ISSN 2527-3671 (*Online*)
ISSN 2087-8893 (*Print*)

Teknologi: Jurnal Ilmiah Sistem Informasi 14 (1) January 2024 61-70

Tersedia *online* di www.journal.unipdu.ac.id

Halaman jurnal di www.journal.unipdu.ac.id/index.php/teknologi

Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache

Imam Suharjo [a], Putry Wahyu Setyaningsih [b]

a Program Studi Informatika, Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia

b Program Studi Sistem Informasi, Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia

email: [a,]imam@mercubuana-yogya.ac.id*

*Korespondensi

Dikirim 27 Desember 2023; **Direvisi** 03 Maret 2024; **Diterima** 15 April 2024; **Diterbitkan** 23 Mei 2024

Abstrak

Keamanan situs web seringkali dihadapi oleh pemiliknya, terutama terkait dengan praktek Black Hat SEO yang menggunakan peretasan untuk memanipulasi mesin pencari. Pengumpulan data dilakukan melalui pencarian Google dalam 24 jam terakhir, dengan proses scraping/crawling menggunakan apify.com. Dari hasil pencarian tersebut, diperoleh 7.604 konten (445 domain) dihack dalam 81 hari untuk domain go.id, dan 3.576 konten (252 domain) dihack dalam 43 hari untuk domain ac.id. Fokus penelitian terbatas pada domain dengan TLD ac.id dan go.id. Hasil analisis data mengungkapkan empat jenis peretasan utama. Pada domain go.id, kasus Reflected XSS in search mencapai 45%, Invisible backlink 8%, konten terhack 45%, dan subdomain 2%. Sedangkan pada domain ac.id, Reflected XSS in search mencapai 34%, Invisible backlink 38%, konten terhack 26%, dan subdomain 2%. Penelitian ini memberikan gambaran bahwa setiap hari terjadi peretasan di antara 5-6 institusi berbeda, baik di lembaga pendidikan maupun pemerintah.

Kata Kunci: domain internet, keamanan siber, backlink, SEO, crawling, keamanan web.

Identification and Analysis of Website Domain Hacking Incidents from Google Cache Data

Abstract

Website security is often a concern for its owners, particularly in relation to Black Hat SEO practices that involve hacking to manipulate search engines. Data collection is conducted through Google searches within the last 24 hours, utilizing the scraping/crawling process with apify.com. From these searches, a total of 7,604 content instances (445 domains) were hacked in 81 days for the go.id domain, and 3,576 instances (252 domains) were hacked in 43 days for the ac.id domain. The research focuses on domains with the TLDs ac.id and go.id. Data analysis reveals four main types of hacking incidents. For go.id domains, cases of Reflected XSS in search reach 45%, Invisible backlinks 8%, hacked content 45%, and subdomains 2%. Meanwhile, for ac.id domains, Reflected XSS in search reaches 34%, Invisible backlinks 38%, hacked content 26%, and subdomains 2%. The study provides insight that hacking incidents occur daily across 5-6 different institutions, both in educational and government institutions.

Keywords: *: Internet domain, cyber security, backlink, SEO, crawling, web security.*

Untuk mengutip artikel ini dengan APA Style:

Suharjo, I., & Setyaningsi, W. P. (2024). Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache. TEKNOLOGI: Jurnal Ilmiah Sistem Informasi, 14(1), 61-70 : https://doi.org/10.26594/teknologi.v14i1.4311

1. Pendahuluan

Tantangan dalam mempertahankan keamanan teknologi informasi terutama website selalu dinamis, selalu berubah bentuk, sifat, dan sumber dari ancaman beragam. Pada era sebelumnya, tantangan pertahanan, keamanan berupa serangan langsung dengan memanfaatkan peralatan perang yang melibatkan kontak fisik yang lebih intens, sedangkan saat ini dengan teknologi dan informasi yang berkembang pesat, tantangan keamanan dan pertahanan menciptakan dimensi baru, yaitu keamanan cyber. Artikel ini akan memaparkan berbagai ancaman dan serangan siber di website menjadi tantangan dalam menjaga keamanan dan lebih fokus pada jenis peretasan pada konten website.

Secara lebih spesifik penelitian ini mempunya 2 tujuan utama yaitu : menghimpun data website yang teretas dari data (*cache*) terindex di mesin pencari dan klasifikasi data berdasarkan jenis peretasan dan domain web.

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)

Penelitian ini penting untuk dilakukan karena kasus peretasan web perlu jadi perhatian serius terutama pengeloa website pemerintah (go.id) dan pendidikan Universitas (ac.id). Selain itu perlu di data, siapa saja yang kena serangan ini, bagian apa saja, konten jenis apa.

