LAPORAN KERJA PRAKTEK

DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK PROVINSI RIAU

MELAKUKAN PENETRATION TESTING PADA *E-REPORTING* MENGGUNAKAN SERANGAN CSRF *(CROSS SITE REQUEST FORGERY)*

RISKY SERI HARTATI

6404201017

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

RISKY SERI HARTATI
6404201017

Pekanbaru, 19 Juli 2024

Pembimbing Magang	Dosen Pembimbing Keamanan Sistem Informasi
Tiara Mulia Putri, S.Kom	**Mansur, M.Kom**
NIP. 19870505 201903 2 001	**NIP. 198209192021211003**

Disetujui
Ketua Program Studi Keamanan Sistem Informasi
Politeknik Negeri Bengkalis

Jarot, M.Kom
NIP. 198611072015041002

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, atas rahmat dan hidayah-Nya sehingga laporan kerja praktek ini dapat diselesaikan dengan baik dan tepat waktu. Laporan ini merupakan salah satu syarat dalam menyelesaikan program studi di Politeknik Negeri Bengkalis, khususnya pada Jurusan Teknik Informatika Sarjana Terapan Keamanan Sistem Informasi.

Kerja praktek ini dilaksanakan di Dinas Komunikasi, Informatika dan Statistik Provinsi Riau, pada Bidang Persandian periode 25 Maret hingga 19 Juli 2024. Tujuan utama dari pelaksanaan kerja praktek ini adalah untuk mengaplikasikan teori dan pengetahuan yang telah diperoleh selama perkuliahan ke dalam dunia kerja yang sesungguhnya, sehingga dapat meningkatkankompetensi dan keterampilan mahasiswa.

Selama pelaksanaan kerja praktek, kami mendapatkan banyak pengalaman berharga dan ilmu pengetahuan yang tidak hanya bersifat teknis tetapi juga manajerial dan interpersonal. Pengalaman ini diharapkan dapat menjadi bekal dalam menghadapi dunia kerja di masa depan.

Pada kesempatan ini, kami ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Johny Custer, S.T., M.T selaku Direktur Politeknik NegeriBengkalis.
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. Ibu Rezki Kurniati, S.Kom., M.Kom, selaku Koordinator Kerja Praktek Program Studi Keamanan Sistem Informasi.
5. Bapak Mansur, S.Kom., M.Kom, selaku Dosen Pembimbing Kerja Praktek Politeknik Negeri Bengkalis.
6. Bapak Candra Lisano, S.T Selaku Kepala Bidang Persandian Diskominfotik Provinsi Riau
7. Mbak Tiara Mulia Putri, S.Kom dan pak Asroy Cristian Sitorus selaku pembimbing di Dinas Komunikasi, Informatika dan Statistik Provinsi Riau, Bidang Persandian yang telah memberikan bimbingan, arahan, dan

kesempatan untuk belajar serta berkontribusi selama kerja praktek berlangsung.

8. Seluruh staf dan karyawan, yang telah memberikan bantuan dan kerjasama selama pelaksanaan kerja praktek.
9. Orang tua dan teman-teman yang selalu memberikan dukungan moril dan materil.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna, oleh karenaitu kami mengharapkan kritik dan saran yang membangun dari semua pihak demi perbaikan dan peningkatan kualitas di masa mendatang. Akhir kata, semoga laporan ini dapat bermanfaat bagi pembaca dan semua pihak yang berkepentingan.Terima kasih.

Bengkalis, 19 April 2024

Risky Seri Hartati

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB 1

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 mahasiswa yang melaksanakan kerja praktek.

Dalam pelaksanaan Kerja Praktek di Kantor Diskominfotik Provinsi Riau penulis mendapatkan tugas untuk melakukan uji penetration testing pada aplikasi pelaporan insiden siber menggunakan serangan CSRF (Cross Site Request Forgery).

1.2. Tujuan Dan Manfaat Kerja Praktek

Tujuan yang diperoleh dari Kerja Praktek adalah sebagai berikut:

1. Menerapkan ilmu yang diperoleh dari kampus.
1. Meningkatkan kemampuan mengenai ilmu Keamanan Sitem Informasi.
2. Menambah pengetahuan, wawasan dan pengalaman serta mengasah kemampuan dan keterampilan penulis dalam dunia kerja.
3. Memudahkan para staff/publik untuk melakukan pelaporan agar cepat ditindaklanjuti insiden siber yang terjadi.
4. 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 *CSRF (Cross Site Request Forgery) dan SQL Injection.*

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

Dalam melakukan uji penetrasi menggunakan teknik Cross-Site Request Forgery (CSRF), output yang dihasilkan mencakup berbagai temuan dan analisis terkait kerentanan aplikasi web terhadap serangan CSRF. Berikut adalah output yang dihasilkan dari uji penetrasi menggunakan teknik CSRF:

1. Identifikasi kerentanan seperti mengidentifikasi daftar endpoint Rentan, yaitu sepert endpoint atau fungsi dalam aplikasi web yang rentan terhadap serangan CSRF. Dan deskripsi kerentanan seperti penjelasan rinci tentang kerentanan yang ditemukan, termasuk bagaimana CSRF dapat dieksploitasi pada endpoint tersebut.
2. Proof of Concept (PoC), berisi kode atau script eksploitasi sperti contoh kode atau skrip yang menunjukkan bagaimana serangan CSRF dapat dilakukan. Ini biasanya berupa formulir HTML atau skrip yang mengirimkan permintaan berbahaya ke server tanpa sepengetahuan pengguna. Selanjutnya demonstrasi Serangan, yaitu bukti bahwa serangan berhasil dilakukan, seperti perubahan data pengguna, transaksi yang tidak sah, atau tindakan lainnya yang membuktikan bahwa serangan CSRF dapat dieksploitasi.
3. Analisis risiko, meganalisis dampak potensial seperti analisis tentang potensi dampak dari kerentanan CSRF, termasuk data yang bisa diakses atau diubah, dan konsekuensi bagi pengguna dan aplikasi. Penilaian risiko berdasarkan tingkat keparahan dan kemungkinan eksploitasi kerentanan.
4. Rekomendasi perbaikan, menentukan langkah-langkah mitigasi seperti Saran dan langkah-langkah yang perlu diambil untuk mengatasi kerentanan CSRF. Ini bisa mencakup penerapan token CSRF, validasi ulang permintaan penting, atau peningkatan autentikasi pengguna.

5. Laporan penetrasi, merupakan dokumentasi lengkap laporan komprehensif yang mencakup semua temuan, bukti, analisis, dan rekomendasi. Laporan ini biasanya disusun dalam format yang mudah dibaca dan dipahami oleh tim teknis maupun manajerial.
6. Peningkatan Keamanan Aplikasi, penerapan Fixes (perbaikan) hasil dari rekomendasi yang diimplementasikan, menunjukkan peningkatan keamanan aplikasi dan langkah-langkah yang telah diambil untuk menutup kerentanan CSRF yang ditemukan.

