identifikasi port pada sebuah host menggunakan tool Parrot Linux dan NMAP[2]. Pengujian kerentanan situs web pada aplikasi web manajemen internet dari Kragan, Karanganyar, dapat digunakan oleh petugas IT sebagai referensi untuk meningkatkan keamanan aplikasi situs web, terutama mengenai hal-hal yang berkaitan dengan A01-Broken Access Control, A03-Injection, A05 Security Misconfiguration, dan A08 Software and Data Integrity Failures.

Seiring dengan perkembangan dan pertumbuhan teknologi yang semakin pesat dan kemudahan memanfaatkan Teknologi Informasi. Dalam hal ini 3 aspek tersebut diperlukan dalam identifikasi risiko keamanan terhadap *website* PT. Dapur Cokelat Indonesia menjadi kritikal dan krusial [10].

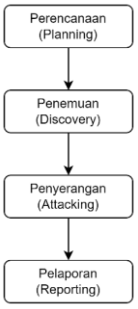
PT. Dapur Cokelat Indonesia dituntut untuk dapat terus bergerak maju, semua data dan informasi diharapkan selalu tersedia dan terjaga integritasnya setiap saat. Oleh karena itu PT. Dapur Cokelat Indonesia sebagai sektor bisnis di bidang makanan dan minuman diharapkan terus berinovasi dan mengikuti perkembangan Teknologi Informasi sehingga bisa menyediakan informasi terkait produk yang dijual secara terkini dan akurat kepada pelanggan.

Bermula dari keresahan beberapa pihak yang sering *complain* terhadap gangguan *website internal* maupun *external*, gangguan sistem dan lain sebagainya. Keresahan ini membuat pihak-pihak yang terkena dampak melakukan laporan gangguan pengaduan terhadap tim IT dengan berbagai macam gangguan masing-masing yang dihadapi. Oleh karena itu munculah solusi untuk mengatasi gangguan atau keresahan yang khususnya terkena dampak gangguan pada *website* dengan cara melakukan uji penetrasi. Peneliti memberikan usulan ini dengan latar belakang sebelumnya yaitu melakukan *explore open source* terkait uji penetrasi dan melakukan metode *interview user* dan observasi di tempat.

Uji penetrasi ini dilakukan dengan usulan yaitu menggunakan langkah sesuai dengan NIST SP 800-115[6]. Kontribusi dan hasil penelitian ini ialah dapat membantu menganalisis celah kerentanan (Vulnerability) serta dapat mengindentifikasi risiko dengan melakukan mitigasi risiko (*Risk Assessment*) pada website dengan maksud dan tujuan supaya dapat meningkatkan tingkat kontrol keamanan pada website PT. Dapur Cokelat Indonesia. Dengan kontribusi tersebut maka langkah-langkah tersebut dijalankan dengan baik agar mendapat hasil yang sesuai dan memiliki manfaat bagi tempat riset dan juga pembaca.

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah Metode *Penetration testing*. Sebuah dokumen yang dikeluarkan oleh National Institute of Standards and Technology (NIST), dokumen NIST SP 800-115, mencakup metode yang digunakan untuk melakukan *Penetration testing* dan Evaluasi Keamanan.



Gambar 1. *Diagram Alir Penetration testing* dengan Metode NIST SP 800-15

Gambar 1 merupakan diagram alir penetration testing dengan metode NIST SP 800-15. Berikut adalah langkah – langkah dari metode yang diterapkan menggunakan *penetration testing* berdasarkan implementasi metode *penetration testing NIST SP 800-15*:

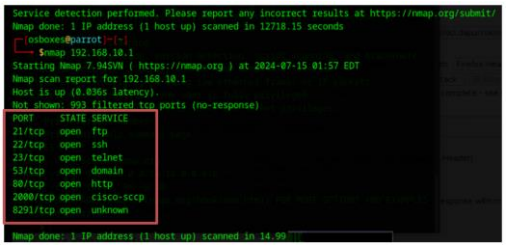
a. **Perencanaan *(Planning),*** pada tahap awal ini dilakukan proses perencanaan *(Planning)* dalam menentukan tujuan pengujian dan ruang lingkup pengujian serta kebutuhan dalam suatu pengujian.
b. **Penemuan *(Discovery)***, pada tahap ini merupakan bagian dari proses pengumpulan informasi *(information gathering)* atau pengumpulan data yang berkaitan dengan *website* target pengujian. Tujuan dari tahap ini adalah untuk mengumpulkan informasi yang relevan dari *website* target seperti port yang terbuka yang dilakukan dengan *tools NMAP*. Dan pada proses ini dilakukan juga proses pemindaian kerentanan terhadap *website* target dengan menggunakan *tools OWASP ZAP*[2].
c. **Penyerangan *(Attacking)***, pada tahap ini yang dilakukan ialah melakukan pengujian kerentanan *website* yang telah didapatkan melalui proses sebelumnya yang di awali dari pengumpulan data dan informasi dari *website target*. Dan selanjutnya pemindaian atau pengujian kerentanan ditindaklanjuti pada proses pengujian penyerangan.
d. **Pelaporan *(Reporting)***, pada tahap ini yang dilakukan ialah fokus pada pelaporan hasil pengujian kerentanan serta menyajikan daftar kerentanan dari *tools OWASP ZAP* yang kemudian diberikan keterangan atas hasil dan temuan dari pengujian yang telah dilakukan serta disajikan juga dalam bentuk *website penetration testing* yang berfungsi untuk menampilkan hasil temuan kerentanan *website target* yang dirancang oleh peneliti[4].

3. HASIL DAN PEMBAHASAN

Pada bagian ini menjelaskan tahapan dari metode *penetration testing*. Tahapan yang dilakukan ialah mulai dari *planning* hingga *reporting* dan dituangkan dalam tampilan layar aplikasi. Tahapan-tahapan tersebut dapat dijelaskan sebagai berikut:

3.1 Identifikasi Ancaman

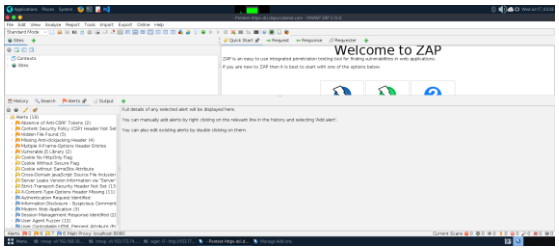
Dalam identifikasi ancaman ini diperlukan pemodelan ancaman yaitu proses yang dilakukan untuk mengoptimalkan keamanan. Hal ini dilakukan untuk mengidentifikasi kerentanan dan menentukan tindakan pencegahan, atau mengurangi dampak ancaman terhadap sistem. Yang dapat dilakukan pada tahap pertama ialah melakukan *port scanning* dengan *NMAP* pada *website target* seperti pada gambar 2.



Gambar 2. *Port Scanning* dengan *NMAP*

3.2 Identifikasi Celah Kerentanan *(Vulnerability)*

Dalam tahapan ini digunakan *framework* Bernama *OWASP ZAP* untuk melihat kerentanan apa saja yang ada pada *website* milik PT. Dapur Cokelat Indonesia. Identifikasi ini dilakukan pada *Parrot OS* yang merupakan *Linux Based* dengan sistem operasi *Debian – 12x 64bit*. Pada gambar 3 dapat dilihat proses *vulnerability scan* dengan OWASP ZAP.



Gambar 3. *Vulnerability Scan* dengan *OWASP ZAP* pada url dci.dapurcokelat.com

Adapun 19 rincian *vulnerability scan* menggunakan *OWASP ZAP* pada *website* target dapat dilihat pada tabel 1.

Tabel 1. Hasil *vulnerability Scan* menggunakan *OWASP ZAP*

Domain	*Alerts*	*Risk*	*Confidence*
https://dci.dapurcokelat.com/	***Absence of Anti-CSRF Tokens***	*Medium*	*Low*
	Content Security Policy (CSP) Header Not Set	*Medium*	*High*
	Hidden File Found	*Medium*	*Low*
	Missing Anti-clickjacking Header	*Medium*	*Medium*
	Multiple X-Frame-Options Header Entries	*Medium*	*Medium*
	Vulnerable JS Library	*Medium*	*Medium*
	Cookie No HttpOnly Flag	*Low*	*Medium*
	Cookie Without Secure Flag	*Low*	*Medium*
	Cookie without SameSite Attribute	*Low*	*Medium*
	Cross-Domain JavaScript Source File Inclusion	*Low*	*Medium*
	Server Leaks Version Information via "Server" HTTP Response Header Field	*Low*	*High*
	Strict-Transport-Security Header Not Set	*Low*	*High*
	X-Content-Type-Options Header Missing	*Low*	*Medium*
	Authentication Request Identified	*Informational*	*High*
	Information Disclosure - Suspicious Comments	*Informational*	*Medium*
	Modern Web Application	*Informational*	*Medium*
	Session Management Response Identified	*Informational*	*Medium*
	User Agent Fuzzer	*Informational*	*Medium*
	User Controllable HTML Element Attribute (Potential XSS)	*Informational*	*Low*