Gambar 1. Penyisipan konten link di bagian bawah tersembunyi sebagai *invisible backlink* di footer

Merujuk data Kementerian Komunikasi dan Informatika (Kominfo) di website pemerintah, terkait keamanan data dan informasi, terutama website jadi media yang rawan terjadi peretasan. Merujuk data Kominfo tahun 2012, peretasan cukup banyak terjadi, ada 50% website resmi pemerintah domain go.id., sedangkan 50% lainnya adalah Alamat website dengan domain lain yang umu digunakan seperti .com, , ac.id, or.id, .net dan .org. (kominfo.go.id, 2022)

Data Statitika.com di bulan Oktober 2020 hingga September 2021, jumlah data spam atau sampah harian secara global data tertinggi pada bulan Juli tahun 2021, ada hampir 283 milyar konten email yang erindikasi sebagai jenis spam dari total 336,41 miliyar email telah terkirim. Sementara data bulan Agustus tahun 2021, jumlahnya turun menjadi jadi 65,5 miliar email spam. Bulan September, jumlah kiriman spam email meningkat 36% sampai 88,88 milyar dari 105,67 milyar email yang dikirim. Sementara negara yang paling banyak mengirim email adalah Amerika Serikat. (www.statista.com, 2023)

Selain email dan peretasan, ancaman keamanan lain terjadi pada formulir terbuka dengan jenis serangann berupa : percobaan injeksi, serangan yang berulang atau konten spamming. Meskipun telah banyak tersedia dan terpasang aplikasi atau sistem perlindungan lain, serangan berjenis kontenn spam juga terjadi pada form komentar. Misalnya, meskipun menggunakan proteksi spam seperti Akismet sebagai plugin anticapm komentar WordPress, komentar spam masih mungkin lolos terkirim dianggap sebagai sebagai spam. Komentar jenis spam ini pada umumnya tidak hanya konten namun juga ada tautan atau *hyperlink* aktif (*backlink*) yang bertujuan untuk mendukung atau SEO sebagai cara optimasi dalam website.

Deface website adalah tindakan peretas yang merusak atau mengubah tampilan homepage sebuah website, seringkali untuk menodai reputasi, mengeksploitasi kerentanan, atau menyampaikan pesan politik. Artikel ini mengkaji evolusi kejahatan dunia maya dalam bentuk deface website dengan metode tinjauan sistematis, termasuk contoh yang terjadi pada website DPR RI tahun 2020. (Aji, 2023.)

Platform Content Management System (CMS) WordPress cukup paling populer digunakan untuk membangun sebuah website, Wordpress digunanakan sekitar 455 juta situs atau sekitar diguanan sekitar 60,3% dari semua sistem manajemen website. CMS WordPress ini selalu update, relatif aman, serta dukungan banyak tema dan pluginnya. Namun terdapat cukup banyak kerentanan ditemukan di website yang menggunakan WordPress, hal ini lebih dikaitkan dengan tambahan plugin atau theme pihak lain yang terpasang di web tersebut serta tidak melakukan pembaharuan. (Murphy, 2021)

2. State of the Art

Kehidupan semakin mudah dengan adanya fasilitas komputasi awan (*clould computing*). Pilihan menyimpan segalam macam data, layanan / aplikasi sekarang lebih mudah dan cepat dengan memanfaatkan cloud computing, yang menjadikannya benar-benar bisa diakses dari mana saja. Perangkat yang dapat diakses di alam berisi berbagai layanan berbasis awan. Namun, masalah keamanan sistem selalu muncul ada di layer 7 aplikasi. **(Putri, 2021)** Lapisan aplikasi bersifat cerdas, yang menyediakan situasi waktu nyata di mana aplikasi yang menuntut dapat diterima atau ditolak berdasarkan permintaannya. Layer aplikasi ini umunya terlihat secara publik dengan akses menajemen umumnya berdasarkannama pengguna dan kredensial.

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)

Sistem untuk mendeteksi serangan melalui jaringan yang handal dapat digunakan untuk mendukung pencegahan berbagai jenis ancaman seperti pada spam formulir atau komentar di website. Gabungan antara berbagai jenis Teknik pengammanan termasuk pendekatan kecerdasan buatan (AI) bisa membantu untuk menghindari dan bahkan mencegah sistem dari berbagai jenis ancaman serangan jaringan atau serangan ke sistem. (Mi, 2019)

Menurut data yang dihimpun dari Internet Live Stat, pertumbuhan jumlah web terus naik, jumlah situs website naik mencapai lebih dari 1,9 miliyar dan terus mengalami peningkatan. Sementara CMS terpopuler yang terpasang pada situs website paling banyak dan umumnya berbasis Bahasa program PHP termasuk Wordpress, Joomla atau CMS yang lain. Data di bulan Desember 2018 presentase pengguna CMS ada 59% Wordpress dan 6% Joomla dan CMS lain. Sebagian besar website tersebut milik perusahaan dan individu yang umunya kurang memperhatikan masalah keamanan. Selain itu, biaya pengembangan aplikasi, pemilik lebih memilih CMS mudah dipasang dan siap untuk mempercepat implementasi di website. (Nguyen, 2019)