BAB II
GAMBARAN UMUM DISKOMINFOTIK PROVINSI RIAU

2.1 Profil dan Sejarah Diskominfotik 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 Perusahaan

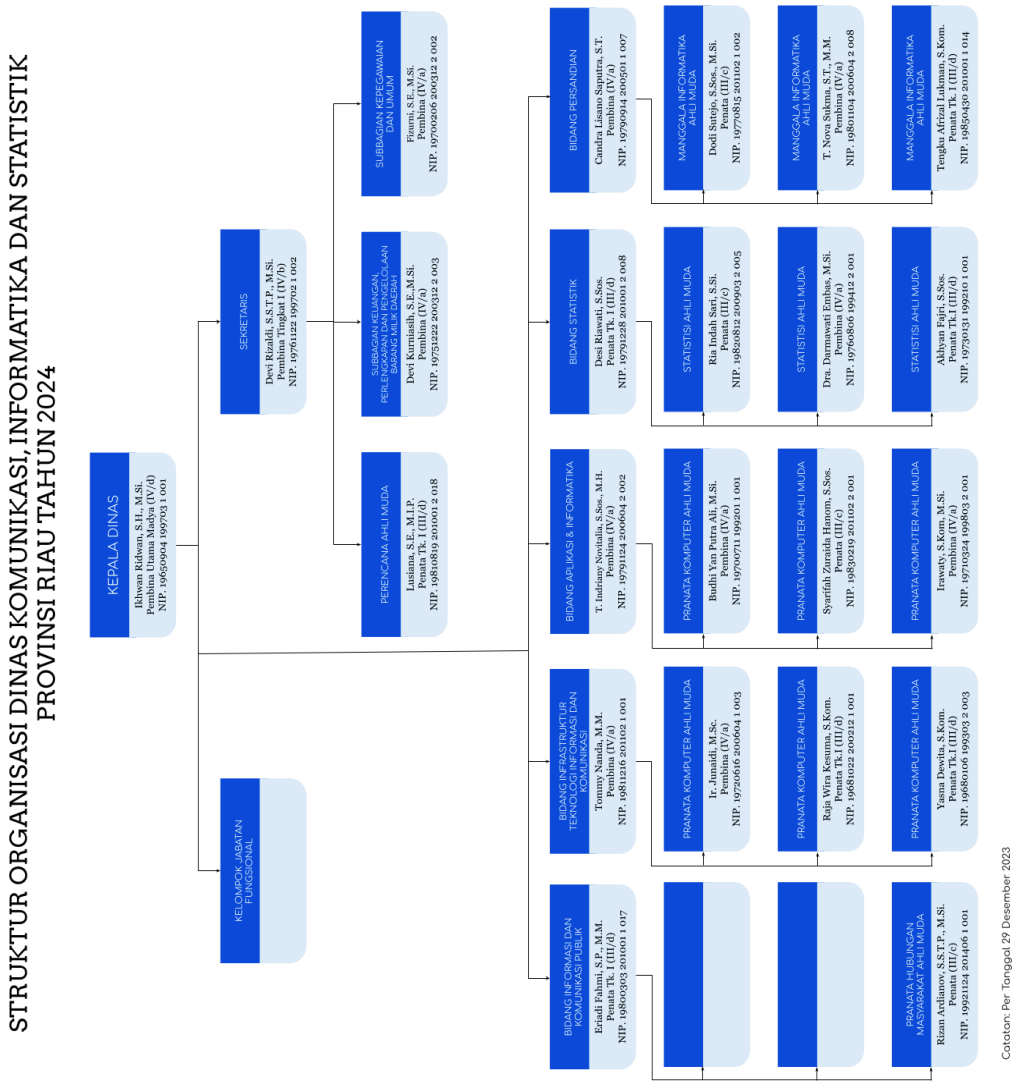
2.2.1 Visi

Terwujudnya Layanan Komunikasi, Informatika dan Statistik yang handal dan berdaya saing.

2.2.2 Misi

Mewujudkan manajemen penyelenggaraan pemerintah yang baik (goodgovernance), efektif dan efesien, professional, transparan dan akuntabel.

2.3 Struktur Organisasi Perusahaan



Gambar 2.1 Struktur Organisasi Diskominfotik Provinsi Riau

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

2.3.1 Kepala Bidang Informatika Komunikasi Public

Kepala bidang komunikasi 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 pemantau, 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 pemimpin sesuai tugas dan fungsinya. Bidang informasi dan komunikasi public terdiri dari:
    a) Kepala Seksi Komunikasi Informasi.
    b) Kepala Seksi Diseminasi Informasi.
    c) Kelapa Seksi Multimedia dan Dokumentasi.

2.4 Ruang Lingkup Perusahaan

Waktu pelaksanaan kerja praktek (KP) dilaksanakan selama 4 bulan terhitung dari tanggal 25 maret 2024 sampai 19 juli 2024. Kerja Praktek dilakukan di Dinas Komunikasi Informatika dan Statistik (Diskominfotik) Provinsi Riau yang beralamat di Jalan Diponegoro, pekanbaru kota, kota pekanbaru, riau. Jam operasional Diskominfotik Provinsi Riau dari senin- rabu yaitu pukul 07:30- 16:00 sedangkan hari kamis-jum’at yaitu pukul 07:30-16:30. Selamat 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 yang dilaksanakan bersifat flexsibel karena pekerjaan dilakukan sesuai arahan pembimbing lapangan. Sepanjang melakukan Kerja Praktek terdapat beberapa pekerjaaan yang diberikan oleh pihak kantora yaitu:

3.3.1 Melakukan Uji Penetrasi Pada Sistem Pelaporan Insiden Siber Menggunakan Serangan CSRF (Cross Site Request Forgery)

Dalam hal ini saya bertugas untuk melakukan *Penetration Testing* dengan menggunakan serangan CSRF (Cross Site Request Forgery) pada website pelaporan insiden siber.

3.2 Perangkat Yang Digunakan

3.2.1. 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, alat hacking, dan aplikasi untuk pengujian penetrasi, analisis jaringan, dan eksploitasi kerentanan.

3.2.2. VirtualBox atau VMware

Adalah perangkat lunak virtualisasi open-source yang banyak digunakan dalam penetration testing (pentest). Dalam konteks pentesting, VirtualBox memungkinkan pentester untuk membuat lingkungan pengujian yang terisolasi dan aman untuk mengidentifikasi dan mengeksploitasi kerentanan dalam sistem dan jaringan.

3.2.3. Kali Linux

Alat yang sangat penting dalam toolkit pentester, menyediakan kumpulan alat yang lengkap dan terintegrasi untuk pengujian keamanan. Dengan

kemampuannya untuk menjalankan berbagai alat keamanan dan fitur dukungan virtualisasi serta pembaharuan yang berkelanjutan.

3.2.4. Burp suite

Burp Suite adalah alat yang membantu menguji keamanan aplikasi web. Dengan Burp Suite, kita bisa melihat dan mengubah data yang dikirim dan diterima oleh aplikasi, menemukan halaman dan titik akhir dalam aplikasi, serta mendeteksi masalah keamanan seperti SQL injection dan XSS. Alat ini juga memungkinkan kita melakukan serangan untuk mencari kelemahan, mengirim ulang dan memodifikasi permintaan, dan menganalisis kekuatan token sesi.

