LAPORAN KERJA PRAKTEK
DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK
PROVINSI RIAU

MELAKUKAN UJI PENETRASI PADA WEBSITE PELAPORAN INSIDEN SIBER MENGGUNAKAN SERANGAN SQL INJECTION

ANGGUN FITRIYANI

6404201018

PROGRAM STUDI KEAMANAN SISTEM INFORMASI

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BENGKALIS

2024

LEMBAR PENGESAHAN
LAPORAN KERJA PRAKTEK
DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK
PROVINSI RIAU

Jl. Diponegoro Nomor 24 A, Kec. Pekanbaru Kota, Kota Pekanbaru, Riau 28127
25 Maret 2024-19 Juli 2024
Ditulis sebagai salah satu syarat untuk menyelesaikan kerja praktek

ANGGUN FITRIYANI
6404201017

Pekanbaru, 19 Juli 2024

Pembimbing Magang

Tiara Mulia Putri, S.Kom
NIP. 19870505 201903 2 001

Dosen Pembimbing Keamanan Sistem Informasi

Mansur, M.Kom
NIP. 198209192021211003

Disetujui
Ketua Program Studi Keamanan Sistem Informasi
Politeknik Negeri Bengkalis

Juroji, M.Kom
NIP. 198611072015041002

KATA PENGANTAR

Puji syukur kepada Allah swt berkat rahmat, hidayah dan karunia-nya penulis dapat menyelesaikan laporan ini dengan baik dan tepat pada waktunya. Dalam laporan ini akan membahas mengenai Kerja Peraktek (KP) yang dilakukan dikantor Dinas Komunikasi, Informatika dan Statistik Provinsi Riau.

Penulis menyadari dalam penyusunan laporan ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karna itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada:

1. Bapak Johny Custer, S.T., M.T selaku Direktur Politeknik Negeri Bengkalis.
2. Bapak Kasmawi, M.Kom, selaku Ketua Jurusan Teknik Informatika Politeknik Negeri Bengkalis.
3. Bapak Jaroji, M.Kom, selaku Ketua Program Studi Keamanan Sistem Informasi Politeknik Negeri Bengkalis.
4. Ibuk Rezki Kurniati, M.Kom, selaku Koordinator Kerja Praktek Program Studi Keamanan Sistem Informasi.
5. Bapak Mansur, M.Kom selaku Dosen Pembimbing Kerja Praktek Politeknik Negeri Bengkalis.
6. Bapak Candra Lisano Putra, S.T selaku Kepala Bidang Pesandian Diskominfotik Provinsi Riau.
7. Bunda T. Nova Sukma, ST, MM selaku Pengawas Lapangan Kerja Praktek Diskominfotik Provinsi Riau.
8. Mbak Tiara Mulia Putri, S.Kom selaku Pembimbing Lapangan Kerja Praktek Diskominfotik Provinsi Riau.
9. Bang Roy selaku mentor Lapangan Kerja Praktek Diskominfotik Provinsi Riau yang telah membimbing kami.
10. Kak Debie, Kak Ika, dan Bang Yogi, selaku senior dan rekan kerja di lapangan.
11. Kedua Orang Tua yang telah mensupport dan memberikan doa restunya di setiap langkah dan tujuan.

Penulis merasa bersyukur karena telah diterima melakukan Kerja Praktek di Dinas Komunikasi Informatika dan Statistik Provinsi Riau, karena adanya pelaksanaan Kerja Praktek ini penulis mendapat kesempatan untuk meningkatkan keterampilan dan menerapkan ilmu pengetahuan yang diajarkan dibangku kuliah dalam dunia pekerjaan secara nyata dan menanamkan prilaku yang baik dalam pekerjaan.

Penulis mengucapkan permohonan maaf kepada semua pihak yang terlibat jika terdapat kesalahan dan kesilapan selama proses Kerja Praktek berlangsung, baik kesalahan yang disengaja maupun tidak disengaja, baik bersifat rohani maupun jasmani. Penulis juga menyadari laporan ini tidak luput dari berbagai kesalahan dan kekurangan. Penulis mengharapkan saran dan kritik yang membangun demi kesempurnaan dan perbaikannya sehingga akhirnya laporan Kerja Praktek ini dapat memberikan manfaat bagi pembaca.

Bengkalis, 21 April 2024

Anggun Fitriyani

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kerja praktek adalah cara bagi mahasiswa untuk mendapatkan pengalaman kerja nyata saat masih kuliah. Selama kerja praktek, mahasiswa akan belajar tentang sistem kerja perusahaan dan perancangan proyek dengan terlibat langsung dalam proyek yang dikerjakan oleh perusahaan tempat mereka bekerja. Melalui kerja praktek ini, mahasiswa diharapkan dapat memahami proses kerja, mulai dari manajemen perusahaan, perancangan, hingga sistem komunikasi dalam proyek. Pengalaman ini akan menjadi bekal berharga bagi mahasiswa ketika memasuki dunia kerja setelah lulus[1].

Keamanan Sistem Informasi adalah program strudi yang mempelajari tentang bagaimana cara memproteksi berbagai industri dan pemerintahan dari serangan yang ada di dunia maya atau cyber attack. Program studi yang satu ini dirancang secara khusus untuk membekali mahasiswa dengan pengetahuan dan juga keahlian dalam pengujian, perancangan, dan juga implementasi pertahanan dalam dunia maya. Keamanan Sistem Informasi mempunyai dasar yang kuat pada komputer sains dan teori serta kemampuan berpikir kritis tentang teknologi dunia maya masa kini. Adanya perkembangan internet yang sangat pesat di zaman modern ini membuat sistem keamanan dalam dunia maya juga semakin terancam dengan berbagai aktivitas para hacker. Sehingga Keamanan Sistem Informasi ini sangat diperlukan untuk Cyber Defense atau pertahanan dunia maya. Disini, para mahasiswa akan belajar untuk membuat berbagai proyek yang memerlukan kolaborasi dengan industri dan pemerintah serta membantu mahasiswa untuk mengeksplorasi berbagai ancaman di dunia maya dan membentuk sistem pertahanannya[2].

Dinas Komunikasi Informatika dan statistik (Diskominfotik) Provinsi Riau merupakan salah satu instansi yang memiliki topuksi kerja yang luas. Tugas yang meliputi bidang informasi, statistik, pengelolaan data elektronik,

urusan publikasi dan kerjasama media urusan public relation. Diskominfotik Provinsi Riau juga memberikan kesempatan untuk siswa dan mahasiswa Kerja Praktek (KP), guna meningkatkan mutu dan wawasan yang dimiliki. Disamping itu selain melaksanakan Kerja Praktek (KP) pada instansi, Diskominfo Provinsi Riau juga memberikan tugas sesuai profesi bidang studi yang digeluti siswa dan mahasiswa yang melaksanakan kerja praktek.

Dalam pelaksanaan Kerja Praktek di Kantor Diskominfotik Provinsi Riau penulis mendapatkan tugas untuk melakukan pentest dengan serangan SQL Injection pada sebuah website pelaporan insiden siber.

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. Memudahkan para staff/publik untuk melakukan pelaporan agar cepat ditindaklanjuti insiden siber yang terjadi.
5. Sebagai salah satu syarat dalam menyelesaikan pendidikan Sarjana Terapan Perangkat Lunak di 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. Mendapatkan ilmu baru dan pengalaman terkait cyber security seperti serangan *SQL Injection CSRF (Cross Site Request Forgery*.
4. Meningkatkan kerja sama antara pihak perkantoran dengan lembaga pendidikan khususnya Program Studi D4-Keamanan Sistem Informasi.

5. Memperoleh kesempatan dalam menganalisis masalah yang ada.

1.3 Luaran Proyek Kerja Praktek

Output yang dihasilkan dari melakukan uji penetrasi menggunakan teknik SQL Injection menunjukkan adanya celah keamanan yang signifikan pada website yang diuji. Dalam pengujian manual, input injeksi sederhana seperti ' OR '1'='1' -- pada parameter login tidak berhasil memotong otentikasi dan memberikan akses tanpa kredensial yang valid, menandakan bahwa input tersebut disanitasi dengan baik. Selain itu, penggunaan alat otomatisasi seperti sqlmap tidak mengidentifikasi parameter rentan dan tidak berhasil mengekstrak informasi sensitif dari database. Temuan ini menunjukkan bahwa website tersebut tidak rentan terhadap serangan SQL Injection.

BAB II

GAMBARAN UMUM DISKOMINFOTIK PROVINSI RIAU

2.1 Profil dan Sejarah Diskominfo Provinsi Riau

Sesuai dengan Peraturan Daerah Provinsi Riau 78 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Riau, Dinas Komunikasi, Informatika dan Statistik Provinsi Riau.

Dinas Komunikasi, Informatika dan Statistik Provinsi Riau mempunyai tugas membantu gubernur dalam melaksanakan urusan Pemerintah yang menjadi kewenangan daerah dan tugas pembantuan yang ditugaskan kepada daerah. Dalam melaksanakan tugas tersebut Dinas Komunikasi Informatika dan Statistik Provinsi Riau menyelenggarakan fungsi perumusan kebijakan pada :

1. Perumusan kebijakan pada Sekretariat, Bidang Informatika dan komunikasi publik, Bidang Pengelolaan dan Infrastruktur E-Government, Bidang layanan E-Government, Bidang Statistik, Bidang Persandian.
2. Pelaksanaan evaluasi dan pelaporan pada Sekretariat, Bidang informasi dan komunikasi publik, Bidang pengelolaan dan Infrastruktur E-Government, Bidang layanan E-Government, Bidang Statistik, Bidang Persandian.
3. Pelaksanaan Administrasi pada Sekretariat, Bidang Informatika dan komunikasi publik, Bidang Pengelolaan dan Infrastruktur E-Government, Bidang layanan E-Government, Bidang Statistik, Bidang Persandian.
4. Pelaksanaan fungsi lain yang diberikan Gubernur terkait dengan tugas dan fungsinya.

