ANALISIS KEAMANAN SISTEM INFORMASI WEBSITE PEKEN SURABAYA MENGGUNAKAN OWASP TOP 10

1st Atha Adiyatma
Department of Information System
Universitas Telkom
Surabaya,Indonesia
athaatha@student.telkomuniversity.ac.id

2nd Kharisma Monika Dian Pertiwi, S.Kom., M.Kom
Department of Information System
Universitas Telkom Surabaya,Indonesia
Kharismamonikadp@telkom.university.ac.id

3rd Muhammad Ilham Alhari, S.Kom., M.Kom
Department of Information System
Universitas Telkom
Surabaya,Indonesia
ilhamalhari@telkom.university.ac.id

***Abstrak* — Gerakan Digitalisasi membuat banyak organisasi membangun aplikasi sistem informasi dengan tujuan proses bisnis yang berjalan lebih efektif dan efisien. Salah satu sistem informasi adalah Peken Surabaya. Peken Surabaya adalah website yang digunakan Pegawai Pemerintah Kota Surabaya ataupun masyarakat umum untuk melakukan belanja berbagai macam kebutuhan sehari-hari pada Toko Kelontong, UMKM maupun SWK yang tersedia pada tiap Kecamatan di Kota Surabaya.. Sistem informasi Peken Surabaya memiliki banyak data penting dan sensitif yang harus dijaga. Keamanan sistem informasi sangat penting untuk menjamin integritas, kerahasiaan, dan ketersediaan data. Penelitian ini bertujuan untuk menganalisis celah keamanan sistem informasi Peken Surabaya menggunakan kerangka kerja (Open Worldwide Application Security Project) OWASP Top 10. Ada beberapa tahapan OWASP yang dilakukan diantaranya Information Gathering, Session Management Testing, Data Validation Testing, dan Webservices Testing. Uji penetrasi adalah salah satu cara untuk melihat tingkat keamanan sebuah sistem, pengujian dilakukan dengan membuat simulasi serangan terhadap aplikasi berbasis web yang akan diuji. Penelitian ini menghasilkan rekomendasi dan panduan yang bermanfaat bagi pihak terkait untuk meningkatkan keamanan sistem informasi. Dengan demikian, penelitian ini berkontribusi secara positif dalam membantu pihak terkait mencegah potensi ancaman keamanan informasi.**

***Kata kunci*— Keamanan Sistem Informasi, OWASP TOP 10, Penetration Testing.**

I. PENDAHULUAN

IMF menyatakan bahwa pandemi COVID-19 telah IMF menyatakan bahwa pandemi COVID-19 telah mempercepat digitalisasi di banyak industri, terutama di sektor ekonomi atau industri yang tertinggal (Almeida, Duarte Santos, and Augusto Monteiro 2020).Website adalah salah satu teknologi digital yang paling umum digunakan banyak perusahaan untuk memberikan informasi kepada masyarakat, klien, atau karyawan mereka (Awad et al. 2019). Dengan menggunakan platform berbasis web mobile ini, Pemerintah Kota (Pemkot) Surabaya berusaha meningkatkan perekonomian warganya, terutama bagi Masyarakat Berpenghasilan Rendah. Upaya ini dilakukan dengan mengoptimalkan penggunaan e-peken untuk meningkatkan volume transaksi perbelanjaan. Sebelumnya, layanan pelanggan e-peken hanya terbatas untuk Aparatur Sipil Negara (ASN) di lingkup Pemkot, namun sekarang telah diperluas untuk diakses oleh masyarakat umum(Anon n.d.).

Keuntungan menggunakan website sebagai aplikasi sistem informasi adalah kemudahan untuk akses dimanapun dan kapanpun. Tetapi melakukan proses digitalisasi juga memiliki tantangan yang tidak bisa diabaikan. Penelitian oleh Almeida (Almeida et al. 2020) berjudul "Tantangan dan Peluang Digitalisasi dalam Masa Setelah Pandemi" mengatakan bahwa *cybersecurity* serta privasi menjadi dua elemen kunci untuk mendukung integrasi teknologi. Meningkatnya aktivitas digital juga memicu peningkatan serangan siber, pada tahun 2022 kasus kebocoran data indonesia mengalami peningkatan. Menurut perusahaan keamanan siber *Surfshark*, pada kuartal tiga tahun 2022 Indonesia telah terjadi kebocoran data sebesar 13 Juta data (Surfshark 2023). Dari tahun 2021 sampai 2023 indonesia sering mengalami masalah dalam serangan siber terutama kasus kebocoran data, Pada tahun 2021 sebanyak 279 juta data penduduk indonesia peserta Badan Penyelenggara Jaminan Sosial Kesehatan atau BPJS bocor dan dijual pada sebuah forum jual beli data (CNN INDONESIA (PT Trans News Corpora) 2021).

Keamanan dalam sebuah aplikasi website juga tidak dapat diabaikan, salah satu contoh serangan yang sering diterima oleh website adalah *web defacement*. Serangan terhadap situs web yang bertujuan untuk merusak atau mengubah konten pada halaman situs web tersebut, dalam "Lanskap Keamanan Siber" Badan Sandi Siber Nasional (BSSN) web defacement selalu masuk ke dalam tiga teratas insiden dalam layanan BBSN, pada tahun 2021 terdapat 5940 kasus web *defacement* dan selama tahun 2022 terjadi 2348 kasus serangan *web defacement* (BSSN (Badan Siber dan

Sandi Negara) 2023), menurut BSSN selama tahun 2022 sektor paling banyak terkena serangan *web defacement* adalah sektor administrasi pemerintahan dengan jumlah kasus 885 kasus. Sepanjang tahun 2020 banyak kasus kebocoran data yang dialami perusahaan swasta seperti e-commerce, Kebocoran data ini terjadi mulai bulan Mei hingga November 2020. Data yang tersebar diantaranya seperti nama akun, alamat e-mail, tanggal lahir, nomor telepon, dan beberapa data pribadi lainnya yang tersimpan di database (Indiana Malia n.d.).

Untuk itu perlu dilakukan analisis keamanan untuk mengetahui apakah aplikasi yang dibangun mempunyai keamanan yang memenuhi standar. Pada penelitian ini akan dilakukan analisis keamanan berupa uji penetrasi terhadap aplikasi berbasis website Peken Surabaya (https://peken.surabaya.go.id/). Uji Penetrasi merupakan tindakan simulasi serangan langsung terhadap suatu aplikasi, yang bertujuan untuk mengidentifikasi kerentanan keamanan pada website dan memahami bagaimana sistem operasional dapat mengatasi serangan langsung. Metode OWASP (Open Web Application Security Project) Top 10 adalah salah satu cara untuk menguji sistem informasi berbasis web. Metode ini dirilis oleh komunitas OWASP dan mencakup sepuluh celah keamanan utama yang dapat mengancam keamanan situs web. Daftar ini terus berubah sesuai dengan kemajuan teknologi website(OWASP n.d.-e). Hasil dari uji penetrasi ini akan memberikan wawasan yang berharga untuk menganalisis kerentanan aplikasi website pada Peken Surabaya dan memberikan rekomendasi guna meningkatkan keamanan aplikasi perusahaan tersebut.

