LAPORAN KERJA PRAKTEK

DINAS KOMUNIKASI INFORMATIKA STATISTIK DAN PERSANDIAN KOTA PEKAN BARU

ANALISA KERENTANAN WEBSITE PEKANBARU.ID MENGGUNAKAN OWASP ZAP

YUDI

64042011084

PROGRAM STUDI KEAMANAN SISTEM INFORMASI

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BENGKALIS

2025

LAPORAN KERJA PRAKTEK
Dinas Komunikasi, Informatika, Statistik, Dan Persandian
Kota Pekanbaru

Ditulis sebagai salah satu syarat untuk menyelesaikan Kerja Praktek

Yudi
6404211084

Bengkalis, 10 Juli 2025

Analis Sistem Informasi
Dinas komunikasi, Informatika,
Statistik, Dan Persandian Kota
Pekanbaru

Muhammad Reza
NIP. 19861107202012101 3

Dosen Pembimbing Program Studi
Keamanan Sistem Informasi

Agus Tedyyana, M.Kom
NIP. 198510052015041001

Disetujui
Ka.Prodi Keamanan Sistem Informasi

Nurmi Hidayasari, M.Kom
NIP.199109012022032006

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga kegiatan dan penyusunan Laporan Kerja Praktek (KP) ini dapat diselesaikan dengan baik dan lancar.

Kerja Praktek merupakan salah satu program wajib bagi mahasiswa Politeknik Negeri Bengkalis, khususnya pada akhir semester VIII, yang bertujuan untuk mengaplikasikan ilmu pengetahuan yang telah diperoleh di bangku perkuliahan ke dalam dunia kerja secara nyata. Dalam pelaksanaannya, penulis melaksanakan kerja praktek di PT Garuda Cyber Indonesia, yang memberikan pengalaman berharga dalam bidang pengembangan teknologi informasi.

Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bimbingan, dukungan, serta motivasi selama pelaksanaan Kerja Praktek ini. Ucapan terima kasih secara khusus penulis sampaikan kepada:

1. Bapak Jhony Custer, S.T., M.T., selaku Direktur Politeknik Negeri Bengkalis.
2. Bapak Kasmawi, M.Kom, selaku Ketua Jurusan Teknik Informatika.
3. Ibu Nurmi Hidayasari, S.T,MT, selaku Ketua Program Studi Keamanan Sistem Informasi.
4. Bapak Agus Tedyyana, M.Kom, selaku dosen pembimbing yang telah memberikan saran serta meluangkan waktunya untuk membimbing penulis dalam menyusun laporan kerja praktek ini.
5. Ibu Rezki Kurniati, M.Kom, selaku Koordinator Kerja Praktek Program Studi Keamanan Sistem Informasi.
6. Bapak Muhammad Reza sebagai pembimbing kerja praktek di diskominfo kota pekanbaru.
7. Kepada seluruh rekan magang di diskominfo kota pekanbaru, terima kasih atas dukungan tak henti dan kekompakan yang selalu terjalin dalam setiap tugas.

8. Kepada kedua orang tua, dan keluarga tercinta, terima kasih atas doa, semangat, dan dukungan tiada henti. Tanpa kalian, perjalanan ini mungkin tak akan seindah dan semudah yang dirasakan.
9. Untuk teman-teman seperjuangan, seluruh rekan di kelas KSI 21B, terima kasih atas semangat, bantuan, dan kerja sama yang luar biasa.

Penulis juga menyampaikan permohonan maaf apabila selama pelaksanaan kerja praktek terdapat kekeliruan atau perilaku yang kurang berkenan. Penulis menyadari bahwa laporan ini masih jauh dari sempurna, baik dari segi isi maupun penyajian. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan untuk perbaikan di masa mendatang.

Akhir kata, semoga laporan kerja praktek ini dapat memberikan manfaat bagi pembaca dan semua pihak yang berkepentingan.

Pekanbaru, 10 Juli 2025

YUDI

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang Pemikiran KP

Kuliah praktik merupakan sebuah kegiatan akademik yang dirancang untuk memberikan pengalaman langsung kepada mahasiswa dalam dunia kerja yang relevan dengan disiplin ilmu yang dipelajari. Dengan adanya kegiatan ini, siswa diharapkan dapat menerapkan teori yang telah mereka pelajari di kelas dalam situasi nyata di lapangan.

Penulis memilih Dinas Komunikasi, Informatika, Statistik, dan Persandian Kota Pekanbaru sebagai tempat pelaksanaan kuliah praktik. Pemilihan ini didasarkan pada peran penting instansi tersebut dalam mengelola infrastruktur teknologi informasi dan komunikasi di pemerintahan daerah, khususnya di bidang keamanan informasi dan pengelolaan situs resmi. Selain itu, penulis berharap dapat memperoleh pengalaman kerja yang sesuai dan relevan dengan bidang studi yang diambil, yaitu Keamanan Sistem Informasi.

Selama mengikuti kuliah praktik, penulis diberikan tugas untuk melakukan analisis keamanan pada website resmi Pemerintah Kota Pekanbaru (pekanbaru.go.id) dengan menggunakan alat OWASP ZAP (Zed Attack Proxy). Oleh karena itu, penting untuk mengidentifikasi potensi kerentanan demi menjaga kerahasiaan dan keamanan layanan informasi publik.

Melalui kegiatan ini, penulis tidak hanya memperoleh pemahaman lebih dalam mengenai proses pemindaian dan analisis kerentanan aplikasi web, tetapi juga mendapatkan wawasan baru tentang pentingnya sistem keamanan informasi dalam konteks pemerintahan. Diharapkan hasil dari kegiatan ini dapat memberikan kontribusi awal dalam meningkatkan keamanan website Pemerintah Kota Pekanbaru dan menjadi dasar untuk pengujian serta pemantauan lebih lanjut di masa yang akan datang.

1.2 Tujuan dan Manfaat KP

Tujuan yang diperoleh dari Kerja Praktek adalah sebagai berikut:

1. Menerapkan ilmu yang diperoleh dari kampus.
2. Meningkatkan kemampuan mengenai ilmu Keamanan Sitem Informasi.
3. Menambah pengetahuan, wawasan dan pengalaman serta mengasah kemampuan dan keterampilan penulis dalam dunia kerja.
4. Sebagai salah satu syarat dalam menyelesaikan pendidikan Sarjana Terapan Keamanan Sistem Informasi Politeknik Negeri Bengkalis.

Adapun manfaat yang diperoleh dari Kerja Praktek (KP) adalah sebagai berikut:

1. Menerapkan ilmu pengetahuan yang didapat dari kampus ke tempat kerja praktek secara nyata.
2. Mendapatkan pengalaman teori terkait Cyber Security.
3. Memperoleh kesempatan dalam menganalisis masalah yang ada.

1.3 Luaran Proyek Kerja Praktek

Dalam melakukan analisa keamanan website yang di berikan oleh Pembina magang di kantor diskominfotik utuk melakukan analisa keamanan website pekanbaru.id dengan melakukan scanning menggunakan OWASP ZAP dan membuat laporan dari hasil scanning yang telah di lakukan. hasil yang di peroleh dari selama KP adalah sebagai berikut:

1. Identifikasi kerantanan yang di dapat dari hasil scanning yang di lakukan menggunakan tolls OWASAP ZAP sesuai dengan tugas yang di berikan selama magang.
2. Menganalisis hasil temuan yang di dapat dan menyusunnya menjadi laporan analisa keamanan untuk di serahkan kepada pihak dikominfotik kota pekanbaru sebagai laporan analisa kerentanan pada website pekanbaru.id.
3. Rekomendasi perbaikan, menentukan langkah-langkah mitigasi seperti Saran

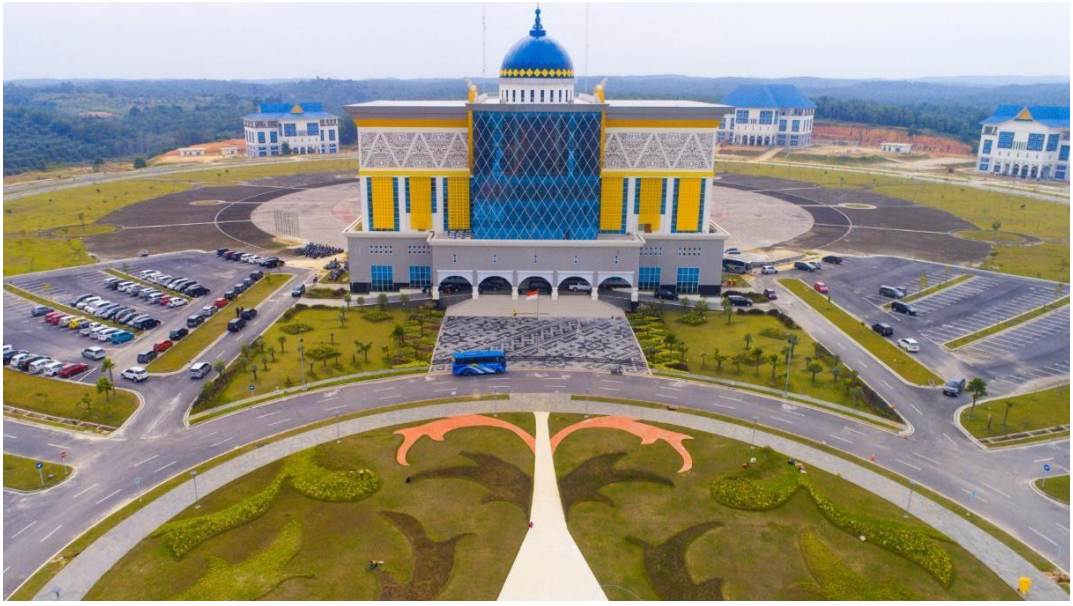
dan langkah-langkah yang perlu diambil untuk mengatasi kerentanan yang di temukan selama proses analisa kerentanan pada website yang di berikan.