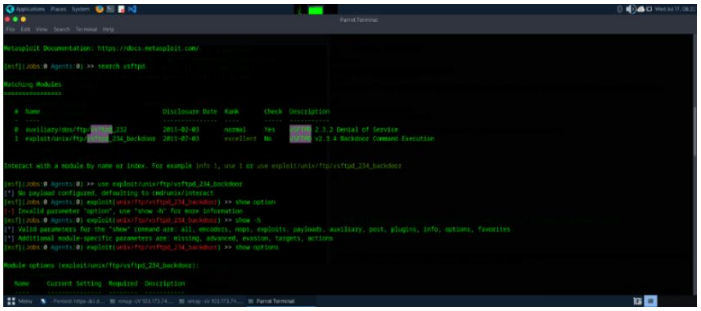
Tabel 2 merupakan tabel analisis dari hasil uji kerentanan (Vulnerability) dengan menggunakan *OWASP ZAP*.

Tabel 2. Hasil analisis hasil uji kerentanan *(Vulnerability)*

Risk	*Confidence*	*Analisis*	*Action*
Medium	*High*	Tingkat Risiko : Sedang Tingkat Kenyamanan Performa : Tinggi	*Mitigate/ Control*, melakukan perubahan/penggantian terhadap bagian kerentanan
Medium	*Low*	Tingkat Risiko : Sedang Tingkat Kenyamanan Performa : Rendah	Diterima*(Accept)*, melakukan pengecekan perubahan/ perbaikan penyimpanan data
Low	*High*	Tingkat Risiko : Rendah Tingkat Kenyamanan Performa : Tinggi	*Mitigate/ Control*, melakukan perubahan/penggantian terhadap bagian kerentanan
Low	*Medium*	Tingkat Risiko : Rendah Tingkat Kenyamanan Performa : Sedang	Diterima*(Accept)*, melakukan pengecekan perubahan/ perbaikan penyimpanan data
Informational	*High*	Tingkat Risiko : - (Sebagai Informasi) Tingkat Kenyamanan Performa : Tinggi	Diterima*(Accept)*, memberikan informasi pada *web* dan tidak diperlukan perbaikan
Informational	*Medium*	Tingkat Risiko : - (Sebagai Informasi) Tingkat Kenyamanan Performa : Sedang	Diterima*(Accept)*, memberikan informasi pada *web* dan tidak diperlukan perbaikan
Informational	*Low*	Tingkat Risiko : - (Sebagai Informasi) Tingkat Kenyamanan Performa : Rendah	Diterima*(Accept)*, memberikan informasi pada *web* dan tidak diperlukan perbaikan

3.3 *Gain Access/ Exploitation*

Setelah dilakukan analisis *vulnerability* yang dilakukan ialah tahapan *exploit* menggunakan *Metasploit* kepada salah satu *port* terbuka seperti pada gambar 3.



Gambar 3. Proses *exploit* dengan *Metasploit*

3.4 *Reporting*

Tahapan ini merupakan proses dokumentasi terkait deskripsi dari analasis kerentanan *(vulnerability) assessment*, *impact* dan juga rekomendasi perbaikan yang dapat dilakukan oleh perusahaan. *Report* ini dibuat berdasarkan *tools OWASP ZAP* dimana terdapat 13 *alert* yang ditemukan (tidak termasuk kategori *risk informational*).

3.5 Identifikasi Asesmen Risiko

Pada tahap ini dilakukan identifikasi risiko-risiko dari setiap domain yang telah diidentifikasi sebelumnya. Identifikasi risiko ini dilakukan dengan cara menerima informasi pengaduan gangguan layanan atau teknis dari setiap domain yang ada. Tujuan tahapan ini dilakukan untuk menginventaris seluruh risiko keamanan.