II. KAJIAN TEORI

A. Sistem Informasi

Sistem informasi adalah kumpulan komponen atau data yang terdiri dari beberapa subsistem yang saling berhubungan, bekerja sama, dan diorganisasikan dengan cara yang memungkinkan pengolahan komponen atau data tersebut menjadi informasi yang bermanfaat untuk mencapai tujuan tertentu (Hakim, Pratama, and Prihatini 2019)

B. Peken Surabaya

PEKEN Surabaya adalah website yang digunakan Pegawai Pemerintah Kota Surabaya ataupun masyarakat umum untuk melakukan belanja berbagai macam kebutuhan sehari-hari pada Toko Kelontong, UMKM maupun SWK yang tersedia pada tiap Kecamatan di Kota Surabaya (Peken Surabaya 2021). Peken mempunya beberapa fitur seperti Fitur Pencarian, Pencarian bisa berdasarkan nama produk atau pencarian berdasarkan nama toko kelontong. Filter berdasarkan Kecamatan, Adapun filter untuk membatasi pencarian berdasarkan kecamatan. Filter berdasarkan Kategori, Terdapat filter untuk membatasi pencarian berdasarkan kategori.

Ada beberapa kategori yang terdapat pada Peken yaitu Bapokting, Craft, Daging Segar Dingin, Fashion dan Food and Culinary. Filter berdasarkan Harga, Terdapat filter untuk membatasi pencarian berdasarkan harga. Masuk/ Login PEKEN Surabaya Untuk melakukan transaksi pada Peken, maka Langkah awal adalah melakukan login/ masuk pada website PEKEN Surabaya menggunakan username dan password masing-masing. Lihat Keranjang, Lihat keranjang apabila sudah selesai melakukan pencarian produk dan ingin melakukan melanjutkan pembelian pada produk tersebut.

C. Keamanan Sistem Informasi

Cybersecurity, juga dikenal sebagai keamanan siber, adalah proses melindungi sistem, jaringan, dan program dari serangan digital (Admin Fikes 2023). Serangan cybersecurity digital biasanya berfokus pada mengubah, mengakses, maupun menghancurkan informasi sensitif seperti mengambil atau memeras uang dari pengguna, dan mengganggu proses bisnis seseorang. Pada era modern, banyak aktivitas manusia bergantung pada teknologi. Oleh karena itu, cybersecurity sangat penting untuk membuat pengguna internet merasa nyaman menggunakan internet, seperti menjaga data pribadi mereka aman, berbelanja online, bertransaksi dengan aman, dan dapat bekerja dari jarak jauh. Oleh karena itu, organisasi dan perusahaan harus memastikan bahwa sistem mereka dilindungi dengan benar dan dapat menerapkan tindakan pencegahan yang tepat untuk mengurangi kemungkinan serangan siber.

D. Keamanan Siber

Serangan cyber adalah upaya mendapatkan akses tidak sah ke sistem komputer untuk mencuri, mengubah, atau menghancurkan data (Microsoft Security 2023). Serangan cyber bertujuan untuk merusak atau mendapatkan kontrol atau akses ke dokumen dan sistem penting dalam jaringan komputer bisnis atau pribadi. Serangan cyber didistribusikan oleh individu atau organisasi untuk tujuan politik, kriminal, atau pribadi guna menghancurkan atau mendapatkan akses ke informasi rahasia. Tahun 2021 dapat dibilang sebagai rekor terburuk dalam sejarah keamanan siber. Kehadiran pandemi COVID-19 nampaknya turut memicu pandemi siber dengan banyaknya kebocoran data, pencurian identitas, hingga serangan- serangan malware(Ary Adianto n.d.) .

E. Serangan Keamanan Siber

Serangan cyber adalah upaya mendapatkan akses tidak sah ke sistem komputer untuk mencuri, mengubah, atau menghancurkan data (Microsoft Security 2023). Serangan cyber bertujuan untuk merusak atau mendapatkan kontrol atau akses ke dokumen dan sistem penting dalam jaringan komputer bisnis atau pribadi. Serangan cyber didistribusikan oleh individu atau organisasi untuk tujuan politik, kriminal, atau pribadi guna menghancurkan atau mendapatkan akses ke informasi rahasia. Tahun 2021 dapat dibilang sebagai rekor terburuk dalam sejarah keamanan siber. Kehadiran pandemi COVID-19 nampaknya turut memicu pandemi siber dengan banyaknya kebocoran data, pencurian identitas, hingga serangan- serangan malware(Ary Adianto n.d.)

F. OWASP

Organisasi non-profit Open Worldwide Application Security Project (OWASP) berfokus pada peningkatan keamanan perangkat lunak (OWASP n.d.-a). OWASP adalah komunitas terbuka yang terdiri dari pengembang

perangkat lunak, ahli keamanan, dan peneliti dari berbagai industri yang berkomitmen untuk membantu organisasi mengembangkan dan mengoperasikan aplikasi yang dapat diandalkan. Semua proyek, alat, dan dokumen OWASP gratis dan dapat diakses oleh siapa saja yang tertarik untuk meningkatkan keamanan aplikasi. OWASP menawarkan sumber daya dan pelatihan untuk membantu pengembang dan profesional keamanan memahami teknik terbaik untuk mengamankan aplikasi web. Proyek OWASP lainnya termasuk daftar 10 risiko keamanan aplikasi web teratas (OWASP top 10), kerangka kerja pengujian keamanan aplikasi web (OWSP WSTG), dan alat pengujian keamanan aplikasi web (OWASP Zed Attack Proxy)

G. Information System Security Assessment Framework (ISSAF)

OWASP Top 10 adalah dokumen kesadaran standar Kerangka kerja *Information System Security Assessment Framework* (ISSAF) adalah kerangka kerja *penetration testing* yang dikembangkan oleh OISSG (*Open Information System Security Group*). *Information System Security Assessment Framework* (ISSAF) adalah kerangka kerja kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi ke dalam berbagai *domain* & merinci kriteria evaluasi atau pengujian khusus untuk masing-masing *domain*. ISSAF dapat digunakan untuk memenuhi persyaratan penilaian keamanan organisasi dan mungkin dapat digunakan sebagai referensi untuk memenuhi kebutuhan keamanan informasi lainnya. ISSAF mencakup aspek penting dari proses keamanan, penilaian dan penguatan untuk mendapatkan gambaran lengkap tentang kerentanan yang dapat terjadi pada sebuah sistem. Metodologi pengujian penetrasi ISSAF dikembangkan untuk mengevaluasi kontrol jaringan, sistem, dan aplikasi (Anon 2005).

H. Komparasi Framework Testing

Perbedaan utama antara OWASP dan ISSAF terletak pada fokusnya. OWASP lebih berfokus pada keamanan perangkat lunak aplikasi dan menyediakan berbagai tools serta forum secara gratis dan terbuka untuk siapa saja yang tertarik untuk memperbaiki keamanan aplikasi. Sementara ISSAF lebih berfokus pada penilaian keamanan sistem informasi dan menyediakan kerangka terstruktur untuk mengkategorikan penilaian keamanan sistem informasi kedalam berbagai domain dan rincian evaluasi yang spesifik. Dengan demikian, OWASP lebih berfokus pada aplikasi keamanan perangkat lunak, sementara ISSAF lebih berfokus pada penilaian keamanan sistem informasi secara menyeluruh. Peneliti menggunakan OWASP dikarenakan peneliti ingin menguji keamanan sistem informasi website PEKEN SURABAYA Dikarenakan lebih mendalam dan lebih uptodate.