4. Laporan analisa kerentanan, merupakan dokumentasi lengkap laporan komprehensif yang mencakup semua temuan, bukti, analisis, dan rekomendasi. Laporan ini disusun dengan mengikuti format yang di berikan.

BAB II
GAMBARAN UMUM PERUSAHAAN/INSTANSI

2.1 Sejarah Singkat Perusahaan/Instansi

Dinas Komunikasi Informatika Statistik dan Persandian adalah salah satu dinas yang ada di lingkungan Pemerintah Kota Pekanbaru. Kantor dari Dinas Komunikasi Informatika Statistik dan Persandian berada di Jalan Abdul Rahman Hamid Kelurahan Tuah Negeri Kecamatan Tenayan Raya, tepatnya di Gedung Pusat lantai tiga Perkantoran Walikota



Gambar 2. 1 Gedung Diskomnfo Kota Pekanbaru

Dinas Komunikasi, Informatika, Statistik dan Persandian mempunyai tugas membantu Walikota merumuskan dan ms Komunikasi Informatika Statistik dan Persandian. Susunan organisasi Dinas Komunikasi Informatika Statistik dan Persandian terdiri dari:

A. Kepala Dinas.

B. Sekretaris, membawahi:
    1. Sub Bagian Umum.
    2. Sub Bagian Keuangan.
    3. Sub Bagian Program.
C. Bidang Statistik:
    1. Seksi Statistik Sosial.
    2. Seksi Statistik Ekonomi.
    3. Seksi Statistik SDA dan Infrastruktur.
D. Bidang Persandian, Aplikasi Dan Tatakelola SPBE, membawahi:
    1. Seksi Pengembangan Aplikasi.
    2. Seksi Tata Kelola SPBE dan Persandian.
    3. Seksi Operasional Persandian dan Pengamanan SPBE.
E. Bidang Layanan Infrastruktur SPBE, membawahi:
    1. Seksi Infrastruktur dan Teknologi.
    2. Seksi Pengelolaan Pusat Data dan Interoperabilitas.
    3. Seksi Interkoneksi dan Jaringan TIK.
F. Bidang Pengelolaan Informasi dan Komunikasi Publik, membawahi:
    1. Seksi Penyuluhan dan Pengendalian Informasi.
    2. Seksi Kemitraan Informasi.
    3. Seksi Pengembangan Multimedia dan Kehumasan.
G. Kelompok Jabatan Fungsional.
H. Unit Pelaksana Teknis (UPT).

Kedudukan penulis saat ini yaitu bertugas sebagai Pengendali Teknologi Seksi Infrastruktur dan Teknologi pada Dinas Komunikasi Informatika Statistik dan Persandian Pemerintah Kota Pekanbaru mempunyai tugas pokok menyiapkan bahan pengelolaan infrastruktur teknologi informasi dan mempunyai fungsi yaitu mengelola infrastruktur teknologi informasi seperti jaringan nirkabel / hotspot internet, closed circuit television area publik, telepon voip / analog / faximile.

2.2 Visi Dan Misi Perusahaan/Instansi

A. Visi

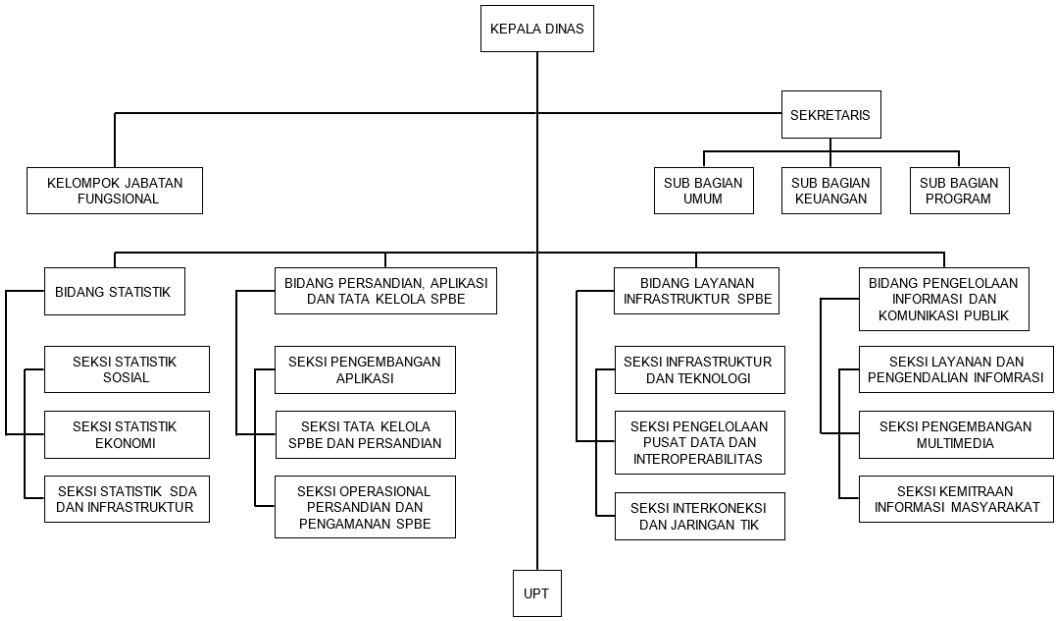
Terwujudnya Penyelenggaraan E-Government Cerdas Melalui Pemanfaatan Komunikasi Dan Informatika Yang Efektif Dan Efisien Untuk Mendukung Kota Pekanbaru Smartcity Yang Madani.

B. Misi

1. Mewujudkan peningkatan e-Government dan peningkatan profesionalisme.
2. Mewujudkan transparansi komunikasi dan informasi yang handal melalui komunikasi sosial, dan kemitraan profesi.

2.3 Struktur Organisasi Perusahaan/Instansi

Secara umum peta jabatan pada Dinas Komunikasi Informatika Statistik dan Persandian dapat dilihat pada gambar di bawah ini.



Gambar 2.2 Struktur Organisasi Perusahaan/Instansi

2.4 Ruang Lingkup Perusahaan/Instansi

Di dalam Perwako Nomor 157 Tahun 2019 tetang budaya kerja di lingkungan Pemerintah Kota Pekanbaru, disebutkan bahwa nilai budaya kerja dikategorikan berdasarkan beberapa dimensi sebagai berikut:

a. Dimensi Akhlak (Profesional, Amanah, dan Santun);
b. Dimensi Karakter (Disiplin, Kreatif, dan Inovatif); dan
c. Dimensi Kualitas (Bekerja Keras, Cerdas, dan Ikhlas, Bererak Cepat, dan Berindak Tepat dan Tuntas

BAB III

BIDANG PEKERJAAN SELAMA KP

3.1 Pekerjaan selama kuliah praktek

Selama Kerja Praktek di Dinas Komunikasi Informatika dan Statistik (Diskominfotik) di bidang Aplikasi kota pekanbaru. Bidang pekerjaan yang dilaksanakan bersifat flexsibel karena pekerjaan dilakukan sesuai arahan pembimbing lapangan. Sepanjang melakukan Kerja Praktek terdapat beberapa pekerjaaan yang diberikan oleh pihak kantora yaitu:

3.1.1 Melakukan scanning menggunakan OWASP ZAP

Melakukan scanning menggunakan tools OWASP ZAP dan menganalisa hasil dari temuan lalu menyusun nya menjadi laporan analisa kerentanan website dan di serah kan kepada pihak diskominfotikes kota pecan baru

3.1.2 Menyusun laporan hasil analisa

Menyusun hasil dari snning dan analisa dalam debuah laporan magang yang menjadi tugas ahkir dari proses kuliah praktek yang di lakukan di diskominfotikes kota pecan baru

3.2 Perangkat yang di gunakan

1. Laptop

   Laptop adalah perangkat komputasi portabel yang dapat digunakan untuk berbagai tujuan, termasuk penyerangan, pengujian keamanan, dan eksplorasi jaringan. Laptop dapat menjalankan berbagai sistem operasi, dan sebagai alat melakukan analis kerentanan system infprmasi.