3.6 Hasil Penilaian Risiko

Berdasarkan analisis terhadap kerentanan *(vulnerability)* dan asesmen risiko yang telah teridentifikasi dan telah diberikan nilai kemungkinan dan dampak, diketahui jumlah *level* risiko terhadap seluruh domain dengan rincian yang dapat dilihat pada tabel 3.

Tabel 3. Hasil penilaian risiko

Domain	Very High	High	Medium	Low	Total
www.dapurcokelat.com	-	1	2	-	3
https://dci.dapurcokelat.com/	-	3	6	7	16
https://delivery.dapurcokelat.com/	-	-	4	3	7
https://shop.dapurcokelat.com/	-	-	1	1	2
Total	0	4	13	11	28
Persentase	0%	14.4%	46 %	39.6%	100%

3.7 Mitigasi Risiko

Setiap risiko yang diidentifikasi yang selanjutnya dilakukan langkah tanggapannya. Tahap pertama dalam melakukan proses ini ialah pemilihan kendali dan strategi mitigasi. Terdapat beberapa pilihan strategi mitigasi yaitu *Avoid, Accept, Mitigate/Control* dan *Transfer.*

3.8 Hasil Uji Coba

Tabel 4 merupakan tabel hasil uji coba pada web penetration testing yang telah dibuat menggunakan metode *penetration testing.*

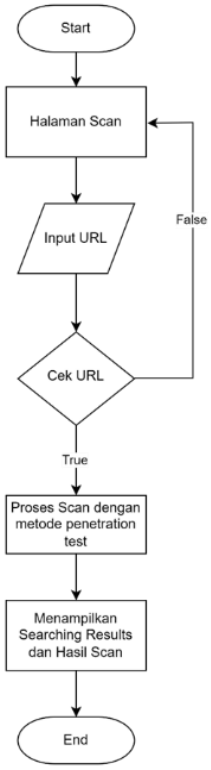
Tabel 4. Hasil uji coba terhadap *website penetration testing*

Kasus dan Hasil Uji Coba (Data Normal)			
Data Masukan	**Diharapkan**	**Pengamatan**	**Kesimpulan**
Input url: http://dapurcokelat.com/	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	[√]Diterima [ ] Ditolak
Input url: http://dci.dapurcokelat.com/	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	[√]Diterima [ ] Ditolak
Input url: http://delivery.dapurcokelat.com/	Menampilkan *searching result* berupa temuan ancaman dari *web*	Menampilkan berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak	[√]Diterima [ ] Ditolak

	(bertanda silang merah) atau tidak (bertanda ceklis hijau)	(bertanda ceklis hijau)	
Input url: http://shop.dapurcokelat.com/	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	Menampilkan *searching result* berupa temuan ancaman dari *web* (bertanda silang merah) atau tidak (bertanda ceklis hijau)	[√]Diterima [ ] Ditolak
Kasus dan Hasil Uji Coba (Data Salah)			
Data Masukan	**Diharapkan**	**Pengamatan**	**Kesimpulan**
Input url tidak sesuai format	Menampilkan pesan error dan tidak menampilkan hasil *searching result*	Menampilkan pesan error dan tidak menampilkan hasil *searching result*	[√]Diterima [ ] Ditolak

3.9 Flowchart

Flowchart halaman *scan* berfungsi melakukan *scanning website target* yang disajikan di dalam *website aplikasi penetration testing*. *Flowchart* tersebut dapat dilihat pada gambar 4.



Gambar 4. *Flowchart scanning* pada web *penetration testing*

3.10 Algoritma

Penjelasan algoritma yang diterapkan menggunakan metode *penetration testing* pada *website penetration testing* dideskripsikan pada algoritma 1.

Algoritma 1. *Scan* dengan metode *Penetration testing*

Start
Tampilkan Halaman *scan*
Masukkan *url*
    if pilih tombol *scan*
        Proses *Scan* dengan metode *penetration test*
    Tampilkan *Searching Results* dan Hasil *Scan*
    else kembali kelangkah 2
End

3.11 Tampilan Layar Aplikasi

Tampilan layar aplikasi merupakan tahapan penerapan dari hasil perancangan yang telah dibuat sebelumnya. Tampilan layar aplikasi bertujuan untuk menghasilkan sebuah *website penetration testing* yang sesuai dengan kebutuhan.

a. Tampilan Halaman Home

Tampilan home memberikan informasi tentang *penetration testing* dan maafaat dari metode yang diterapkan. Tampilan tersebut dapat dilihat pada gambar 5.