3.2.5. Web Browser

Web browser dapat didefinisikan sebagai perangkat lunak yang memungkinkan interaksi dengan web server dan berbagai layanan internet lainnya. Web browser sering menjadi target eksploitasi karena mereka berinteraksi dengan berbagai jenis konten web yang mungkin mengandung kode berbahaya. Kerentanan dalam browser atau plugin dapat dimanfaatkan untuk menjalankan kode arbitrer, mencuri informasi, atau melakukan serangan seperti cross-site scripting (XSS) dan cross-site request forgery (CSRF).

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. Menyelesaikan tugas project yang dikerjakan.
2) Mendapatkan pemahaman yang lebih mendalam tentang bagaimana konsep-konsep teori diterapkan dalam lingkungan kerja nyata.

3) Bagaimana tanggung jawab dalam setiap tugas yang telah diberikan dan disiplin terhadap waktu.
4) Melakukan penetration testing pada *E-Reporting* dengan menggunakan serangan *CSRF (Cross Site Request Forgery)*
5) Terselesainya pengujian sistem informasi manajemen pengetahuan provinsi Riau.

BAB IV

PENGUJIAN

4.1 Metodologi

4.1.1 Prosedur Uji Penetrasi Menggunakan Teknik serangan CSRF (Cross-Site Request Forgery)

1) Persiapan
    1. Menentukan target, identifikasi aplikasi web atau halaman spesifik yang akan diuji.
    2. Mengumpulkan informasi, cari tahu tentang arsitektur aplikasi, endpoint yang digunakan, formulir yang ada, dan parameter yang mungkin rentan terhadap CSRF.
    3. Menyiapkan lingkungan pengujian, buat akun pengguna yang sah di aplikasi target dan pastikan Anda memiliki alat yang diperlukan seperti Burp Suite, OWASP ZAP, atau alat pengujian lainnya.
2) Identifikasi Kerentanan
    1. Analisis Formulir dan Permintaan

       Gunakan alat proxy seperti Burp Suite untuk menginspeksi permintaan HTTP yang dikirim oleh aplikasi. Dan Cari tahu apakah formulir yang mengubah data (misalnya, update profil, transfer uang) menggunakan token anti-CSRF.
    2. Hapus Token CSRF

       Coba hapus token CSRF dari permintaan dan kirim ulang permintaan menggunakan alat proxy. Jika permintaan tetap diproses, ini menunjukkan bahwa aplikasi mungkin rentan terhadap CSRF.
3) Buat Eksploitasi CSRF
    1. Buat Halaman Berbahaya

       Buat halaman HTML atau skrip yang berisi kode untuk mengirim permintaan berbahaya ke aplikasi target tanpa token CSRF. Contoh eksploitasi sederhana.

```
<html>
<body>
  <form action="https://target.com/transfer"
method="POST">
    <input type="hidden" name="amount" value="1000">
    <input type="hidden" name="account"
value="1234567890">
    <input type="submit" value="Submit">
  </form>
  <script>
    document.forms[0].submit();
  </script>
</body>
```

2. Host Halaman Berbahaya

Upload halaman ini ke server yang Anda kendalikan atau gunakan metode lain untuk mengarahkan korban mengunjungi halaman tersebut (misalnya, melalui email phishing atau pesan yang menarik).

4) Uji Eksploitasi

1. Login sebagai pengguna korban, menggunakan akun pengguna sah dan login ke aplikasi target di browser.
2. Kunjungi halaman berbahaya, membuka halaman berbahaya di browser yang sama dan lihat apakah tindakan yang tidak sah terjadi di aplikasi target (misalnya, transfer uang berhasil)

5) Dokumentasi dan Pelaporan

1. Dokumentasikan temuan, mencatat setiap langkah yang diambil, hasil pengujian, dan bukti serangan yang berhasil (misalnya, screenshot atau log HTTP).
2. Membuat laporan, menyusun laporan yang merinci kerentanan, dampaknya, dan rekomendasi mitigasi. Sertakan bukti konsep (PoC) dan langkah-langkah yang diambil selama pengujian.

6) Mitigasi dan Pencegahan

   1. Gunakan token anti-csrf, mengimplementasikan token anti-CSRF pada setiap permintaan yang mengubah data di server.
   2. Verifikasi Origin dan Referer, memeriksa header Origin dan Referer pada setiap permintaan untuk memastikan mereka berasal dari sumber yang sah.
   3. Validasi input secara ketat, memastikan semua input yang diterima oleh server divalidasi dengan benar untuk mencegah injeksi berbahaya.

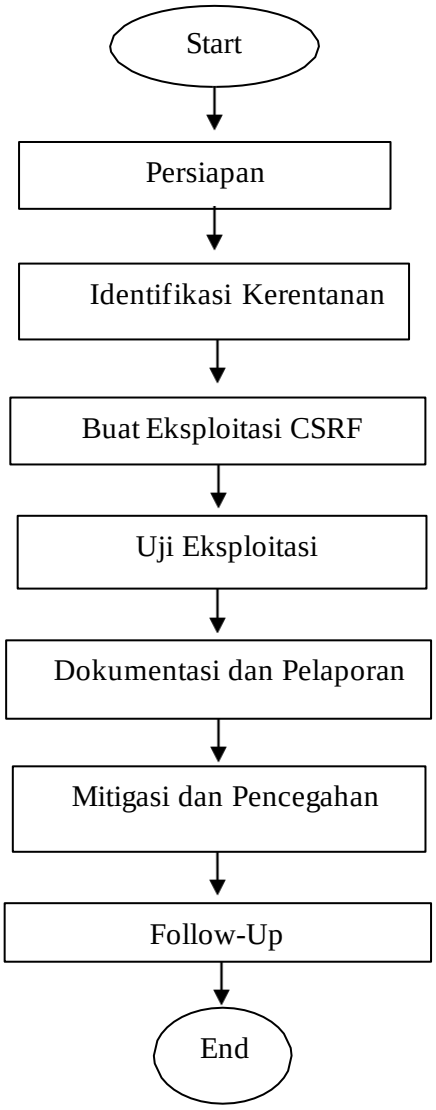
7) Follow-Up, tindak lanjut dan perbaikan, berkontribusi dengan tim pengembang untuk memastikan bahwa kerentanan telah diperbaiki. Dan melakukan pengujian ulang untuk memastikan bahwa mitigasi yang diterapkan efektif dan tidak ada kerentanan baru yang muncul.