2.2 Visi dan Misi Diskominfotik Provinsi Riau

1. **Visi**

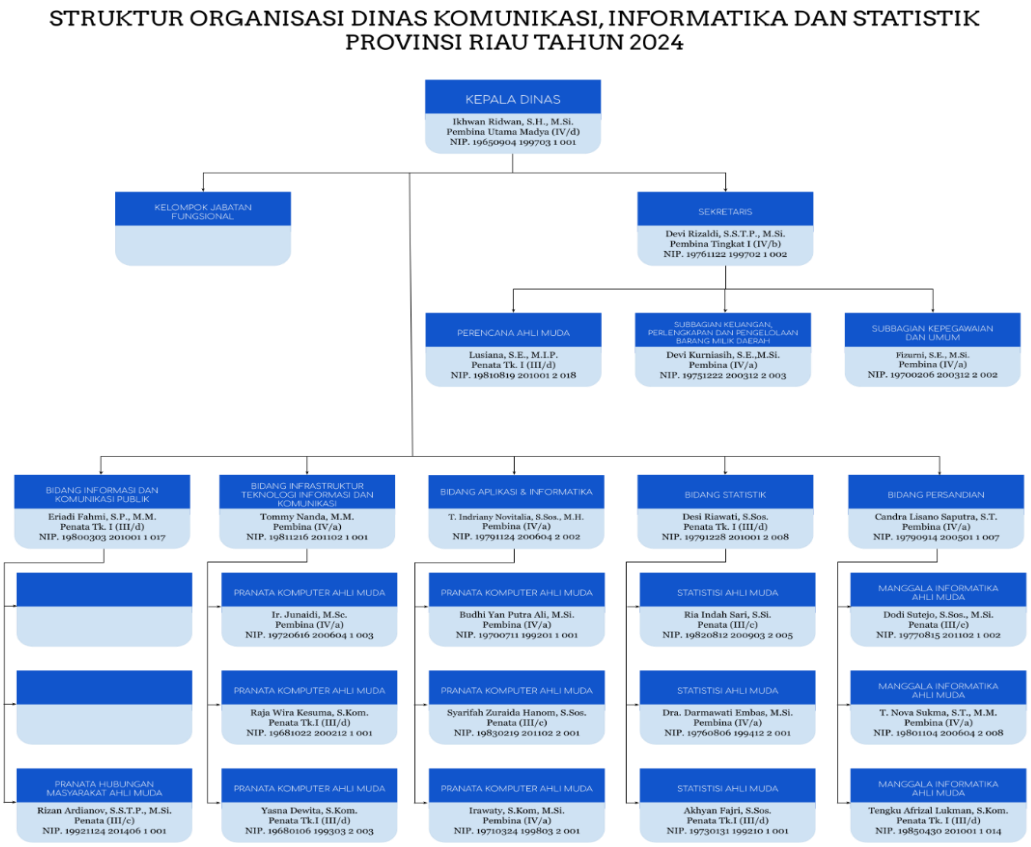
   Terwujudnya Layanan komunikasi, Informatika dan statistik yang handal dan berdaya saing.

2. **Misi**

   Mewujudkan manajemen penyelenggaraan pemerintah yang baik (good governance), efektif dan efesien, profesional, transparan dan akuntabel

2.3 Struktur Organisasi

Struktur organisasi pada Diskominfotik provinsi Riau disusun dengan ketentuan-ketentuan dengan fungsi, kewajiban dan tanggung jawab dari masing-masing bagian pada setiap bidang. Struktur organisasi pada Diskominfotik Provinsi Riau yang dapat dilihat pada gambar dibawah ini.



Gambar 2. 1 Struktur Organisasi Diskominfotik Provinsi Riau

(Sumber : https://diskominfotik.riau.go.id/)

2.3.1. Kepala Bidang Informatika Komunikasi Publik

Kepala bidang komukasi dan informasi publik mempunyai tugas melakukan koordinasi, fasilitas dan evaluasi pada seksi komunikasi informasi, seksi diseminasi informasi, seksi multimedia dan dokumentasi. Untuk melaksanakan tugas kepala bidang menyelenggarakan fungsi.

1. Penyusunan program kerja dan rencana operasional pada bidang informasi dan komunikasi publik.
2. Penyelenggaraan koordinasi, fasilitasi dan memeriksa hasil pelaksanaan tugas di lingkungan bidang informasi dan komunikasi publik. Penyelenggaraan pemantauan, evaluasi dan pelaporan pelaksanaan tugas sesuai dengan tugas yang telah dilaksanakan kepada kepala dinas komunikasi informatika dan statistik.
3. Pelaksanaan tugas kedinasan lain yang diberikan pimpinan sesuai tugas dan fungsinya. Bidang informasi dan komunikasi publik terdiri dari :
    a. Kepala seksi Komunikasi Informasi.
    b. Kepala seksi Diseminasi Informasi.
    c. Kepala seksi Multimedia dan Dokumentasi.

2.4 Ruang Lingkup Instansi Diskominfotik Provinsi Riau.

Waktu pelaksanaan Kerja Praktek (KP) dilaksanakan selama 4 Bulan terhitung dari tanggal 25 Maret 2024 sampai 19 Juli 2024. Kerja Praktek dilaksanakan di Dinas Komunikasi Informatika dan Statistik (Diskominfotik) Provinsi Riau yang beralamat di Jalan Diponegoro No 24 A, Pekanbaru Kota, Kota Pekanbaru, Riau. Jam operasional Diskominfotik Provinsi Riau dari Senin-Rabu yaitu pukul 07:30-16:00 sedangkan hari Kamis-Jumat yaitu pukul 07:30-16:30. Selama kerja praktek kegiatan yang dikerjakan random.

BAB III

BIDANG PEKERJAAN SELAMA KERJA PRAKTEK

3.1 Bidang Pekerjaan Selama Kerja Praktek

Selama Kerja Praktek di Dinas Komunikasi Informatika dan Statistik (Diskominfotik) di Bidang PERSANDIAN Provinsi Riau. Bidang pekerjaan bersifat flexible karena pekerjaan dilakukan sesuai arahan dari pembimbing lapangan. Selama melaksanakan Kerja Praktek terdapat beberapa pekerjaan yang di berikan oleh pihak kantor :

3.1.1 Uji Penetrasi Pada Sistem Pelaporan Insiden Siber Menggunakan Serangan SQL Injection

Dalam kegiatan ini saya bertugas melakukkan pentes dengan menggunakan serangan SQL Injection pada website pelaporan insiden siber.

3.2 Perangkat yang Digunakan

3.2.1 Web Browser

Web browser adalah aplikasi perangkat lunak yang memungkinkan pengguna untuk mengakses dan berinteraksi dengan konten di World Wide Web. Web browser berfungsi sebagai perantara antara pengguna dan internet, menerjemahkan kode HTML, CSS, JavaScript, dan berbagai bahasa pemrograman web lainnya menjadi halaman web yang dapat dilihat dan diinteraksikan oleh pengguna. Beberapa contoh web browser populer termasuk Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, dan Opera.

3.2.2 Laptop

Laptop merupakan perangkat keras yang digunakan untuk membuat proyek dan laporan Kerja Praktek dan penunjang lain selama melaksanakan kegiatan di tempat kerja praktek.

3.2.3 SQL Map

SQLMap adalah alat otomatis untuk mendeteksi dan mengeksploitasi kerentanan SQL Injection di aplikasi web. SQL Injection adalah teknik di mana peretas memasukkan kode SQL yang tidak diinginkan ke dalam kueri SQL yang dihasilkan oleh aplikasi web, memungkinkan mereka untuk mengakses atau memodifikasi data dalam database.

3.3 Kendala Saat Pelaksanaan Kerja Praktek

Kendala yang dialami saat melaksanakan Kerja Praktek yaitu kurangnya kemampuan untuk menyelesaikan pekerjaan yang di berikan dari tempat kerja, sehingga membutuhkan waktu untuk memahami projek yang diberikan.

3.4 Target Yang Diharapkan

Adapun target yang di harapkan selama pelaksanaan kerja praktek di Diskominfotik Bidang PERSANDIAN Provinsi Riau adalah :

1. Memahami sistem kerja di kantor Bidang PERSANDIAN Diskominfotik Provinsi Riau.
2. Menyelesaikan tugas yang dikerjakan.

BAB IV

PENGUJIAN

4.1 Metodologi

4.1.1 Prosedur Uji Penetrasi Menggunakan Teknik SQL Injection

1. Persiapan
    a. Identifikasi Target: Tentukan URL dan parameter yang akan diuji. Contohnya, halaman login, formulir pencarian, atau parameter URL lainnya.
    b. Pengumpulan Informasi: Cari tahu tentang teknologi yang digunakan, seperti jenis database (MySQL, PostgreSQL, MSSQL, dll.), framework web, dan pola input yang diterima.
2. Pengujian Manual
    a. Uji Input Dasar: Mulai dengan memasukkan karakter khusus (seperti ', ", --, ;) pada parameter input untuk melihat respons anomali dari server.
    b. Payload Sederhana: Coba payload injeksi sederhana seperti ' OR '1'='1 pada kolom input untuk melihat apakah query SQL dapat dimanipulasi.
    c. Analisis Respons: Periksa perubahan pada halaman web atau pesan kesalahan yang menunjukkan adanya celah SQL Injection, seperti kesalahan database atau hasil login yang tidak terduga.
3. Penggunaan Alat Otomatisasi
    a. Sqlmap: Gunakan alat otomatis seperti sqlmap untuk memindai dan mengeksploitasi celah SQL Injection lebih lanjut.
    b. Contoh perintah dasar: **sqlmap -u "http://example.com/login?username=admin&password=admin" --batch –dump**
    c. Parameter: Sesuaikan parameter URL dengan parameter input yang ingin diuji.

d. Opsi Tambahan: Gunakan opsi tambahan sqlmap untuk spesifikasinya seperti tipe database, level injeksi, atau eksploitasi tabel tertentu.