Pada tahun 2019, sebagian besar dari sekitar dua miliar situs website online internet dioperasikan oleh baik oleh individu maupun organisasi yang tidak memiliki keterampilan memadai, sumber daya guna mengamankan. Banyak website ini menjadi salah satu target untuk di eksploitasi sistem dan kelemahan baik untuk motif finansial atau yang lain. Van-Linh Nguyen, dkk dari Universitas Nasional Chung Cheng, Taiwan, sebelumnya telah meneliti teknik yang digunakan oleh hacker / cracker ini dan menyusun kerangka kerja untuk mencegah jenis serangan sejenis. (Nguyen, 2019)

Spam konten yang menempel di website adalah jenis spam yang ikut popular ketika konten website tersebut popular. Spam konten terbanyak dan paling luas cakupannya karena mengeksploitasi model supaya masuk dalam pencarian informasi internet mesin pencari sepeti Google. Model konten spam masuk jadi bagian konten web dan konten ini yang selanjutnya ikut memberi peringkat halaman berdasar algoritma mesin pencari, masuk peringkat halaman hasil pencarian. (Farizi, 2020). Pelaku kejahan jenis ini juga melakukan analisis kelemahan pada model yang diterapkan dan mengeksploitasinya. Spam jenis ini bisa terdapat di judul, bagian meta tag head, isi konten utama, anchor text serta dalam bentuk URL spam yang dimodifikasi (Rahman, 2020).

Judul tulisan (*title*) di website memainkan peran krusial dalam mencari sebuah informasi, judul dan cuplikan konten akan ditampilkan di mesin pencari. Pelaku sering kali uunya mengisi judul secara berlebihan untuk meningkatkan hasil terbiak peringkat halaman hasil pencarian, yang dikenal sebagai "title spamming." Dalam praktik ini, judul diisi dengan kata kunci berlebihan yang tidak relevan dengan konten. Selain itu, "body spamming" terjadi ketika isi halaman dimodifikasi dengan konten yang sering dicari, tetapi tidak relevan dengan topik utama. Meta-tag juga memainkan peran penting dalam SEO, karena mereka memberikan deskripsi dokumen yang digunakan oleh mesin pencari untuk menentukan hasil pencarian. Spammer bisa memanipulasi meta-tag untuk meningkatkan peringkat halaman secara tidak etis. "URL spamming" adalah praktik di mana konten yang diinginkan disisipkan langsung ke dalam URL, yang dapat menyesatkan mesin pencari dan pengguna. (Rahman, 2020)

Terjadi peningkatan signifikan dalam penggunaan teknik spam jenis SEO serta penyebaran malware bertujuan merusak indeks hasil pencarian di berbagai platform dan aplikasi. Praktik ini dilakukan dengan menambahkan konten yang mungkin hanya ada kemiripan atau bahkan konten tidak sesuai dengan tema dan ide asli dari aplikasi /website tersebut. (Arghire, 2020). Jenis link antar halaman atau ke website luar atau konten komentar yang tidak sesuai dengan tema web dapat membingungkan pengunjung dan mengarahkan pengunjung web ke situs yang yang jadi target mereka. Situs website yang popular, banayk pengjungnynan sering menjadi target menarik bagi peretas. Hambatan yang terjadi dalam menerapkan perlindungan keamanan adalah akses web yang terbuka kapan saja dan akses bagi siapa saja. Alasan yang lebih serius adalah kurangnya informasi atau ketidakmampuan pengembang yang tidak berpengalaman dalam SEO. (Petkova, 2019)

Bagi sebuah institusi, keberhasilan situs web phishing yang menduplikasi dapat merusak reputasi organisasi atau menjadi dasar serangan takeover subdomain. Serangan takeover subdomain ini dapat sepenuhnya lolos dari deteksi sertifikat SSL dan berdampak langsung pada perusahaan. Serangan takeover subdomain yang berhasil memiliki tingkat ancaman yang lebih tinggi karena subdomain yang dikuasai memiliki sertifikat SSL yang sama dengan situs web induknya, meskipun serangan ini tidak memerlukan keahlian teknis yang tinggi untuk dieksploitasi. (Yunjia Wang, 2021)

3. Metode Penelitian

Penelitian identifiaksi dan analsisi spam SEO wensite ini dilakukan menggunakan : Laptop/ Komputer, data domain website online internet dan hosting, sumber data yang dihimpun/data dari mesin pencari Google dengan data terbaru, aplikasi pengolah data dan tool apify.com ***(apify.com, 2023)***. Penelitian dilakukan dengan memanfaatkan data dari website/ domain yang terkena kasus peretasan. Jenis type data diambil

Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70
ISSN 2502-3357 (*Online*)
ISSN 2503-0477 (*Print*)

