

# **ANALISIS KERENTANAN DATA PENGGUNA INSTAGRAM TERHADAP PHISING MENGGUNAKAN SETOOLKIT**



## **SKRIPSI**

**Diajukan Sebagai Syarat Untuk Memperoleh Gelar Sarjana Strata Satu Komputer  
Pada Program Studi Teknologi Informasi Fakultas Teknik Universitas  
Muhammadiyah Palembang**

**Oleh :**

**Naufal Aditya Prayoga**

**162020042**

**PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH PALEMBANG  
2024**

**HALAMAN PENGESAHAN PEMBIMBING**  
**ANALISIS KERENTANAN DATA PENGGUNA INSTAGRAM**  
**TERHADAP PHISING MENGGUNAKAN SETOOLKIT**

Oleh :

Naufal Aditya Prayoga

162020042

Dosen Pembimbing Utama



Dedi Haryanto S. Kom., M. Kom  
NBM/NIDN: 1337459/0201089001

Dosen Pembimbing Pendamping



Karnadi, S. Kom., M. Kom  
NBM/NIDN: 1088893/0210038202

Disetujui,  
Dekan Fakultas Teknik



Ir. A. Junaidi, M.T  
NBM/NIDN: 763050/0202026502

Program Studi Teknologi Informasi  
Ketua Program Studi



Karnadi, S. Kom., M. Kom  
NBM/NIDN: 1088893/0210038202

## HALAMAN PENGESAHAN PENGUJI

Judul Skripsi : **Analisis Kerentanan Data Pengguna Instagram Terhadap Phising Menggunakan Setoolkit** Oleh **Naufal Aditya Prayoga** dengan **Nim 162020042** telah dipertahankan didepan komisi penguji pada hari .. tanggal ... Agustus 2024 dan dinyatakan

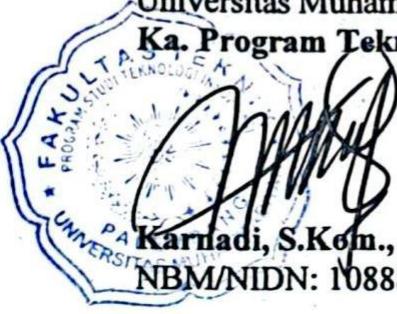
Palembang, Agustus 2024

Mengetahui,

Program Strata 1

Universitas Muhammadiyah Palembang, Tim Penguji:  
**Ka. Program Teknologi Informasi**

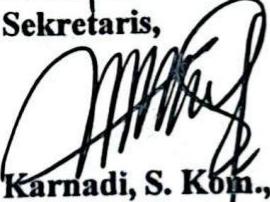
Ketua,



**Karnadi, S.Kom., M.Kom**  
NBM/NIDN: 1088893/0210038202

  
**Dedi Haryanto S. Kom., M. Kom**  
NBM/NIDN: 1337459/0201089001

Sekretaris,

  
**Karnadi, S. Kom., M. Kom**  
NBM/NIDN: 1088893/0210038202

Penguji I,

  
**Jimmie S.Kom., M.Kom**  
NBM/NIDN: 1340253/0222047702

Penguji II,

  
**Apriyansyah S.Kom., M.Kom**  
NBM/NIDN: 1339399/0204049001

## HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Naufal Aditya Prayoga

NIM : 162020042

Dengan ini menyatakan bahwa

1. Karya tulis saya (Skripsi) merupakan sebuah karya asli serta belum pernah diajukan untuk memperoleh gelar akademik dengan baik (Sarjana) di Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang atau Perguruan Tinggi lainnya
2. Karya tulis saya (Skripsi) merupakan hasil murni memiliki gagasan, pokok permasalahan, serta hasil penilaian saya sendiri, tanpa kerja sama terhadap pihak lain melaikkan dengan arahan dosen pembimbing.
3. Karya tulis saya (Skripsi) tidak terdapat karya serta pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali serta tertulis dengan jelas dicantumkan nama penggarang serta memasukan kedalam daftar Pustaka.
4. Karya tulis saya (Skripsi) yang dihasilkan sudah melakukan pengecekan dengan keaslianya menggunakan plagirisme checker yang dipublikasikan melalui internet sehingga bisa diakses secara daring.
5. Dengan ini surat pernyataan yang saya buat secara sungguh-sungguh serta apabila terbukti terdapat penyimpangan serta ketidakbenaran dari pernyataan, maka saya