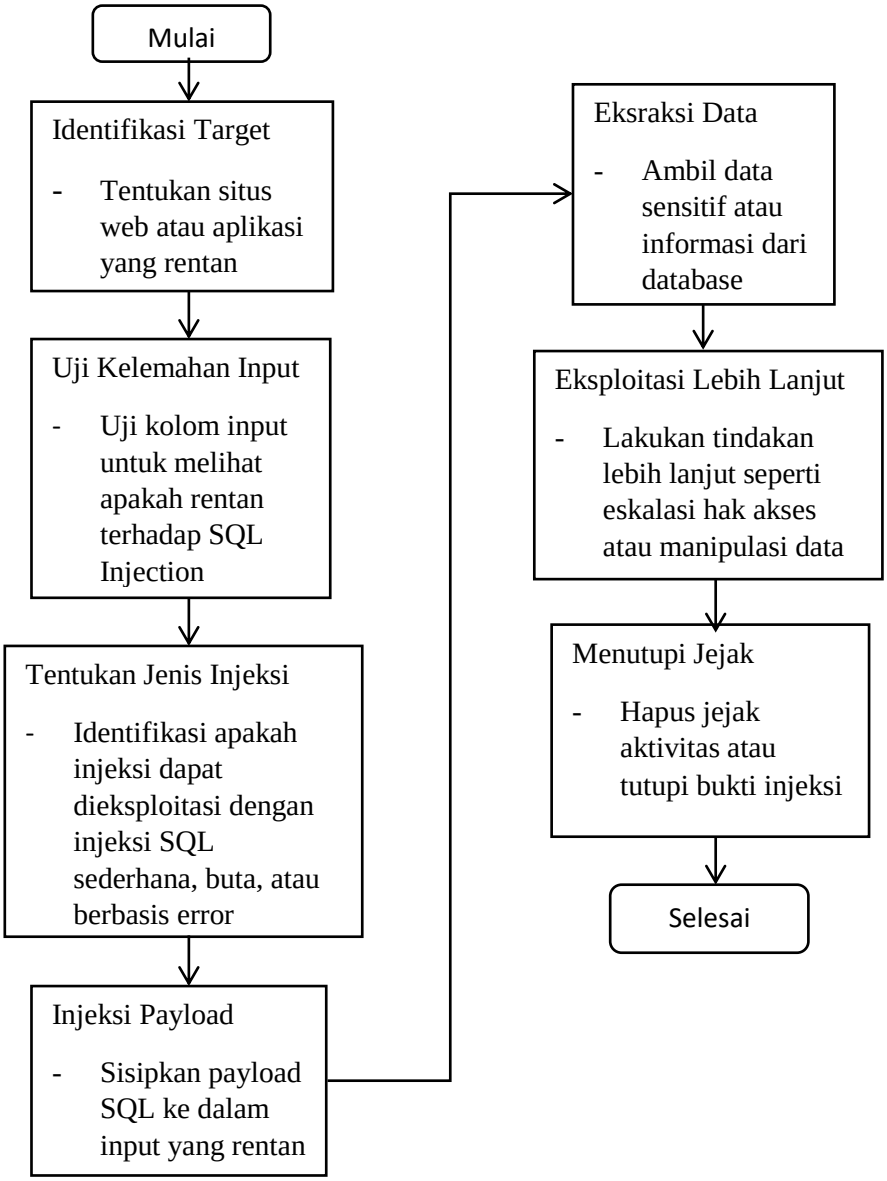
4. Eksploitasi dan Verifikasi:
   a. Ekstraksi Data: Jika celah terdeteksi, coba ekstraksi data sensitif dari database, seperti daftar pengguna dan kata sandi.
   b. Payload Lanjutan: Gunakan payload lebih kompleks untuk melakukan operasi seperti UNION SELECT, blind SQL injection, atau waktu berbasis SQL injection.
   c. Verifikasi Eksploitasi: Verifikasi bahwa data yang diekstrak adalah valid dan sesuai dengan yang diharapkan dari database target.
5. Analisis Risiko:
   a. Tingkatkan Risiko: Tentukan tingkat keparahan celah yang ditemukan berdasarkan potensi dampak dan akses yang dapat diperoleh oleh penyerang.
   b. Dokumentasi Temuan: Catat semua payload yang berhasil, parameter yang rentan, data yang diekstraksi, dan tingkat risiko.
6. Pelaporan:
   a. Laporan Hasil Pengujian: Buat laporan yang mencakup deskripsi celah, bukti eksploitasi, dan tangkapan layar atau log dari proses pengujian.
   b. Rekomendasi Perbaikan: Berikan rekomendasi untuk mitigasi seperti penggunaan prepared statements, validasi input yang lebih ketat, dan pembaruan sistem keamanan.
   c. Kesimpulan: Sampaikan kesimpulan dari pengujian, termasuk apakah website rentan terhadap SQL Injection dan langkah-langkah yang perlu diambil untuk meningkatkan keamanannya.

Dengan mengikuti prosedur ini, penguji dapat mengidentifikasi, mengeksploitasi, dan memberikan solusi untuk celah SQL Injection secara efektif, sehingga meningkatkan keamanan aplikasi web target.

4.1.2 Metodologi Pengumpulan Data

Metodologi pengumpulan datanya menggunakan bantuan tools NMAP, SQLMAP, dan tools yang dikembangkan oleh bang roy selaku mentor di tempat magang.

4.1.3 Proses Perancangan



Penjelasan Setiap Tahap:

1. Mulai : Mulai proses dengan menentukan bahwa tujuan Anda adalah melakukan SQL Injection.

2. Identifikasi Target : Pilih situs web atau aplikasi yang ingin Anda uji. Identifikasi target yang mungkin rentan terhadap SQL Injection.
3. Uji Kelemahan Input : Uji kolom input, seperti formulir pencarian atau login, untuk melihat apakah mereka rentan terhadap SQL Injection dengan memasukkan karakter khusus atau kueri SQL.
4. Tentukan Jenis Injeksi : Tentukan jenis SQL Injection yang dapat dieksploitasi berdasarkan respon yang diterima dari input uji.
5. Injeksi Payload : Masukkan payload SQL yang sesuai ke dalam kolom input untuk mengeksploitasi kelemahan.
6. Ekstraksi Data : Ekstraksi data sensitif dari basis data melalui injeksi SQL yang berhasil.
7. Eksploitasi Lebih Lanjut : Setelah berhasil mendapatkan akses, lakukan tindakan tambahan seperti meningkatkan hak akses atau memanipulasi data.
8. Menutupi Jejak : Hapus atau sembunyikan jejak aktivitas Anda untuk menghindari deteksi.
9. Selesai : Proses selesai.

4.1.4 Tahapan dan Jadwal Pelaksanaan

4.1.4.1 Tahap yang dilakukan

1. Identifikasi Titik Rentan
    a. Scanning : Penyerang akan menggunakan alat otomatis atau manual untuk memindai aplikasi web dan menemukan formulir, parameter URL, atau input lain yang mungkin rentan.
    b. Uji Coba Manual : Menyuntikkan karakter khusus seperti tanda kutip tunggal (') dalam input pengguna (misalnya, kolom pencarian, formulir login) untuk melihat apakah terjadi kesalahan atau output yang tidak diinginkan yang menunjukkan kerentanan SQL Injection.

2. Pemahaman Struktur Query
    a. Menentukan Jenis Database : Menggunakan teknik uji coba untuk mengidentifikasi jenis database (misalnya, MySQL, SQL Server, PostgreSQL) yang digunakan oleh aplikasi web.
    b. Pengujian Error-Based : Menyuntikkan input yang memicu pesan kesalahan database untuk mengungkapkan struktur query dan nama tabel.
3. Melakukan Injeksi Dasar
    a. Injeksi Klasik : Menyisipkan perintah SQL sederhana untuk mengubah logika query, misalnya, dalam formulir login : ' OR '1'='1' –
    b. Ini dapat membuat kondisi selalu benar dan memungkinkan akses tanpa otorisasi.
4. Ekstraksi Informasi
    a. Union-Based Injection **:** Menyuntikkan perintah UNION untuk menggabungkan hasil dari query asli dengan data dari tabel lain, misalnya : ' UNION SELECT username, password FROM users –
    b. Ini memungkinkan penyerang untuk mengakses informasi sensitif seperti username dan password.
5. Eksploitasi Lanjutan
    a. Blind SQL Injection : Jika aplikasi tidak mengembalikan pesan kesalahan, penyerang dapat menggunakan teknik Blind SQL Injection dengan memanipulasi respons aplikasi (misalnya, waktu respons) untuk memperoleh informasi.
    b. Boolean-Based : Menggunakan pernyataan yang mengubah output halaman berdasarkan kondisi benar/salah.
    c. Time-Based : Menyuntikkan perintah yang menyebabkan penundaan waktu jika kondisi tertentu benar.

6. Memodifikasi atau Menghapus Data
    a. Manipulasi Data : Menyuntikkan perintah untuk mengubah data dalam database, misalnya : ' UPDATE users SET password='newpassword' WHERE
    b. Penghapusan Data : Menyuntikkan perintah untuk menghapus data, misalnya : ' DROP TABLE users –
7. Menutupi Jejak
    a. Menghapus Log: Menyuntikkan perintah untuk menghapus atau mengubah log yang mungkin mencatat aktivitas penyerang.
    b. Menggunakan Teknik Obfuscation: Mengaburkan atau menyandikan payload untuk menghindari deteksi oleh sistem keamanan.
8. Eksploitasi Lanjutan
    a. Eskalasi Privilege: Menggunakan akses yang diperoleh untuk meningkatkan hak akses dalam sistem.
    b. Menanam Backdoor: Menginjeksi kode untuk menciptakan titik akses yang dapat digunakan kembali di masa depan.