I. OWASP TOP 10

OWASP Top 10 adalah dokumen kesadaran standar untuk pengembang dan keamanan aplikasi web. Dokumen ini mewakili konsensus yang luas tentang risiko keamanan yang paling kritis pada aplikasi web (OWASP n.d.-e). Perusahaan harus mengadopsi dokumen ini dan memulai proses untuk memastikan bahwa aplikasi web mereka meminimalkan risiko-risiko ini. Menggunakan OWASP Top 10 mungkin merupakan langkah pertama yang paling efektif untuk mengubah budaya pengembangan perangkat lunak dalam organisasi Anda menjadi budaya yang menghasilkan kode yang lebih aman.

J. Pengujian Black Box

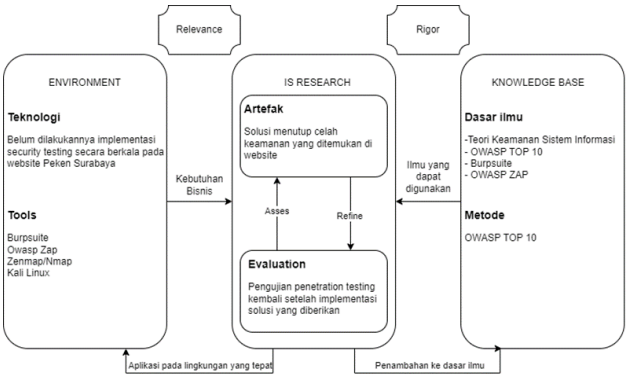
Pengujian kotak hitam melibatkan pengujian sistem tanpa pengetahuan sebelumnya tentang cara kerja internalnya. Penguji memberikan input, dan mengamati output yang dihasilkan oleh sistem yang diuji. Hal ini memungkinkan untuk mengidentifikasi bagaimana sistem merespons tindakan pengguna yang diharapkan dan tidak diharapkan, waktu respons, masalah kegunaan, dan masalah keandalan [36].

III. Metode Penelitian

3.1 Metode yang digunakan

Pada perancangan model pengukuran layanan teknologi informasi (TI), mengadaptasi dari metodologi yang digunakan oleh Hevner (#1 and Surendro 2015). Dapat diketahui pada **Error! Reference source not found.** bahwa terdapat tiga ruang lingkup yaitu lingkungan, penelitian dan dasar ilmu. Pada aspek lingkungan dipengaruhi oleh teknologi dan tools dimana hal tersebut mempengaruhi proses pada aplikasi web PekenSurabaya. Penelitian dilakukan untuk menganalisis keamanana sistem website berdasarkan ketentuan Owasp Top 10. Dasar ilmu yaitu berdasarkan teori KSI, OWASP TOP 10, Burpsuite, OWASP ZAP serta metode OWASP TOP 10.

Metode yang digunakan dalam penelitian ini adalah OWASP TOP 10. OWASP TOP 10 adalah metode yang dimiliki oleh Open Web Application Security Project (OWASP), sebuah organisasi yang berfokus pada meningkatkan keamanan perangkat lunak. Setiap tahun, OWASP merilis daftar sepuluh kerentanan ini untuk meningkatkan kesadaran akan risiko yang terkait dengan keamanan aplikasi web. OWASP TOP 10 yang dimana terdapat 10 kerentanan website.



Gambar 1. Model Konseptual Hevne

IV. HASIL DAN PEMBAHASAN

4.1 Information Gathering

Information gathering merupakan tahap awal yang dilakukan dalam proses Penetration Testing dalam penelitian ini. Tahap information gathering dilakukan menggunakan tool Nmap (Network Mapper). Nmap (Network Mapper) merupakan sebuah alat fungsional yang digunakan untuk memindai file jaringan untuk koneksi terbuka. Pada tahap ini bertujuan untuk mengidentifikasi aset yang berhubungan dengan website.

4.1.1 Identifikasi Target

Identifikasi target dalam cybersecurity merujuk pada proses mengidentifikasi sistem, jaringan, aplikasi, atau data yang mungkin menjadi sasaran serangan siber. Proses identifikasi target ini penting untuk membangun strategi pertahanan yang efektif dan untuk menentukan prioritas dalam upaya perlindungan keamanan siber. Dengan memahami aset mana yang paling rentan dan paling bernilai, organisasi dapat mengalokasikan sumber daya dan tindakan keamanan dengan lebih tepat.

```
Sponsoring Registrar Organization: Kementerian Komunikasi dan Informatika
Sponsoring Registrar URL: domain.go.id
Sponsoring Registrar Street: Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City: Jakarta Pusat
Sponsoring Registrar State/Province: Jakarta
Sponsoring Registrar Postal Code: 10110
Sponsoring Registrar Country: ID
Sponsoring Registrar Phone: 6281292920929
Sponsoring Registrar Email: helpdeskdomain@mail.kominfo.go.id
Name Server: dns1.pusatdns.com
Name Server: dns2.pusatdns.com
Name Server: dns2.surabaya.go.id
Name Server: ns1.pusatdns.com
Name Server: perseus.surabaya.go.id
Name Server: pluto.surabaya.go.id
```

Gambar 4. 1 WhoIs

Pada Gambar 4. 1 WhoIs menemukan hasil bahwa domain yang digunakan yaitu .go.id. Website tersebut diregister pada Jl. Medan Merdeka Barat, Jakarta Pusat, Jakarta. Ditemukan juga email yang digunakan pada website yaitu helpdeskdomain@mail.kominfo.go.id

4.1.2 Pemindaian Port

Pemindaian port (port scanning) adalah teknik yang digunakan untuk mengidentifikasi layanan yang berjalan pada sistem jaringan dengan memeriksa port yang terbuka. Port dalam jaringan komputer adalah titik akhir komunikasi logis yang digunakan untuk mengidentifikasi proses atau layanan tertentu yang berjalan pada sistem.

```
┌──(athaaa㉿athaaa)-[~]
└─$ nmap -sV 112.140.160.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 20:50 EDT
Nmap scan report for 112.140.160.92
Host is up (0.052s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
```

Gambar 4. 2 Nmap -sV

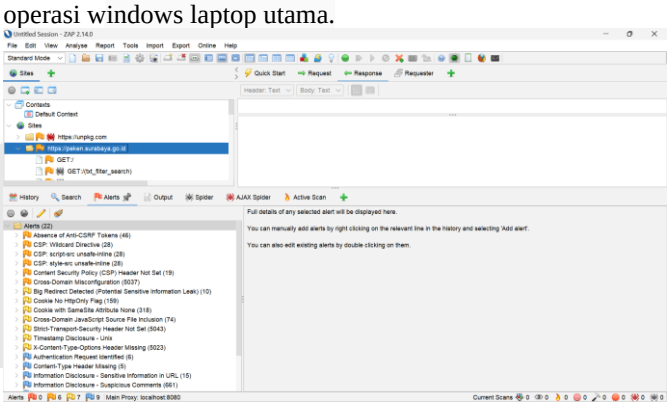
Pada gambar 4.2 peneliti mneggunakan command Nmap -sV dikarenakan peneliti ingin melihat port apa saja yang terbuka, terlihat pada gambar bahwa port 80 dan 443 terbuka dan menggunakan service http version nginx