2. OWASP ZAP

OWASP ZAP (Zed Attack Proxy) adalah alat open-source yang dikembangkan oleh OWASP untuk menguji keamanan aplikasi web. Alat ini digunakan untuk mendeteksi berbagai kerentanan seperti SQL Injection, XSS, dan masalah autentikasi dengan cara melakukan pemindaian otomatis maupun manual terhadap aplikasi web. ZAP bekerja sebagai proxy yang menganalisis lalu lintas data antara pengguna dan server, serta dilengkapi fitur seperti spider, fuzzer, dan scanner untuk membantu pengembang maupun analis keamanan dalam mengidentifikasi celah keamanan. Karena bersifat gratis dan mudah digunakan, ZAP banyak dimanfaatkan dalam proses pengujian keamanan dan DevSecOps.

3. Subfinder

Subfinder adalah alat open-source yang digunakan untuk menemukan subdomain dari suatu domain secara otomatis. Dikembangkan oleh ProjectDiscovery, Subfinder bekerja dengan cara melakukan pencarian pasif menggunakan berbagai sumber publik (seperti DNS, search engine, dan layanan API) tanpa melakukan brute-force, sehingga cepat dan tidak mencolok. Alat ini sangat berguna dalam proses reconnaissance (pengintaian) awal saat melakukan analisis keamanan atau pemetaan aset domain, terutama untuk mengidentifikasi titik-titik potensial yang dapat menjadi celah serangan dalam sistem web.

4. Nmap

Nmap (Network Mapper) adalah alat open-source yang digunakan untuk memindai jaringan dan mengumpulkan informasi tentang perangkat yang terhubung, seperti sistem operasi, port yang terbuka, layanan yang berjalan, dan potensi celah keamanan. Nmap sering digunakan oleh administrator jaringan dan analis keamanan untuk melakukan pemetaan jaringan, mendeteksi host aktif, serta mengidentifikasi kerentanan pada sistem sebelum dilakukan pengujian lebih lanjut. Alat ini mendukung berbagai teknik pemindaian, seperti TCP SYN scan,

UDP scan, dan OS detection, serta dapat dijalankan melalui antarmuka baris perintah atau GUI (Zenmap).

3.3 Kendala saat kuliah praktek

Kendala yang di hadapi saat melaksanakan tugas dari kuliah praktek yaitu kurangnya device yang di gunakan untuk melakukan analisa keamanan wesite pekanbaru.id karna tidak di sediakan langsung oleh tempat magang sehingga membutuhkan waktu untuk menyelesaikan tugas yang di berikan.

3.4 Target yang di harapkan

Adapun target yang di harapkan selama pelaksanaan kerja praktek di Diskominfotik Bidang Aplikasi kota pekanbaru adalah :

1) Mendapatkan pemahaman yang lebih mendalam tentang bagaimana konsep-konsep teori diterapkan dalam lingkungan kerja nyata.
2) Bagaimana tanggung jawab dalam setiap tugas yang telah diberikan dan disiplin terhadap waktu.
3) Melakukan scanning untuk mengetahui celah kerentanan website dan memberikan rekomendasi perbaikan apabila di temukan adanya celah kerentanan dalam website pekanbaru.id.
4) Terselesainya analisa kerentanan website pekanbaru.id dengan hasil akhir laporan analisa kerentanan website pekanbaru.id yang di berikan kepada Pembina lapangan kp.

BAB IV

ANALISA KERENTANAN WEBSITE PEKANBARU MENGGUNAKAN OWASP ZAP

4.1 Metodologi

4.1.1 Prosedur Analisa Website Menggunakan OWASP ZAP

Pada tahapan ini adalah prosedur yang di jalankan selama penelitian sesuai dengan prosedur yang telah di rencanakan, prosedur yang telah di rencanakan adalah sebagai berikut.

1. Persiapan Alat dan Lingkungan

   Instal OWASP ZAP (tersedia untuk Windows, Linux, dan macOS) Pastikan browser (seperti Firefox/Chrome) terkonfigurasi untuk menggunakan proxy OWASP ZAP (default: `localhost:8080`). Matikan VPN atau antivirus jika menyebabkan konflik koneksi.

2. Konfigurasi Proxy di Browser

   Arahkan pengaturan proxy browser ke `127.0.0.1` port `8080`. Tujuannya agar semua trafik dari browser melewati OWASP ZAP untuk dianalisis.

3. Menjalankan OWASP ZAP

   Buka OWASP ZAP dan pilih mode Manual Explore atau Automated Scan. Masukkan URL target (misalnya: `http://contohwebsite.go.id`) untuk memulai. pemindaian.

4. Melakukan Passive Scan

   Jelajahi situs web secara manual menggunakan browser. OWASP ZAP akan mencatat dan menganalisis semua permintaan HTTP/S yang dilewati tanpa melakukan serangan aktif.

5. Melakukan Active Scan

   Setelah semua halaman direkam, klik kanan pada root URL dan pilih

"Attack > Active Scan" OWASP ZAP akan mulai menguji kerentanan dengan berbagai teknik uji penetrasi otomatis.

6. Analisis Hasil Scan

   Periksa tab Alerts untuk melihat daftar kerentanan yang ditemukan. Setiap entri akan menyertakan: jenis kerentanan, tingkat risiko (Low, Medium, High), dan rekomendasi perbaikan.

7. Ekspor Laporan

   Hasil scan dapat diekspor dalam berbagai format seperti HTML, XML, atau PDF. Klik `Report` > `Generate Report` untuk menyimpan dokumentasi hasil analisa.

8. Dokumentasi dan Rekomendasi

   Simpulkan kerentanan utama dan berikan rekomendasi teknis atau non-teknis.

Laporan ini dapat dijadikan dasar untuk perbaikan keamanan oleh tim pengembang.

4.1.2 Metodologi Pengumpulan Data

Dalam penelitian ini, data dikumpulkan dengan menggunakan metode observasi langsung dan dokumentasi teknis melalui proses analisa kerentanan website menggunakan tools keamanan OWASP ZAP (Zed Attack Proxy). Proses pengumpulan data dilakukan secara sistematis untuk mengidentifikasi celah keamanan yang terdapat pada website target.

Adapun langkah-langkah pengumpulan data yang dilakukan adalah sebagai berikut:

1. Identifikasi Target Website

   Menentukan domain atau subdomain website yang akan dianalisis. Website ini merupakan objek uji yang digunakan untuk proses scanning kerentanan.

2. Konfigurasi Lingkungan Pengujian

Mengatur dan menyiapkan lingkungan pengujian, seperti instalasi OWASP ZAP, pengaturan proxy pada browser, serta koneksi jaringan agar proses analisa dapat berjalan optimal.

3. Observasi Lalu Lintas HTTP/HTTPS (Passive Scanning)

   Melakukan eksplorasi manual pada website menggunakan browser yang telah terhubung ke OWASP ZAP. Selama proses ini, OWASP ZAP secara otomatis melakukan passive scan untuk mendeteksi potensi celah keamanan tanpa mengganggu sistem target.

4. Melakukan Active Scanning

   Setelah proses penjelajahan dilakukan, dilanjutkan dengan active scan untuk menguji kerentanan secara langsung menggunakan teknik otomatis yang disediakan oleh OWASP ZAP, seperti injection, authentication test, maupun path traversal.

5. Pencatatan dan Dokumentasi Hasil

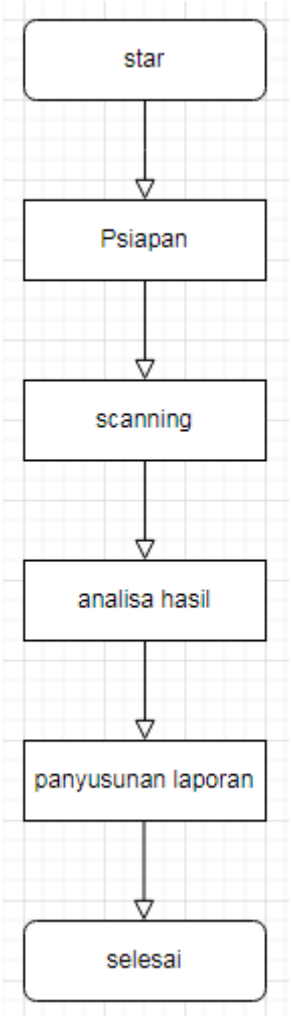
   Semua hasil yang ditemukan selama proses scanning, termasuk jenis kerentanan, level risiko, URL yang terdampak, dan rekomendasi perbaikan, dicatat secara otomatis oleh OWASP ZAP dan diekspor ke dalam bentuk laporan (format HTML/PDF).

6. Analisis Data

   Data hasil scanning dianalisis untuk menilai tingkat keamanan website. Analisa mencakup jenis dan jumlah kerentanan, serta tingkat risiko yang dihadapi oleh sistem web berdasarkan hasil OWASP ZAP.

Metode ini mendukung proses evaluasi keamanan web secara menyeluruh dengan pendekatan teknis dan berbasis tools, sehingga dapat memberikan hasil yang objektif dan terukur.