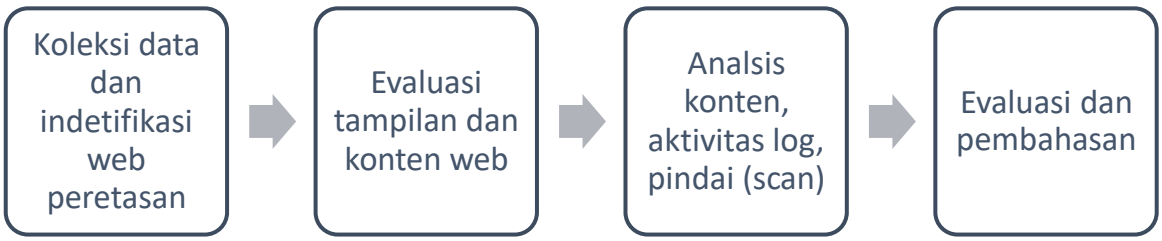
berupa : nama domain, URL, waktu, pemilik domain, jenis peretasan. Data perolehan penelitian ini kemudian dihimpun dan dilakukan analisis.

Gambar 2. Hasil pencarian Google : website yang tersusupi konten peretas (dalam 24 terakhir)

Metode untuk mengidentifikasi dan menganalisis terjadinya peretasan pada domain website dari data Google Cache, dilakukan dengan langkah-langkah berikut: Mengakses Pencarian Google dengan menggunakan data percarian terakhir dengan menggunakan kata kunci terkait perjudian dan melihat cache. Ini dilakukan berulang setap hari. Selanjutnya mengevaluasi tampilan halaman dengan melihat tinjau tampilan halaman dan perhatikan apakah terdapat elemen yang tidak seharusnya ada, seperti pesan error atau iklan yang mencurigakan. Periksa tampilan halaman sama dengan tampilan asli domain website. Jika tidak, kemungkinan besar terdapat peretasan yang terjadi.
Parameter Parameter utama yang digunakan dalan pencarian yang barusan teridex di Google dalam 24 jam terakhir: *Exact location (Google UULE parameter) : biw=1400&tbs=qdr%3Ad dengan Results per Google page : 100 dan Search terms or URLs : slot+gacor site:go.id.*

Contoh implementasi dalam Google Search Videos Scraper di Apyfy : *{"searchQuery": {"term": "slot gacor site:go.id", "url":"http://www.google.co.id/search?num=100&q=slot+gacor%20site:go.id&uule=biw=1400&tbs=qdr%3Ad", "device": "DESKTOP", "page": 1, "type": "SEARCH", "domain": "google.co.id", "biw=1400", "resultsPerPage": "100" }.*

Penerapan pencarian langsung dengan Google akan memberikan hasil seperti pada Gambar 2 (hasil pencarian dalam 24 jam terakhir (menurut data di penyimpanan hasil pencarian Google) dan semenjak perintah ini dijalankan pada domain :go.id.



Gambar 3. Jalan Penelitian

Setelah melakukan langkah-langkah di atas, dapat menganalisis dan menentukan penyebab terjadinya peretasan pada domain website sesuai dengan jakan penelitian Gambar 3.

4. Hasil dan Pembahasan

Pengambilan sampel data dalam peneliltian ini dengan domain go.id dilakukan selama 81 hari dari 31 Mei 2023 hingga 12 September 2023. Sementara sampel domain kampus ac.id selama 43 hari dilakukan dalam rentang waktu pada 31 Juni hingga 12 September 2023. Data diambil dari halaman yang terindex di Google

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)

dalam 24 jam terakhir, perintah dijalankan oleh script yang berjakan di apify.com, berjalan setiap hari. (apify.com, 2023)