Gambar 4. 3 Nmap -O

Pada

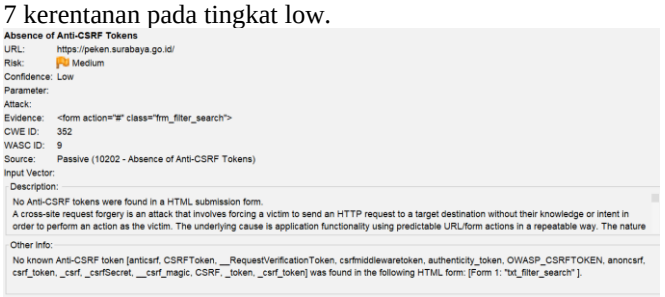
Gambar 4. 3 Nmap -O peneliti menggunakan command Nmap -O yang berfungsi untuk melakukan scanning OS apa saja yang digunakan oleh host. **Vulnerability Analysis**

Vulnerability scanning merupakan tahap selanjutnya yang dilakukan setelah tahap information gathering yang dilakukan dalam proses Penetration Testing. Tahap ini berfungsi untuk menemukan celah kerentanan keamanan pada object Website. Tahap ini dilakukan menggunakan software OWASP ZAP yang telah dilakukan instalasi pada sistem operasi windows laptop utama.



Gambar 4. 4 Scan Owasp Zap

Berdasarkan Gambar 4. 4 Scan Owasp Zap hasil scan menunjukkan terdapat 6 kerentanan pada tingkat medium dan 7 kerentanan pada tingkat low.



Absence of Anti-CSRF Tokens

URL: https://pekan.surabaya.go.id/
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="#" class="frm_filter_search">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:

Description:

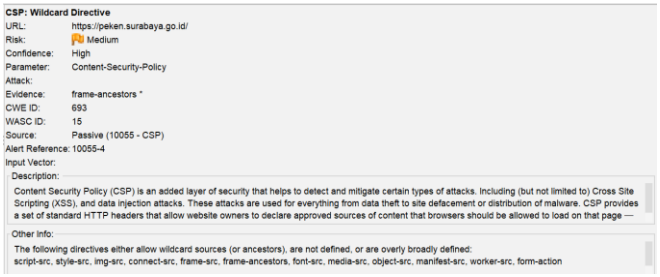
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "txt_filter_search"].

Gambar 4. 5 Kerentanan Medium 1

Pada Gambar 4. 5 Kerentanan Medium 1 menunjukkan bahwa terdapat kerentanan berupa “asbence of the anti-CSRF Tokens” yang bermaksud bahwa dalam HTLM form tidak ditemukan Anti-CSRF Token yang dapat menyebabkan data dari user otomatis bergerak sendiri tanpa ada perintah



Gambar 4. 6 Kerentanan Medium 2

Pada gambar Gambar 4. 6 Kerentanan Medium 2 menunjukkan adanya kerentanan berupa Content Security Policy yang bermaksud adanya kemungkinan dapat terjadinya attack berupa Cross Site Scripting (XSS) dan Data injection attack

Gambar 4. 7 Kerentanan Medium 3

Pada Gambar 4. 7 Kerentanan Medium 3 menunjukkan adanya kerentanan berupa Content Security Policy yang bermaksud adanya kemungkinan dapat terjadinya attack berupa Cross Site Scripting (XSS) dan Data injection attack

Gambar 4. 8 Kerentanan Medium 4

Pada Gambar 4. 8 Kerentanan Medium 4 menunjukkan adanya kerentanan berupa Content Security Policy yang bermaksud adanya kemungkinan dapat terjadinya attack berupa Cross Site Scripting (XSS) dan Data injection attack

Gambar 4. 9 Kerentanan Medium 5

Pada Gambar 4. 9 Kerentanan Medium 5 menunjukkan adanya kerentanan berupa Content Security Policy yang bermaksud adanya kemungkinan dapat terjadinya attack berupa Cross Site Scripting (XSS) dan Data injection attack

Gambar 4. 10 Kerentanan Medium 6

Pada Gambar 4. 10 Kerentanan Medium 6 Memiliki kerentanan berupa “Cross-Domain Misconfiguration” yang bermaksud bahwa data browser berkemungkinan akan memiliki masalah dalam memuat, untuk solusi dalam kerentanan ini dapat menggunakan konfigurasikan header HTTP " Access-Control-Allow-Origin " ke sekumpulan domain yang lebih terbatas, atau hapus semua header CORS sepenuhnya,

Teknik Pengujian	*Tools*	Hasil Caption	*Status*	*Evidence*
Identifikasi Target	nslookup	Melakukan Pencarian IP address dan informasi terkait dengan command nslookup	Berhasil	Gambar 4. 1 WhoIs
Pemindaian Port	nmap	Melakukan pencarian port yang terhubung ke server	Berhasil	Gambar 4. 2 Nmap -sV dan  Gambar 4. 3 Nmap -O
Vulnerability Analysisi	Owasp Zap	Melakukan scan kerentanan pada website yang dituju	Berhasil	Gambar 4. 4 Scan Owasp Zap

4.2 Penetration Testing

Pengujian pada tahap penetration dilakukan melalui simulasi serangan pada website target, yang pada pengujian ini dilakukan mengikuti ketentuan Owasp Top 10. Domain yang diuji pada tahap penetration meliputi domain utama dan subdomain website target. Untuk tahapan dalam melakukan penetration testing peneliti menggunakan beberapa tools yang dapat digunakan sesuai panduan dalam website Owasp Top 10.

4.2.1 A01 Broken Access Control

Akses Kontrol menetapkan sebuah peraturan yang dimana user tidak dapat melakukan sebuah aksi diluar permission yang diberikan. Kegagalan atas hal ini dapat mengakibatkan pengeluaran informasi yang tidak diizinkan, modifikasi, atau penghancuran dari semua data atau pemberlakuan sebuah fungsi bisnis di luar limit

sebuah user.

Tahap pengujian menggunakan 2 metode

Langkah-Langkah Strategi manual dan tools

Peneliti menemukan adanya 2 cara untuk pengecekan Broken Access Control yaitu secara manual menggunakan link dalam website dan tools yang digunakan untuk melakukan penyerangan

Strategi Manual : Pada link peken.surabaya.go.id bisa menambahkan ‘robot.txt’ dan ‘admin’ untuk pengecekan apakah link admin dan robot.txt sudah terhapus dalam website. Mengapa menggunakan ‘robot.txt’ dikarenakan jika pembuat website kemungkinan sebelum deploy akan membuat php bernama robot.txt untuk melakukan pengecekan. Dan untuk ‘admin’ jika link admin tidak dihide maka pengguna user bisa mengakses link admin .