4.1.2 Metodologi Pengumpulan Data

Metode pengumpulan data berdasarkan teknik dari serangan itu sendiri yaitu serangan csrf. Berikut adalah metodologi pengumpulan data yang terstruktur untuk pentest menggunakan teknik serangan CSRF[3]:

1. Analalisa, merupakan metode awal dalam melakukan penelitian, analisa digunakan untuk menganalisis rancangan sistem yang ada pada lokasi penelitian.
2. Perancangan, merupakan metode kedua dimana tahap ini mampu menerjemahkan spesifikasi kebutuhan perangkat lunak sistem operasi kali linux untuk diimplementasi pada metode analisa.
3. Pengujian, merupakan metode ketiga, yakni tahap pengujian penetration testing untuk mendapatkan hasil dan menemukan celah keamanan.
4. Dokumentasi, merupakan metode selanjutnya, pada proses ini, yakni melakukan studi pustaka, mempelajari jurnal yang relevan serta sumber lain yang berkaitan dengan penelitian untuk dijadikan referensi.

4.1.3 Proses Perancangan Sistem



Berikut merupakan penjelasan setiap tahap dalam flowchart:

1. Persiapan

   Pada tahap ini mentukan ruang lingkup dan tujuan dari pengujian, termasuk didalamnya sistem yang akan diuji dan metode yang digunakan.

2. Identifikasi Kerentanan

   Pada tahap ini mengumpulkan data yang selanjutnya diklarifikasikan sebagai data pasif dari pengujian penetrasi karena mengumpulkan data secara manual, melalui dokumen terkait atau informasi publik atau bertanya langsung kepada pihak-pihak yang terlibat langsung dengan sistem.

3. Buat Eksploitasi CSRF

   Pada tahap ini melakukan pengumpulkan informasi menggunakan halaman url yang berbahaya dari tahap ini jika proses eksploitasi berhasil maka kita memperoleh data yang bersifat penting pengguna asli dari target.

4. Uji Eksploitasi

   Pada tahap ini tahapan analisis informasi secara detail resiko yang diperoleh sebelumnnya dan celah keamanan yang mungkin disebabkan oleh kerentanan pada sistem.

5. Dokumentasi dan Pelaporan

   Pada tahap ini mencatat setiap langkah yang diambil, hasil pengujian, dan bukti serangan yang berhasil. Dan menyusun laporan yang merinci kerentanan, dampaknya, dan rekomendasi mitigasi.

6. Mitigasi dan Pencegahan

   Pada tahap ini analisis akhir secara keseluruhan menggambarkan semuaa temuan dan setelah adanya rencana analisis yang sistematis, petunjuk teknis untuk meningkatkan keselamatan.

7. Follow up

   Pada tahap ini berkontribusi dengan tim pengembang untuk memastikan bahwa kerentanan telah diperbaiki. Dan melakukan pengujian ulang untuk memastikan bahwa mitigasi yang diterapkan efektif dan tidak ada kerentanan baru yang muncul.

4.1.4 Tahapan dan Jadwal Pelaksanaan

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

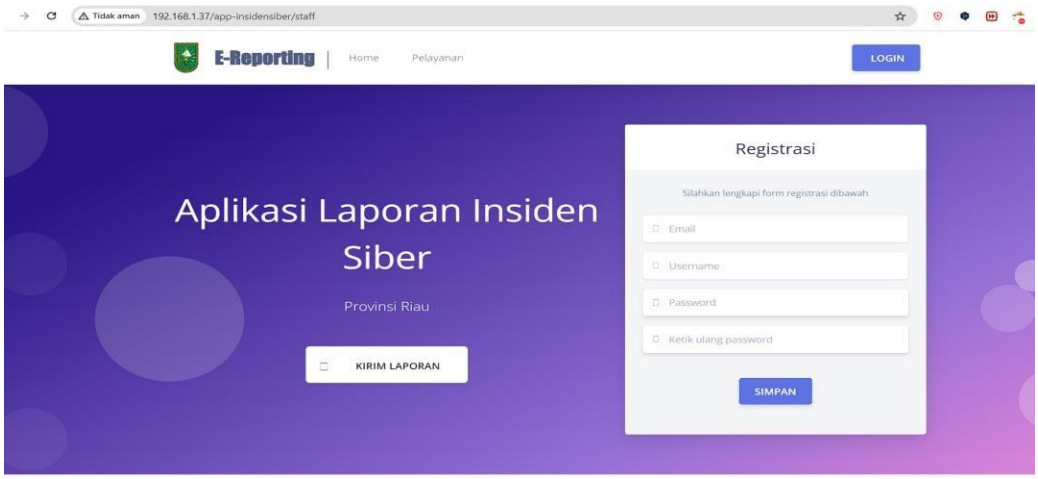
Tabel 4.1 Tabel Jadwal Pelaksanaan

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.	Planning dan Scanning																
2.	Eksploitasi																
3.	Monitoring																
4.	Analisa dan pelaporan																

4.2 Perancangan dan Implementasi

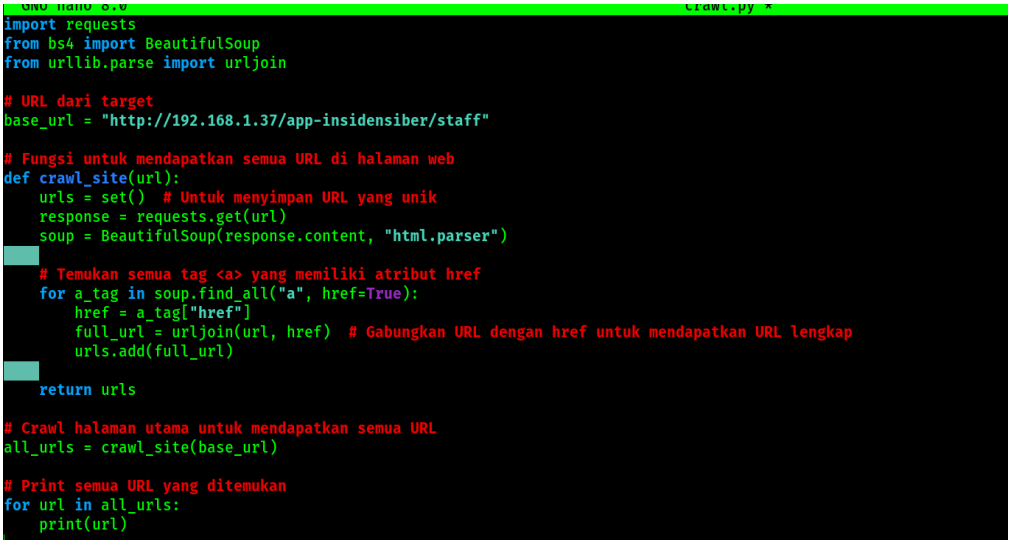
Berikut merupakan rancangan dan implementasi sistem dalam melakukan uji kerentanan serangan csrf (Cross-Site Request Forgery):

1) Menentukan web aplikasi yang akan di uji kerentanannya terhadap CSRF. Untuk pengujian ini menggunakan web berikut ini:



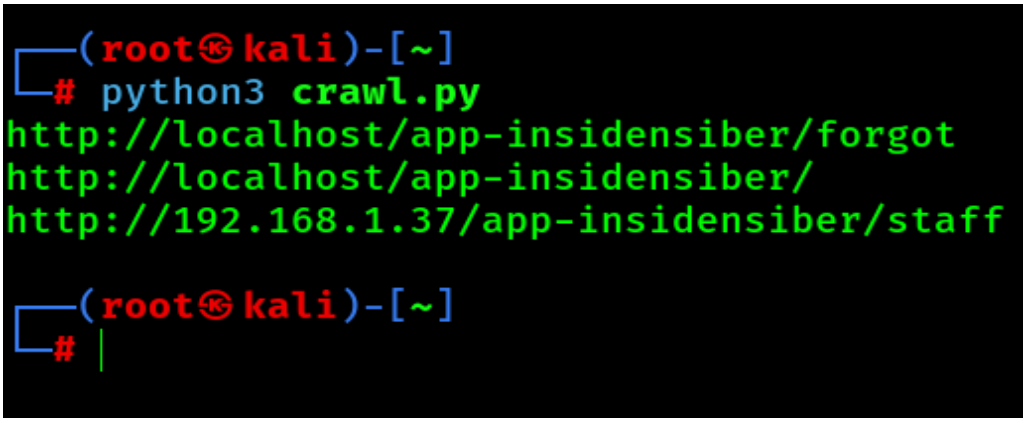
Gambar 4.1 Aplikasi Layanan Insiden Siber

2) Menentukan endpoint atau fitur yang dapat di uji yang dapat dimanfaatkan oleh kerentanan CSRF. Langkah pertama saya menggunakan crawling untuk menadaptkan seluruh endpoint. Saya menggunakan library request dan BeautifulSoup untuk melakukan crawling dan menemukan semua endpoint pada website tersebut.



```
import requests
from bs4 import BeautifulSoup
from urllib.parse import urljoin

# URL dari target
base_url = "http://192.168.1.37/app-insidensiber/staff"

# Fungsi untuk mendapatkan semua URL di halaman web
def crawl_site(url):
    urls = set()  # Untuk menyimpan URL yang unik
    response = requests.get(url)
    soup = BeautifulSoup(response.content, "html.parser")

    # Temukan semua tag <a> yang memiliki atribut href
    for a_tag in soup.find_all("a", href=True):
        href = a_tag["href"]
        full_url = urljoin(url, href)  # Gabungkan URL dengan href untuk mendapatkan URL lengkap
        urls.add(full_url)

    return urls

# Crawl halaman utama untuk mendapatkan semua URL
all_urls = crawl_site(base_url)

# Print semua URL yang ditemukan
for url in all_urls:
    print(url)
```

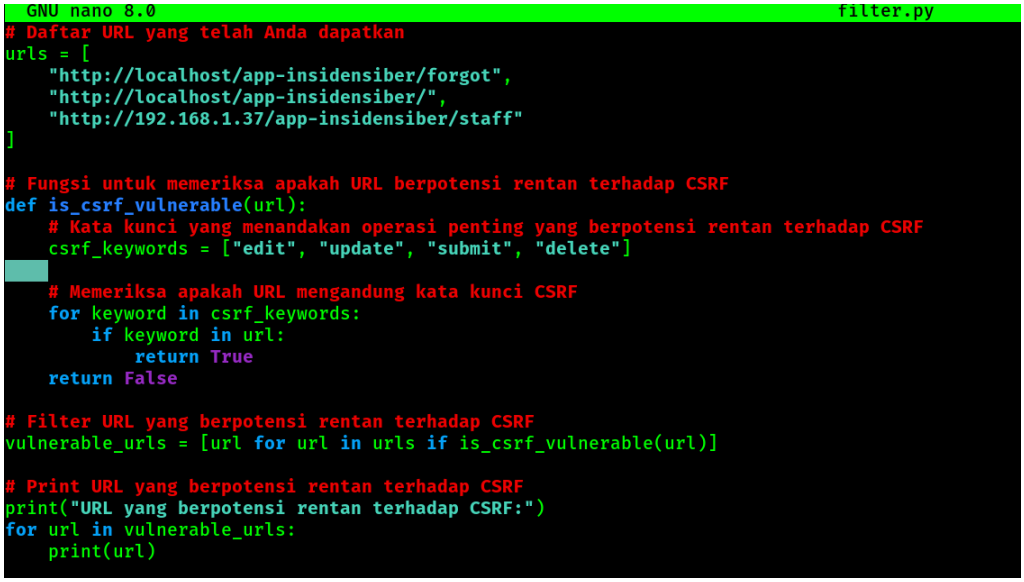
Gambar 4.2 Menentukan Endpoint pada website



```
┌──(root㉿kali)-[~]
└─# python3 crawl.py
http://localhost/app-insidensiber/forgot
http://localhost/app-insidensiber/
http://192.168.1.37/app-insidensiber/staff

┌──(root㉿kali)-[~]
└─#
```

Gambar 4.3 Hasil dari Endpoint

3) Setelah saya mendapatkan hasilnya, kemudian selanjutnya melakukan filtering endpoint yang berpotensi terhadap kerentanan CSRF. Berikut adalah tools untuk memfilter url yang berpotensi rentan terhadap CSRF berdasarkan kata kunci yang umum terkait operasi-operasi yang beresiko.

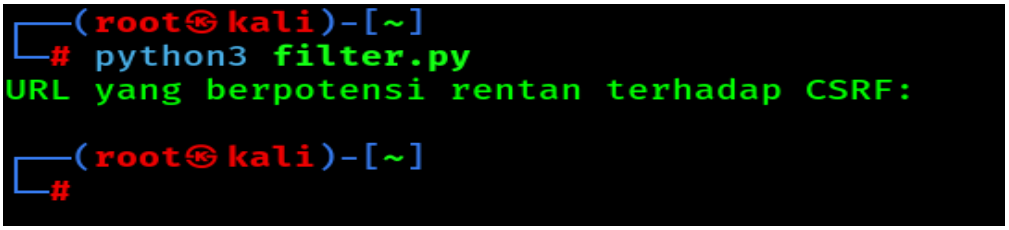


Gambar 4.4 Melakukan Filtering Endpoint

Keterangan:

1. Pola Kata Kunci: Menggunakan daftar kata kunci seperti "edit", "update", "submit", dan "delete" untuk mencocokkan URL yang berpotensi melakukan operasi penting.
2. Fungsi is_csrf_vulnerable: Memeriksa setiap URL dari daftar yang Anda miliki untuk menentukan apakah mereka memenuhi kriteria rentan terhadap CSRF berdasarkan kata kunci yang diberikan.
3. Filtering: Menggunakan list comprehension untuk memfilter hanya URL yang memenuhi kriteria CSRF untuk ditampilkan.

4) Dari hasil eksekusi program ini menunjukkan bahwa skrip telah dijalankan tanpa ada URL yang ditemukan yang berpotensi rentan terhadap Cross-Site Request Forgery (CSRF). Dalam konteks pengujian keamanan, ini bisa memiliki beberapa makna:



Gambar 4.5 Hasil dari Filtering Endpoint

1. Tidak Ada URL yang Rentan: Tidak ada URL yang ditemukan dalam daftar yang diproses yang memenuhi kriteria yang saya tetapkan untuk rentan terhadap CSRF. Ini bisa berarti bahwa aplikasi web yang saya uji mungkin memiliki pengaturan keamanan yang baik untuk melindungi terhadap serangan CSRF, atau mungkin tidak ada operasi penting yang dapat dimanfaatkan secara langsung melalui CSRF.