4.1.3 Proses Perancangan



Gambar 4.1 Flow Chart Proses Perancangan

Berikut ini adalah penjelasan dari setiap tahapan dalam flowchart di atas:

1. Star

   Ini adalah titik awal dari proses. Menandakan bahwa alur kerja akan dimulai dari sini.

2. Persiapan

   Tahap persiapan di mana semua bahan dan alat yang diperlukan untuk proses

selanjutnya disiapkan. Ini bisa meliputi pengumpulan informasi, perencanaan, dan pengaturan sumber daya.

3. Scanning

   Pada tahap ini, data atau objek yang menjadi fokus dianalisis atau dipindai. Ini bisa berarti memindai dokumen, gambar, atau bahkan perangkat keras.

4. Analisa Hasil

   Setelah proses scanning, hasil yang didapat perlu dianalisis. Di sini, informasi yang diperoleh dievaluasi untuk menentukan langkah selanjutnya atau untuk mengidentifikasi masalah yang perlu diperbaiki.

5. Penyusunan Laporan

   Berdasarkan analisis yang dilakukan, laporan disusun untuk mendokumentasikan temuan dan rekomendasi. Laporan ini penting untuk komunikasi hasil kepada pihak terkait.

6. Selesai

   Ini adalah tahap akhir di mana tindakan perbaikan dilakukan berdasarkan hasil analisis dan laporan. Pada titik ini, lampu yang bermasalah akan diperbaiki.

Setiap tahap memiliki peran penting dalam memastikan proses dapat berjalan dengan lancar seperti yang di inginkan

4.1.4 Tahapan dan Jadwal Pelaksanaan

Adapun jadwal pelaksanaan yang dilakukan selama penetrartion testing aplikasi pelaporan insiden siber dapat dilihat dari tabel berikut:

No	Uraian Kegiatan	Bulan																	
		Maret			April				Mei				Juni				Juli		
		2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	
1.	Planning																		
2.	Scanning																		
3.	Analisa																		
4.	Pelaporan																		

Gambar 4.2 Tahap Jadwal Pelaksanaan

4.2 Perancangan dan Implementasi

1. Mulai

Melakukan pencarian terhadap website yang akan di analisa sesuai arahan yang telah di berikan oleh pembimbing lapangan selama magang kerja praktek yang di lakukan.

2. Persiapan

Mempersiapkan tools yang yang akan di gunakan yaitu owasp zap untuk melakukan analisa keamanan website, menentukan target domain yang akan di analisa dan membuat rencana penyusunan laporan hasil dari analisa website yang di berikan.

3. Memindai

- Tujuan : Mengumpulkan data potensi kerentanan dan permukaan

serangan website.

- Langkah-langkah :
    - Menggunakan Subfinder untuk menemukan subdomain aktif Pekanbaru.go.id (ditemukan 242 subdomain).
    - Menggunakan Nmap untuk mengkodekan port terbuka dan layanan aktif pada domain utama dan subdomain.
    - Menggunakan OWASP ZAP (Passive Scan) untuk mengidentifikasi kelemahan seperti keamanan header, cookie, clickjacking, dan protokol HTTP/HTTPS.
    - Mencatat semua hasil pemindaian secara terstruktur.

4. Analisa Hasil

- Tujuan : Mengevaluasi dan mengelompokkan temuan berdasarkan tingkat risiko serta memberikan pemahaman teknis terhadap hasil scan.
- Langkah-langkah :
    - Mengelompokkan hasil ke dalam kategori risiko: Sedang, Rendah, Informasional.
    - Menganalisis kerentanan seperti Tidak adanya keamanan header (CSP, X- Frame-Options, HSTS, dll), Cookie yang tidak aman, Server informasi yang terekspos.
    - Menyusun tabel temuan untuk memudahkan pembacaan dampak dan solusi teknis.
    - Menyadari bahwa kegiatan terbatas hanya pada scanning pasif tanpa eksploitasi langsung .

5. Penyusunan Laporan

- Tujuan : Menyusun laporan praktik kerja yang sistematis, mencakup seluruh temuan dan rekomendasi.

- Langkah-langkah :
    - Menyusun ringkasan alat yang digunakan dan tujuan masing-masing.
    - Menyusun hasil temuan dalam bentuk tabel kerentanan (tingkat risiko, penyebab, dampak, dan solusi).
    - Menambahkan interpretasi dari hasil scanning Nmap dan Subfinder terkait peta permukaan serangan dan layanan yang terbuka.
    - Membuat kesimpulan umum dan saran perbaikan dari sisi keamanan informasi.
    - Membaca laporan dapat dipahami oleh pihak non-teknis dan teknis.

6. Selesai
    - Proses praktik kerja dianggap selesai setelah seluruh rangkaian pemindaian, analisa, dan penyusunan laporan selesai dilakukan, dan laporan siap dipresentasikan.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan kegiatan scanning keamanan yang dilakukan secara mandiri selama masa kerja praktek menggunakan beberapa tools seperti OWASP ZAP, Nmap, dan Subfinder terhadap domain utama pekanbaru.go.id beserta subdomain-nya, diperoleh beberapa temuan penting terkait potensi kerentanan sistem.

1. Jumlah Subdomain Teridentifikasi

   Sebanyak 242 subdomain berhasil ditemukan, dengan sebagian di antaranya aktif dan dapat diakses publik. Beberapa subdomain ini menunjukkan akses ke lingkungan internal atau uji coba yang belum diamankan secara optimal.

2. Temuan Kerentanan dari OWASP ZAP

   Dari hasil pemindaian OWASP ZAP, ditemukan beberapa kelemahan keamanan yang tergolong dalam tingkat Medium hingga Low, antara lain:

   - Tidak adanya header Content Security Policy (CSP).
   - Form input yang belum sepenuhnya aman dari transisi HTTP ke HTTPS.
   - Header keamanan penting seperti Strict-Transport-Security, X-Content-Type- Options, dan HTTPOnly Cookie belum diterapkan.

3. Hasil Nmap Scan

   Pemindaian port dengan Nmap menunjukkan sejumlah port terbuka yang bervariasi dari port standar (80, 443) hingga port tidak umum. Banyaknya port terbuka dapat menjadi celah yang dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan eksploitasi lebih lanjut.

4. Penerapan Keamanan Masih Kurang Konsisten

Beberapa subdomain tidak menggunakan protokol HTTPS, atau tidak menampilkan header keamanan dasar. Hal ini mengindikasikan kurangnya konsistensi dalam pengelolaan standar keamanan antar subdomain.

5.2 Saran

1. Penerapan Keamanan Berbasis Header

Disarankan agar seluruh subdomain dan domain utama menerapkan header keamanan standar seperti CSP, HSTS, X-Frame-Options, X-Content-Type-Options, dan pengaturan Cookie HTTPOnly serta Secure untuk mencegah eksploitasi berbasis web.

2. Pembatasan Akses ke Lingkungan Internal/Uji Coba

Subdomain yang digunakan untuk pengujian atau pengembangan sebaiknya tidak diakses publik atau dilindungi dengan autentikasi, serta disaring melalui firewall.

3. Audit dan Pemantauan Berkala

Pemerintah Kota Pekanbaru melalui Dinas Kominfo perlu menjadwalkan audit keamanan secara berkala terhadap seluruh aset digital, baik domain utama maupun subdomain, guna memastikan tidak ada celah keamanan baru yang muncul.

4. Penerapan Manajemen Subdomain

Penting untuk memiliki kontrol dan dokumentasi terhadap seluruh subdomain yang dimiliki, termasuk siapa yang mengelola, fungsinya, dan status keamanannya.

5. Peningkatan Kapasitas SDM Keamanan

Perlu dilakukan pelatihan dan peningkatan kesadaran kepada pengelola web atau admin OPD terkait standar dan praktik keamanan siber untuk memastikan website pemerintah tetap aman digunakan masyarakat.

DAFTAR PUSTAKA

[1] Dinas Komunikasi Informatika Statistik dan Persandian, Profil Instansi. Pekanbaru: Pemerintah Kota Pekanbaru, 2023.

LAMPIRAN

- Surat Keterangan (dari Perusahaan)

PEMERINTAH KOTA PEKANBARU
DINAS KOMUNIKASI INFORMATIKA
STATISTIK DAN PERSANDIAN
Jalan Abdul Rahman Hamid Kel. Tuah Negeri Kec. Tenayan Raya
Pekanbaru 20289

SURAT KETERANGAN
NOMOR: B.400.14.5.4/Kominfo-SPBE/59/2025

Berdasarkan Surat dari Politeknik Negeri Bengkalis Nomor: 1329/PL31/TU/2025 tanggal 5 Maret 2025 terkait Permohonan Kerja Praktik (KP).

Kepala Dinas Komunikasi Informatika Statistik dan Persandian Kota Pekanbaru dengan ini menyatakan bahwa:

Nama : YUDI
NIM : 6404211084
Program Studi : KEAMANAN INFORMASI
Jenjang : D-IV

Mahasiswa tersebut di atas benar telah melakukan Kerja Praktik (KP) pada Bidang Persandian Aplikasi dan Tata Kelola SPBE Dinas Komunikasi Informatika Statistik dan Persandian Kota Pekanbaru pada tanggal 10 Maret s/d 10 Juli 2025.