Mengapa robot.txt dikarenakan pengembang website terkadang melupakan untuk menghapus link website yang dummy

Strategi Tools :

Peneliti menggunakan dirsearch dan curl, dirsearch dapat digunakan untuk mencari direktori yang rentan pada website dan curl digunakan untuk penyerangan berupa mencari database pada direktori yang ditemukan.

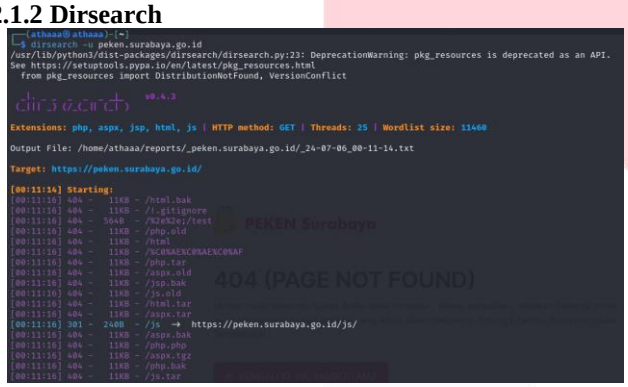
1. Buka cmd dan ketik “dirsearch ‘Link website’ “
2. Terdapat 3 warna yang muncul melalui proses ‘dirsearch’
3. Gunakan tools ‘curl’ untuk lebih menggali lebih dalam pada link yang muncul

4.2.1.1 Manual

Gambar 4. 11 Admin

Pada **Error! Reference source not found.** peneliti m encoba untuk membuka link admin namun tidak dapat ditemukan dikarenakan website sudah mengganti atau menghapus link admin yang ada

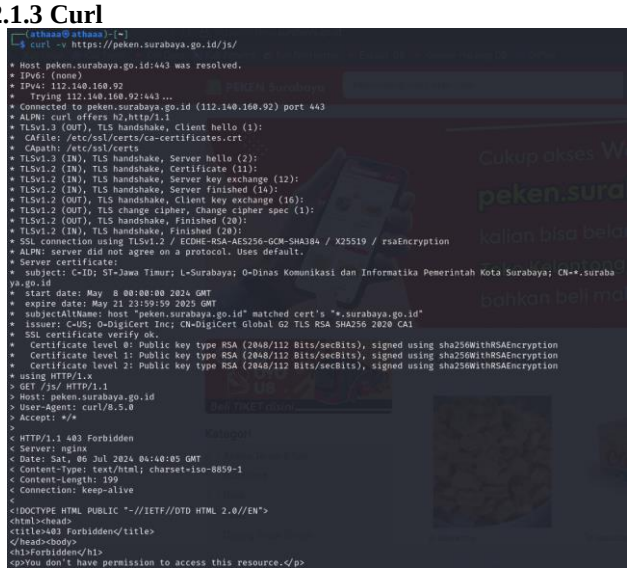
4.2.1.2 Dirsearch



Gambar 4. 12 Dirsearch

Pada Gambar 4. 12 Dirsearch peneliti menggunakan command dirsearch untuk mencari direktori apa saja yang ada pada website peken surabaya, untuk link website yang berwarna ungu bertanda bahwa link yang ditemukan tidak dapat untuk dilakukan penyerangan dan untuk link yang dapat dilakukan penyerangan link website berwarna hijau

4.2.1.3 Curl

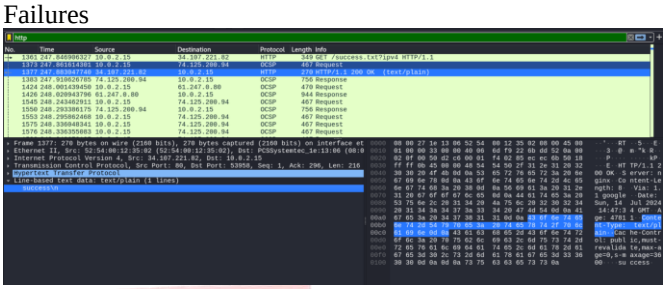


Gambar 4. 13 Curl

Pada Gambar 4. 13 Curl Peneliti menggunakan link js dikarenakan pada saat melakukan scan dengan dirsearch link js bisa untuk dilakukan penyerangan, hasil dari Curl ini menunjukkan bahwa link js tidak dapat dilakukan dikarenakan keterbatasan access untuk membuka resource yang ada

4.2.2 Cryptographic Failures

Cryptographic Failures terjadi ketika informasi tidak dilindungi secara memadai. Data sensitif termasuk misalnya informasi pembayaran, kredensial, nomor telepon, alamat email, data pribadi. Jenis pelanggaran data ini sering kali merugikan secara finansial merusak bagi bisnis. Penyerang yang mendapatkan akses ke data yang tidak terlindungi telah menjadi serangan yang paling umum yang berdampak dalam beberapa tahun terakhir. Kelemahan yang paling umum adalah data sensitif tidak dienkripsi. Peneliti menggunakan wireshark untuk melakukan penyerangan Cryptographic Failures



Gambar 4. 14 Wireshark

Pada Gambar 4. 14 Wireshark terdapat hasil dari wireshark yang menunjukkan bahwa sinyal http berupa login berhasil/success yang termasuk kerentanan dikarenakan sinyal http berhasil masuk ke tools wireshark

4.2.3 Injection

Tujuan dari penyerang yang melakukan serangan injeksi adalah untuk menemukan cara untuk memasukkan data ke dalam sebuah aplikasi yang kemudian ditafsirkan/dijalankan oleh aplikasi tersebut. Kurangnyavalidasi data masukan/keluaran yang tepat memungkinkan jenis serangan ini terjadi. Penyerang yang mengeksploitasi kelemahan injeksi dapat membuat, membaca, memodifikasi, atau menghapus data sewenang-wenang yang tersedia untuk aplikasi. Dalam skenario terburuk, serangan injeksi dapat menyebabkan penyerang

Peneliti menggunakan sqlmap untuk melakukan penyerangan A03 injection dikarenakan di dalam kali-linux sqlmap merupakan tools yang berhubungan dengan injeksi.

Langkah-Langkah Strategi tools :

1. Menentukan parameter didalam website yang bisa untuk dilakukan injeksi yaitu terdapat parameter yang menunjukkan nama database
2. Buka cmd dan ketik “sqlmap -u ‘link’ “, untuk penyerangan menggunakan command sqlmap dikarenakan kita menggunakan tools sqlmap, untuk -u merupakan singkatan dari url
3. Jika parameter berhasil di injeksi hasil yang ada adalah list database didalam website

Gambar 4. 15 SqlMap

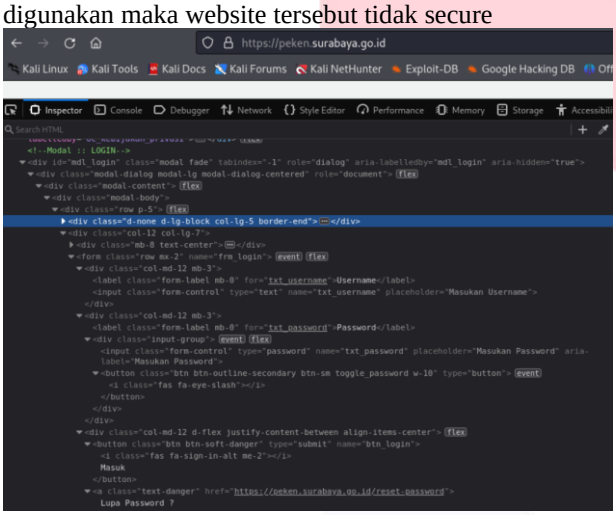
Pada Gambar 4. 15 SqlMap menggunakan command sqlmap -url yang berupa sqlmap -u peken.surabaya.go.id/order?type=shopping dikarenakan terdapat parameter shopping yang merupakan letak tempat database berada, dari hasil serangan pada parameter tidak dapat dilakukan serangan.