2. Perlu Diperiksa Lebih Lanjut: Meskipun tidak ada URL yang terdaftar, ini tidak selalu berarti bahwa aplikasi web sepenuhnya aman dari serangan CSRF. Mungkin diperlukan tinjauan lebih lanjut terhadap fitur-fitur aplikasi web yang lebih dalam untuk memastikan tidak ada celah yang terlewatkan.

3. Perlindungan Terhadap CSRF: Hasil ini dapat menunjukkan bahwa implementasi aplikasi web telah mengimplementasikan perlindungan yang memadai terhadap serangan CSRF, seperti menggunakan token CSRF atau memvalidasi referer header.

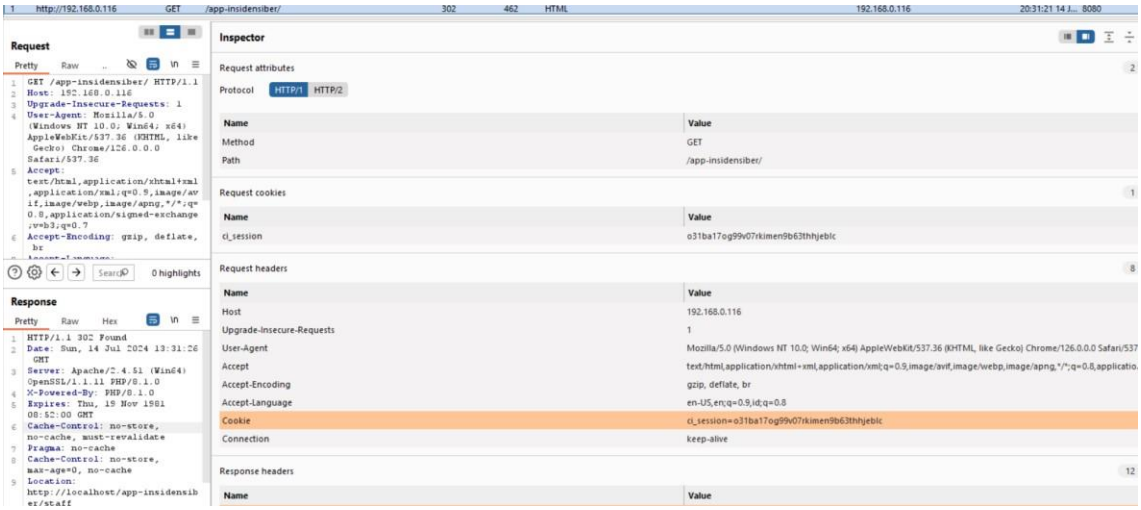
Berikut merupakan rancangan dan implementasi sistem dalam melakukan uji kerentanan serangan csrf (Cross-Site Request Forgery) menggunakan BURPSUITE:

1) Rekam Permintaan: Di Burp Suite, buka tab "Proxy" dan pastikan "Intercept" dinyalakan. Lalu, buka aplikasi web target yang ingin Anda uji.

```
GET /app-insidensiber/ HTTP/1.1
Host: 192.168.0.116
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
ation/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,id;q=0.8
Cookie: ci_session=o3lbal7og99v07rkimen9b63thhjeblc
Connection: keep-alive
```

Gambar 4.6 Uji Kerentanan CSRF menggunakan Burpsuite

2) Identifikasi Request yang Digunakan: Temukan permintaan HTTP POST yang mengandung tindakan yang dapat dimanfaatkan untuk CSRF (misalnya, mengirim formulir, mengubah data, dll). Dari hasil yang diberikan, tidak ada indikasi permintanan parameter POST.



Gambar 4.7 Hasil Pengujian Menggunakan Burpsuite

Kesimpulan:

Berdasarkan pengujian kerentanan CSRF menggunakan Burp Suite dan Crawl:

1. Implementasi Perlindungan CSRF, hasil uji menunjukkan bahwa aplikasi web telah mengimplementasikan perlindungan terhadap serangan CSRF dengan baik. Ini biasanya meliputi penggunaan token CSRF yang valid dan/atau validasi header referer untuk memastikan bahwa permintaan berasal dari sumber yang sah.

2. Kesimpulan Positif, dengan tidak berhasilnya serangan CSRF ini, menunjukkan bahwa pengaturan keamanan aplikasi pelaporan insiden siber memungkinkan untuk memblokir serangan jenis ini secara efektif. Hal ini penting untuk menjaga integritas dan keamanan data pengguna.

3. 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.

4. Rekomendasi: Disarankan untuk tetap memperbarui dan meningkatkan praktik keamanan seperti validasi input, penggunaan token CSRF yang kuat, dan pembaruan reguler terhadap kerangka kerja dan pustaka yang digunakan dalam pengembangan aplikasi web.

Dengan demikian, kesimpulan keseluruhan adalah bahwa aplikasi pelaporan insiden siber saat ini dilindungi dengan baik dari serangan CSRF, tetapi penting untuk tetap waspada dan proaktif dalam menjaga keamanan dan perlindungan data pengguna di masa mendatang.

Berikut merupakan tabel hasil uji penetration menggunakan metode serangan CSRF (Cross-Site Request Forgery) yang menunjukkan hasil bahwa aplikasi tidak rentan terhadap serangan tersebut:

Tabel 4.2 Tabel Hasil Pengujian

No.	Endpoint	Parameter	Token CSRF	Hasil Uji	Hasil Uji
1.	/update-profile	/update-profile	Valid	Tidak Rentan	CSRF token valid dan diterima
2.	/change-password	old_password, new_password	Valid	Tidak Rentan	CSRF token valid dan diterima
3.	/submit-form	form_data	Invalid	Tidak Rentan	CSRF token tidak valid, permintaan ditolak
4.	/delete-account	user_id	Valid	Tidak Rentan	CSRF token valid dan diterima
5.	/transfer-funds	account_id, amount	Valid	Tidak Rentan	CSRF token valid dan diterima
6.	/settings/update-email	new_email	Invalid	Tidak Rentan	CSRF token tidak valid, permintaan ditolak

Tabel diatas menunjukkan bahwa aplikasi telah berhasil melindungi dirinya dari serangan CSRF. Setiap permintaan dengan token CSRF yang valid diproses dengan benar, sementara permintaan dengan token yang tidak valid ditolak. Ini menandakan bahwa aplikasi memiliki mekanisme perlindungan CSRF yang efektif dan tidak rentan terhadap serangan CSRF dalam pengujian yang dilakukan.