Demikian surat keterangan ini diberikan agar dapat dipergunakan sebagaimana mestinya.

Pekanbaru, 11 Juli 2025

Ditandatangani Secara Elektronik Oleh:
Plt. Kepala Dinas Komunikasi
Informatika Statistik dan Persandian

DENI HIDAYAT, ST, MM
NIP. 197801062005011003

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Besar Sertifikasi Elektronik (BSrE), Badan Siber dan Sandi Negara

- Surat Balasan diterima magang pada perusahaan

PEMERINTAH KOTA PEKANBARU
DINAS KOMUNIKASI INFORMATIKA STATISTIK DAN PERSANDIAN
Komp. Perkantoran Walikota Pekanbaru Lt. III
Jalan Abdul Rahman Hamid Kel. Tuah Negeri Kec. Tenayan Raya
P E K A N B A R U - 28285

Pekanbaru, 10 Maret 2025

Nomor : B.400.7.22.1/KOMINFO-SEKRE/
Lampiran : 15/2025
Hal :
Kerja Praktik (KP)

Yth. Kepada
a.n Direktur,
Wakil Direktur III
di –
Tempat

Dengan Hormat,

Menindaklanjuti surat dari Politeknik Negeri Bengkalis nomor : 1329/PL31/TU/2025 tanggal 5 Maret 2025. Perihal Kerja Praktik (KP), dapat diinformasikan bahwa :

No	Nama Mahasiswa	NIM	Program Studi
1	Yudi	6404211084	D-IV Keamanan Sistem Informasi
2	Hadit Billa Darma Pane	6404211070	D-IV Keamanan Sistem Informasi

Dapat melaksanakan Kerja Praktik (KP) di lingkungan Dinas Komunikasi Informatika Statistik dan Persandian Kota Pekanbaru terhitung mulai 10 Maret 2025 s/d 10 Juli 2025.

Demikian disampaikan, atas perhatiannya diucapkan terima kasih.

Ditandatangani Secara Elektronik Oleh:
Plt. Kepala Dinas Komunikasi Informatika Statistik dan Persandian

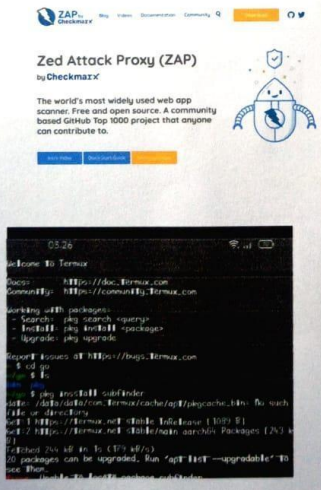
FIRMAN HADI, S.STP., M.Si
NIP. 19861109200412100l

Tembusan :
1. *Yang Bersangkutan*
2. *Arsip*

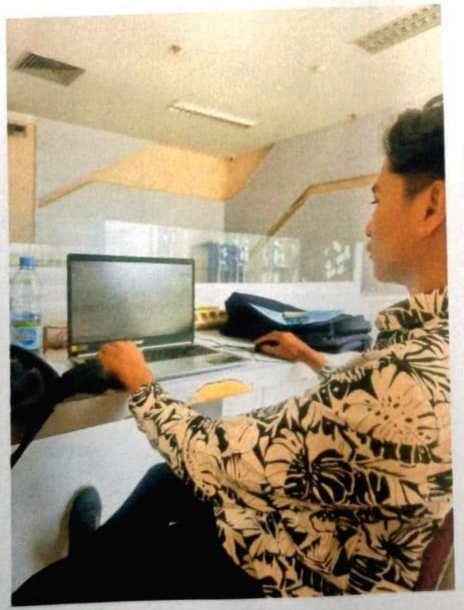
- Log Harian/Mingguan yang telah diparaf

KEGIATAN MINGGUAN
KERJA PRAKTEK (KP)

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Persiapan tools untuk melakukan scanning website pekanbaru.go.id	Muhammad Reza	
	Catatan Pembimbing Industri 10 – 16 Maret		

No	GAMBAR KERJA	KETERANGAN
		Persiapan tools (instalasi Termux, Nmap, OWASP ZAP, Subfinder)

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Penyusunan akhir laporan kp	Muhammad Reza	
	Catatan Pembimbing Industri 30 Juni – 4 Juli 2025		

No	GAMBAR KERJA	KETERANGAN
		Penyusunan akhir dokumen laporan KP

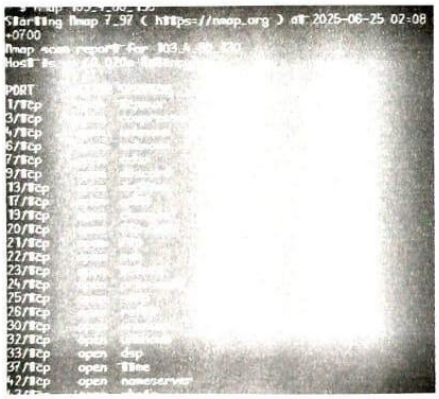
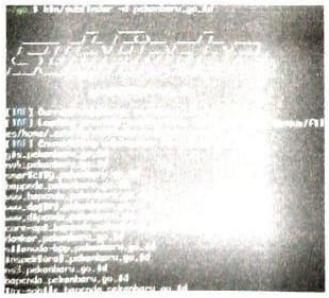
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Penulisan kesimpulan dari hasil temuan yang telah di dapatkan dari hasil scanning	Muhammad Reza	
	Catatan Pembimbing Industri 23-27 Juni 2025		

No	GAMBAR KERJA	KETERANGAN
	BAB V **PENUTUP** **5.1. Kesimpulan** Berdasarkan kegiatan scanning keamanan yang dilakukan secara mandiri selama masa kerja praktek menggunakan beberapa tools seperti OWASP ZAP, Nmap, dan Subfinder terhadap domain utama pekanbaru.go.id beserta subdomain-nya, diperoleh beberapa temuan penting terkait potensi kerentanan sistem. 1. Jumlah Subdomain Teridentifikasi Sebanyak 242 subdomain berhasil ditemukan, dengan sebagian di antaranya aktif dan dapat diakses publik. Beberapa subdomain ini menunjukkan akses ke lingkungan internal atau uji coba yang belum diamankan secara optimal. 2. Temuan Kerentanan dari OWASP ZAP Dari hasil pemindaian OWASP ZAP, ditemukan beberapa kelemahan keamanan yang tergolong dalam tingkat Medium hingga Low, antara lain: ▪ Tidak adanya header Content Security Policy (CSP). ▪ Form input yang belum sepenuhnya aman dari transisi HTTP ke HTTPS. ▪ Header keamanan penting seperti Strict-Transport-Security, X-Content-Type-Options, dan HTTPOnly Cookie belum diterapkan. 3. Hasil Nmap Scan Pemindaian port dengan Nmap menunjukkan sejumlah port terbuka yang bervariasi dari port standar (80, 443) hingga port tidak umum. Banyaknya port terbuka dapat menjadi celah yang dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan eksploitasi lebih lanjut. 4. Penerapan Keamanan Masih Kurang Konsisten	Penulisan kesimpulan dan saran

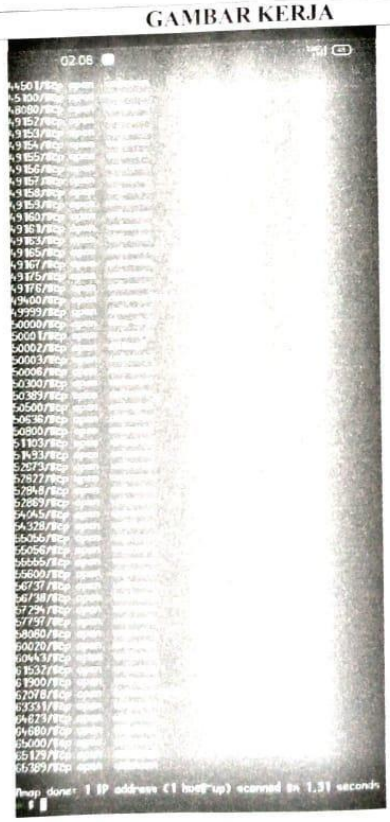
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Persiapan mendowload tools owasp zap untuk melakukan scanning	Muhammad Reza	
	Catatan Pembimbing Industri 5-9 Mei 2025		