bersedia menerima sanksi sesuai dengan peraturan serta perundang- undangan akademik Program Studi di Fakultas Universitas Muhammadiyah Palembang.

6. Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya

Palembang, 30 Juli 2024  
Yang membuat pernyataan



Naufal Aditya Prayoga  
162020042

## MOTTO

“Apapun yang terjadi jangan pernah menghadap ke belakang, Tetap fokus apa yang ada di depan” -Naufal 2024

فَإِنِّي أَلِئِرُ رَبِّكُمَا  
لَكُمْ بَنِ

Artinya : “Maka nikmat Tuhanmu yang manakah yang kamu dustakan?”  
(QS. Ar-Rahman: 13)

إِنَّمَا أَمْرُهُ إِذَا أَرَادَ شَيْئًا أَنْ يَقُولَ لَهُ كُنْ فَيَكُونُ

Artinya : “Artinya: Sesungguhnya keadaan-Nya apabila Dia menghendaki sesuatu hanyalah berkata kepadanya: "Jadilah!" maka terjadilah ia.  
(QS. Yasin: 82)

## ABSTRAK

Penelitian ini menganalisis kerentanan data pengguna Instagram terhadap serangan phishing di kota Palembang menggunakan Social Engineering Toolkit (SET). Tujuannya adalah untuk mengidentifikasi potensi celah keamanan dalam sistem Instagram yang dapat dieksplorasi melalui teknik phishing, serta mengevaluasi efektivitas langkah-langkah keamanan saat ini. Hasil penelitian diharapkan dapat memberikan wawasan mendalam tentang risiko keamanan data pengguna Instagram, serta menjadi dasar untuk pengembangan strategi keamanan yang lebih efektif. Implikasi penelitian mencakup peningkatan kesadaran keamanan pengguna dan penyempurnaan kebijakan keamanan platform media sosial.

**Kata kunci:** Keamanan Data, Social Engineering Toolkit, Phishing, Media Sosial, Instagram

## ABSTRACT

*This research analyzes the vulnerability of Instagram user data to phishing attacks in the city of Palembang using the Social Engineering Toolkit (SET). The goal is to identify potential security gaps in Instagram systems that could be exploited through phishing techniques, as well as evaluate the effectiveness of current security measures., as well as provide a basis for developing more effective security strategies. Research implications include increasing user security awareness and improving social media platform security policies.*

*Keywords: Data Security, Social Engineering Toolkit, Phishing, Social Media, Instagram*

## KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang senantiasa memberikan rahmat dan hidayah Nya sehingga skripsi yang diajukan untuk memenuhi tugas dan syarat dalam memperoleh gelar Sarjana Komputer, pada program studi Teknologi Informasi Universitas Muhammadiyah Palembang. Agar dapat terselesaikan dengan baik. Skripsi ini berjudul: **"Analisis Kerentanan Data Pengguna Instagram Terhadap Phising Menggunakan Setoolkit"** dapat terselesaikan dengan baik.