BAB V

PENUTUP

5.1. Kesimpulan

Kesimpulan untuk judul "Melakukan Penetration Testing Pada E- Reporting Menggunakan Serangan Csrf (Cross Site Request Forgery)" antara lain yaitu:

1. Berdasarkan pengujian kerentanan CSRF menggunakan Burp Suite dan Crawl ini, implementasi perlindungan CSRF, hasil uji menunjukkan bahwa aplikasi pelaporan insiden siber telah mengimplementasikan perlindungan terhadap serangan CSRF dengan baik.
2. Dengan tidak berhasilnya serangan CSRF ini, menunjukkan bahwa pengaturan keamanan aplikasi pelaporan insiden siber memungkinkan untuk memblokir serangan jenis ini secara efektif. Hal ini penting untuk menjaga integritas dan keamanan data pengguna.
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 penetration testing pada e- reporting menggunakan serangan csrf (cross site request forgery) sampai pada pembuatan laporan kerja praktek ini adalah sebagai berikut:

1. 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.
2. Disarankan untuk tetap memperbarui dan meningkatkan praktik keamanan seperti validasi input, penggunaan token CSRF yang kuat, dan pembaruan

reguler terhadap kerangka kerja dan pustaka yang digunakan dalam pengembangan aplikasi web.

DAFTAR PUSTAKA

[1] U. M. Area, “Universitas medan area,” pp. 1–12.

[2] Gramedia Blog, “Jurusan Keamanan Sistem Informasi,” *Gramedia.com*, 2022. https://www.gramedia.com/pendidikan/jurusan-keamanan-sistem-informasi/ (accessed Sep. 03, 2024).

[3] M. A. Adiguna and B. W. Widagdo, “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r),” *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, 2022, doi: 10.47970/siskom-kb.v5i2.268.

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/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 Keamanan Sistem Informasi
4.	Rhima Diana	6304201241	Sarjana Terapan Keamanan Sistem Informasi

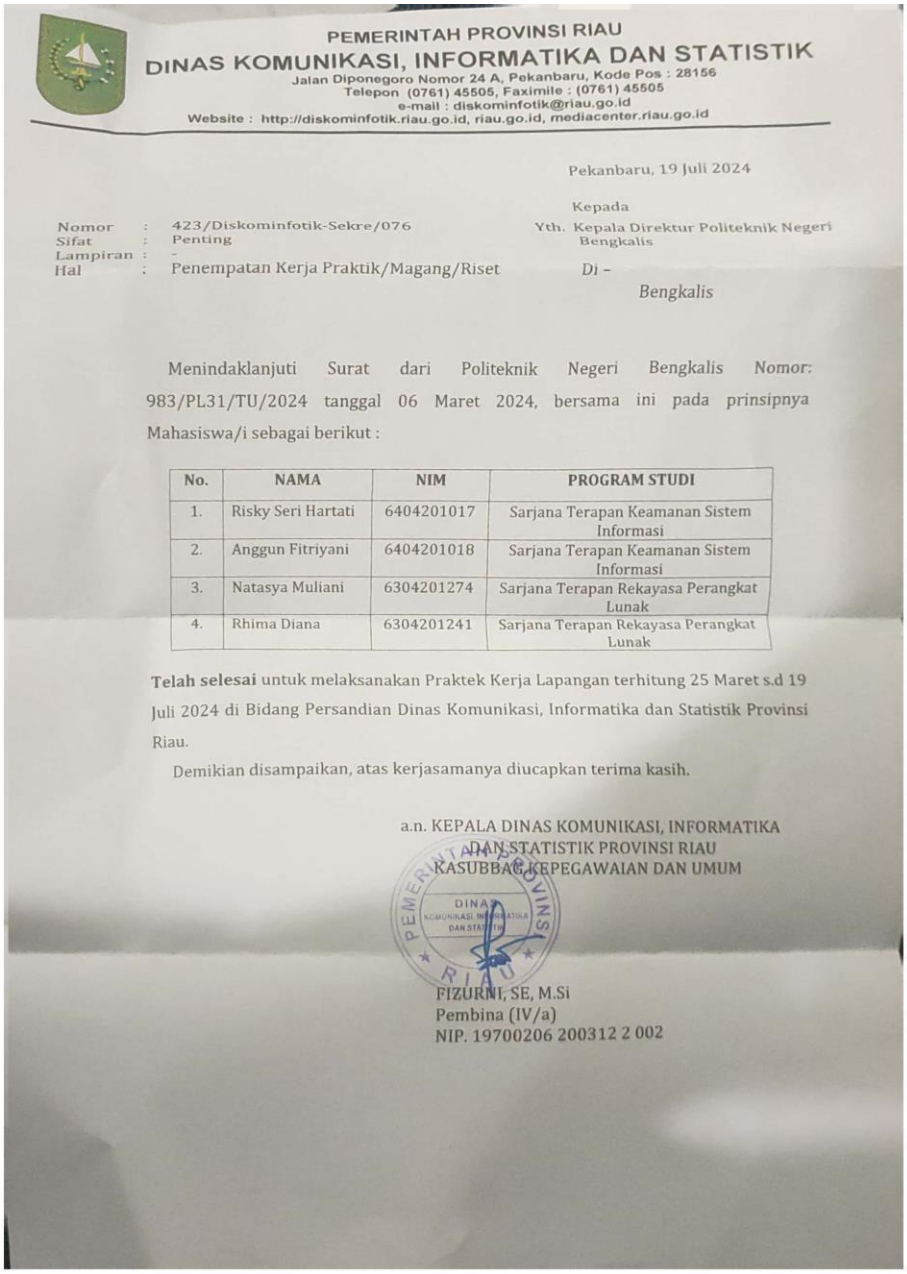
Diterima untuk melaksanakan Praktek Kerja Lapangan terhitung 21 Maret s.d 19 Juli 2024 di Bidang Persandian Dinas Komunikasi, Informatika dan Statistik Provinsi Riau.

Demikian disampaikan, atas kerjasamanya diucapkan terima kasih.

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

FIKURNI, 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 : Risky Seri Hartati
NIM : 6404201017
Program Studi : Keamanan Sistem Informasi
Politeknik Negeri Bengkalis

No.	Aspek Penilaian	Bobot	Nilai
1	Disiplin	20%	94
2	Tanggung- jawab	25%	95
3	Penyesuaian diri	10%	94
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 dilaksanakan 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 : Rizky Seri Hartati
Nim : 6404201017
Hari / Minggu : Senin – Jumat / Minggu Pertama
Tanggal : 25 - 29 Maret 2024

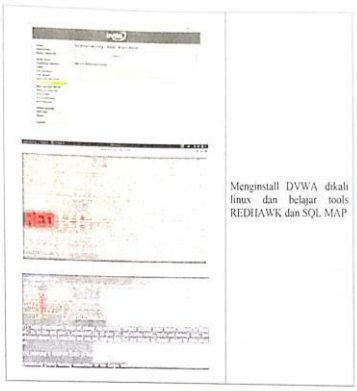
URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Pemberian arahan mengenai jam masuk kerja dan cara berpakaian 2. Perkenalan gedung kantor diskominfotik provinsi riau 3. Perkenalan diri di kantor bidang persandian diskominfotik provinsi riau 4. Pembagian tugas kepada rekan tim untuk project yang akan dilakukan 5. Libur hari paskah	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Pengenalan tentang project yang akan dilakukan yaitu teknik serangan CSRF