No	GAMBAR KERJA	KETERANGAN
		Persiapan tools OWASP ZAP

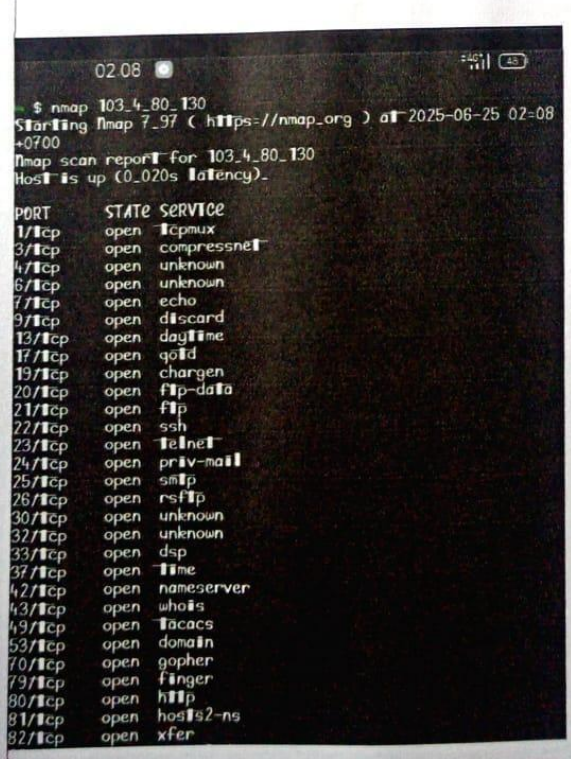
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Dokumentasikan hasil dari scanning website	Muhammad Reza	
	Catatan Pembimbing Industri 26-28 Mei 2025		

No	GAMBAR KERJA	KETERANGAN
	 	Dokumentasi hasil Nmap & Subfinder

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Melakukan identifikasi potensi kerentanan dari hasil temuan scanning nmap	Muhammad Reza	
	Catatan Pembimbing Industri 28 April – 2 Mei 2025		

No	GAMBAR KERJA	KETERANGAN
		Identifikasi potensi kerentanan layanan dari hasil Nmap

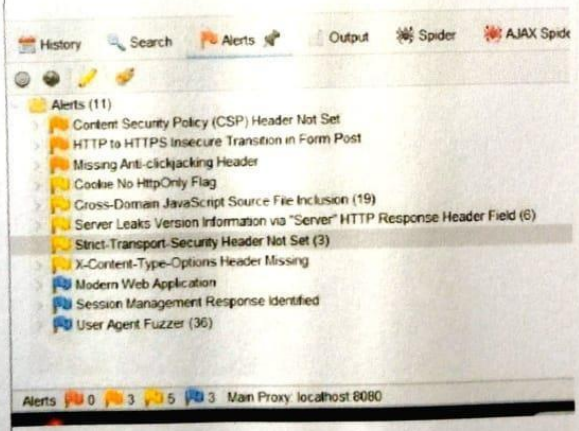
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Scanning menggunakan tools nmap untuk mengetahui port yang terbuka	Muhammad Reza	
	Catatan Pembimbing Industri 14-18 April 2025		

No	GAMBAR KERJA	KETERANGAN
		Scanning port dan service menggunakan Nmap

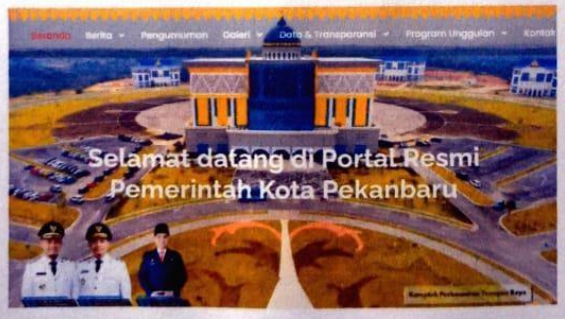
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Penyapaian hasil laporan yang telah di buat selama kuliah praktek dan perpisahan/penutupan kuliah praktek dengan instansi yang ada	Muhammad Reza	
	Catatan Pembimbing Industri 7-10 Juli 2025		

No	GAMBAR KERJA	KETERANGAN
		Penyampaian laporan akhir ke instansi **Penutupan kegiatan kerja praktek**

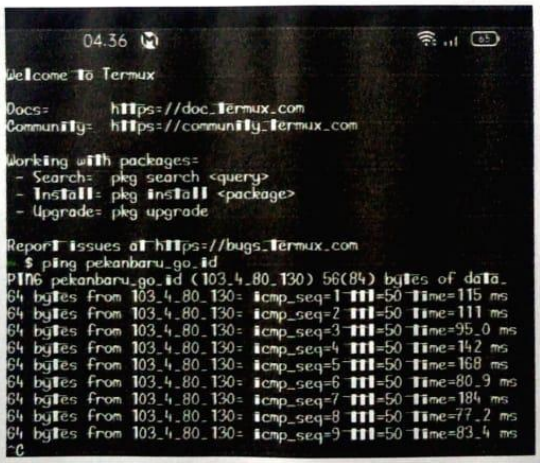
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Melakukan analisa dari kategori low, medium, informational yang di temukan	Muhammad Reza	
	Catatan Pembimbing Industri 19-23 Mei 2025		

No	GAMBAR KERJA	KETERANGAN
		Kategorisasi risiko berdasarkan severity (Low, Medium, Informational)

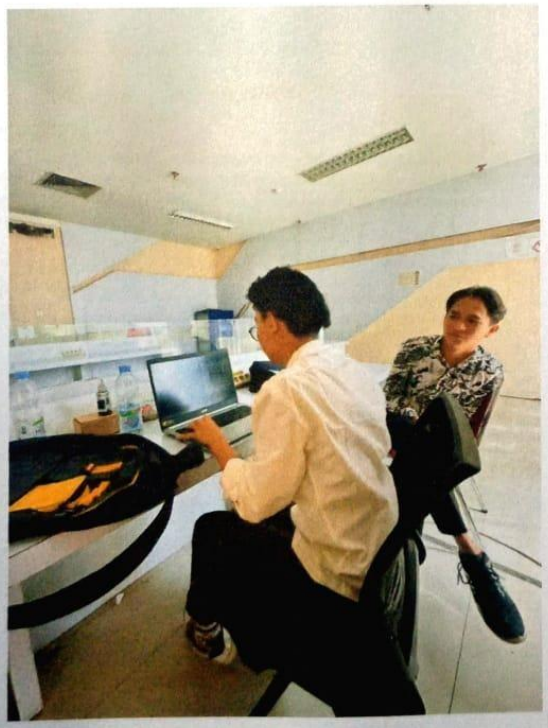
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Proses pengenalan atau pencarian target scanning	Muhammad Reza	
	Catatan Pembimbing Industri 17-21 maret 2025		

No	GAMBAR KERJA	KETERANGAN
		Pengenalan target domain

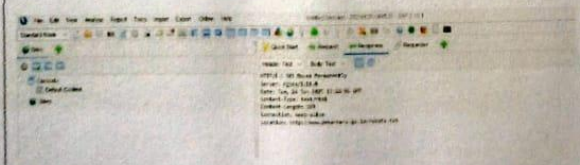
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Menganalisa hasil scanning sub domain yang di temukan	Muhammad Reza	
	Catatan Pembimbing Industri 7-11 April 2025		

No	GAMBAR KERJA	KETERANGAN
		Verifikasi subdomain aktif (ping, curl, HTTP check)

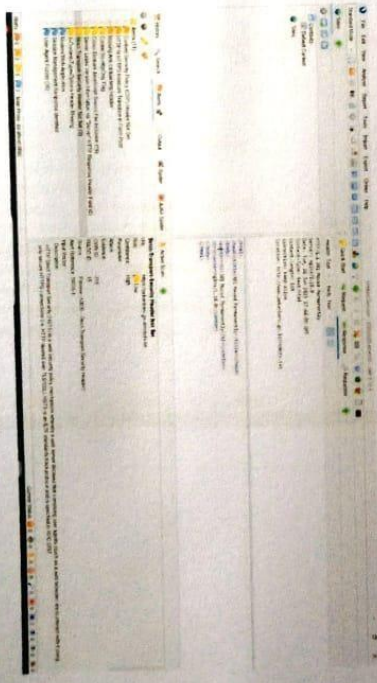
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Mulai menyusun laporan hasil scanning yang telah di lakukan	Muhammad Reza	
	Catatan Pembimbing Industri 16-20 Juni 2025		

No	GAMBAR KERJA	KETERANGAN
		Mulai penyusunan laporan kerja praktek bagian **pendahuluan dan tinjauan pustaka**

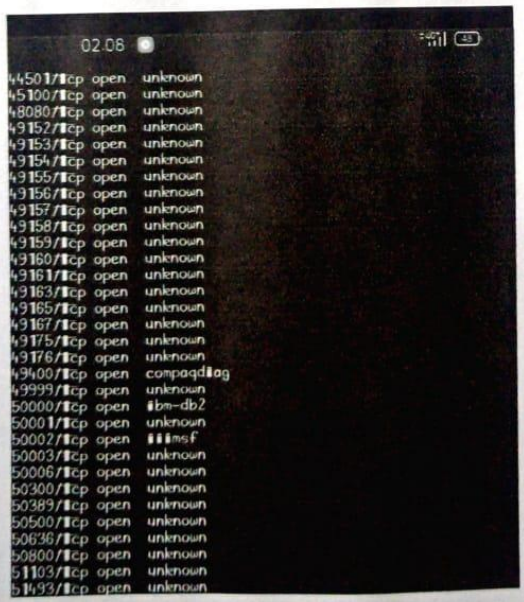
No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Mulai melakukan scanning pada website target	Muhammad Reza	
	Catatan Pembimbing Industri 24-28 Maret 2025		