Pada kesempatan ini, penulis hendak menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan moril maupun materil sehingga skripsi ini dapat selesai. Ucapan terima kasih ini peneliti tunjukkan kepada :

1. Bapak **Prof. Dr. Abid Djazuli, S.E., M.M** selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak **Ir. A. Junaidi M.T** selaku Dekan Fakultas Teknik Universitas Muhammadiyah Palembang.
3. Bapak **Karnadi, S.Kom., M.Kom** selaku Kepala Prodi Teknologi Informasi. Sekaligus Dosen Pembimbing Pendamping
4. Bapak **Dedi Haryanto, S.Kom., M.Kom** selaku Dosen pembimbing utama yang telah membimbing peneliti untuk menyelesaikan skripsi ini.
5. Bapak **Apriansyah, S. Kom., M. Kom** selaku Dosen pembimbing akademi yang

telah memberikan saran serta dukungan untuk dapat menyelesaikan skripsi ini

6. Seluruh **Bapak/Ibu Dosen** yang telah menyumbangkan pengetahuan dan bimbingan dalam perkuliahan sampai peneliti selesai dalam penelitian skripsi ini
7. Penghargaan dan Terima kasih yang setulus-tulusnya kepada kedua orang tua penulis Ayahanda tercinta **Andy Irawan** dan Ibunda tercinta **Laili Hastuti** yang telah memberikan semangat kepada penulis untuk dapat menyelesaikan skripsi ini.
8. Terima kasih yang setulus tulusnya kepada pacar tercinta **Alana Zahwa Azizah** yang telah memberikan semangat serta dukungan dalam penulisan skripsi ini hingga selesai.
9. Terima kasih kepada teman seperjuangan **Muhammad Alfi Syahrin, Ferdianto Pratama, Prastyo Sakti Wibowo** yang telah memberikan semangat pada penulisan skripsi hingga selesai.
10. Serta ucapan terima kasih kepada diri sendiri yang telah berjuang sampai pada titik ini sehingga bisa menyelesaikan skripsi ini dengan banyak tantangan dan dukungan dari orang sekitar

Saran dan kritik yang sifatnya membangun sangat penulis harapkan. Semoga skripsi ini bermanfaat dan dapat memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

## DAFTAR ISI

<b>HALAMAN PENGESAHAN PEMBIMBING .....</b>	<b>ii</b>
<b>HALAMAN PENGESAHAN PENGUJI.....</b>	<b>iii</b>
<b>HALAMAN PERNYATAAN .....</b>	<b>iv</b>
<b>MOTTO.....</b>	<b>vi</b>
<b>ABSTRAK.....</b>	<b>vi</b>
<b>ABSTRACT .....</b>	<b>viii</b>
<b>KATA PENGANTAR .....</b>	<b>ix</b>
<b>DAFTAR ISI .....</b>	<b>xi</b>
<b>DAFTAR GAMBAR .....</b>	<b>xiii</b>
<b>DAFTAR TABEL .....</b>	<b>xiv</b>
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1. 1 Latar Belakang .....	1
1.2 Identifikasi Masalah .....	4
1.3 Tujuan .....	5
1.4 Manfaat .....	6
<b>BAB II TINJAUAN PUSTAKA .....</b>	<b>8</b>
2.1 Keamanan Data Pengguna di Instagram.....	8
2.2 Phishing sebagai Teknik Serangan .....	8
2.3 Social Engineering Toolkit (SET) .....	9
2.4 Kerentanan Sistem dan Pengujian Penetrasi.....	9
2.5 Kesadaran Pengguna dan Edukasi Keamanan.....	9

2.6 Penelitian Terdahulu.....	10
-------------------------------	----

**BAB III METODOLOGI PENELITIAN..... 21**

3.1 Jenis Penelitian .....	21
3.1.1 Teknik Penelitian.....	21
3.1.2 Phishing .....	22
3.1.3 Implementasi Teknik Phising .....	23
3.5 Jadwal Penelitian .....	23
3.5.1 Waktu dan Tempat Penelitian.....	23

**BAB IV HASIL DAN PEMBAHASAN ..... 26**

4.1 Hasil.....	26
4.2 Analisis setoolkit .....	26
4.3 Implementasi Teknik Phising Pada Media Sosial.....	27
4.4 Report Data.....	29