4.2.4 A04 Insecure Design

Desain yang tidak aman adalah kategori yang luas yang mewakili berbagai kelemahan, yang dinyatakan sebagai "desain kontrol yang hilang atau tidak efektif." Desain yang tidak aman bukan merupakan sumber dari semua 10 kategori risiko lainnya. Terdapat perbedaan antara desain yang tidak aman dan implementasi yang tidak aman. Kami membedakan antara cacat desain dan cacat implementasi karena suatu alasan, keduanya memiliki akar penyebab dan perbaikan yang berbeda. Desain yang aman masih dapat memiliki cacat implementasi yang menyebabkan kerentanan yang dapat dieksploitasi. Desain yang tidak aman tidak dapat diperbaiki dengan implementasi yang sempurna karena menurut definisi.

Langkah-Langkah Strategi tools :

1. Bisa dilakukan dengan inspect website yang akan di-test, jika didalam form website terdapat ID & Password yang digunakan maka website tersebut tidak secure



Gambar 4. 16 Login

Gambar 4. 17 Detail Barang

4.2.5 Security Misconfiguration

Security Misconfiguration sangat lazim terjadi karena dapat terjadi di tingkat mana pun aplikasi, misalnya layanan jaringan, server web, basis data, kerangka kerja, atau penyimpanan. Kesalahan konfigurasi termasuk izin yang tidak dikonfigurasi dengan benar, diaktifkan atau diinstal fitur yang tidak perlu, akun default yang dapat diakses, fitur keamanan yang dinonaktifkan, perangkat lunak yang rentan atau kedaluwarsa, dan masih banyak lagi. Kelemahan ini dapat dieksploitasi oleh penyerang untuk mendapatkan akses yang tidak sah atau bahkan benar-benar membahayakan sistem.

Langkah-Langkah Strategi tools :

1. Ketikkan ‘<>/’”&:’ pada searchbar pada website yang akan di test, jika hasil search menunjukkan pencarian tidak ditemukan (Gambar 4. 18 Search Bar Peken) maka website sudah memenuhi keamanan, jika website menunjukkan database yang dipakai maka website tidak aman

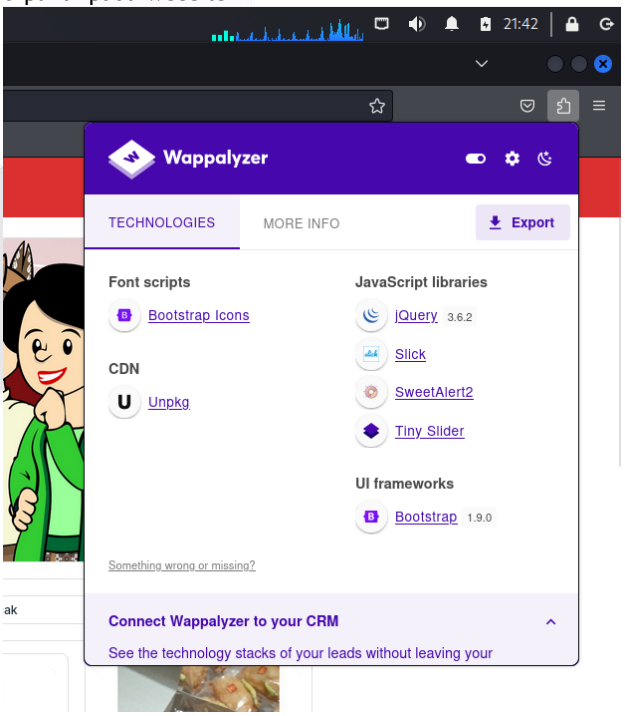
Gambar 4. 18 Search Bar Peken

4.2.6 A06 Vulnerable and Outdated Component

Menggunakan komponen yang tidak didukung atau kedaluwarsa dapat menyebabkan aplikasi menjadi rentan. Meskipun komponen tersebut saat ini tidak rentan, risikonya meningkat jika komponen tersebut tetap ketinggalan zaman. Penyerang yang mengeksploitasi komponen yang rentan dapat menyebabkan kehilangan data yang serius atau pengambilalihan server pengambilalihan. Alat bantu otomatis dapat digunakan untuk menemukan dan mengeksploitasi komponen yang rentan

Langkah-Langkah Strategi tools :

1. Untuk A06 bisa dilakukan dengan extension Bernama ‘Wappalyzer’, setelah terinstall tools wappalyzer dapat digunakan untuk pengecekan versi komponen yang dipakai pada website



Gambar 4. 19 Wappalyzer

Terlihat dari Gambar 4. 19 Wappalyzer diatas untuk jQuery memakai versi 3.6.2 yang tergolong versi lama, untuk versi terbaru dari jQuery terbaru yaitu 3.7.2. Dan untuk bootstrap terlihat masih menggunakan versi 1.9.0, untuk versi terbaru yaitu 5.3.3

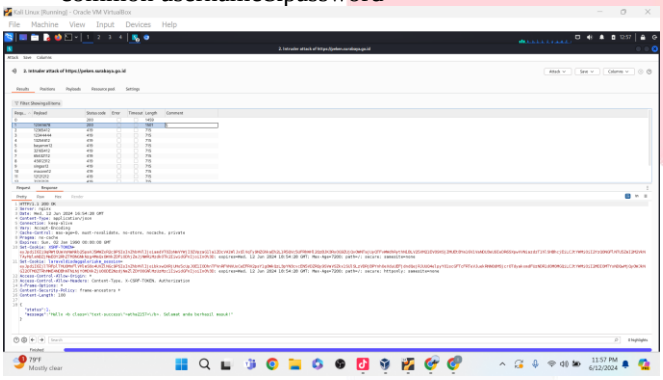
4.2.7 A07 Identification and Authentication Failures

Fungsi otentikasi dan manajemen sesi dalam aplikasi web digunakan untuk memverifikasi identitas pengguna. Implementasi yang salah dari fungsi-fungsi ini memungkinkan penyerang untuk mengkompromikan kata

sandi, kunci, atau token sesi. Penyerang dapat mengeksploitasi otentikasi yang rusak dengan pengisian kredensial, brute otomatis, brute force, dan serangan kamus untuk mengasumsikan identitas pengguna lain. Daftar nama pengguna dan kata sandi dapat digunakan dalam serangan otomatis untuk mendapatkan akses ke sistem.