4.1.4.2 Jadwal Pelaksanaan

Adapun jadwal perancangan projek ini adalah dalam 4 bulan terakhir kerja praktek. Bisa dilihat pada tabel berikut.

Tabel 4. 1 Tabel Jadwal Pelaksanaan

No	Uraian Kegiatan	Bulan															
		Maret	April				Mei				Juni				Juli		
		4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
1	Persipan dan Perencanaan																
2	Pengujian dan Eksekusi																
3	Analisis dan Pelaporan																

4.2 Perancangan dan Implementasi

4.2.1 Perancangan

Tujuan

a. Mengidentifikasi kelemahan dalam input validasi terhadap serangan SQL Injection.
b. Mengevaluasi dampak dari kelemahan yang ditemukan.
c. Menyarankan tindakan mitigasi untuk memperbaiki kelemahan.

Lingkup

a. Situs web atau aplikasi tertentu yang memiliki formulir input.
b. Area yang akan diuji mencakup formulir login, pencarian, dan input lainnya yang terhubung ke basis data.

Metodologi

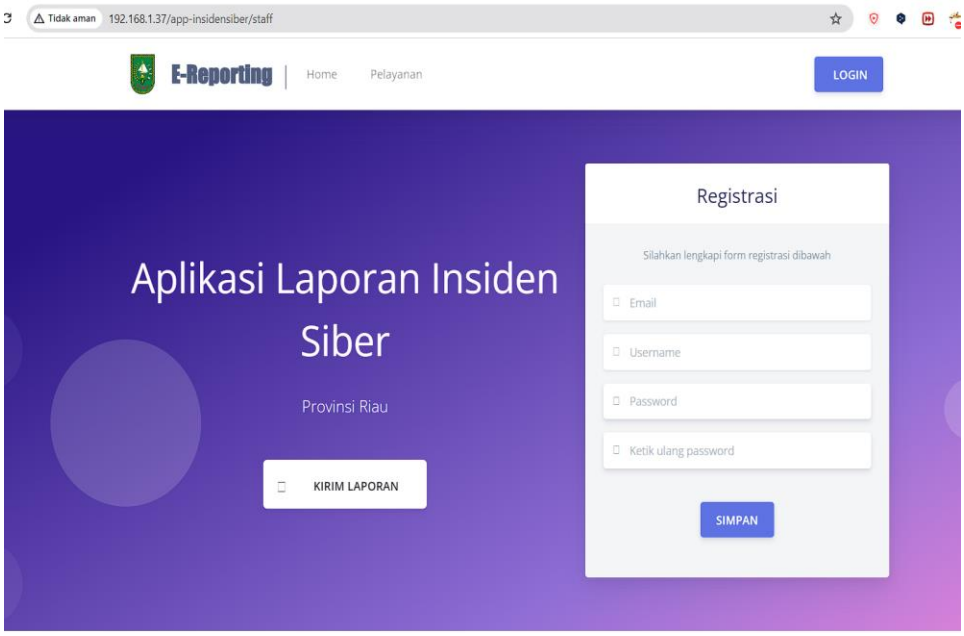
a. Reconnaissance: Mengumpulkan informasi tentang target.
b. Vulnerability Analysis: Mengidentifikasi potensi kelemahan.
c. Exploitation: Mencoba memanfaatkan kelemahan yang ditemukan.
d. Post-Exploitation: Mengevaluasi dampak dan mengambil data yang bisa diekstrak.
e. Reporting: Menyusun laporan temuan dan rekomendasi mitigasi.

4.2.2 Rancangan Sistem

Berikut adalah rancangan untuk melakukan serangan SQL Injection:

1. Berikut adalah tampilan dari website yang akan di uji menggunakan Teknik sql injection.

   Langkah pertama kita melakukan information gathering untuk mengumpulkan informasi sebanyak banyaknya dari website ini, dengan cara melakukan scanning.



Gambar 4. 1 Aplikasi Laporan Insiden Siber

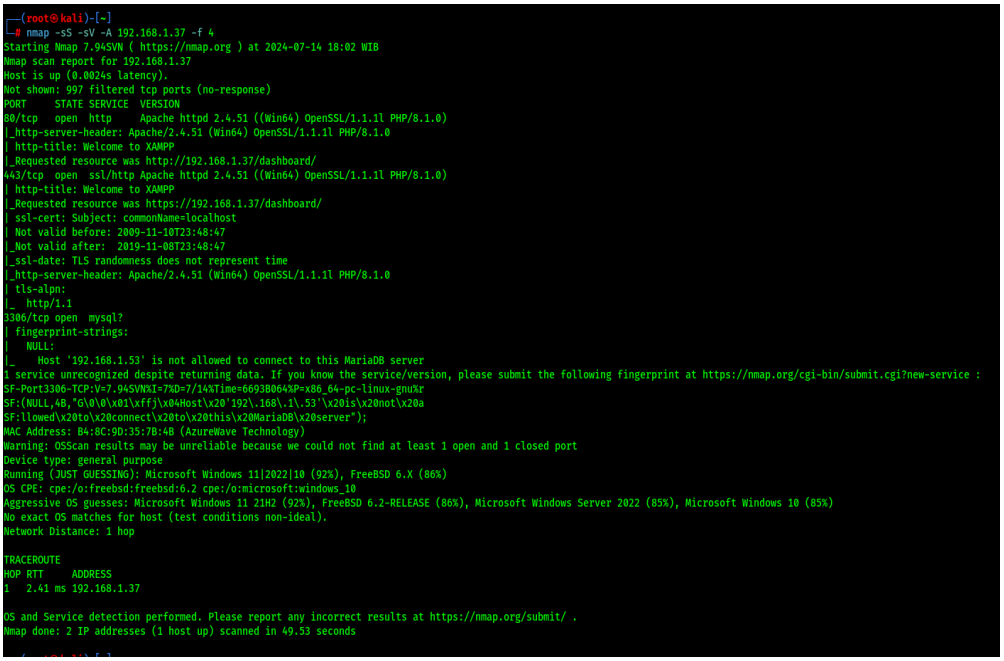
2. Kita akan melakukan information gathering menggunakan tools nmap. Nmap adalah sebuah tools yang berfungsi untuk memindai dan mengumpulkan informasi tentang host target. Untuk sintaks yang di gunakan adalah **nmap -sS -sV -A 192.168.1.37 -f 4**.

   Keterangan:

   - sS: Opsi ini menjalankan "TCP SYN scan" (juga dikenal sebagai "half-open scan"). Ini adalah metode pemindaian yang cepat dan tidak terlalu terdeteksi oleh sistem IDS (Intrusion Detection System) karena hanya mengirim SYN (synchronize) dan tidak menyelesaikan koneksi penuh.
   - sV: Opsi ini mencoba untuk mendeteksi versi layanan yang berjalan pada port terbuka. Dengan kata lain, nmap akan mencoba mengidentifikasi aplikasi dan versinya yang berjalan di port tersebut.
   - A: Opsi ini mengaktifkan beberapa fitur yang lebih lanjut, termasuk deteksi OS (Operating System), deteksi versi, script

scanning, dan traceroute. Opsi ini memberikan lebih banyak informasi tentang host target.

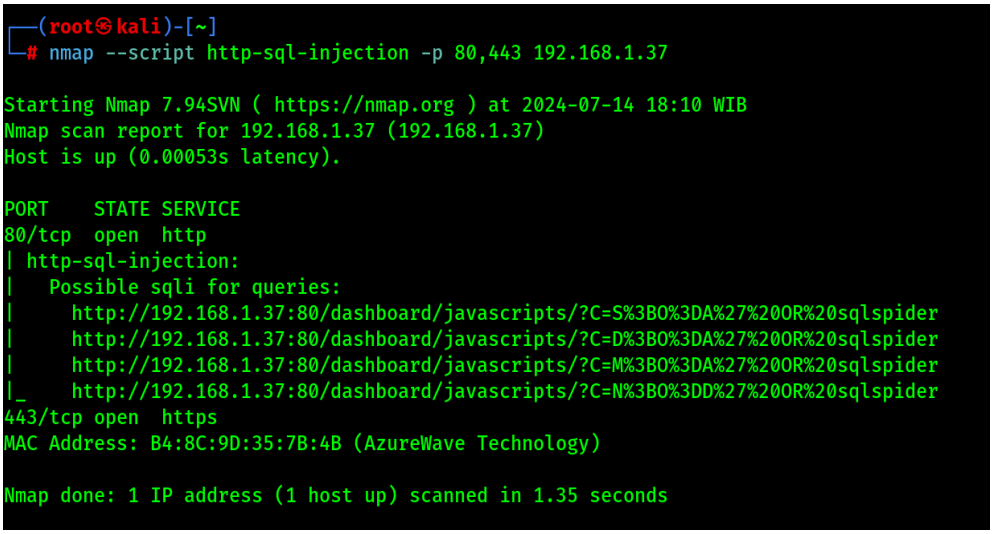
- f 4: Opsi ini memecah paket scan menjadi fragmen yang lebih kecil. Ini sering digunakan untuk menghindari firewall atau IDS/IPS yang mungkin mendeteksi pemindaian berdasarkan ukuran paket. Namun, penggunaan -f tanpa nilai biasanya mengindikasikan fragmentasi yang lebih agresif, sedangkan nilai 4 ini tidak biasa dan mungkin merupakan kesalahan ketik atau pilihan yang tidak standar.



Gambar 4. 2 Menjalankan Perintah Nmap

Hasil pemindaian ini memberikan informasi yang komprehensif tentang layanan yang berjalan pada host tersebut, versi aplikasi, serta beberapa detail tentang sertifikat SSL dan kemungkinan sistem operasi yang digunakan. Namun, dengan menggunakan skrip yang tepat dari Nmap Scripting Engine (NSE), Anda bisa mengumpulkan beberapa informasi yang dapat membantu dalam mengidentifikasi potensi kerentanan SQL Injection.