	A	B	C	D	E	F	G	H
1	No.	Title	URL	Description	domain	domain	Jenis	Search termsearchQuery.term
7576	7575	71	Hasil Pencarian untuk "slot	https://tribratanews.ntb.polri.go.id/news/	tribratanews.ntb.polri.go.i	polri.go.id	in search	23 hours ago
7577	7576	72	Hasil Pencarian untuk "slot-	https://tribratanews.ntb.polri.go.id/news/	tribratanews.ntb.polri.go.i	polri.go.id	in search	24 hours ago
7578	7577	73	vhntlmc.xyz~],slot gacor	https://tribratanews.ntb.polri.go.id/news/	tribratanews.ntb.polri.go.i	polri.go.id	in search	24 hours ago
7579	7578	74	Hasil Pencarian untuk "slot-	https://tribratanews.ntb.polri.go.id/news/	tribratanews.ntb.polri.go.i	polri.go.id	in search	22 hours ago
7580	7579	75	Slot Togelking Online	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	11 hours agoTentunya sebagai penyed
7581	7580	76	Staf/Pelaksana | Pengadila	https://dilmil-banjarmasin.go.id/?page_id=	dilmil-banjarmasin.go.id	dilmil-banjarmasin.go.id	in search	13 hours ago... slot.site/ · istana
7582	7581	77	Peta Wilayah Yuridiksi | Pe	https://dilmil-banjarmasin.go.id/?page_id=	dilmil-banjarmasin.go.id	dilmil-banjarmasin.go.id	in search	18 hours ago... slot.site/ · istana
7583	7582	78	LAPORAN HARTA KEKAYA	https://dilmil-banjarmasin.go.id/?page_id=	dilmil-banjarmasin.go.id	dilmil-banjarmasin.go.id	in search	16 hours ago... slot.site/ · istana
7584	7583	79	Slot Alibabaslot168	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	1 hour agoMemilih salah satu mesin
7585	7584	80	Slot Jokislot138 Online	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	4 hours agoPanenslot77 merupakan sa
7586	7585	81	Slot186: 10 Situs Slot Gacc	https://gatewayoss.pom.go.id/gateway/s	gatewayoss.pom.go.id	pom.go.id	konten retas	9 hours agoDengan beragam jenis per
7587	7586	82	Slot Koboislot Online	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	4 hours agoAgen slot online selalu
7588	7587	83	8 jaya togel sdy: Daftar Situ	https://diskop.ntbprov.go.id/bet/benefitho	diskop.ntbprov.go.id	ntbprov.go.id	konten retas	14 hours agoML88 adalah agen slot o
7589	7588	84	Informasi Pengadilan	https://www.pa-sukabumi.go.id/informasi	www.pa-sukabumi.go.id	pa-sukabumi.go.id	Invisible backlink	8 hours ago... slot-thailand/ · slo
7590	7589	85	DKP Serahkan 55 Unit Mes	https://www.sumbarprov.go.id/home/new	www.sumbarprov.go.id	sumbarprov.go.id	Invisible backlink	16 hours ago... slot gacor slot gac
7591	7590	86	Judi Briobola	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	12 hours agoJudy Briobola – Raja98
7592	7591	87	Dino99	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	11 hours agoSelain itu, Slot Gacor
7593	7592	88	tanjaba – Pemerintah Kabu	https://tanjabbarkab.go.id/v2/?author=3	tanjabbarkab.go.id	tanjabbarkab.go.id	in search	12 hours agoSlot Gacor Hari Ini Sya
7594	7593	89	Judi Selera303	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	9 hours agoIngin menikmati perasaan
7595	7594	90	Gudangwin	https://rsud.sijunjung.go.id/doflamingo/gu	rsud.sijunjung.go.id	sijunjung.go.id	konten retas	22 hours agoKeamanan yang terjamin
7596	7595	91	Judi Wede168	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	6 hours agoMudah menang hari ini Ga
7597	7596	92	Legalisasi Dokumen Pendid	https://lampung.kemenkumham.go.id/pus-	lampung.kemenkumham.g	kemenkumham.go.id	Invisible backlink	18 hours agoBK8 slot gacor · phn.jd
7598	7597	93	Persiapkan Penilaian Kenai	https://jabar.kemenkumham.go.id/berita-k	jabar.kemenkumham.go.id	kemenkumham.go.id	Invisible backlink	18 hours agoSlot Gacor 2023 · https
7599	7598	94	Kakanwil (R. Andika Dwi Pr	https://jabar.kemenkumham.go.id/berita-k	jabar.kemenkumham.go.id	kemenkumham.go.id	Invisible backlink	18 hours agoSlot Gacor 2023 · https
7600	7599	95	Slot Primerplay Online	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	18 hours agoLakers4d telah menyedia
7601	7600	96	Slot Legototo Online	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	3 hours agoOleh karena itu, Live RT
7602	7601	97	Slot Kakekslot	https://dinaspertanian.sijunjung.go.id/dofl	dinaspertanian.sijunjung.g	sijunjung.go.id	konten retas	21 hours agoSlot Kakekslot – Mesin
7603	7602	98	Kunjungi Lapas Narkotika d	https://lampung.kemenkumham.go.id/pus-	lampung.kemenkumham.g	kemenkumham.go.id	Invisible backlink	19 hours agoBK8 slot gacor · phn.jd
7604	7603	99	Partisipasi Kemenkumham I	https://jogja.kemenkumham.go.id/berita-k	jogja.kemenkumham.go.id	kemenkumham.go.id	Invisible backlink	17 hours ago... slot-gacor/index.ht
7605	7604	100	Gandeng Poltekkes Tj.Kara	https://lampung.kemenkumham.go.id/beri	lampung.kemenkumham.g	kemenkumham.go.id	Invisible backlink	19 hours agoBK8 slot gacor · phn.jd

Gambar 4. Cuplikan data Web (URL) yang diretas, domain dan jenis peretasan.