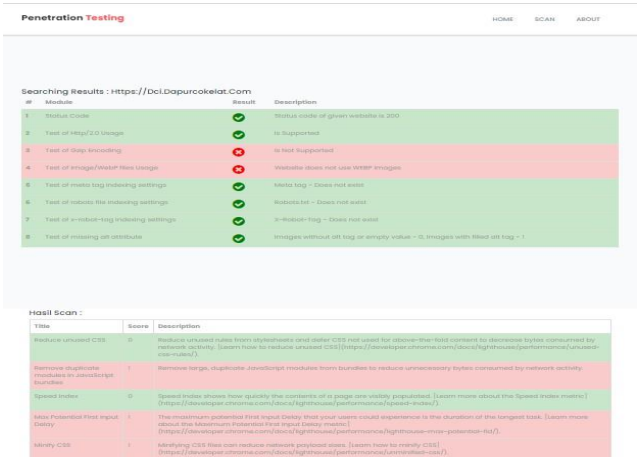
Gambar 5. Tampilan halaman *home*

b. Tampilan Halaman *Scan*

Tampilan *scan* merupakan tampilan *user* untuk melakukan pemindaian *(scanning) website* target dengan melakukan *input url website* yang di targetkan oleh pengguna. Berikut ini merupakan tampilan *scan* yang dapat dilihat pada gambar 6.

Gambar 6. Tampilan halaman *Scan*

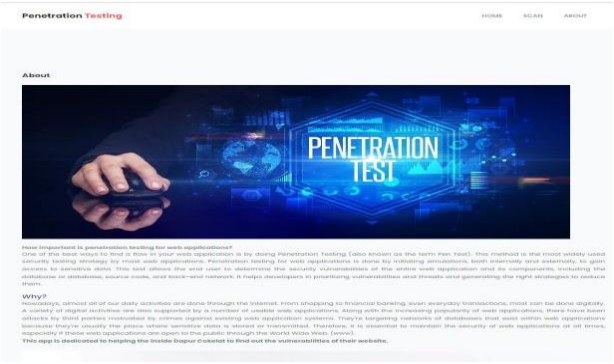
Setelah *user* melakukan input *url* yang ditargetkan, *website penetration testing* menampilkan *searching results* dan hasil *scan* dapat dilihat pada gambar 7.



Gambar 7. Tampilan *searching result* dan hasil *scan*

c. Tampilan Halaman *About*

Tampilan about merupakan tampilan pengguna untuk melihat informasi tentang meningkatkan keamanan terhadap *website* pada PT. Dapur Cokelat Indonesia. Tampilan tersebut dapat dilihat pada gambar 8.



Gambar 8. Tampilan halaman *about*

3.12 Analisa Hasil Penelitian

Dalam penelitian ini, telah dilakukan analisis kerentanan dan asesment risiko pada *website* milik PT.Dapur Cokelat. Maka dari itu kesimpulan yang dapat diambil ialah analisis kerentanan dan scanning menggunakan OWASP ZAP bisa di klasifikasikan terdapat 48 celah kerentanan yang ada pada 4 domain website milik PT. Dapur Cokelat Indonesia. Risiko yang di dapat ialah 3 risiko pada domain: *www.dapurcokelat.com*, 16 risiko pada domain *https://dci.dapurcokelat.com*, 7 risiko pada domain *https://delivery.dapurcokelat.com*, dan 2 risiko pada domain *https://shop.dapurcokelat.com*.

