

**DETEKSI DAN ANALISIS POLA SERANGAN WEB DEFACEMENT
BERMUATAN PROMOSI JUDI ONLINE PADA SITUS WEBSITE**



SKRIPSI

Untuk Memenuhi Persyaratan Mencapai Gelar Sarjana Komputer (S.Kom) Pada
Program Studi Teknologi Informasi Fakultas Teknik UM Palembang

Disusun Oleh :
Amanda Rahma Dwi
162022061

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026**

**DETEKSI DAN ANALISIS POLA SERANGAN WEB DEFACEMENT
BERMUATAN PROMOSI JUDI ONLINE PADA SITUS WEBSITE**



SKRIPSI

Untuk Memenuhi Persyaratan Mencapai Gelar Sarjana Komputer (S.Kom) Pada
Program Studi Teknologi Informasi Fakultas Teknik UM Palembang

Disusun Oleh :
Amanda Rahma Dwi
162022061

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH PALEMBANG
2026**

HALAMAN PENGESAHAN

DETEKSI DAN ANALISIS POLA SERANGAN WEB DEFACEMENT BERMUATAN PROMOSI JUDI ONLINE PADA SITUS WEBSITE



Oleh :

AMANDA RAHMA DWI
162022061

Menyetujui,

Pembimbing Utama,

Dr. IR. Zulhipni Reno Saputra S.T., M.Kom
NBM/NIDN : 1338529/0205118002

Pembimbing Pendamping,

Apriansyah, S.kom., M.Kom
NBM/NIDN:1339399/0204049001

Disetujui,
Dekan Fakultas Teknik



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

Program Studi Teknologi informasi
Ketua Program Studi



Kurnadi S.Kom., M.kom
NBM/NIDN: 1088893/0210038202

HALAMAN PERSETUJUAN

Judul Proposal Penelitian : Deteksi Dan Analisis Pola Serangan Web Defacement
Bermuatan Judi Online Pada Situs Website

Oleh Amanda Rahma Dwi NIM 162022061 Skripsi ini telah disetujui dan
disahkan oleh Tim Penguji Program Studi Teknologi Informasi Manajemen Tata
Kelola Program Strata 1 Universitas Muhammadiyah Palembang pada 25 April
2026 dan telah Dinyatakan LULUS

Mengetahui,

Ketua Program Studi Teknologi Informasi
Universitas Muhammadiyah Palembang

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

Tim Penguji
Ketua Penguji

Dr. Ir. Zulhipni Reno Saputra, S. T., M. Kom
NBM/NIDN: 1338529/0205118002

Penguji 1,

Dr. Lucky Indra Kesuma, S.SI., M.Kom
NBM/NIDN: 1582348/0225099002

Penguji 2,

M Ilhan, S.T., M.Kom
NBM/NIDN: 1299825/0207129001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Amanda Rahma Dwi
NIM : 162022061
Fakultas/Prodi : Teknik / Teknologi Informasi
Judul Skripsi : Deteksi dan Analisis Pola Serangan Web Defacement Bermuatan Judi Online Pada Situs Website

Menyatakan dengan sebenar-benarnya bahwa skripsi ini adalah benar-benar hasil karya asli saya sendiri bukan merupakan plagiarism, pencurian hasil karya orang lain, hasil kerja orang lain untuk kepentingan saya karena hubungan material maupun non-material, ataupun segala kemungkinan lain yang pada hakekatnya bukan merupakan karya tulis skripsi saya secara orisinil dan otentik.

Bila dikemudian hari diduga kuat ada ketidaksesuaian antara fakta dengan kenyataan ini, saya bersedia diproses oleh tim Fakultas yang dibentuk untuk melakukan verifikasi, dengan sanksi terberat berupa pembatalan kelulusan/kesarjanaan.

Demikian surat pernyataan ini saya buat dengan kesadaran sendiri dan tidak atas tekanan ataupun paksaan dari pihak maupun demi menegakan integritas akademik di institusi ini.

Hormat Saya,



Amanda Rahma Dwi
162022061

MOTTO DAN PERSEMBAHAN

MOTTO

“Pendidikan memiliki akar yang pahit, tapi buahnya manis”

PERSEMBAHAN

Sebagai bentuk syukur atas segala keberkahan dan bimbingan-Nya, karya sederhana ini Penulis persembahkan dengan tulus kepada:

1. Teristimewah, penulis mengucapkan terimakasih yang sebesar-besarnya kepada kedua orang tua tercinta. Cinta pertama dan panutanku, Ayahanda Yuhermansyah dan pintu surgaku Ibunda Firda Hayati, Dua sosok yang paling berjasa dalam kehidupan penulis. Meskipun Ayah dan Ibu tidak berkesempatan menempuh Pendidikan hingga bangku perkuliahan, keduanya selalu mengupayakan agar anak-anaknya dapat menempuh Pendidikan setinggi-tingginya. Dengan segala keterbatasan yang ada, Ayah dan Ibu selalu menjadi sumber kekuatan, penguat Langkah, dan tempat Kembali bagi penulis dalam setiap proses yang dijalani. Sebagai anak kedua, penulis bersyukur dan bangga dapat menyelesaikan Pendidikan sarjana sebagai lulusan pertama di keluarga. Setiap cucuran keringat, kerja keras, dan tanggung jawab Ayah dalam menafkahi keluarga menjadi jalan bagi penulis untuk dapat mengenyam Pendidikan hingga di tahap ini, Sekaligus menjadi teladan tentang artiketeguhan dan tanggung jawab. Ibu senantiasa menghadirkan doa, motivasi, nasihat, dan kasih sayang tanpa batas yang terus mengiringi setiap Langkah penulis, dengan kesabaran dan pengorbanan yang tak pernah terhitung. Seluruh dukungan, perhatian serta keikhlasan Ayah dan Ibu menjadi sumber kekuatan, inspirasi, serta pelita yang senantiasa menerangi perjalanan penulis dalam menyelesaikan Pendidikan sarjana ini. Semoga Allah SWT senantiasa melimpahkan Kesehatan, keberkahan, umur Panjang serta membalas seluruh kebaikan, pengorbanan, dan keiklasan Ayah dan Ibu dengan pahala yang berlipat ganda.

2. Kepada Kakak dan Kakak Ipar Tercinta, Donny Ramanda dan Extita Pristani. Terimakasih sudah selalu memberikan yang terbaik untuk adik-adikmu, termasuk penulis. Kasih sayang dan dukunganmu sangat berarti dalam perjalanan ini. Terimakasih Telah berjuang Bersama penulis mendengarkan keluh kesah, mengorbankan banyak waktu, tenaga, materi, dan Upaya untuk mendukung penulis meraih mimpi. Terimakasih sudah menjadi kakak yang baik dan selalu ada untuk adikmu ini, Semoga Allah selalu senantiasa memberkahi kalian dengan Kesehatan, kebahagiaan, keberkahan dan umur Panjang.
3. Adikku Terkasih, Aliesha Nazaha Sakeera. Terimakasih telah menjadi sumber kebahagiaan dan semangat dalam setiap Langkah penulis. Saat ini kakakmu sedang berjuang, membuka jalan untuk masa depanmu, agar kelak kamu tidak merasakan kesusahan, aku akan menjadi peta untukmu.
4. Bapak Dr. Ir. Zulhipni Reno Saputra, S.T., M.Kom. Selaku Dosen pembimbing utama dan Bapak Apriansyah, S.Kom., M.Kom selaku Dosen pembimbing kedua, Terimakasih yang sebesar- besarnya atas kesediaan Bapak untuk meluangkan waktu di Tengah kesibukan, atas kesabaran, perhatian, arahan, serta nasihat yang disampaikan dengan tutur kata menenangkan dan tidak pernah menyakiti, sehingga seluruh proses bimbingan dapat dijalani dengan rasa aman dan nyaman.
5. Bapak Jimmie, S.Kom., M.Kom. Selaku Dosen pembimbing Akademik, Terimakasih banyak telah mengarahkan dan membimbing untuk semua hal yang berkaitan dengan studi penulis.
6. Seluruh Dosen beserta Staf Prodi Teknologi Informasi yang telah memberikan bimbingan, ilmu pengetahuan, serta wawasan yang luas kepada penulis selama proses perkuliahan.
7. Terimakasih untuk seluruh keluarga besar atas doa dan dukungan yang telah diberikan selama proses perkuliahan.
8. Kepada sahabat penulis dari kecil, Dina Precilia, Cheny Wulandari, Juwita. Terima kasih atas kebersamaan, dukungan, dan kehadiran yang begitu berarti dari dulu hingga penyusunan skripsi ini. Setiap bantuan dalam

menyelesaikan tugas, semangat akademik yang selalu diberikan, serta perhatian dan kepedulian yang tulus menjadi penguat Langkah penulis untuk terus belajar dan bertahan dalam setiap proses. Kehadiran kalian sebagai pendengar setia dan teman dalam berbagai situasi turut meringankan beban serta menjaga semangat penulis hingga akhirnya mampu menyelesaikan studi ini.