No	GAMBAR KERJA	KETERANGAN
		Mulai scanning subdomain Pekanbaru.go.id

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Melakukan scanning menggunakan owasp zap	Muhammad Reza	
	Catatan Pembimbing Industri 12-16 Mei 2025		

No	GAMBAR KERJA	KETERANGAN
		Mulai passive scanning domain

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Melakukan analisis port yang terbuka dari hasil scanning yang di temukan	Muhammad Reza	
	Catatan Pembimbing Industri 21-25 April 2025		

No	GAMBAR KERJA	KETERANGAN
		Analisis port terbuka dan identifikasi layanan

No	URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1.	Revew ulang hasil temuan yang telah di dapat untuk memastikan keakuratan data	Muhammad Reza	
	Catatan Pembimbing Industri 10-13 Juni 2025		

No	GAMBAR KERJA	KETERANGAN
		Review & verifikasi ulang hasil scanning

- Form Penilaian dari Perusahaan

PENILAIAN DARI PERUSAHAAN KERJA PRAKTEK
Dinas Komunikasi, Informatika, Statistik, Dan Persandian
Kota Pekanbaru

Nama : Yudi
NIM : 6404211084
Program Studi : Keamanan Sistem Informasi
Politeknik Negeri Bengkalis

No.	Aspek Penilaian	Bobot	Nilai
1	Disiplin	20%	19
2	Tanggung- jawab	25%	24
3	Penyesuaian diri	10%	9
4	Hasil Kerja	30%	28
5	Perilaku secara umum	15%	14
	Total Jumlah (1+2+3+4+5) 100%		94

Keterangan :
Nilai : Kriteria
81 – 100 : Istimewa
71 – 80 : Baik sekali
66 – 70 : Baik
61 – 65 : Cukup Baik
56 – 60 : Cukup

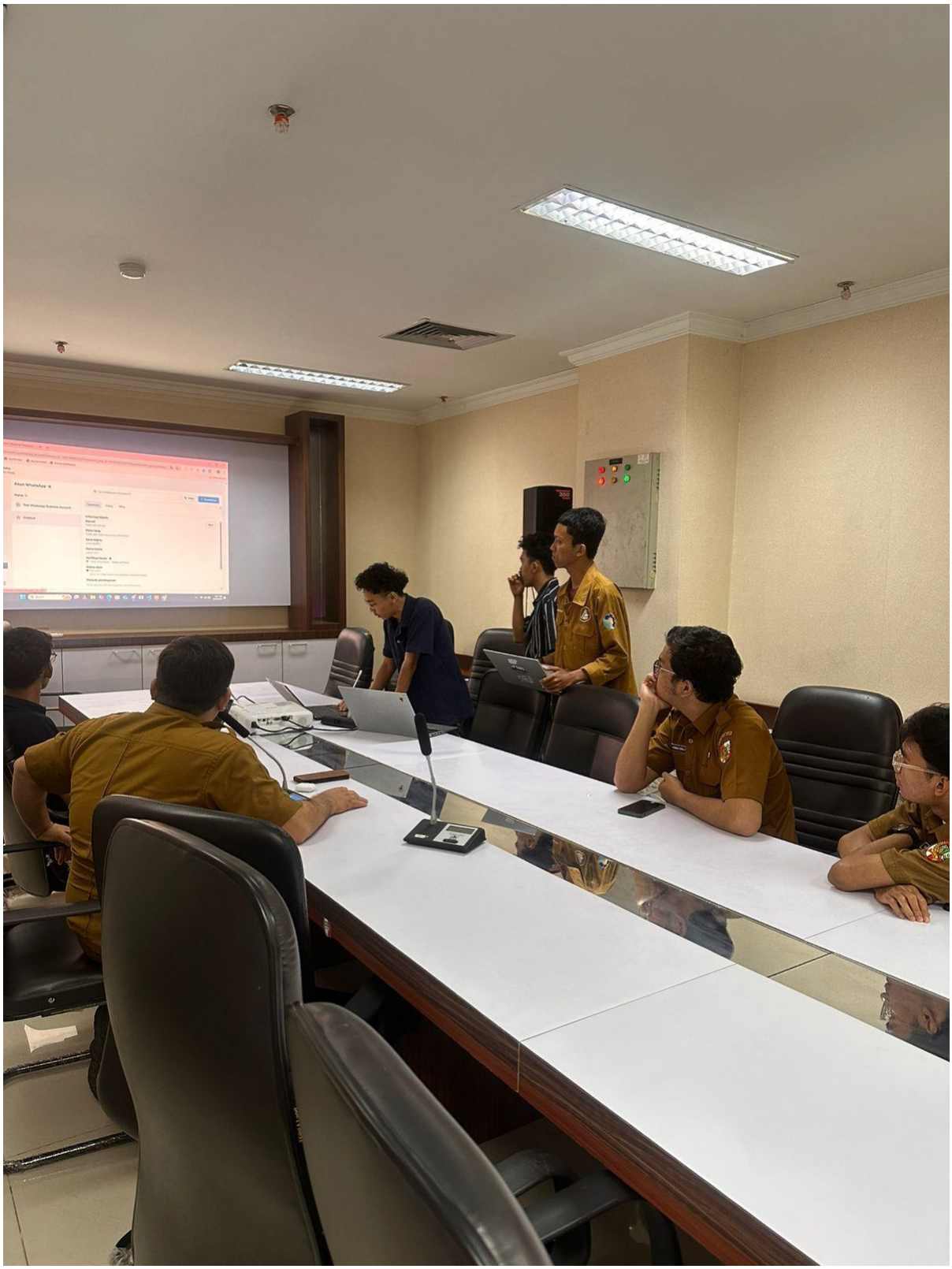
Catatan :
.....
.....
.....
.....