Selama pengambilan sampel dalam 81 terhadap web yang diretas konten perjudian yang diambil harian, ada 445 domain institusi pemerintah go.id yang terdampak. Dari data ini terdapat total ada 1.253 subdomain terdampak, dengan jumlah page sebanyak 7.604 alamat URL. Rincian jenis dari total halaman sebanyak 7.604 halaman terdampak: *reflected XSS in search* 3.418 (45%), *invisible backlink* 621 (8%), konten diretas 3.431 (45%) dan *sub domain hacking (takeover)* 134 (2%).

Sementara pengambilan sampel domain kampus ac.id dilakukan selama 43 hari. Web kampus yang terdampak peretasan ada 252 domain institusi pendidikan (ac.id). Jika dirincin terdapat total ada 397 subdomain terdampak, dengan jumlah page sebanyak 3.576 alamat URL. Rincian jenis dari total halaman sebanyak 3,576 halaman terdampak : *reflected XSS in search* 1.209 (34%), *invisible backlink* 1.348 (38%), konten diretas 931 (26%) *sub domain takeover* 88 (2%).

Dari sampel data ini tersebut diperkirakan akan terjadi peretasan web sejumlah 5-6 institusi yang berbeda dalam setiap hari baik di institusi kampus ataupun pemerintah. Sementara jumlah laman yang terdampak peretasn ini dari setiap domain sangat bervaritif, sebagai besar kurang dari 10 halaman. Ada beberapa domain dengan lebih dari 10 laman terdampak bahkan ada beberapa web yang dengan ratusan laman terdampak. Berikut adalah rincian dari 4 jenis kasus peretasan terkait konten perjudian di web pemerintah dan kampus

4.1. Reflected XSS in Search

In search (reflected XSS), konten yang sengaja dimasukan ke fitur pencarian di web (kolom pencarian *search*). Atau injeksi konten melalui URL dan hasil injeksi ini tampil di web. Penambahan konten di kolom pencarian ini akan membentuk URL yang unik. Konten yang diketik juga akan muncul di page tersebut. Umumnya konten ini tidak membentuk link aktif.

Hasil dari peretas jenis ini mudah ditemukan oleh pemilik dengan menggunakan mesin pencari Google seperti terlihat pada Gambar 5 , tidak merusak data server, hanya akan menambah konten terindex di mesin pencari saja. Pemilik web mengubah fitur pencarian agar konten yang diketik di URL tidak langsung masuk jadi konten page tersebut.

Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70
ISSN 2502-3357 (*Online*)
ISSN 2503-0477 (*Print*)

Gambar 5. Konten yang terindex di Google

Reflected XSS ini secara umum, konten peretas tidak tersimpan di web atau database, namun konten injeksi tampil dan terindex di Google (ada di Google cache). Jenis retasan ini peretas menyisipkan alamat URL atau domain berharap jadi link alktif, namun umumnya link aktif tidak bisa dibuat dengan cara ini, seperti contoh pada Gambar 6.

Gambar 6. Link aktif dari hasil pencarian di Google, sama dengan cache di Google

Jika konten disisipkan melalui form pencarian (search) dan kemudian ditampilkan pada halaman hasil pencarian atau halaman lain, hal ini masih dapat disebut sebagai "Reflected XSS". Dalam kasus ini, serangan tersebut melibatkan penyisipan skrip berbahaya melalui input pencarian, dan hasilnya direfleksikan kembali kepada pengguna dalam halaman hasil pencarian. Contoh URL *reflected XSS* : https://some-domain/?kg=lwkhu&s=contoh%20konten%20sisipan

Pada kasus lasin bisa juga menggunakan skrip JavaScript berbahaya disisipkan dalam parameter pencarian, dan hasil pencarian akan mencantumkan skrip tersebut, yang kemudian dieksekusi pada peramban web pengguna.

4.2. Invisible backlink

Banyak juga ditemukan sisipan backlink ditanamkan di suatu situs web (sebelum header atau setelah footer) dengan atribut hidden, tidak terlihat atau tidak dapat diakses oleh pengguna yang mengunjungi halaman tersebut. Situasi web yang konten link ini sering disebut sebagai "invisible backlink" atau "hidden backlink". Dari data yang diambil kasus ini sering muncul dan nomor kedua setelah peretaan konten. Invisible backlink semacam ini seringkali digunakan dalam upaya manipulasi mesin pencari atau SEO dengan cara mencoba meningkatkan peringkat situs web tertentu tanpa pengetahuan pengguna seperti contoh di Gambar 7.