9. Sahabat seperjuangan Anisa Fitria, Dwi Retno Aji. Terimakasih telah memberikan pengalaman berharga selama masa perkuliahan. Kebersamaan, kerja sama, serta berbagai pembelajaran yang di peroleh selama awal perkuliahan hingga saat ini.
10. Teman-teman Angkatan 2022 Teknologi Informasi, Yang telah kebersamai penulis dalam suka, duka dan cerita selama di bangku perkuliahan. Terimakasih atas kebersamaan, kekompakan, dan segala kenangan indah yang tak akan pernah penulis lupakan.
11. Seluruh pihak yang terlibat, memberikan doa serta dukungan dalam proses penyusunan skripsi ini yang tidak dapat penulis sebutkan satu per satu.
12. Terakhir, Kepada diri saya sendiri Amanda Rahma Dwi. Terima kasih telah bertahan sejauh ini dan terus berjalan melewati segala tantangan yang semesta hadirkan. Apresiasi yang sebesar-besarnya telah berjuang untuk menyelesaikan apa yang telah dimulai. Setiap air mata, doa dan usaha telah menjadisaksi betapa berharganya proses ini. Mari bekerja sama untuk lebih berkembang lagi menjadi pribadi yang lebih baik dari hari ke hari.

ABSTRAK

Penelitian ini bertujuan untuk mengembangkan sistem deteksi web defacement bermuatan promosi judi online dengan memanfaatkan teknik Open Source Intelligence (OSINT) dan analisis konten berbasis Python. Latar belakang penelitian ini didasarkan pada meningkatnya kasus penyalahgunaan website sebagai media penyisipan konten judi online melalui teknik defacement yang dapat merusak integritas dan kepercayaan terhadap website. Metode yang digunakan dalam penelitian ini adalah metode deskriptif dengan pendekatan kuantitatif serta bersifat terapan. Proses penelitian meliputi pengumpulan data menggunakan teknik OSINT dan Google Dork, preprocessing dan validasi data, analisis konten website menggunakan Python, serta perhitungan skor untuk menentukan tingkat indikasi defacement. Sistem yang dibangun mampu mendeteksi kemunculan kata kunci mencurigakan, tautan eksternal, serta perubahan struktur halaman. Hasil analisis kemudian diklasifikasikan ke dalam kategori clean, suspicious, dan defaced. Berdasarkan hasil pengujian, sistem mampu mengidentifikasi website yang terindikasi defacement secara otomatis dengan tingkat akurasi yang baik serta waktu pemrosesan yang relatif cepat. Selain itu, penelitian ini juga menghasilkan dataset serta analisis pola serangan yang menunjukkan karakteristik umum dari penyisipan konten judi online. Dengan demikian, sistem yang dikembangkan dapat menjadi solusi dalam mendeteksi dan menganalisis serangan web defacement secara efektif.

Kata kunci: Web Defacement, OSINT, Python, Scoring, Deteksi Otomatis

ABSTRACT

This study aims to develop a web defacement detection system containing online gambling promotion content using Open Source Intelligence (OSINT) techniques and Python-based content analysis. The background of this research is driven by the increasing number of cases where websites are misused as a medium for inserting illegal gambling content through defacement techniques, which can damage the integrity and trustworthiness of websites. The method used in this research is a descriptive method with a quantitative approach and is categorized as applied research. The research process includes data collection using OSINT and Google Dork techniques, data preprocessing and validation, website content analysis using Python, and scoring calculation to determine the level of defacement indication. The developed system is capable of detecting suspicious keywords, external links, and abnormal page structures. The analysis results are then classified into three categories: clean, suspicious, and defaced. Based on the testing results, the system can automatically identify defaced websites with good accuracy and relatively fast processing time. In addition, this study produces a dataset and attack pattern analysis that reveals common characteristics of online gambling content insertion. Therefore, the developed system can be used as an effective solution for detecting and analyzing web defacement attacks.

Keywords: *Web Defacement, OSINT, Python, Scoring, Automatic Detection*

KATA PENGANTAR

Alhamdulillahirabbil'alamin, Puji Syukur Penulis Panjatkan Kehadiran Allah SWT yang telah memberikan Rahmat dan karunia-Nya kepada kita, sehingga penyusunan Skripsi ini insyaallah dapat diselesaikan dengan baik dan tepat pada waktu yang telah di tentukan. Skripsi ini disusun untuk memenuhi syarat Ujian Komprehensif Mahasiswa Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang.

Pada Kesempatan ini Penulis Mengucapkan Terimakasih kepada pihak pihak yang telah membantu dalam Pelaksanaan dan Penyusunan Skripsi ini diantaranya :

1. Bapak Prof. Dr. Abid Djazuli, S.E., M.M selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak Ir. A. Junaidi, M.T. selaku Dekan FT Universitas Muhammadiyah Palembang.
3. Bapak Karnadi S.Kom., M.Kom selaku Ketua Program Studi Teknologi Informasi.
4. Bapak Dr.Ir. Zulhipni Reno Saptura S.T., M.Kom sebagai Dosen Pembimbing Utama Proposal Penelitian.
5. Bapak Apriansyah S.Kom., M.Kom sebagai Dosen Pembimbing Pendamping.
6. Orang tua dan keluarga yang telah memberikan dukungan maupun materi dalam menyelesaikan skripsi ini.