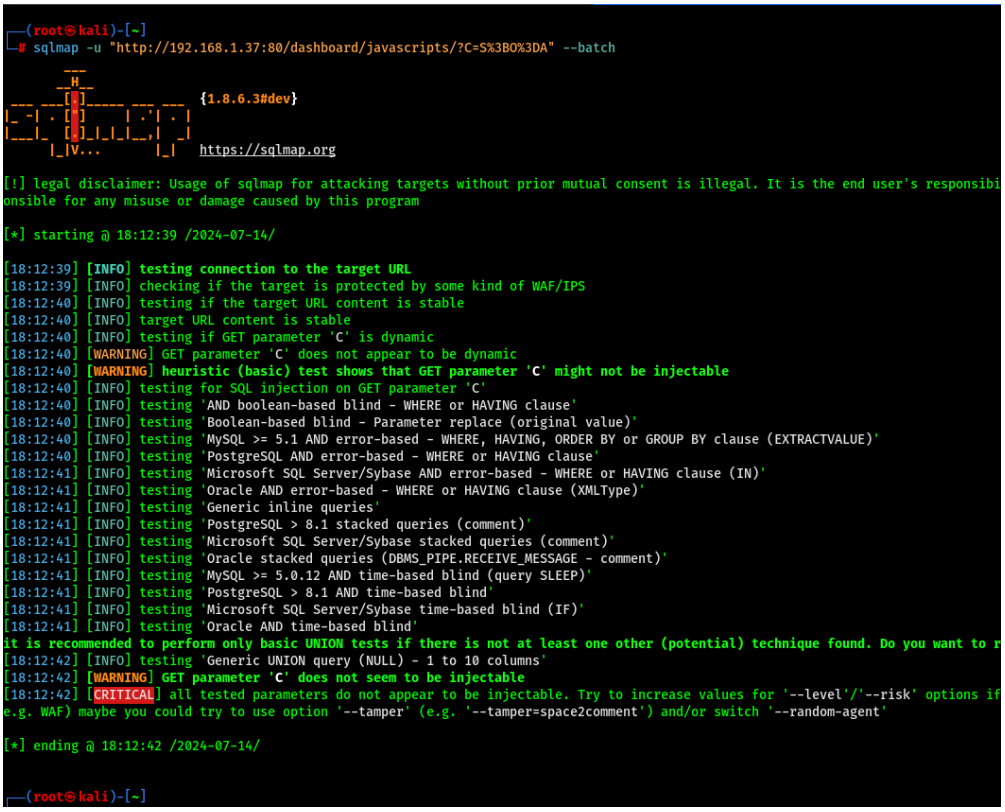
Untuk sintaks yang digunakan adalah **nmap --script http-sql-injection -p 80,443 192.168.1.37**.



Gambar 4. 3 Menjalankan Nmap Script

Pemindaian ini menunjukkan bahwa ada kemungkinan kerentanan SQL Injection pada URL yang ditentukan di atas. Parameter C dalam direktori dashboard/javascripts/ tampaknya rentan terhadap injeksi SQL.

3. Setelah kita mendapatkan informasi dari hasil scanning yang telah dilakukan, kemudian kita melakukan pengujian lebih lanjut menggunakan tools **sqlmap** untuk mengeksploitasi dan memverifikasi kerentanan ini. untuk sintaks yang digunakan adalah: **sqlmap -u "http://192.168.1.37:80/dashboard/javascripts/?C=S%3BO%3DA --batch"**.



Gambar 4. 4 Hasil Pemindaian SQLMAP

Berdasarkan hasil pemindaian sqlmap terhadap URL http://192.168.1.37:80/dashboard/javascripts/?C=S%3BO%3DA dan yang lainnya, berikut adalah kesimpulan dan analisisnya:

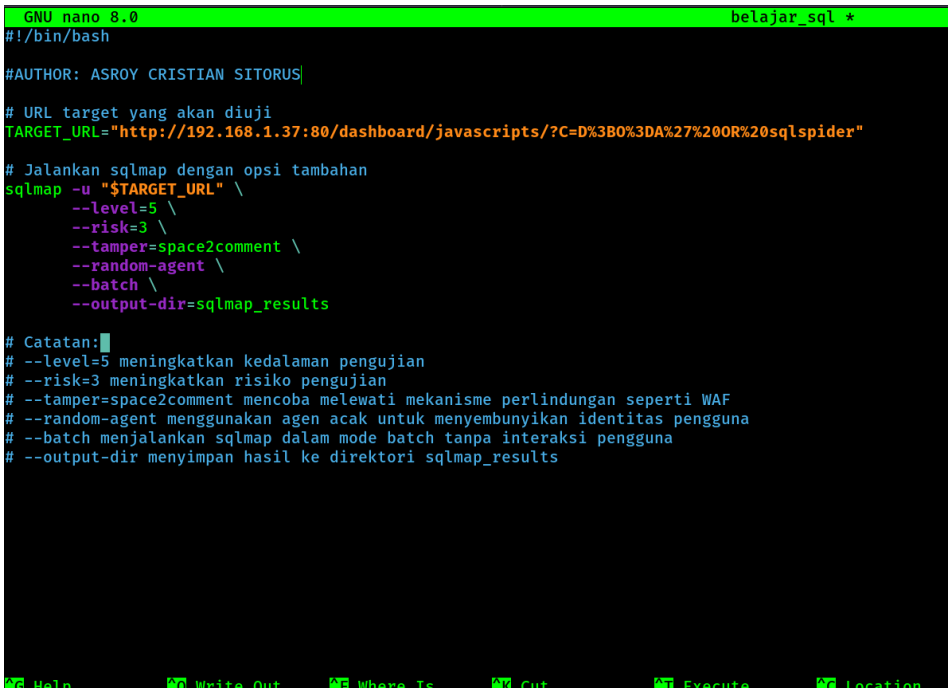
1. Hasil Pemindaian SQL Injection:

- Tes Stabilitas URL: URL target dinyatakan stabil.
- Tes Dinamis Parameter 'C': Parameter 'C' tidak terlihat dinamis.
- Tes Injeksi SQL: Berbagai teknik injeksi SQL yang diuji oleh sqlmap (boolean-based, error-based, time-based, dan UNION query) tidak menemukan indikasi bahwa parameter 'C' dapat diinjeksi.
- Rekomendasi Tambahan: sqlmap merekomendasikan untuk meningkatkan nilai --level dan --risk atau menggunakan opsi --tamper dan --random-agent jika dicurigai ada mekanisme perlindungan seperti WAF

2. Kesimpulan:

- Tidak Ditemukan SQL Injection: Berdasarkan hasil tes otomatis dari sqlmap, parameter 'C' pada URL yang diuji tidak tampak rentan terhadap SQL Injection.
- Kemungkinan Perlindungan Tambahan: Ada kemungkinan bahwa mekanisme perlindungan seperti WAF (Web Application Firewall) atau konfigurasi server yang kuat menghalangi upaya injeksi SQL.

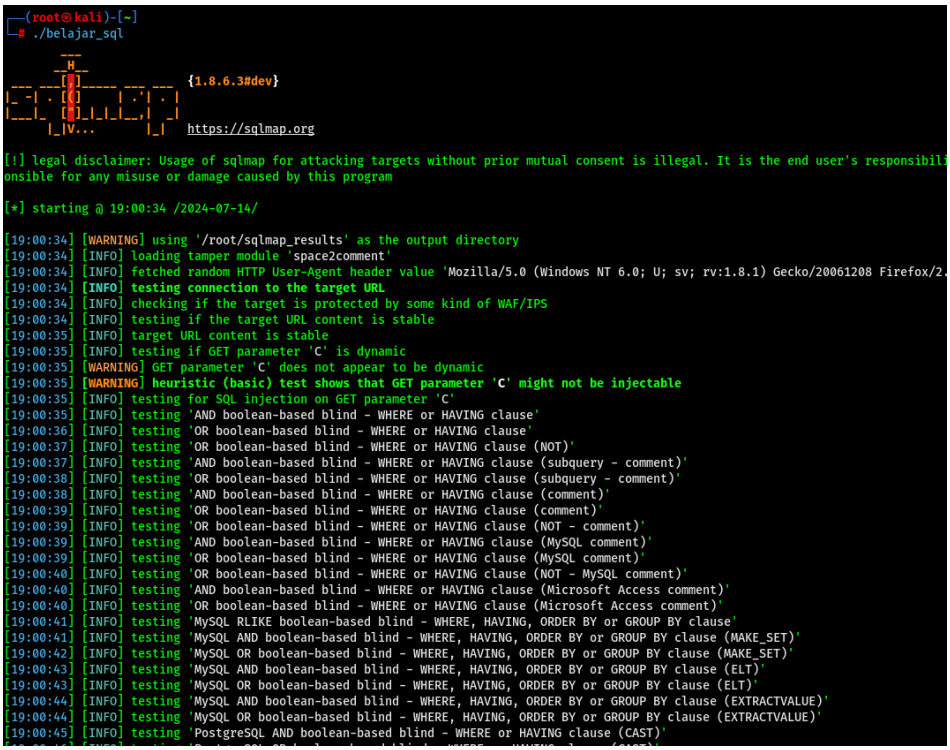
4. Langkah selanjutnya melakukan pengujian manual untuk memverifikasi lebih lanjut, terutama jika ada kecurigaan mekanisme perlindungan. Untuk meningkatkan Tingkat pengujian dan mencoba melewati perlingungan seperti WAF. Saya konsultasi kepada abang dan kakak tim csirt yang ada di bidang persandian di Diskominfotik Provinsi Riau. Dari hasil konsultasi, abang dan kakak tersebut membuat sebuah tools atau program yang dapat membantu saya dalam melakukan proses pengujian ini.