Pekanbaru, 10 Juli 2025

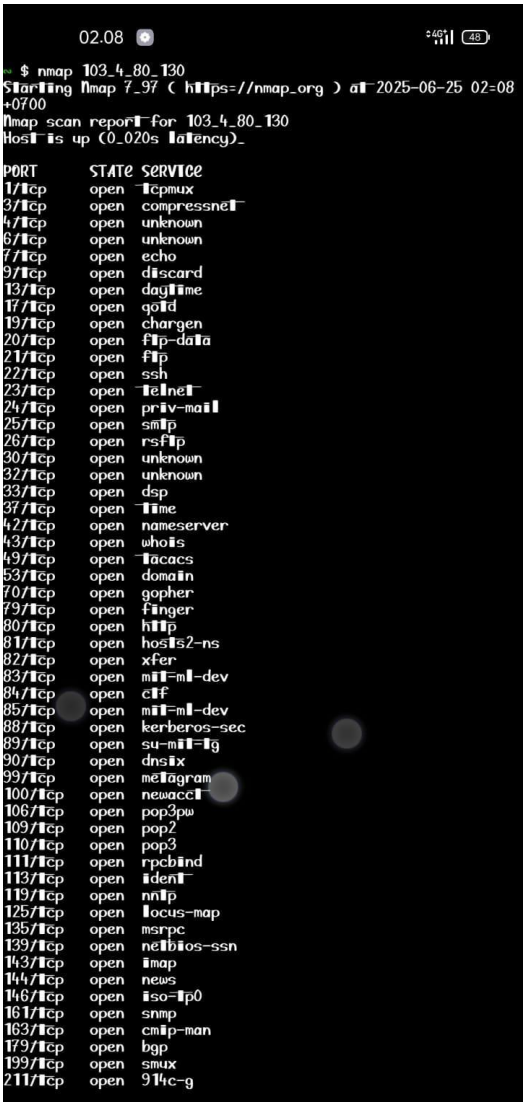
Muhammad Reza
Analis Sistem Informasi

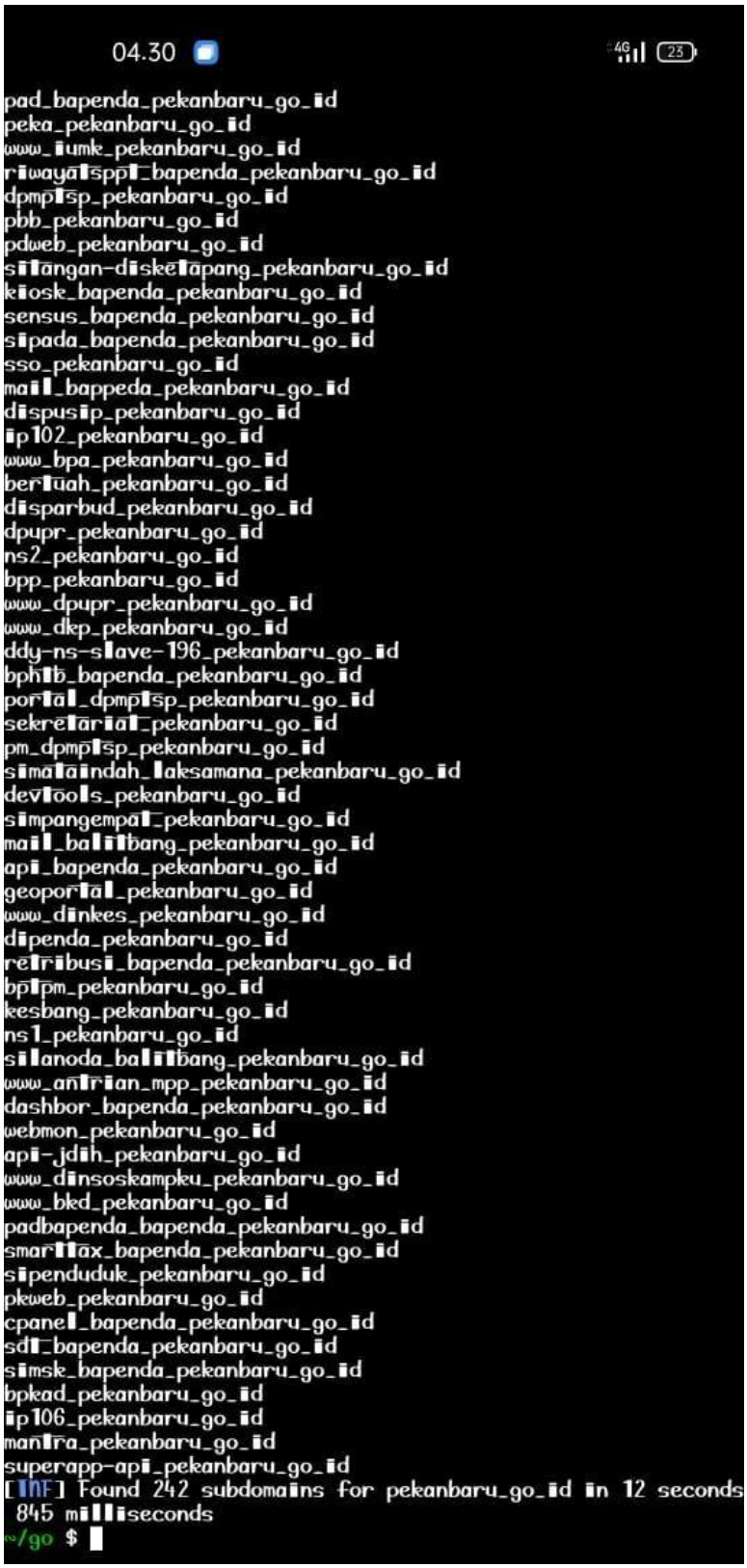
Dokumentasi Evaluasi dan Implementasi Project

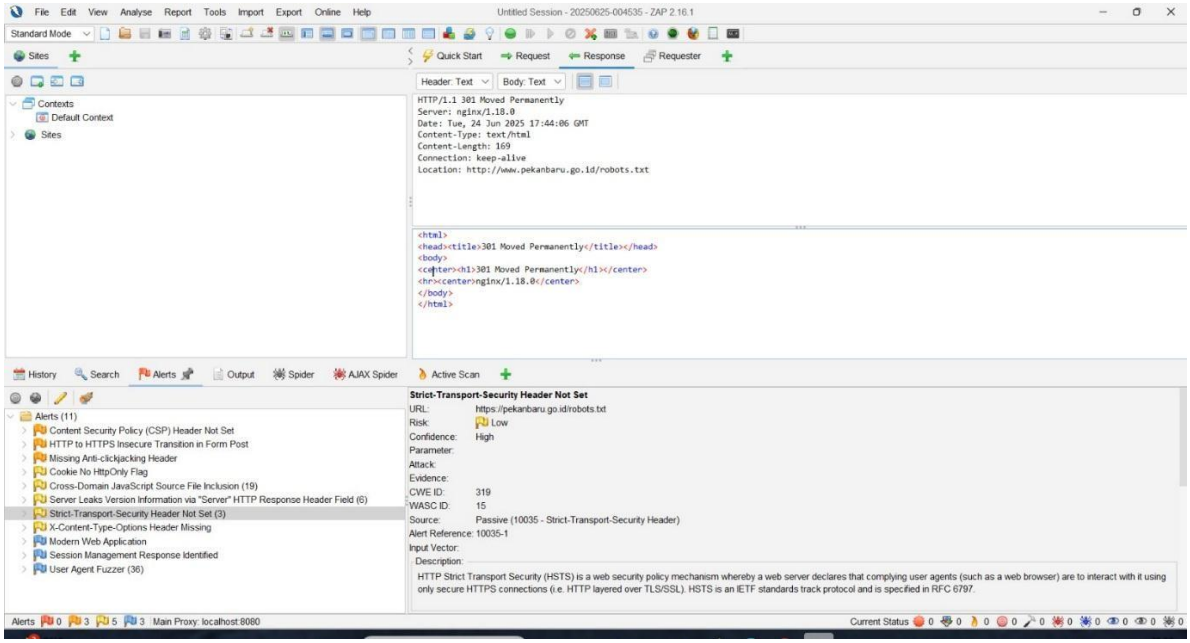

Le Minerale



- Dokumen lainnya yang berhubungan dengan KP




04.30
pad_bapenda_pekanbaru_go_id
peka_pekanbaru_go_id
www_iumk_pekanbaru_go_id
riwayatspptbapenda_pekanbaru_go_id
dpmptsp_pekanbaru_go_id
pbb_pekanbaru_go_id
pdweb_pekanbaru_go_id
silangan-diskelapang_pekanbaru_go_id
kiosk_bapenda_pekanbaru_go_id
sensus_bapenda_pekanbaru_go_id
sipada_bapenda_pekanbaru_go_id
sso_pekanbaru_go_id
mail_bappeda_pekanbaru_go_id
dispusip_pekanbaru_go_id
ip102_pekanbaru_go_id
www_bpa_pekanbaru_go_id
berituah_pekanbaru_go_id
disparbud_pekanbaru_go_id
dpupr_pekanbaru_go_id
ns2_pekanbaru_go_id
bpp_pekanbaru_go_id
www_dpupr_pekanbaru_go_id
www_dkp_pekanbaru_go_id
ddy-ns-slave-196_pekanbaru_go_id
bphtb_bapenda_pekanbaru_go_id
portal_dpmptsp_pekanbaru_go_id
sekretariat_pekanbaru_go_id
pm_dpmptsp_pekanbaru_go_id
simalaindah_laksamana_pekanbaru_go_id
devtools_pekanbaru_go_id
simpangempat_pekanbaru_go_id
mail_balaibang_pekanbaru_go_id
api_bapenda_pekanbaru_go_id
geoportal_pekanbaru_go_id
www_dinkes_pekanbaru_go_id
dipenda_pekanbaru_go_id
retribusi_bapenda_pekanbaru_go_id
bptpm_pekanbaru_go_id
kesbang_pekanbaru_go_id
ns1_pekanbaru_go_id
silanoda_balaibang_pekanbaru_go_id
www_antrian_mpp_pekanbaru_go_id
dashbor_bapenda_pekanbaru_go_id
webmon_pekanbaru_go_id
api-jdih_pekanbaru_go_id
www_dinsoskampku_pekanbaru_go_id
www_bkd_pekanbaru_go_id
padbapenda_bapenda_pekanbaru_go_id
smartax_bapenda_pekanbaru_go_id
sipenduduk_pekanbaru_go_id
pkweb_pekanbaru_go_id
cpanel_bapenda_pekanbaru_go_id
sdt_bapenda_pekanbaru_go_id
simsk_bapenda_pekanbaru_go_id
bpkad_pekanbaru_go_id
ip106_pekanbaru_go_id
mantra_pekanbaru_go_id
superapp-api_pekanbaru_go_id
[INF] Found 242 subdomains for pekanbaru_go_id in 12 seconds
845 milliseconds
~/go $


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20250625-004535 - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 301 Moved Permanently
Server: nginx/1.18.0
Date: Tue, 24 Jun 2025 17:44:06 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: http://www.pekanbaru.go.id/robots.txt
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<h1>301 Moved Permanently</h1>
<hr> nginx/1.18.0
</body>
</html>
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Alerts (11)
Content Security Policy (CSP) Header Not Set
HTTP to HTTPS Insecure Transition in Form Post
Missing Anti-clickjacking Header
Cookie No HttpOnly Flag
Cross-Domain JavaScript Source File Inclusion (19)
Server Leaks Version Information via "Server" HTTP Response Header Field (6)
Strict-Transport-Security Header Not Set (3)
X-Content-Type-Options Header Missing
Modern Web Application
Session Management Response Identified
User Agent Fuzzer (36)
Strict-Transport-Security Header Not Set
URL: https://pekanbaru.go.id/robots.txt
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 319
WASC ID: 15
Source: Passive (10035 - Strict-Transport-Security Header)
Alert Reference: 10035-1
Input Vector:
Description:
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Alerts 0 3 5 3 Main Proxy: localhost:8080
Current Status