Penulis menyadari keterbatasan kemampuan yang dimiliki, karena itu kritik dan saran yang membangun dari berbagai pihak sangat dibutuhkan untuk perbaikan dan kesempurnaan Skripsi ini.

Palembang, 29 April 2026



Amanda Rahma Dwi
162022061

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PERNYATAAN.....	iv
MOTTO DAN PERSEMBAHAN.....	v
ABSTRAK	viii
ABSTRACK	ix
KATA PENGANTAR.....	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.1 Identifikasi Masalah	5
1.2 Rumusan Masalah	6
1.4 Batasan Masalah.....	6
1.5 Tujuan Penelitian.....	7
1.6 Manfaat Penelitian	7
1.7 Sistematika Penulisan	7
BAB II LANDASAN TEORI	10
2.1 Landasan Teori	10
2.1.1 <i>Web Defacement</i>	10
2.1.2 Keamanan Website dan Kerentanan.....	11
2.1.3 Deteksi Serangan <i>Web Defacement</i>	12
2.1.4 Teknik <i>Open Source Intelligence</i> (OSINT).....	13
2.1.5 Teknik <i>Google Dork</i>	13
2.1.6 Analisis Konten Berbasis <i>Python</i>	14

2.1.7 Konsep <i>Scrolling</i> dan Klasifikasi	15
2.1.8 Judi Online	15
2.1.9 <i>Flowchart</i>	16
2.2 <i>State Of The Art</i> dan Kebaruan	18
BAB III JADWAL PENELITIAN	22
3.1 Jenis Penelitian.....	22
3.2 Waktu dan Tempat Penelitian.....	23
3.2.1 Tempat Penelitian	23
3.2.2 Jadwal Penelitian.....	24
3.3 Kerangka Penelitian	25
3.4 Metode Pengumpulan Data	27
3.4.1 Identifikasi Kebutuhan Data	28
3.4.2 Pengumpulan Data dengan OSINT dan <i>Google Dork</i>	28
3.4.3 Validasi dan Seleksi Data	29
3.4.4 Dokumentasi dan Penyimpanan Data	29
3.5 Metode Penelitian.....	29
3.6 Metode Analisis Data	33
3.6.1 Analisis Frekuensi Kata Kunci.....	33
3.6.2 Analisis Intensitas Serangan.....	34
3.6.3 Analisis Klasifikasi dan Akurasi Sistem	34
3.6.4 Analisis Kecepatan Sistem	35
3.6.5 Analisis Pola Serangan.....	35
3.4 Tahapan Penelitian	36
3.4.1 Flowchart OSINT.....	36
3.4.2 Pengumpulan Data Target	37
3.4.3 Operator Khusus.....	37
3.4.4 Proses dan Validasi Data	38
3.4.5 Analisis Konten Website (Deteksi <i>Defacement</i>)	39
3.4.6 Perhitungan Skor dan Klasifikasi.....	39
3.4.7 Penyusunan Dataset	40
3.4.8 Analisis Pola Serangan.....	40

BAB IV HASIL DAN PEMBAHASAN	42
4.1 Implementasi Sistem Deteksi Berbasis Python.....	42
4.1.1 Pengumpulan Data Target (OSINT & <i>Dorking</i>)	42
4.1.2 Implementasi Algoritma Inspeksi Konten dan Perhitungan Skor	44
4.1.3 Rumus Perhitungan Deteksi Defacement.....	46
4.2 Hasil Pengujian dan Analisis Data	48
4.2.1 Eksekusi Sistem dan <i>Output</i> Deteksi	48
4.2.2 Analisa Kecepatan Sistem.....	54
4.2.3 Analisa Akurasi Sistem	55
4.2.4 Pola Serangan Judi Online	57
4.3 Evaluasi Sistem	61
BAB V KESIMPULAN DAN SARAN	65
5.1 Kesimpulan	65
5.2 Saran.....	66
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2. 1 Trafik Anomali.....	11
Gambar 3. 1 Lokasi	23
Gambar 3. 2 Kerangka Penelitian.....	27
Gambar 3. 3 Flowchart Osint	37

DAFTAR TABEL

Tabel 2. 1 Flowchart	16
Tabel 2. 2 State Of The Art.....	19
Tabel 3. 1 Jadwal Penelitian	24
Tabel 3. 2 Metodologi Penelitian.....	31
Tabel 3. 3 Operator Google Dork	38
Tabel 4. 1 Potongan Source Code (OSINT)	43
Tabel 4. 2 Master Status Data.....	44
Tabel 4. 3 Potongan Source Code Deteksi Deacement	45
Tabel 4. 4 Potongan Source Code Keyword Score.....	45
Tabel 4. 5 Hasil Dari Proses Pengujian Pagi Hari	49
Tabel 4. 6 Hasil Dari Proses Pengujian Siang Hari	50
Tabel 4. 7 Hasil Dari Proses Pengujian Malam Hari.....	51