Hari / Minggu : Senin – Jumat / Minggu Kedua
Tanggal : 1 - 5 Maret 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Sharing tentang cyber security 2. Belajar tools yang terdapat pada kali linux 3. Belajar install DVWA di kali linux 4. Cuti bersama hari raya Idul Fitri	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN



	Menginstall DVWA dikali linux dan belajar tools REDHAWK dan SQL MAP

Hari / Minggu : Senin - Jumat / Minggu Ketiga
Tanggal : 8 – 12 April 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
Cuti bersama Hari Raya 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 2. Belajar mengenai tool SQL MAP	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Mencari referensi tentang serangan SQL Injection Dan review mengenai tools SQL MAP

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

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Implementasi serangan SQLMap dikali linux	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Implementasi serangan SQLMap dikali linux

Tanggal : 29 April – 3 Mei 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Mempelajari materi serangan CSRF 2. Review teori dari serangan CSRF 3. Belajar serangan CSRF dan mengimplementasi	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Implementasi serangan CSRF di DVWA

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

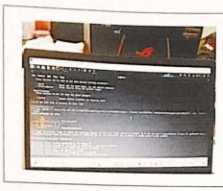
URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Review ulang serangan CSRF 2. Presentasi progres pengerjaan project 3. Libur kenaikan ISA AL-MASIH 4. Cuti bersama	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Dokumentasi presentasi progres pengerjaan project di depan atasan bersama pembimbing industri

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

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Implementasi serangan SQL Injection 2. Review serangan SQL Injection 3. Pengenalan tentang Sosial Engenering	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN



Implementasi serangan SQL Injection di DVWA

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

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

GAMBARAN KERJA	KETERANGAN
 	Acara pembentukan CSIRT Kab/ kota dihotel Bono

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

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

GAMBARAN KERJA	KETERANGAN
	Membuat Laporan Magang

Hari / Minggu : Senin - Jumat / Minggu Kesebelas
Tanggal : 3 - 7 Juni 2024

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

GAMBARAN KERJA	KETERANGAN
	Gambaran serangan CSRF

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

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

GAMBARAN KERJA	KETERANGAN
	Progres pengimplementasian pengerjaan serangan CSRF

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
	Proses pembuatan Laporan Magang

Hari / Minggu : Senin - Jumat / Minggu Keempat Belas
Tanggal : 24 - 28 Juni 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Rapat 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
	Rapat Evaluasi Dokumen ISO 27001 ; 2022

Hari / Minggu : Kamis / Minggu Kelima Belas
Tanggal : 1 - 5 Juli 2024

URAIAN KEGIATAN	PEMBERI TUGAS	PARAF
1. Melanjutkan pengerjaan laporan magang 2. Melakukan pentes serangan CSRF 3. Input SIPD	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Prose input SIPD

Hari / Minggu : Senin - Jumat / Minggu Keenam Belas
Tanggal : 8 - 12 Juli 2024

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

GAMBARAN KERJA	KETERANGAN
 	Kunjungan oleh Dosen Koordinator Kerja Praktek dari Politeknik Negeri Bengkalis dan pembuatan laporan

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 3. Melengkapi berkas magang	Tiara Mulia Putri, S.Kom	
Catatan Pembimbing Industri		

GAMBARAN KERJA	KETERANGAN
	Bahan presentasi hasil project
	Berkas yang akan ditanda tangani oleh pembimbing dan atasan
	Presentasi final project

Pengawas Magang

T. Nova Sukma, ST, MM
NIP. 19801104 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 Lisana Saputra, S.T
NIP. 19790914 200501 1 007

Lampiran 5. 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 : Risky Seri Hartati
NIM : 6404201017
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	Cuti Bersama Eid Fitri	-	-

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			
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	Hadir		
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	Libur Satu Muharram-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	Pembimbing Magang
T. Nova Sukma, ST, MM.	Tiara Mulia Putri, S.Kom
NIP. 19801104 200604 2 008	**NIP. 19870505 201903 2 001**

Kepala Bidang Persandian
Dinas Komunikasi Informatika dan Statistik Provinsi Riau

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

Lampiran 6. Dokumentasi Kegiatan

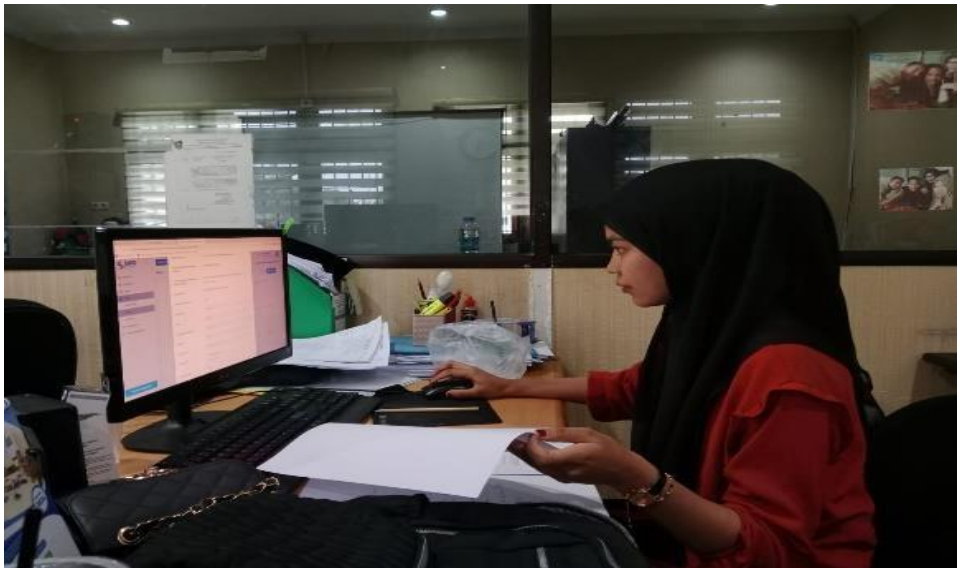
1. Upacara Pagi setiap hari dikantor pusat

2. Senam pagi dikantor pusat setiap hari kamis pagi

3. Acara pembentukan CSIRT Kab/Kota

4. Rapat Internal Mengenai ISO

5. Penginputan SIPD (Sistem Informasi Pemerintahan Daerah)



6. Kunjungan dosen ke Dinas Komunikasi Informatika dan Statistik Provinsi Riau di Bidang Persandian

7. Presentasi Final Project

Lampiran 7. Sertifikat Magang


DINAS KOMUNIKASI,
INFORMATIKA DAN STATISTIK
PROVINSI RIAU

Sertifikat

Diberikan Kepada

RISKY SERI HARTATI

Telah melaksanakan **Praktek Kerja Lapangan** pada Dinas Komunikasi, Informatika dan Statistik Provinsi Riau dari tanggal
25 Maret s/d 19 Juli 2024

KEPALA DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK PROVINSI RIAU

IKHWAN RIDWAN, SH, M.Si
Pembina Utama Madya
NIP.19650904 199703 1 001