**BAB V KESIMPULAN DAN SARAN..... 31**

5.1 Kesimpulan.....	31
5.2 Saran .....	32

**DAFTAR PUSTAKA**

**LAMPIRAN**

## DAFTAR GAMBAR

Gambar 3.1 Skenario Phising.....	23
Gambar 4.1 command setoolkit.....	26
Gambar 4.2 Site Cloner .....	27
Gambar 4.3 Url To Clone .....	28
Gambar 4.4 Halaman Kloning.....	28
Gambar 4.4 Report Data.....	29

## **BAB I**

### **PENDAHULUAN**

#### **1.1 Latar Belakang**

Teknologi yang semakin berkembang pesat dari tahun ke tahun telah merubah berbagai aktivitas dalam aspek kehidupan termasuk bidang sosial dan budaya, dimana pada dasarnya keberagaman sosial dan budaya merupakan landasan terciptanya sosial media yang menjadi jembatan komunikasi dan informasi seluruh penjuru dunia[1]. Teknologi informasi merupakan suatu teknologi yang berhubungan dengan mengolah data untuk menghasilkan informasi yang relevan, akurat dan tepat. Teknologi ini menggunakan seperangkat komputer untuk mengolah data dengan menghubungkan satu komputer dengan komputer lainnya sesuai dengan kebutuhan, teknologi informasi dapat memberikan dampak kinerja menjadi efektif dan efisien, selain itu suatu sistem harus mengetahui apakah komponen sistem informasi tersebut berjalan dengan semestinya.

Instagram adalah platform media sosial yang diluncurkan pada 6 Oktober 2010 oleh Kevin Systrom dan Mike Krieger. Awalnya, aplikasi ini dirancang untuk berbagi foto dan video dengan menggunakan berbagai filter yang dapat mempercantik gambar. Dalam waktu singkat, Instagram menarik perhatian banyak pengguna dan menjadi salah satu aplikasi terpopuler di dunia.

Pada tahun 2012, Facebook mengakuisisi Instagram seharga sekitar 1 miliar dolar

AS, yang semakin meningkatkan eksposurnya dan memungkinkan pengembangan fitur-fitur baru. Sejak saat itu, Instagram terus berkembang dengan menambahkan berbagai fungsi seperti Stories, IGTV, dan Reels, yang memungkinkan pengguna untuk berbagi konten dengan cara yang lebih dinamis.

Dengan lebih dari satu miliar pengguna aktif bulanan, Instagram tidak hanya menjadi platform untuk berbagi foto, tetapi juga tempat untuk pemasaran, komunikasi, dan interaksi sosial. Pengaruhnya yang besar terlihat dalam berbagai aspek kehidupan, mulai dari tren mode, kuliner, hingga gaya hidup, menjadikannya salah satu alat utama bagi influencer dan merek untuk terhubung dengan audiens mereka.

Seiring dengan perkembangan teknologi dan perubahan perilaku pengguna, Instagram terus beradaptasi dengan menghadirkan fitur-fitur inovatif untuk memenuhi kebutuhan penggunanya dan tetap relevan di dunia digital yang cepat berubah[2].

Dalam mengatasi ancaman keamanan data pengguna Instagram melalui teknik phishing, diperlukan solusi yang holistik. Ini mencakup implementasi sistem deteksi phishing canggih dengan kecerdasan buatan dan analisis perilaku, peningkatan kesadaran keamanan pengguna melalui kampanye edukasi, penguatan langkah-langkah perlindungan data seperti enkripsi end-to-end, audit keamanan reguler, dan pembaruan perangkat lunak tepat waktu. Pengembangan kebijakan keamanan yang ketat dan kolaborasi dengan ahli keamanan siber serta pihak berwenang juga menjadi kunci dalam menjaga keamanan data pengguna Instagram. Dengan menerapkan langkah-langkah ini, diharapkan Instagram dapat meningkatkan pertahanan mereka

dan menyediakan lingkungan online yang lebih aman bagi pengguna mereka. Sehingga penulis memberikan judul pada proposal penelitian ini “**Analisis Kerentanan Data Pengguna Instagram Terhadap Phising Menggunakan Setoolkit**”. Dari latar belakang di atas dapat dirumuskan satu permasalahan “bisakah laman media sosial di kloning menggunakan teknik phising pada sistem login”, tujuan dari penelitian ini adalah melakukan testing terhadap halaman login Instagram untuk mengetahui apakah media sosial tersebut dapat di kloning sehingga dapat menimbulkan pencurian data pada saat melakukan login maka dilakukan testing menggunakan setoolkit[3].