BAB I

PENDAHULUAN

1.1 Latar Belakang

Transformasi digital melalui kemajuan teknologi informasi dan komunikasi saat ini telah membawa perubahan mendasar di berbagai lini kehidupan masyarakat. Teknologi informasi secara umum dapat diartikan sebagai bidang yang mencakup perancangan, penerapan, pengembangan, serta pengelolaan sistem informasi berbasis komputer, baik dari sisi perangkat keras maupun perangkat lunak [1]. Internet menjadi salah satu media utama dalam penyediaan informasi, komunikasi, riset, serta berbagai sumber daya yang tidak terbatas, sehingga dapat dimanfaatkan oleh masyarakat untuk mendukung produktivitas dan kreativitas[2]. Kemudahan dalam mengakses internet juga mendorong meningkatnya ketergantungan masyarakat terhadap teknologi digital dalam memenuhi kebutuhan sehari-hari.

Kemajuan teknologi juga memberikan dampak positif yang signifikan di berbagai sektor. Dalam bidang ekonomi, teknologi digital mendorong adanya industri kreatif, *e-commerce*, dan layanan berbasis daring yang mempermudah transaksi dan interaksi antar individu. Di sisi lain, bidang pendidikan, kesehatan, serta pemerintahan turut merasakan manfaat besar melalui sistem berbasis teknologi yang lebih efisien dan transparan. Meskipun demikian, akselerasi teknologi tidak selamanya membawa kemaslahatan. Terdapat risiko sistemik seperti adiksi media sosial, konsumsi gim daring yang imoderat, perundungan siber,

serta proliferasi hoaks yang berpotensi mendegradasi fokus mahasiswa dalam lingkungan akademik.[3].

Di sisi lain, perkembangan teknologi yang semakin pesat juga membuka peluang munculnya berbagai bentuk kejahatan siber yang semakin kompleks. Salah satu ancaman yang terus meningkat adalah serangan web defacement, yaitu aksi peretas yang mengubah tampilan atau konten suatu situs tanpa izin. Dalam beberapa tahun terakhir, pola serangan ini tidak hanya dilakukan untuk menunjukkan kemampuan peretas, tetapi juga dimanfaatkan sebagai media promosi konten ilegal, khususnya judi online. Situs-situs yang terdeface sering disisipi tautan, gambar, atau pesan yang mengarahkan pengunjung ke platform judi online demi kepentingan ekonomi para pelaku[4]. Kondisi ini semakin mengkhawatirkan karena serangan web defacement dapat menyerang berbagai jenis situs, mulai dari pemerintah, Pendidikan, hingga bisnis kecil, sehingga berdampak pada menurunnya kredibilitas pemilik situs dan meningkatnya potensi penyebaran aktivitas ilegal di internet[5].

Berbagai serangan web defacement yang bermuatan promosi judi online umumnya menasar berbagai jenis situs dan domain, baik dengan Tingkat otoritas tinggi maupun rendah. Domain seperti .go.id, .ac.id, .sch.id, dan or.id sering menjadi target karena memiliki reputasi yang kuat sehingga lebih efektif bagi pelaku untuk menyebarkan konten ilegal melalui manipulasi tampilan situs[6]. Di sisi lain, domain komersial seperti .com, .co.id, dan .net juga rentan karena banyak digunakan oleh pelaku usaha kecil yang sering kali memiliki kelemahan pada sisi keamanan server dan pengelolaan hosting[7]. Melalui analisis berbasis domain,

aktivitas defacement dapat diidentifikasi dengan mendeteksi perubahan elemen halaman seperti injeksi skrip, tautan asing, atau file yang ditanamkan oleh peretas. Teknik OSINT dan Google Dork memungkinkan penelusuran situs terdampak secara lebih terarah dengan memanfaatkan kata kunci, direktori, dan struktur URL berbasis domain. Oleh karena itu, pemahaman terhadap karakteristik setiap domain menjadi penting dalam upaya pencegahan serta deteksi terhadap penyebaran konten ilegal melalui serangan web defacement.

Fenomena serangan Web Defacement kini semakin sering di manfaatkan oleh pelaku kejahatan siber sebagai sarana promosi situs judi online. Banyak kasus menunjukkan bahwa website yang awalnya memiliki konten resmi berubah tampilan menjadi media promosi judi dengan menampilkan banner, tautan, maupun ajakan bermain secara online. Serangan ini tidak hanya merusak tampilan website yang diserang, tetapi juga berpotensi menyesatkan pengguna dengan mengarahkan ke situs-situs berbahaya yang berisi konten ilegal. Fenomena ini mengindikasikan transformasi kejahatan siber yang kian terstruktur. Aksi *web defacement* kini telah bergeser dari sekadar ajang pembuktian eksistensi menjadi instrumen profit komersial, khususnya sebagai sarana infiltrasi perjudian daring. Mengingat implikasinya yang sangat bergantung pada perilaku pengguna, maraknya perjudian *online* sebagai akses negatif teknologi memerlukan kajian lintas perspektif. Hal ini dikarenakan dampak destruktif yang ditimbulkan tidak berhenti pada level personal, namun berisiko menciptakan instabilitas pada institusi keluarga dan tatanan sosial [8].