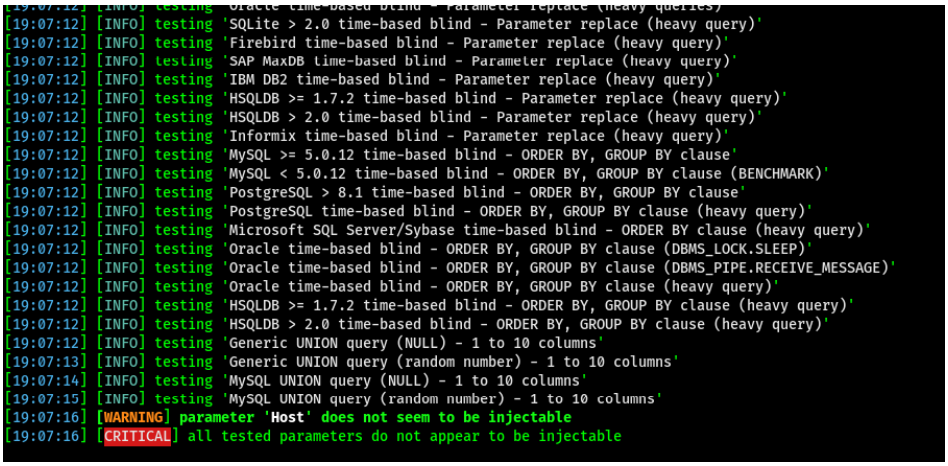
Gambar 4. 5 Pengujian Manual

Untuk menjalankan tools tersebut dapat menggunakan sintaks **./belajar_sql**.

Tools ini akan menjalankan sqlmap dengan konfigurasi yang lebih agresif dan menyimpan hasil pengujian dalam direktori yang ditentukan, memungkinkan kita untuk menganalisis hasilnya setelah pengujian selesai.



Gambar 4. 6 Hasil Pemindaian 1



Gambar 4. 7 Hasil Pemindaian 2

5. Berdasarkan hasil pemindaian sqlmap yang baru, berikut adalah kesimpulan yang dapat kita tarik:
    1. Tidak Ditemukan SQL Injection:
        - Semua parameter yang diuji oleh sqlmap (termasuk parameter Host) tidak tampak rentan terhadap SQL Injection.
        - sqlmap melakukan berbagai tes menggunakan teknik yang berbeda (time-based, UNION query, dan lain-lain), tetapi tidak menemukan indikasi bahwa parameter yang diuji dapat diinjeksi.
    2. Tes Tambahan yang Dilakukan:
        - sqlmap melakukan pengujian mendalam dengan meningkatkan tingkat dan risiko pengujian.
        - Pengujian dilakukan dengan menggunakan berbagai teknik injeksi SQL yang mencakup database seperti MySQL, PostgreSQL, Microsoft SQL Server, Oracle, dan lain-lain.
        - Tes juga mencoba menggunakan query UNION dengan berbagai variasi (NULL, random number).

No	Target	Metode Uji	Hasil Uji	Keterangan
1	Form Login	SQL Injection	Tidak Rentan	Tidak ditemukan celah pada input form login

Keterangan :

- Tidak Rentan berarti tidak ditemukan celah keamanan yang bisa dieksploitasi.
- Pengujian ini menunjukkan bahwa form login aman dari serangan SQL Injection.

Tabel di atas menunjukkan bahwa form login telah diuji dengan metode SQL Injection dan tidak ditemukan celah keamanan.

BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan untuk judul “Melakukan Uji Penetrasi Pada Website Pelaporan Insiden Siber Menggunakan Serangan Sql Injection”antara lain yaitu:

1. Berdasarkan pengujian pada website pelaporan insiden siber tidak ditemukan SQL Injection, semua parameter yang diuji oleh sqlmap (termasuk parameter Host) tidak tampak rentan terhadap SQL Injection. Sqlmap melakukan berbagai tes menggunakan teknik yang berbeda (time-based, UNION query, dan lain-lain), tetapi tidak menemukan indikasi bahwa parameter yang diuji dapat diinjeksi.
2. Dengan tidak berhasilnya serangan SQL Injection ini, langkah selanjutnya yang dilakukan tes Tambahan yang dilakukan dan dapat disimpulkan sebagai berikut
   a. sqlmap melakukan pengujian mendalam dengan meningkatkan tingkat dan risiko pengujian.
   b. Pengujian dilakukan dengan menggunakan berbagai teknik injeksi SQL yang mencakup database seperti MySQL, PostgreSQL, Microsoft SQL Server, Oracle, dan lain-lain.
   c. Tes juga mencoba menggunakan query UNION dengan berbagai variasi (NULL, random number).
3. Aplikasi pelaporan insiden siber merupakan aplikasi yang dirancang untuk melapor kejadian insiden siber dan memudahkan pengguna dalam menginformasikan insiden yang terjadi. Staff/publik dapat mengetahui statusnya apakah ditindaklanjuti atau ditolak.

5.2 Saran

Beberapa saran yang dapat diambil dari proses Melakukan Uji Penetrasi Pada Website Pelaporan Insiden Siber Menggunakan Serangan Sql Injection sampai pada pembuatan laporan kerja praktek ini adalah Pentingnya Pemantauan dan Pembaruan, meskipun hasilnya positif perlu dicatat bahwa keamanan aplikasi web harus terus dimonitor dan dievaluasi secara berkala. Ancaman keamanan dapat berkembang seiring waktu, dan ada kemungkinan adanya celah baru yang perlu diperhatikan.

DAFTAR PUSTAKA

[1] “Universitas medan area”.

[2] Gramedia Blog, “Jurusan Keamanan Sistem Informasi,” *Gramedia.com,* 2022.

LAMPIRAN

Lampiran 1. Surat Balasan diterima magang pada perusahaan

PEMERINTAH PROVINSI RIAU
DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
Jalan Diponegoro Nomor 24 A, Pekanbaru, Kode Pos : 28156
Telepon (0761) 45505, Faximile : (0761) 45505
e-mail : diskominfotik@riau.go.id
Website : http://diskominfotik.riau.go.id, riau.go.id, mediacenter.riau.go.id

Pekanbaru, 19 Maret 2024

Nomor : 423/Diskominfotik-Sekre/013
Sifat : Penting
Lampiran : -
Hal : Penempatan Kerja Praktik/Magang/Riset

Kepada
Yth. Kepala Direktur Politeknik
Negeri Bengkalis
Di –
Bengkalis

Menindaklanjuti Surat dari Politeknik Negeri Bengkalis Nomor: 983/PL.31/TU/2024 tanggal 06 Maret 2024, bersama ini pada prinsipnya Mahasiswa/i sebagai berikut :

No.	NAMA	NIM	PROGRAM STUDI
1.	Risky Seri Hartati	6404201017	Sarjana Terapan Keamanan Sistem Informasi
2.	Anggun Fitriyani	6404201018	Sarjana Terapan Keamanan Sistem Informasi
3.	Natasya Muliani	6304201274	Sarjana Terapan Keamanan Sistem Informasi
4.	Rhima Diana	6304201241	Sarjana Terapan Keamanan Sistem Informasi

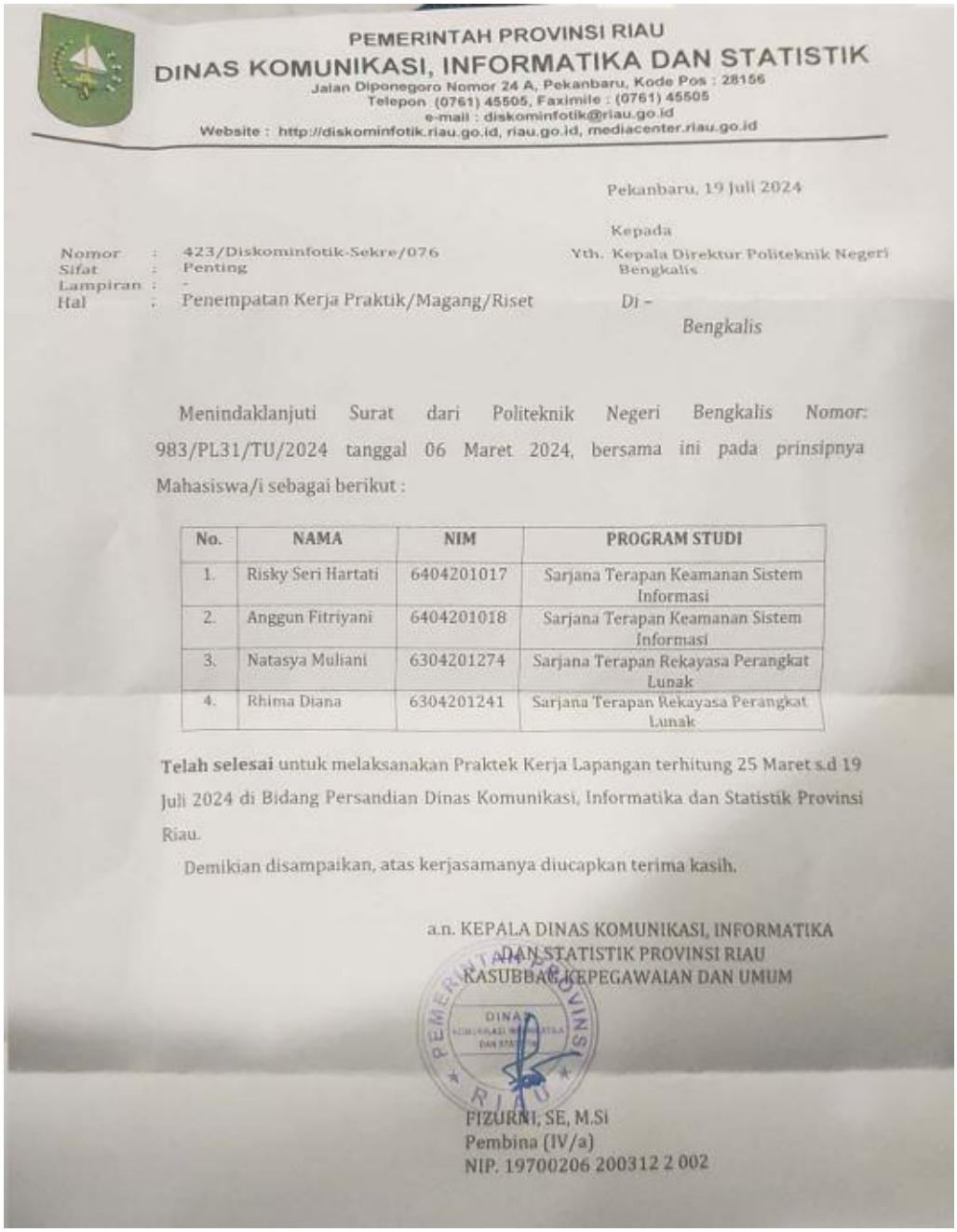
Diterima untuk melaksanakan Praktek Kerja Lapangan terhitung 21 Maret s.d 19 Juli 2024 di Bidang Persandian Dinas Komunikasi, Informatika dan Statistik Provinsi Riau.