#### 1) Akses Online

Materi pembelajaran, sumber daya, dan aktivitas belajar dapat diakses melalui internet, memungkinkan peserta didik untuk belajar dari mana saja yang memiliki koneksi internet.

#### 2) Penggunaan Teknologi

Pemanfaatan teknologi digital, seperti platform online, perangkat lunak pembelajaran, dan media multimedia untuk menyampaikan materi dengan cara yang interaktif dan menarik.

#### 3) Fleksibilitas Waktu

Memungkinkan peserta didik untuk mengatur jadwal belajar mereka sendiri.

#### 4) Interaktivitas

Menyediakan fitur interaktif, seperti ujian online, diskusi forum, tugas daring, dan elemen multimedia.

Berdasarkan permasalahan yang ada pada paragraf diatas, penulis membuat sebuah penelitian yang berjudul “Analisis Kerentanan Data Pengguna Instagram Terhadap Phising Menggunakan Setoolkit” Dengan adanya penelitian ini, penulis dapat mengukur tingkat kepuasan pengguna aplikasi Instagram terhadap keamanannya

## **1.2 Identifikasi Masalah**

Identifikasi masalah dalam keamanan data pengguna Instagram mencakup sejumlah permasalahan yang memerlukan perhatian mendalam. Pertama, adanya potensi celah keamanan, terutama melalui teknik phishing, membuka pintu lebar bagi pihak yang tidak bertanggung jawab untuk meretas dan mengakses informasi pribadi pengguna dengan dampak serius. Selain itu, permasalahan kesadaran keamanan di kalangan pengguna menjadi elemen penting, di mana rendahnya tingkat kesadaran dapat membuat mereka lebih rentan terhadap serangan phishing yang bertujuan meraih data pribadi. Keterbatasan pemahaman tentang taktik penipuan online dan kurangnya edukasi mengenai cara mengidentifikasi serangan phishing dapat meningkatkan risiko akses yang tidak sah ke akun pengguna. Selanjutnya, perlindungan data yang belum optimal, termasuk penggunaan enkripsi yang tidak memadai, meninggalkan informasi pengguna rentan terhadap potensi eksploitasi oleh pihak yang tidak sah. Terakhir, tantangan terkait dengan pembaruan keamanan dan respons yang cepat terhadap ancaman baru menjadi aspek krusial, mengingat dinamika perubahan dan perkembangan di ranah keamanan siber yang terus berkembang. Keseluruhan, pemahaman mendalam terhadap identifikasi masalah ini menjadi dasar esensial dalam

merumuskan solusi yang holistik dan efektif untuk meningkatkan keamanan data pengguna Instagram.

### **1.3 Tujuan**

Tujuan dari penelitian ini adalah untuk menyelidiki dan menganalisis tingkat keamanan data pengguna Instagram menggunakan SETOOLKIT melalui implementasi teknik phishing. Penelitian bertujuan untuk mengidentifikasi potensi celah keamanan dalam sistem Instagram yang dapat dieksplorasi oleh serangan phishing, dengan fokus pada kerentanan yang mungkin terkait dengan akses tidak sah dan pengungkapan informasi pribadi pengguna. Selain itu, penelitian ini bertujuan untuk memberikan wawasan mendalam tentang efektivitas langkah-langkah keamanan saat ini dan untuk merumuskan solusi yang proaktif guna meningkatkan pertahanan keamanan data pengguna. Dengan demikian, tujuan penelitian ini tidak hanya terbatas pada pengidentifikasi masalah, tetapi juga pada pengembangan rekomendasi strategis untuk mengatasi dan mencegah potensi risiko keamanan siber di masa depan. Keseluruhan, tujuan penelitian ini adalah untuk memberikan kontribusi pada pemahaman kita tentang keamanan data dalam konteks media sosial dan untuk memberikan dasar bagi perbaikan kebijakan dan praktik keamanan di platform Instagram.