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)

Contoh 7. Tampilan kode sumber (HTML) dari halaman yang terkena invisible backlink

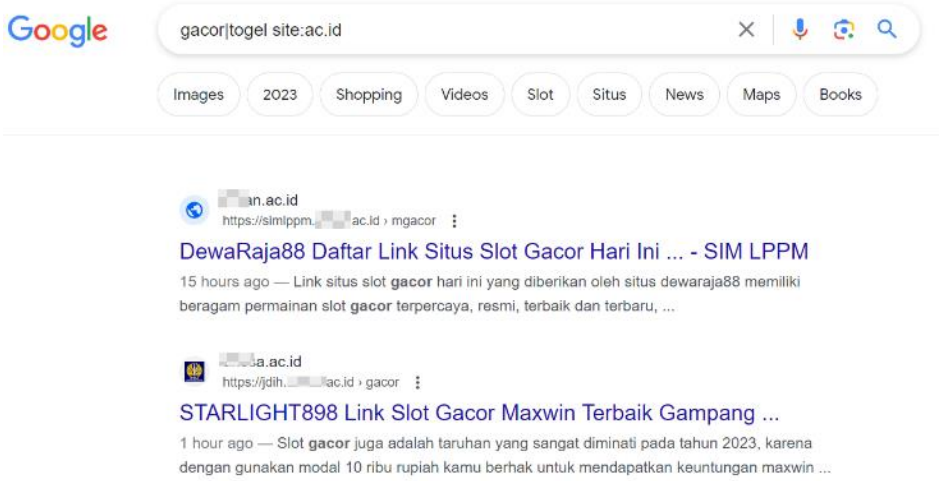
Upaya untuk menyembunyikan backlink atau melibatkan dalam teknik manipulatif dapat melanggar pedoman etika dan aturan mesin pencari, dan dapat berakibat pada penalti terhadap peringkat mesin pencari atau bahkan penghapusan dari indeks pencarian. Praktik yang lebih baik adalah fokus pada pembangunan backlink yang berkualits dan natural, dan tidak mencoba untuk melakukan manipulasi yang dapat merugikan integritas mesin pencari.

Dari sampel web yang terkena peretasan jenis invisible backlink ini, merupakan kasus yang paling lama diketahui dan ditangani. Pemilik web kadang tidak mengetahui jika di web ada link jenis ini, sehingga konten invisible backlink bisa saja tertanam dalam jangka waktu lama tanda di ketahui pengelola web.

4.3. Konten Retas (Defacement)

Paling banyak ditemukan dalam data lebih dari 50% kejadian keamanan web adalah jenis peretasan kontan. Data web yang terkena defacement diamati adalah seseorang menyisipkan konten perjudian ke dalam sebuah situs web tanpa izin dari pemiliknya, seperti terlihat apda Gambar 8 defacemen konten judi pada domain ac.id (site:ac.id).

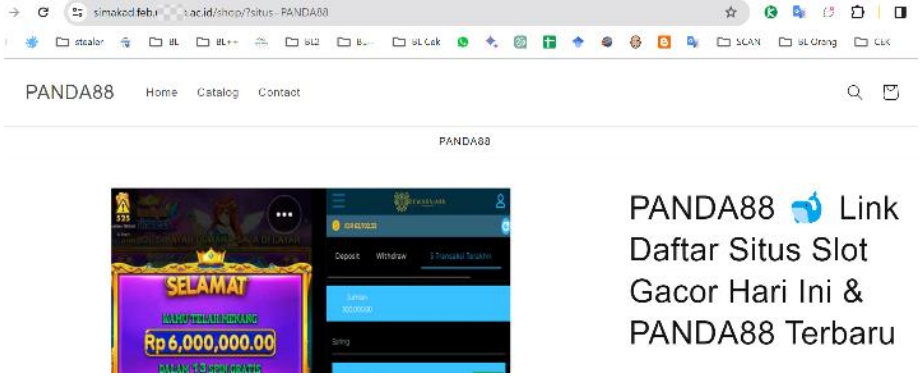
Konten ini dapat dianggap sebagai kasus *defacement* (*hacked defacement*) ini tindakan merusak atau merubah tampilan situs web dengan cara menyisipkan konten yang tidak diinginkan atau merusak. Dalam konteks ini, konten judi yang disisipkan tanpa izin dapat dianggap sebagai bentuk defacement.



Gambar 8. Proses pencarian konten diretas dengan Google

Kasus seperti ini melibatkan pelanggaran keamanan web di mana pihak yang tidak berwenang berhasil mengakses atau memanipulasi halaman web untuk menyisipkan konten yang tidak sah. Defacement dapat mencakup berbagai jenis konten yang merugikan atau melanggar hukum, dalam data ini banyak ditemukan konten perjudian yang mengarah ke web lain. Peretas menyiisipkan konten dan link aktif ke web lain.