Penelitian mengenai serangan web defacement telah banyak dilakukan pada berbagai jenis website seperti instalasi pemerintahan, lembaga pendidikan, dan perusahaan misalnya, penelitian oleh Rahmawati dkk [9] membahas analisis serangan defacement pada website pemerintahan menggunakan metode Vulnerability scanning untuk mengidentifikasi celah keamanan pada server public. Penelitian lain oleh Hikmatyar dkk [10] mengembangkan sistem deteksi otomatis untuk mendeteksi perubahan tampilan web akibat serangan defacement pada website profil perusahaan. Sementara itu, studi yang dilakukan oleh Nurseno dkk [11] menggunakan pendekatan OSINT untuk melacak aktivitas peretasan dan penyebaran konten berbahaya pada domain pendidikan. Hasil dari berbagai penelitian tersebut menunjukkan bahwa web defacement masih menjadi ancaman nyata bagi berbagai sektor dan penting untuk dilakukan analisis lebih lanjut terhadap pola dan metode serangan yang digunakan.

Meskipun banyak penelitian telah menyoroti kasus web defacement pada situs pemerintahan, pendidikan, maupun perusahaan, kajian yang berfokus secara khusus pada serangan defacement yang digunakan untuk menyebarkan atau mempromosikan konten judi online masih sangat terbatas. Penelitian oleh Haryadi dkk.[9] menunjukkan bahwa Sebagian besar serangan defacement pada pemerintah dilakukan untuk tujuan politis atau unjuk kemampuan, bukan untuk keuntungan ekonomi. Hal ini berbeda dengan pola serangan yang ditemukan pada situs judi online, di mana peretas sering kali memanfaatkan hasil serangan untuk menampilkan tautan dan promosi layanan perjudian secara illegal. Selain itu, Raharja [6] menegaskan bahwa metode OSINT dapat digunakan untk

mengidentifikasi situs-situs yang terindikasi terlibat dalam aktivitas judi online, namun penerapannya dalam konteks analisis web defacement masih jarang dilakukan. Oleh karena itu, penelitian ini dibuat untuk mengisi kesenjangan tersebut dengan mengembangkan pendekatan deteksi terhadap website yang terindikasi mengalami serangan web defacement bermuatan judi online menggunakan kombinasi metode OSINT dan Teknik Google Dork, Sehingga pola serangan, tujuan peretas, dan mekanisme penyebaran promosi judi online dapat dianalisis secara lebih komprehensif.

Berdasarkan permasalahan yang telah dijelaskan pada latar belakang, maka penulis tertarik untuk mengangkat topik dalam sebuah Skripsi dengan judul **“Deteksi Dan Analisis Pola Serangan Web Defacement Bermuatan Promosi Judi Online Pada Situs Website”**

1.1 Identifikasi Masalah

Merujuk pada uraian latar belakang tersebut, ditemukan beberapa persoalan pokok yang menjadi fokus identifikasi masalah dalam penelitian ini, yaitu::

1. Proses pendeteksian serangan web defacement bermuatan promosi judi online masih belum terstruktur dan belum memanfaatkan metode yang sistematis, sehingga hasil deteksi kurang optimal.
2. Pemanfaatan metode OSINT dan teknik Google Dork dalam mengidentifikasi indikasi web defacement belum diimplementasikan secara maksimal dalam suatu sistem yang terintegrasi.

3. Belum adanya analisis yang mendalam terhadap pola serangan web defacement bermuatan judi online, sehingga karakteristik, teknik, dan kecenderungan serangan belum dapat dipahami dengan baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan dalam penelitian ini dapat dirumuskan sebagai berikut :

1. Bagaimana merancang sistem deteksi web defacement bermuatan promosi judi online menggunakan metode OSINT dan teknik Google Dork secara efektif?
2. Bagaimana implementasi metode OSINT dan Google Dork dalam proses pengumpulan serta identifikasi data serangan web defacement pada website?
3. Bagaimana hasil analisis pola serangan web defacement bermuatan judi online berdasarkan data yang diperoleh dari sistem yang telah dibangun?

1.4 Batasan Masalah

Berdasarkan latar belakang yang telah dijelaskan maka, Batasan masalah pada penelitian ini adalah sebagai berikut :

1. Penelitian ini hanya berfokus pada deteksi web defacement bermuatan promosi judi online, tidak mencakup jenis serangan siber lainnya.
2. Metode yang digunakan terbatas pada pemanfaatan OSINT dan Google Dork tanpa melakukan akses langsung atau eksploitasi terhadap sistem target.