## 1.4 Manfaat

Berdasarkan hasil penelitian , berikut adalah beberapa manfaat potensial dari skripsi ini:

1. Manfaat Teoritis:

- a) Memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang keamanan siber, khususnya terkait kerentanan data pengguna media sosial.
- b) Memperkaya literatur akademis tentang teknik phishing dan penggunaan SETOOLKIT dalam konteks keamanan aplikasi media sosial.
- c) Memberikan pemahaman lebih mendalam tentang perilaku pengguna media sosial dalam menghadapi ancaman keamanan siber.

2. Manfaat Praktis:

a) Bagi Pengguna Instagram:

1. Meningkatkan kesadaran pengguna Instagram tentang risiko keamanan data mereka.
2. Memberikan informasi tentang cara melindungi diri dari serangan phishing.

b) Bagi Pengembang Aplikasi:

1. Mengidentifikasi potensi celah keamanan dalam sistem login Instagram.
2. Memberikan masukan untuk peningkatan keamanan aplikasi Instagram.

c) Bagi Pemerintah dan Pembuat Kebijakan:

1. Menyediakan data empiris yang dapat digunakan sebagai dasar pembuatan kebijakan keamanan siber.

2. Membantu dalam merumuskan strategi edukasi masyarakat tentang keamanan data digital.
3. Manfaat Metodologis:
  1. Mendemonstrasikan penggunaan SETOOLKIT sebagai alat penelitian dalam konteks keamanan media sosial.
  2. Memberikan contoh pendekatan kuantitatif dalam penelitian keamanan siber.
4. Manfaat Sosial:
  1. Berkontribusi pada peningkatan keamanan digital masyarakat secara umum.
  2. Membantu mencegah potensi kerugian finansial dan non-finansial akibat pencurian data.

## DAFTAR PUSTAKA

- [1] M. Julia and A. J. Masyuroh, “Literature Review Determinasi Struktur Organisasi: Teknologi, Lingkungan Dan Strategi Organisasi,” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 4, pp. 383–395, 2022, [Online]. Available: <https://dinastirev.org/JEMSI/article/view/895/582>
- [2] Sutarmen, *Pengantar teknologi informasi Sutarmen*, vol. 43. 2019. [Online]. Available: <http://badanpenerbit.org/index.php/dpypress/article/view/18>
- [3] F. A. Zahwa and I. Syafi’i, “Pemilihan Pengembangan Media Pembelajaran Berbasis Teknologi Informasi,” *Equilib. J. Penelit. Pendidik. dan Ekon.*, vol. 19, no. 01, pp. 61–78, 2022, doi: 10.25134/equi.v19i01.3963.
- [4] D. Haryanto and Z. R. S. Elsi, “Perancangan Jaringan Komputer Berbasi Lan Di Ruang Lab Sma Muhammadiyah 1 Muara Padang,” *J. Digit. Teknol. Inf.*, vol. 4, no. 1, p. 27, 2021, doi: 10.32502/digital.v4i1.3156.
- [5] K. Kusumawati, “Pemanfaatan Teknologi Informasi Dalam Pendidikan,” *J. Limits*, vol. 5, no. 1, pp. 7–14, 2023, doi: 10.59134/jlmt.v5i1.311.
- [6] P. Riwayadi, “Miarso, Yusufhadi, 2005, Menyemai Benih Teknologi Pendidikan, Kencana, Jakarta 2. Diarsipkan oleh PLS UM untuk Imadiklus.com,” 2005.
- [7] S. Suryadi, “Peranan Perkembangan Teknologi Informasi Dan Komunikasi Dalam Kegiatan Pembelajaran Dan Perkembangan Dunia Pendidikan,” *J.*