Langkah-Langkah Strategi tools :

1. Buka tools burpsuite pada kali-linux
2. Sambungkan website dengan tools burpsuite
3. Masuk ke bagian intruder
4. Pada menu position ada username dan password, username dan password bisa ditambahkan ‘add$’
5. Masuk ke bagian payload, terdapat payload setting, klik “load” dan masukkan list common username&password, setelah itu klik start attack
6. Tunggu hasil dari proses yang dilakukan, terdapat 3 code yang akan menunjukkan hasil dari percobaan common username&password



Gambar 4. 20 List Common

Gambar 4. 21 Nomor 1501

Pada Gambar 4. 20 List Common ada 3 size data yang berbeda dengan nomor 1459, 1501, 715. nomor 1459 menunjukkan bahwa password yang dimasukkan salah, untuk nomor 1501 (Gambar 4. 21 Nomor 1501) menunjukkan bahwa password yang dicoba berhasil untuk masuk, untuk nomor 715 menunjukkan limit password yang bisa di input di website tersebut

4.2.8 A08 Software and Data Integrity

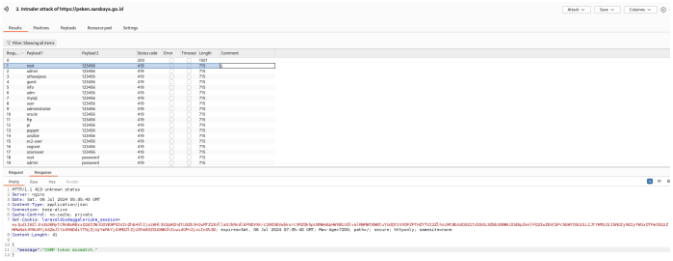
Penelitian ini tidak mencakup percobaan A08 karena peneliti mengalami kesulitan dalam menemukan database yang dapat digunakan untuk simulasi serangan. Keterbatasan akses terhadap basis data yang relevan menghambat pelaksanaan uji coba yang direncanakan, sehingga percobaan A08 tidak dapat dilanjutkan

4.2.8 A09 Security Logging and Monitoring Failures

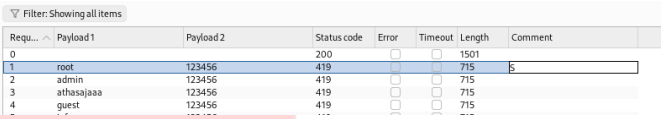
Security Logging and Monitoring Failures bukanlah sebuah kerentanan, melainkan sebuah masalah yang memungkinkan penyerang untuk melakukan serangan. Security Logging and Monitoring Failures yang tidak memadai adalah dasar dari hampir hampir setiap insiden besar. Kurangnya pemantauan dan respon yang tepat waktu memungkinkan penyerang untuk mencapai tujuan mereka tanpa terdeteksi. Mengidentifikasi dan mengatasi pelanggaran data secepat mungkin, mengurangi biaya dan kerusakan yang terjadi.

Langkah-Langkah Strategi tools :

1. Buka tools burpsuite pada kali-linux
2. Sambungkan website dengan tools burpsuite
3. Masuk ke bagian intruder
4. Pada menu position ada username dan password, username dan password bisa ditambahkan ‘add$’
5. Masuk ke bagian payload, terdapat payload setting, klik “load” dan masukkan list common username&password, setelah itu klik start attack
6. Tunggu hasil dari proses yang dilakukan, jika website tersebut memiliki Batasan dalam memasukkan password maka website tersebut aman



Gambar 4. 22 List Common



Gambar 4. 23 3x Input Password

Pada Gambar 4. 23 3x Input Password dikarenakan terdapat 3x percobaan memasukkan password jadi website sudah terhandle dengan aman

4.2.10 A10 Server-Side Request Forgery

Dalam Server-Side Request Forgery (SSRF), skrip berbahaya disisipkan ke dalam situs web yang dipercaya, yang berarti merupakan jenis injeksi. Serangan-serangan ini dapat terjadi di mana saja aplikasi web menggunakan input dari pengguna, tanpa memvalidasi atau menyandikannya Penyerang menggunakan XSS untuk mengirim skrip berbahaya ke browser pengguna akhir. Karena website mengira bahwa skrip tersebut berasal dari sumber tepercaya, skrip tersebut akan dieksekusi dan kemudian akan memiliki akses ke cookie, token sesi, atau informasi sensitif lainnya.

Langkah-Langkah Strategi tools :

1. Buka tools burpsuite pada kali-linux
2. Sambungkan website dengan tools burpsuite
3. Masuk ke bagian repeater
4. Pada menu position ada username dan password, username dan password bisa ditambahkan ‘add$’ dan kirim ke ‘intruder’
5. Pada intruder ganti attack type menjadi cluster bomb setelah itu ganti payload set menjadi 2 dan masukkan list username dan password lalu click start attack
6. Hasil yang didapat akan menunjukkan informasi berupa cookie yang ada

Gambar 4. 24 Hasil Pencarian Cookie

Pada Gambar 4. 24 Hasil Pencarian Cookie merupakan cara untuk menemukan stock API dengan menggunakan burpsuite dan http history. Stock API tidak ditemukan dan SSRF token ditemukan yang merupakan bagian dari keamanan website.

Table 4. 1 Testing

Teknik Pengujian	*Tools*	Hasil Caption	*Status*	*Evidence*
A01	DirSearch, Curl	Ditemukan Beberapa kerentanan namun	Gagal	Gambar 4. 12 Dirsearch,

		kerentanan tersebut tidak bisa diakses oleh tools yang digunakan		Gambar 4. 13 Curl
A02	Wireshark	Scanning A02 Menggunakan tools Wireshark	Berhasil	Gambar 4. 14 Wireshark
A03	SqlMap	Ditemukan 3 parameter yang bisa diinjeksi namun hasil injeksi yang dilakukan tidak berhasil	Gagal	Gambar 4. 15 SqlMap
A04	Inspect	Hasil menunjukan bahwa website sudah terjaga dengan baik	Gagal	Gambar 4. 16 LoginGambar 4. 17 Detail Barang
A05	Kali-linux	Melakukan penyerangan dengan code **<>/'"&!** Tidak ditemukan kerentanan	Gagal	Gambar 4. 18 Search Bar Peken
A06	Wappalyzer	Melakukan pengecekan versi komponen yang dipakai pada website	Berhasil	Gambar 4. 19 Wappalyzer
A07	Burpsuite	Melakukan pengecekan random password pada website	Berhasil	Gambar 4. 20 List Common
A08	Gagal	Gagal	Gagal	--
A09	Burpsuite	Dikarenana terdapat 3x access salah dalam memasukkan password jadi penyerangan menggunakan list username&password tidak bisa	Gagal	Gambar 4. 23 3x Input Password
A10	Burpsuite	Dilakukan Penyerangan menggunakan burpsuite dan ditemukan jika API website tidak dapat ditemukan	Gagal	Gambar 4. 24 Hasil Pencarian Cookie

V. KESIMPULAN

Penelitian ini berhasil mensimulasikan dan menentukan Pengujian sistem informasi Peken Surabaya menggunakan metode OWASP Top 10 dilakukan dengan mengidentifikasi dan menganalisis sepuluh jenis kerentanan keamanan yang paling umum pada aplikasi web. Metode ini mencakup berbagai jenis serangan seperti injeksi, otentikasi yang tidak memadai, dan eksposur data sensitif. Dari 10 kerentanan yang dilakukan menunjukkan hasil bahwa website Peken Surabaya memiliki tingkat keamanan yang baik, namun ada perbaikan di poin A03 dan A06 yang menunjukkan bahwa website masih memiliki parameter untuk dilakukan injeksi dan memiliki komponen website yang telah kadaluarsa.