Demikian disampaikan, atas kerjasamanya diucapkan terima kasih.

a.n. KEPALA DINAS KOMUNIKASI, INFORMATIKA
DAN STATISTIK PROVINSI RIAU
KASUBBAG KEPEGAWAIAN DAN UMUM

FITRINI, SE, M.Si
Pembina (IV/a)
NIP. 19700206 200312 2 002

Lampiran 2. Surat Keterangan telah selesai mengerjakan kerja Praktek



PEMERINTAH PROVINSI RIAU
DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
Jalan Diponegoro Nomor 24 A, Pekanbaru, Kode Pos : 28156
Telepon (0761) 45505, Faximile : (0761) 45505
e-mail : diskominfotik@riau.go.id
Website : http://diskominfotik.riau.go.id, riau.go.id, mediacenter.riau.go.id

Pekanbaru, 19 Juli 2024

Nomor : 423/Diskominfotik-Sekre/076
Sifat : Penting
Lampiran : -
Hal : Penempatan Kerja Praktik/Magang/Riset

Kepada
Yth. Kepala Direktur Politeknik Negeri Bengkalis
Di -
Bengkalis

Menindaklanjuti Surat dari Politeknik Negeri Bengkalis Nomor: 983/PL31/TU/2024 tanggal 06 Maret 2024, bersama ini pada prinsipnya Mahasiswa/i sebagai berikut :

No.	NAMA	NIM	PROGRAM STUDI
1.	Risky Seri Hartati	6404201017	Sarjana Terapan Keamanan Sistem Informasi
2.	Anggun Fitriyani	6404201018	Sarjana Terapan Keamanan Sistem Informasi
3.	Natasya Muliani	6304201274	Sarjana Terapan Rekayasa Perangkat Lunak
4.	Rhima Diana	6304201241	Sarjana Terapan Rekayasa Perangkat Lunak

Telah selesai untuk melaksanakan Praktek Kerja Lapangan terhitung 25 Maret s.d 19 Juli 2024 di Bidang Persandian Dinas Komunikasi, Informatika dan Statistik Provinsi Riau.

Demikian disampaikan, atas kerjasamanya diucapkan terima kasih.

a.n. KEPALA DINAS KOMUNIKASI, INFORMATIKA
DAN STATISTIK PROVINSI RIAU
KASUBBAG KEPEGAWAIAN DAN UMUM

FIZURNI, SE, M.Si
Pembina (IV/a)
NIP. 19700206 200312 2 002

Lampiran 3. Lembaran Penilaian Kerja Praktek

PENILAIAN DARI PERUSAHAAN KERJA PRAKTEK
DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK
PROVINSI RIAU

Nama : Anggun Fitriyani
NIM : 6404201018
Program Studi : Keamanan Sistem Informasi
Politeknik Negeri Bengkalis

No.	Aspek Penilaian	Bobot	Nilai
1	Disiplin	20%	94
2	Tanggung- jawab	25%	94
3	Penyesuaian diri	10%	95
4	Hasil Kerja	30%	93
5	Perilaku secara umum	15%	94
	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 : Pelaksanaan magang telah selesai dg baik.

Pekanbaru, 19 Juli 2024
Pembimbing Magang

Tiara Mulia Putri, S.Kom
NIP. 19870505 201903 2 001

Lampiran 4. Logbook Harian/Mingguan

KEGIATAN HARIAN
KERJA PRAKTEK (KP)

Nama : Anggun Fitriyani
NIM : 6404201018
Hari / Minggu : Senin-Jumat / Minggu Pertama
Tanggal : 25-29 Maret 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Pemberian arahan dari anggota Dinas Komunikasi Informatika dan Statistik Provinsi Riau mengenai jam masuk kerja dan cara berpakaian 2. Perkenalan diri kepada staff bidang persandian Diskomintotik Provinsi Riau dan penyampaian ide-ide untuk Project yang akan dilakukan. 3. Pembagian tugas kepada rekan tim untuk project yang akan dibuat. 4. Libur hari paskah	Tiara Mulia Putri, S.Kom	

Catatan Pembimbing Industri

GAMBARAN KERJA	KETERANGAN
	Pentes dengan serangan SQL Injection

Hari / Minggu : Senin-Jumat / Minggu Kedua
Tanggal : 01-05 April 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Sharing tentang cyber security 2. Cuti Bersama Idul Fitri	Tiara Mulia Putri, S.Kom	

Catatan Pembimbing Industri

GAMBARAN KERJA	KETERANGAN
	Menginstall DVWA dan mempelajari serangan SQL Injection di DVWA

Hari / Minggu : Senin-Jumat / Minggu Ketiga
Tanggal : 08-12 April 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Cuti Bersama Idul Fitri	-	-

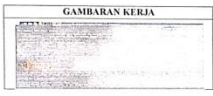
Catatan Pembimbing Industri

GAMBARAN KERJA	KETERANGAN
-	-

Hari / Minggu : Senin-Jumat / Minggu Keempat
Tanggal : 15-19 April 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Mencari referensi tentang serangan SQL Injection	Tiara Mulia Putri, S.Kom	

Catatan Pembimbing Industri

GAMBARAN KERJA	KETERANGAN
	Mencari referensi dan mempelajari serangan SQLMap

Hari / Minggu : Senin-Jumat / Minggu Kelima
Tanggal : 22-26 April 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Membuat laporan kerja praktek 2. Mempelajari serangan SQLMap	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Mempelajari dan melakukan serangan SQLMap

Hari / Minggu : Senin-Jumat / Minggu Keenam
Tanggal : 29-03 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Mempelajari SQLMap 2. Libur Hari Buruh	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Melakukan serangan SQLMap dengan DVWA

Hari / Minggu : Senin-Jumat / Minggu Ketujuh
Tanggal : 6-10 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Mempelajari SQLMap 2. Membuat PPT untuk persiapan presentasi progres projek yang diberikan	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Presentasi terkait progres projek magang

Hari / Minggu : Senin-Jumat / Minggu Kedelapan
Tanggal : 13-17 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Simulasi kebakaran di kantor diskominfotik lama 2. Mempelajari serangan SQL Injection 3. Pengenalan tentang sosial engginneering 4. Menjadi notulen Rapat persiapan acara asistensi pembentukan CSIRT kab/kota	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Membuat video Simulasi kebakaran

Hari / Minggu : Senin-Jumat / Minggu Kesembilan
Tanggal : 20-24 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Persiapan acara CSIRT di hoton bono 2. Acara pembentukan CSIRT dihotel bono	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Acara pembentukan CSIRT kab/kota di hotel bono

Hari / Minggu : Senin-Jumat / Minggu Kesepuluh
Tanggal : 27-31 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Membuat laporan magang 2. Mencari referensi SQL Injection	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Membuat laporan magang

Hari / Minggu : Senin - Jumat / Minggu Kesebelas
Tanggal : 03-07 Juni 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melanjutkan membuat laporan magang 2. Mencari referensi terkait serangan SQL Injection	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Mencari referensi terkait serangan SQL Injection

Hari / Minggu : Senin / Minggu Kedua belas
Tanggal : 10-14 Juni 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melanjutkan laporan magang 2. Mempelajari SQLMap	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Mempelajari serangan SQLMap

Hari / Minggu : Senin-Jumat / Minggu Ketiga belas
Tanggal : 17-21 Juni 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Cuti hari raya idul adha 2. Melanjutkan membuat laporan magang	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Membuat laporan magang

Hari / Minggu : Senin-Jumat / Minggu keempat belas
Tanggal : 24-28 Juni 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Rapar terkait website yang terkena serangan deface 2. Mengikuti rapat internal mengenai evaluasi dokumen ISO 27001:2022 3. Pengukuran ISO dengan SMKI bersama pihak kantor	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Mengikuti rapat

Hari / Minggu : Senin-Jumat / Minggu Kelima belas
Tanggal : 01-05 Juli 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melanjutkan pengerjaan laporan magang 2. Melakukan pentes serangan sql injection di dvwa	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Melakukan pentes dengan serangan SQL Injection di DVWA

Hari / Minggu : Senin-Jumat / Minggu Keenam belas
Tanggal : 08-12 Juli 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Membuat laporan pentes 2. Melanjutkan membuat laporan magang 3. Kunjungan dari dosen ketempat magang	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Membuat laporan pentes Kunjungan dari dosen ke tempat magang

Hari / Minggu : Senin-Jumat / Minggu ketujuh belas
Tanggal : 15-19 Juli 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melakukan pentes pada web localhost insiden ciber 2. Presentasi terkait progres akhir hasil laporan kp	Tiara Mulia Putri, S.Kom	