3. Data yang dianalisis berasal dari website yang terindeks mesin pencari dan difokuskan pada identifikasi pola konten serta perubahan halaman.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut :

1. Mengembangkan metode deteksi awal web defacement bermuatan promosi judi online menggunakan OSINT dan Google Dork.
2. Mengidentifikasi dan memvalidasi website yang mengalami defacement berdasarkan hasil pencarian.
3. Menganalisis pola serangan berdasarkan kata kunci, struktur halaman, dan karakteristik konten.

1.6 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Menambah pengetahuan di bidang keamanan siber, khususnya terkait deteksi web defacement.
2. Membantu dalam mendeteksi dini website yang terindikasi mengalami defacement.
3. Menjadi referensi bagi penelitian selanjutnya yang menggunakan metode OSINT dan Google Dork.

1.7 Sistematika Penulisan

Karya tulis ini terdiri dari lima bab masing-masing dengan pembahasan yang diatur sesuai sistematika berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang yang menjelaskan alasan pentingnya penelitian dilakukan serta fenomena yang melatarbelakanginya. Selain itu, dijelaskan identifikasi masalah dan rumusan masalah sebagai fokus utama penelitian. Batasan masalah disusun untuk memperjelas ruang lingkup penelitian agar tidak melebar. Tujuan dan manfaat penelitian juga dipaparkan untuk menunjukkan kontribusi yang diharapkan. Pada bagian akhir, disajikan sistematika penulisan sebagai gambaran isi skripsi.

BAB II TINJAUAN PUSTAKA

Bab ini menyajikan kerangka teoretis yang mendasari penelitian, yang mencakup pendalaman konsep *web defacement* serta keamanan situs web. Selain itu, dipaparkan pula metodologi pengumpulan data melalui teknik OSINT dan *Google Dork*. Diskusi mengenai analisis konten berbasis Python serta mekanisme penilaian (*scoring*) juga diintegrasikan untuk memperkuat analisis. Sebagai pelengkap, bab ini menyertakan tinjauan penelitian terdahulu sebagai komparasi untuk mempertegas posisi penelitian ini di atas landasan konseptual yang kokoh

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan metode yang digunakan dalam penelitian secara rinci dan sistematis. Di dalamnya mencakup jenis penelitian, waktu dan tempat penelitian, serta kerangka penelitian. Selain itu, dijelaskan teknik pengumpulan data menggunakan OSINT dan *Google Dork*. Proses validasi, pengolahan, dan analisis

data juga diuraikan secara jelas. Bab ini menjadi pedoman dalam pelaksanaan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil dari implementasi sistem yang telah dibangun. Proses pengujian sistem dijelaskan untuk menunjukkan cara kerja dan performa sistem. Selain itu, dilakukan analisis terhadap data hasil deteksi yang diperoleh. Pembahasan juga mencakup pola serangan yang berhasil diidentifikasi. Bab ini menunjukkan hasil nyata dari penelitian yang dilakukan.

BAB V PENUTUP

Bab ini menyajikan sintesis akhir berupa kesimpulan yang ditarik dari hasil analisis data penelitian. Rumusan kesimpulan tersebut disusun secara sistematis agar selaras dengan tujuan dan pokok permasalahan yang telah ditetapkan. Selain itu, bagian ini memuat saran konstruktif bagi pengembangan studi selanjutnya, baik dari sisi penyempurnaan metodologi maupun eskalasi sistem. Sebagai bagian akhir, bab ini merangkum seluruh esensi dan temuan dari rangkaian penelitian skripsi ini.

DAFTAR PUSTAKA

- [1] A. Premana, G. Fitralisma, A. Yulianto, M. B. Zaman, dan M. A. Wiryo, “Pemanfaatan Teknologi Informasi Pada Pertumbuhan Ekonomi Dalam Era Disrupsi 4 . 0,” vol. 1, no. 01, hal. 1–6, 2020.
- [2] J. Firdaus, N. Wulan, dan T. Hidayat, “Peranan Penggunaan Internet dan Sosial Media dalam Meningkatkan Kegiatan Produktif Bagi Masyarakat,” vol. 1, no. 2, hal. 25–30, 2024.
- [3] K. Prasanti dan I. H. Wiranata, “Dampak Negatif Penyalahgunaan Teknologi Terhadap Proses Pendidikan,” hal. 335–345.
- [4] P. Agustin dan A. Wahyu, “Analisis Keamanan Situs ‘ . go . id ’ Terhadap Serangan Web Defacement ‘ Judi Online ,”” vol. 24, no. 1, hal. 1–10, 2025.
- [5] M. Rizky, R. Pahlevi, C. Umam, dan L. B. Handoko, “Deteksi dan Pencegahan Web Defacing Judi Online dengan Wazuh SIEM dan Snort IDS Berbasis Signature,” hal. 197–208, 2025, doi: 10.33364/algorithm/v.22-1.2220.
- [6] Y. Raharja dan U. M. Sidoarjo, “Implementasi metode osint untuk mengidentifikasi serangan judi online pada website,” vol. 1, hal. 359–364, 2023.
- [7] I. Suharjo dan P. Wahyu, “Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache Identification and Analysis of Website Domain Hacking Incidents from Google Cache Data,” vol. 14, no. January, hal. 61–70, 2024.