REFERENSI

Adelia, and Kridanto Surendro. 2015. *Perancangan Model Pengukuran Layanan Teknologi Informasi Pada Perguruan Tinggi (Studi Kasus: Perguruan Tinggi X)*. Vol. 1.

Admin Fikes. 2023. "23 JENIS SERANGAN CYBERSECURITY." *Universitas Alma Ata*. Retrieved November 21, 2023 (https://fikes.almaata.ac.id/23-jenis-serangan-cybersecurity/).

Almeida, Fernando, Jose Duarte Santos, and Jose Augusto Monteiro. 2020. "The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World." *IEEE Engineering Management Review* 48(3):97–103. doi: 10.1109/EMR.2020.3013206.

Amukta Nayak. n.d. "OWASP Top 10 Deep Dive: Getting a Clear View on Vulnerable and Outdated Components." *Rapid1*.

Anon. 2005. *Information Systems Security Assessment Framework (ISSAF) Draft 0.2*.

Anon. n.d. "E-Peken Go Publik, Belanja Kebutuhan Pokok Makin Mudah." *Tempo.Co*.

Armando, Rio, Ag Kom, Agnam Melyantara, Rizma Elfariani, Desy Fitri, Aulia Latuconsina, and Muhammad Nasrullah. 2022. "IT Support Website Security Evaluation Using Vulnerability Assessment Tools." *Journal of Information Systems and Informatics* 4(4).

Ary Adianto. n.d. "Mengenal 14 Jenis Serangan Siber Dan Cara Mencegahnya." *Helios INFORMATIKA NUSANTARA*.

Awad, Mohammed, Muhammed Ali, Maen Takruri, and Shereen Ismail. 2019. "Security Vulnerabilities Related to Web-Based Data." *Telkomnika (Telecommunication Computing Electronics and Control)* 17(2):852–56. doi: 10.12928/TELKOMNIKA.v17i2.10484.

BSSN (Badan Siber dan Sandi Negara). 2023. "BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 Untuk Literasi Budaya Keamanan Siber." *BSSN*. Retrieved November 20, 2023 (https://www.bssn.go.id/lanskap2022/).

BurpSuite. n.d. "BurpSuite." *Kali.Org*.

CNN INDONESIA (PT Trans News Corpora). 2021. "Data 279 Juta Penduduk RI Diduga Bocor Dan Diperjualbelikan." *CNN INDONESIA*. Retrieved November 20, 2023 (https://www.cnnindonesia.com/teknologi/20210520140736-185-644759/279-juta-data-penduduk-ri-diduga-bocor-dan-dijual-di-forum).

Cyolo Team. n.d. "OWASP Top 10: Injection – What It Is And How To Protect Our Applications." *Cyolo*. Retrieved November 22, 2023 (https://cyolo.io/blog/owasp-top-10-injection-what-it-is-and-how-to-protect-our-applications#:~:text=During%20an%20injection%2C%20an%20attacker%20will%20transmit%20malicious,10%20and%20is%20important%20to%20look%20out%20for.).

Elanda, Anggi, and Robby Lintang Buana. 2021. *Analisis Kualitas Keamanan Sistem Informasi E-OFFICE Berbasis Website Pada STMIK ROSMA Menggunakan OWASP TOP 10*. Vol. 6.

Eran Shmuely. n.d. "Identification And Authentication Failures And How To Prevent Them." *Cyolo*.

Febriana, Rona. n.d. "Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top

10 Owasp Attack." *Jurnal Ilmiah Wahana Pendidikan* 2022(12):327–34. doi: 10.5281/zenodo.6945632.

Gilberto Najera-Gutierrez and Juned Ahmed Ansari. n.d. *Web Penetration Testing with Kali Linux - Third Edition: Explore the Methods and Tools of Ethical Hacking with Kali Linux*. Vol. 426. Packt Publishing - ebooks Account.

Hakim, Ahmad Azizul, Singgi Pratama, and Fransiska Prihatini. 2019. "Sistem Informasi Manajemen Hubungan Pelanggan Berbasis Web Pada PT. Arya Media Tour & Travel." 5(2):123–36.

Indiana Malia. n.d. "Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen E-Commerce." *Idmtimes*.

James Clement. n.d. "OWASP Top Ten: #9 Security Logging and Monitoring Failures." *FORESITE CYBERSECURITY*.

Microsoft Security. 2023. "Apa Itu Serangan Cyber?" *Microsoft*. Retrieved November 21, 2023 (https://www.microsoft.com/id-id/security/business/security-101/what-is-a-cyberattack#:~:text=Serangan%20cyber%20adalah%20upaya%20mendapatkan,%2C%20mengubah%2C%20atau%20menghancurkan%20data.).

NMAP. n.d. "Zenmap GUI." *NMAP.ORG*. Retrieved November 23, 2023 (https://nmap.org/zenmap/).

Nurul, Shinta, Shynta Anggrainy, and Siska Aprelyani. 2022. "Faktor- Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi, Teknologi Informasi Dan Network." 3(5). doi: 10.31933/jemsi.v3i5.

Oracle. 2020. *Oracle VM VirtualBox Datasheet*.

OWASP. n.d.-a. "About the OWASP Foundation." *OWASP*. Retrieved November 20, 2023 (https://owasp.org/about/).

OWASP. n.d.-b. "Broken Access Control." *OWASP TOP 10*. Retrieved November 22, 2023 (https://owasp.org/Top10/A01_2021-Broken_Access_Control/).

OWASP. n.d.-c. "Cryptographic Failures." *OWASP TOP 10*. Retrieved November 22, 2023 (https://owasp.org/Top10/A02_2021-Cryptographic_Failures/).

OWASP. n.d.-d. "Insecure Design." *OWASP TOP 10*. Retrieved November 22, 2023 (https://owasp.org/Top10/A04_2021-Insecure_Design/).

OWASP. n.d.-e. "OWASP Top Ten." *OWASP*. Retrieved November 20, 2023 (https://owasp.org/www-project-top-ten/).

OWASP. n.d.-f. "Security Misconfiguration." *OWASP TOP 10*.

OWASP. n.d.-g. "Server-Side Request Forgery (SSRF)." *OWASP TOP 10*.

OWASP. n.d.-h. "Software and Data Integrity Failures." *OWASP TOP 10*.

Peken Surabaya. 2021. "User Guide."

Revolino Syarif, Tio, and Didit Andri Jatmiko. n.d. *Analisis Perbandingan Metode Web Security PTES, ISSAF Dan OWASP Di Dinas Komunikasi Dan Informasi Kota Bandung*.

Surfshark. 2023. "Data Breach Monitoring." *Surfshark* 0–0. Retrieved November 20, 2023 (https://surfshark.com/research/data-breach-monitoring).

zaproxy. n.d. "Introducing ZAP." *Zaproxy*. Retrieved November 20, 2023 (https://www.zaproxy.org/getting-started/).