Catatan Pembimbing Industri

GAMBARAN KERJA	KETERANGAN
	Presentasi hasil akhir projek

Pembimbing Magang

Tiara Mulia Putri, S.Kom
NIP. 198708052019032001

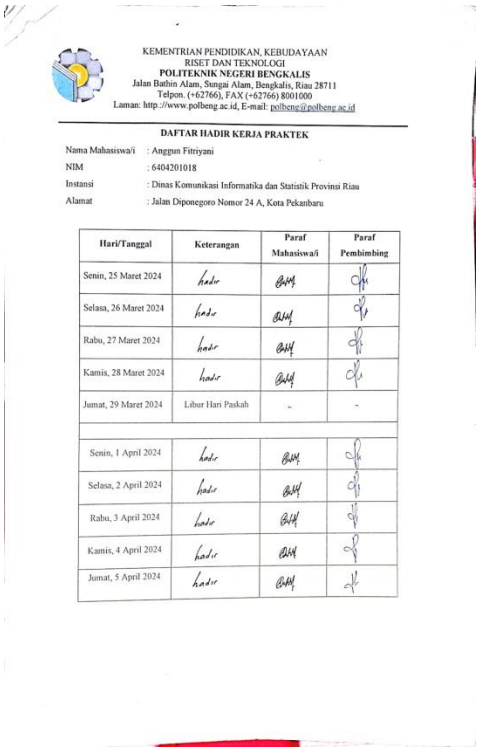
Pengawas Magang

T. Nova Sigma, ST., MM
NIP. 19801104 200604 2 008

Kepala Bidang Pemuridan
Dinas Komunikasi Informatika dan Statistik Provinsi Riau

Candra Liano Saputra, S.T
NIP. 19790914 200501 1 007

Lampiran 4. Absen Harian

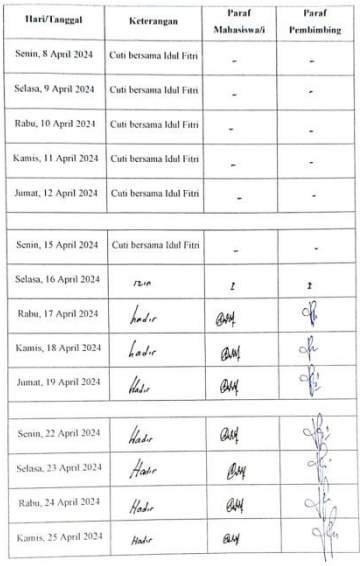


KEMENTRIAN PENDIDIKAN, KEBUDAYAAN
RISET DAN TEKNOLOGI
POLITEKNIK NEGERI BENGKALIS
Jalan Bathin Alam, Sungai Alam, Bengkalis, Riau 28711
Telpon. (+62766), FAX (+62766) 8001000
Laman: http://www.polbeng.ac.id, E-mail: polbeng@polbeng.ac.id

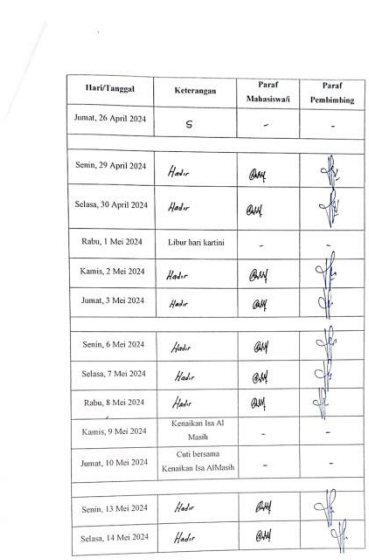
DAFTAR HADIR KERJA PRAKTEK

Nama Mahasiswa/i : Anggun Fitriyani
NIM : 6404201018
Instansi : Dinas Komunikasi Informatika dan Statistik Provinsi Riau
Alamat : Jalan Diponegoro Nomor 24 A, Kota Pekanbaru

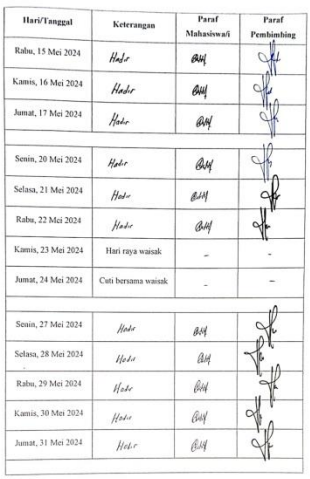
Hari/Tanggal	Keterangan	Paraf Mahasiswa/i	Paraf Pembimbing
Senin, 25 Maret 2024	hadir		
Selasa, 26 Maret 2024	hadir		
Rabu, 27 Maret 2024	hadir		
Kamis, 28 Maret 2024	hadir		
Jumat, 29 Maret 2024	Libur Hari Paskah	-	-
Senin, 1 April 2024	hadir		
Selasa, 2 April 2024	hadir		
Rabu, 3 April 2024	hadir		
Kamis, 4 April 2024	hadir		
Jumat, 5 April 2024	hadir		



Hari/Tanggal	Keterangan	Paraf Mahasiswa/i	Paraf Pembimbing
Senin, 8 April 2024	Cuti bersama Idul Fitri	-	-
Selasa, 9 April 2024	Cuti bersama Idul Fitri	-	-
Rabu, 10 April 2024	Cuti bersama Idul Fitri	-	-
Kamis, 11 April 2024	Cuti bersama Idul Fitri	-	-
Jumat, 12 April 2024	Cuti bersama Idul Fitri	-	-
Senin, 15 April 2024	Cuti bersama Idul Fitri	-	-
Selasa, 16 April 2024	Izin	1	1
Rabu, 17 April 2024	hadir		
Kamis, 18 April 2024	hadir		
Jumat, 19 April 2024	Hadir		
Senin, 22 April 2024	Hadir		
Selasa, 23 April 2024	Hadir		
Rabu, 24 April 2024	Hadir		
Kamis, 25 April 2024	Hadir		



Hari/Tanggal	Keterangan	Paraf Mahasiswa/i	Paraf Pembimbing
Jumat, 26 April 2024	S	-	-
Senin, 29 April 2024	Hadir		
Selasa, 30 April 2024	Hadir		
Rabu, 1 Mei 2024	Libur hari kartini	-	-
Kamis, 2 Mei 2024	Hadir		
Jumat, 3 Mei 2024	Hadir		
Senin, 6 Mei 2024	Hadir		
Selasa, 7 Mei 2024	Hadir		
Rabu, 8 Mei 2024	Hadir		
Kamis, 9 Mei 2024	Kenaikan Isa Al Masih	-	-
Jumat, 10 Mei 2024	Cuti bersama Kenaikan Isa AlMasih	-	-
Senin, 13 Mei 2024	Hadir		
Selasa, 14 Mei 2024	Hadir		



Hari/Tanggal	Keterangan	Paraf Mahasiswa/i	Paraf Pembimbing
Rabu, 15 Mei 2024	Hadir		
Kamis, 16 Mei 2024	Hadir		
Jumat, 17 Mei 2024	Hadir		
Senin, 20 Mei 2024	Hadir		
Selasa, 21 Mei 2024	Hadir		
Rabu, 22 Mei 2024	Hadir		
Kamis, 23 Mei 2024	Hari raya waisak	-	-
Jumat, 24 Mei 2024	Cuti bersama waisak	-	-
Senin, 27 Mei 2024	Hadir		
Selasa, 28 Mei 2024	Hadir		
Rabu, 29 Mei 2024	Hadir		
Kamis, 30 Mei 2024	Hadir		
Jumat, 31 Mei 2024	Hadir		

Hari/Tanggal	Keterangan	Paraf Mahasiswa/i	Paraf Pembimbing
Senin, 3 Juni 2024	Hadir		
Selasa, 4 Juni 2024	Hadir		
Rabu, 5 Juni 2024	Hadir		
Kamis, 6 Juni 2024	Hadir		
Jumat, 7 Juni 2024	Hadir		
Senin, 10 Juni 2024	Hadir		
Selasa, 11 Juni 2024	Hadir		
Rabu, 12 Juni 2024	Hadir		
Kamis, 13 Juni 2024	Hadir		
Jumat, 14 Juni 2024	Hadir		
Senin, 17 Juni 2024	Cuti bersama Idul Adha	-	-
Selasa, 18 Juni 2024	Cuti bersama Idul Adha	-	-
Rabu, 19 Juni 2024	Hadir		
Kamis, 20 Juni 2024	Hadir		
Jumat, 21 Juni 2024	Hadir		
Senin, 24 Juni 2024	Hadir		
Selasa, 25 Juni 2024	Hadir		
Rabu, 26 Juni 2024	Hadir		
Kamis, 27 Juni 2024	Hadir		
Jumat, 28 Juni 2024	Hadir		
Senin, 1 Juli 2024	Hadir		
Selasa, 2 Juli 2024	Hadir		
Rabu, 3 Juli 2024	Hadir		
Kamis, 4 Juli 2024	Hadir		
Jumat, 5 Juli 2024	Hadir		
Senin, 8 Juli 2024	Hadir		
Selasa, 9 Juli 2024	Hadir		
Rabu, 10 Juli 2024	Hadir		
Kamis, 11 Juli 2024	Hadir		
Jumat, 12 Juli 2024	Hadir		
Senin, 15 Juli 2024	Hadir		
Selasa, 16 Juli 2024	Hadir		
Rabu, 17 Juli 2024	Hadir		
Kamis, 18 Juli 2024	Hadir		
Jumat, 19 Juli 2024	Hadir		

Diketahui Oleh :

Pengawas Magang

T. Nova Sakma, SE, MM.
NIP. 198011 04 200604 2 008

Pembimbing Magang

Tiara Mulia Putri, S.Kom
NIP. 19870505 201903 2 001

Kepala Bidang Persandian
Dinas Komunikasi Informatika dan Statistik Provinsi Riau

Candra Lesano Saputra, S.T
NIP. 19790914 200501 1 007

Lampiran 5. Dokumentasi Kegiatan

1. **Presentasi Final Project**

2. **Penyerahan Cendramata Pada Instansi**

Lampiran 6. Sertifikat Magang