- [8] A. Laras, N. Salvabillah, C. Caroline, J. D. H, F. Dinda, dan M. Finanto, “Analisis Dampak Judi Online di Indonesia Fakultas Psikologi ; Universitas Bhayangkara Jakarta Raya terkait , seperti penipuan dan pencurian , karena individu yang kecanduan sering kali mencari,” vol. 4, no. 2, hal. 140–151, 2025.
- [9] D. Hariyadi, “Analisis Serangan Web Defacement pada Situs Web Pemerintah Menggunakan ELK Stack,” vol. 4, no. 1, hal. 1–8, 2019.
- [10] J. I. Dan, “ANALISIS PERBANDINGAN VULNERABILITY SCANNING PADA WEBSITE DVWA,” vol. 3, no. 2, hal. 89–97, 2023.
- [11] “nurseno,” 2024.
- [12] M. M. Osint, “Identifikasi Kerentanan Terhadap Serangan Slot,” vol. 1, no. 2, hal. 1–8, 2022, doi: 10.29322/IJSRP.X.X.2018.pXXXX.
- [13] M. Alfa, R. Fikri, A. I. Hadiana, dan R. Ilyas, “Pemanfaatan Open-Source Intelligence untuk Deteksi dan Penanganan Cybercrime Judi Online Berbasis Forensik Digital,” hal. 22–35, 2025, doi: 10.33364/algorithm/v.22-2.2314.
- [14] A. M. Pratama, M. Data, dan W. Yahya, “Deteksi Konten Ilegal Pada Situs Web Menggunakan Elasticsearch,” vol. 9, no. 10, hal. 1–9, 2025.
- [15] M. Hikmatyar, A. Sudiarjo, M. I. Arief, dan N. Fadilah, “Pengembangan Aplikasi Scanning Defacement Judi Online untuk Website Profile pada Server,” vol. 2, hal. 171–175, 2024.
- [16] L. M. Zagi, “Just Dork and Crawl: Measuring Illegal Online Gambling Defacement in Indonesian Websites”.
- [17] F. D. Vol, “Tindakan kejahatan,” vol. 6, no. 1, hal. 25–29, 2023.

- [18] W. D. : J. O. B. Si. dan S. N. (BSSN), “Web Defacement : Judi Online, Langkah langkah penanggulangan insiden web defacement judi online dan mitigasi”.
- [19] “Lanskap Keamanan Siber Indonesia 2024: Tren dan Tantangan.” [Daring]. Tersedia pada: <https://rtikjatim.or.id/lanskap-keamanan-siber-indonesia-2024-tren-dan-tantangan/>
- [20] C. Kurniawan, A. Triayudi, I. Technology, dan U. Nasional, “File Integrity Monitoring as a Method for Detecting and Preventing Web Defacement Attacks,” vol. 9, no. 2, hal. 276–285, 2024, doi: 10.15575/join.v9i2.1326.
- [21] X. D. Hoang, T. H. Nguyen, dan H. D. Pham, “A novel model for detecting web defacement attacks transformer using plain text features,” vol. 37, no. 1, hal. 232–240, 2025, doi: 10.11591/ijeecs.v37.i1.pp232-240.
- [22] D. Sahputra, A. Afifa, A. M. Salwa, dan N. Yudhistira, “Dampak Judi Online Terhadap Kalangan Remaja (Studi Kasus Tebing Tinggi),” vol. 6, no. 2, hal. 139–156, 2022.
- [23] N. A. Syakira, N. F. Ramadhahana, dan N. D. Anggita, “Dampak Konsumerisme Berupa Judi Online di Indonesia : Perspektif Ekonomi , Sosial , dan Mental,” vol. 16, no. 2, 2024.
- [24] S. Teras, W. Rahayu, A. Salim, dan A. E. Saputra, “Tinjauan Yuridis Tindak Pidana Judi Online Yang Melibatkan Anak Sebagai Pelaku,” vol. 3, no. 4, hal. 3517–3523, 2025.
- [25] S. M. Indra dan T. Srihadiati, “Analisis Kriminologi Peran Konstruksi Media Terhadap Penyebaran Konten Judi Online dalam Media Sosial Facebook,” vol.

7, no. 5, hal. 3608–3619, 2025.