4. KESIMPULAN

Hasil analisis dapat memberikan informasi kepada manajemen PT. Dapur Cokelat untuk menganalisis celah kerentanan pada *website* mereka. Dengan memahami ancaman atau celah keamanan yang ditemukan diharapkan dapat meningkatkan tingkat keamanan (Integritas) dari sisi TI pada perusahaan. Oleh karena itu mengingat masih terdapat kekurangan pada penelitian ini, diharapkan bisa dilakukan untuk mencapai hasil yang lebih baik lagi kedepannya. Saran yang bisa diberikan untuk meningkatkan performa aplikasi antara lain yaitu aplikasi dapat dikembangkan dengan penambahan fitur yang dapat menunjang bagi pengguna/*user*, aplikasi dapat dibuat secara public apabila memungkinkan dan tidak terpusat pada domain tertentu, dan perlu adanya pengembangan aplikasi lebih lanjut terkait integrasi data supaya hasil yang ditampilkan lebih akurat berdasarkan data yang digunakan, serta pengujian dapat juga dilakukan pada server dan hardware perusahaan untuk tahap selanjutnya.

UCAPAN TERIMA KASIH

Terima kasih kepada semua pihak PT. Dapur Cokelat Indonesia sebagai tempat usaha yang telah mempercayai dan memberikan kesempatan kepada peneliti untuk melakukan penelitian ini hingga terselesaikan dengan baik.

DAFTAR PUSTAKA

[1] Aryanti, Dewi. Nurholis. Utamajaya, Joy Nashar, Analisis Kerentanan Keamanan *Website* Menggunakan Metode OWASP (Open Web Application Security Project) Pada Dinas Tenaga Kerja, *"Jurnal Nasional Indonesia",* vol.1, no.3, 15-25, Mar. 2021.

[2] Fachri, Fahmi. Fadlil, Abdul. Riadi, Imam, Analisis Keamanan Webserver Menggunakan Penetration Test, *"Jurnal Informatika"*,vol.8, no.2, 183-190, sept 2021.

[3] Hasibuan, Abdul Fattah. Tommy. Handoko, Divi, Analisis Keretanan *Website* Dengan Aplikasi OWASP ZAP. *"Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI)"*, vol.2,no.2, 257-270, Mei. 2023.

[4] Linggih Jaelani,Widi. Yanto. Khoirunnisa, Fitri, *Penetration testing Website* Dengan Metode Black Box Testing Untuk Meningkatkan Keamanan *Website* Pada Instansi (Redacted). *"Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika"*,vol.05, no.1, 1-8, Juni. 2023.

[5] Maliq Ibrahim, Adha. Defisa, Tomi. Bayu Seta, Henki. Wayan Widi, I , Analisis Keamanan Sistem pada *Website* Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and *Penetration testing* (VAPT), *"Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)"*, vol.1, 312-325, April. 2022.

[6] Putra Armadhani, Ade. Nofriansyah, Dicky. Ibnutama, Khairi, Analisis Keamanan Untuk Mengetahui Vulnerability Pada DVWA Lab Testing Menggunakan *Penetration testing* Standart OWASP, *"Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)"* vol.21 , no.2, 80-88, Agust 2022.

[7] Priyawati, Diah. Rokhmah, Siti. Utomo, Ihsan Cahyo, *Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP*, *"International Journal of Computer and Information System (IJCIS)"*, vol.3, 2745-9659. Sept. 2022.

[8] Rozali, Mhd. Sinaga, Mikha Dayan), Diagnosis Keamanan Web Menggunakan Metode Uji Penetrasi *Website* Sekolah, *"Jurnal Info Digit"* , vol.2, no.1, 248-262, Jan 2024.

[9] Sebrina, Aida Fitriya. Junaidi, Achmad. Sihananto, Andreas Nugroho, Testing posketanmu *website* with google *penetration testing* and OWASP Top 10, *"Jurnal Mantik - Institute of Computer Science (IOCS)"*, vol.8, 636-645, Jan. 2024.

[10] Sofyan, Herry. Sugiarto, Meilan. Akbar, Bagus Muhammad, Implementation of *Penetration testing* on *Website*s to Improve Security of Information Assets UPN "Veteran" Yogyakarta, *"Jurnal Informatika dan Teknologi Informasi"*, vol.20, no.2, pp. 153-162, Jun 2023.

[11] Yamin, Noer, Reyhan, Todo. Suarjana, Dwi, I, Made, Agus, Pratama, Eka, I, Putu, Agus, *Penetration testing* on the SISAKTI *Application* at Udayana University Using the OWASP Testing Guide Version 4, *"Jurnal Ilmiah Merpati"*, vol.10, no.3, 157-166, Dec 2022.