- Inform.*, vol. 3, no. 3, pp. 9–19, 2019, doi: 10.36987/informatika.v3i3.219.
- [8] Nurdyansyah, “Sumber Daya dalam Teknologi Pendidikan,” *Sumber Daya dalam Teknol. Pendidik.*, pp. 1–22, 2017, [Online]. Available: [http://eprints.umsida.ac.id/1625/1/Sumber\\_Daya\\_dalam\\_Teknologi\\_Pendidikan.pdf](http://eprints.umsida.ac.id/1625/1/Sumber_Daya_dalam_Teknologi_Pendidikan.pdf)
- [9] A. Maritsa, U. Hanifah Salsabila, M. Wafiq, P. Rahma Anindya, and M. Azhar Ma’shum, “Pengaruh Teknologi Dalam Dunia Pendidikan,” *Al-Mutharrahah J. Penelit. dan Kaji. Sos. Keagamaan*, vol. 18, no. 2, pp. 91–100, 2021, doi: 10.46781/al-mutharrahah.v18i2.303.
- [10] I. G. N. S. Wijaya and I. W. K. Suwastika, “Analisa Kepuasan Pengguna E-Learning Menggunakan Metode Kano,” *J. Sist. dan Inform.*, vol. 12, no. 1, pp. 128–138, 2017.
- [11] M. A. Bora, “Analisa Kepuasan Penggunaan E-Learning Cloud Sekolah Tinggi Teknik (STT) Ibnu Sina Batam,” *J. Ind. Kreat.*, vol. 1, no. 01, p. 55, 2017, doi: 10.36352/jik.v1i01.49.
- [12] M. S. Muarie and F. Nopriani, “Mengukur Tingkat Kepuasan Pengguna E-Learning (Uin Raden Fatah Palembang),” *JUSIM (Jurnal Sist. Inf. Musirawas)*, vol. 5, no. 01, pp. 79–86, 2020, doi: 10.32767/jusim.v5i01.756.
- [13] E. Yulianingsih, “Analisis Kepuasan Terhadap Penggunaan E-Learning Menggunakan Technology Acceptance Model Dan End User Computing Satisfaction,” *J. Ilm. MATRIK*, vol. 8, no. 1, pp. 27–42, 2016, [Online]. Available:

<https://journal.binadarma.ac.id/index.php/jurnalmatrik/article/view/396>

- [14] P. Sari, “Memotivasi Belajar Dengan Menggunakan E-Learning,” vol. VI, no. 2, pp. 20–35, 2015.
- [15] N. L. U. Chusna, “Pembelajaran E-Learning,” *Pros. Semin. Nas. Pendidik. KALUNI*, vol. 2, pp. 113–117, 2019, doi: 10.30998/prokaluni.v2i0.36.
- [16] U. N. Manado, “I Wayan Damai,” no. 1, pp. 121–133, 2021, [Online]. Available: <https://prosiding.iahntp.ac.id>
- [17] M. J. Pranita, D. H. Zulfikar, and C. E. Gunawan, “Analisis Kepuasan Pengguna Sistem Keagenan PERISAI Menggunakan End User Computing Satisfaction (Studi Kasus: BPJS Ketenagakerjaan Kantor Cabang Palembang),” *Jusifo*, vol. 5, no. 2, pp. 91–104, 2019, doi: 10.19109/jusifo.v5i2.5191.
- [18] E. Rosita, W. Hidayat, and W. Yuliani, “Uji Validitas Dan Reliabilitas Kuesioner Perilaku Prososial,” *Fokus (Kajian Bimbing. Konseling dalam Pendidikan)*, vol. 4, no. 4, p. 279, 2021, doi: 10.22460/fokus.v4i4.7413.
- [19] N. Azhar and M. Ardi, “Uji validitas dan reliabilitas paket multimedia interaktif,” *IlmuKomputer.Com*, pp. 1–15, 2008.