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)



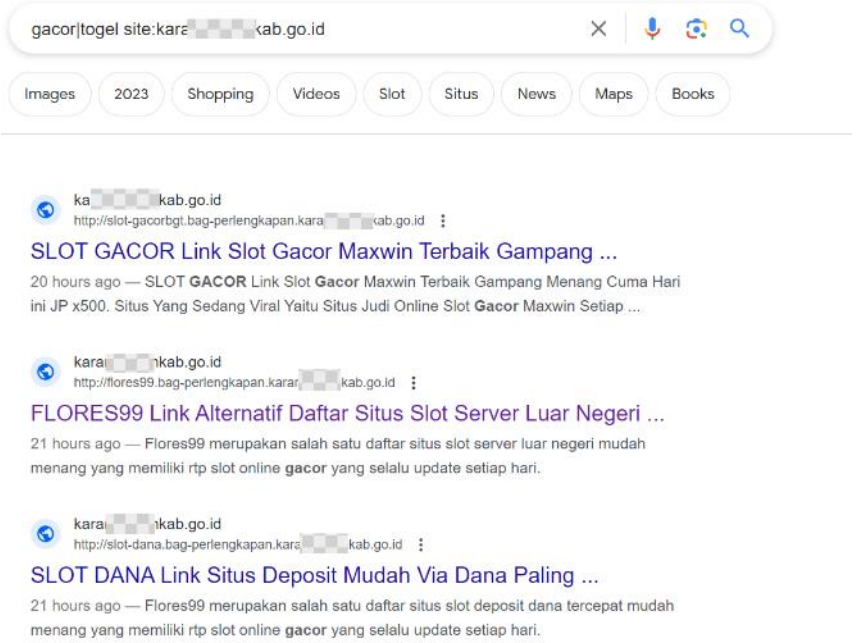
Gambar 9. Tampilan Konten retas defacement dengan URL dan konten yang tampil

Pada web yang sudah di deface mengatasi dan mengamankan situs web setelah defacement terdeteksi. Ini melibatkan membersihkan konten yang tidak sah, memperkuat keamanan situs, dan melakukan tindakan untuk mencegah kejadian serupa berikutnya.
Identifikasi konten jenis defacement paling mudah ditemukan dan diatasi dengan cara dihapus. Namun penghapusan konten hanya solusi sementara, perlu dicari dari mana sumber peretas bisa masuk ke web dan mengubah isi web.

4.4. Sub-domain takeover

Subdomain *takeover* terjadi ketika seseorang dapat mengambil alih kendali atau menguasai subdomain yang sebelumnya digunakan oleh pihak yang sah. Dari data yang ada, kasus ini jarang terjadi, namun ditemukan juga ada sekitar 1-3% dari kasus peretasan merupakan sub dmoan take over.

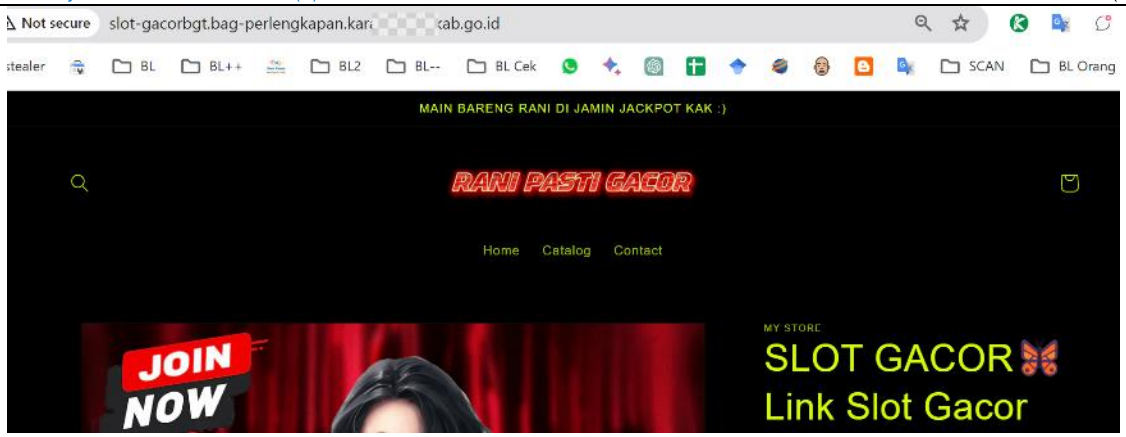
Dalam kasus ini, jika peretas berhasil membuat subdomain baru (misalnya, barusaja.namadomain.go.id) dan mengisi konten perjudian di dalamnya, ini dapat dianggap sebagai subdomain takeover.



Contoh 10. Gambar sub domain takeover yang teridex di Google

Subdomain takeover umumnya terjadi ketika subdomain yang pernah digunakan oleh pihak sah (seperti pendaftaran subdomain yang telah kedaluwarsa) dihapus dan didaftarkan kembali oleh orang lain.
Bisa juga terjadi karena peretas bisa masuk ke panel domain atau panel hosting dan bisa menambahkan record DNS baru. Peretas kemudian dapat meregistrasi atau mengendalikan subdomain tersebut dan mengisinya dengan konten yang mungkin tidak sah atau merugikan.

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)



Gambar 11. contoh sub domain takeover dan sudah diretas dengan konten negative

Peretas bisa mengubah/menambah data DNS (record DNS) sehingga submain ilegal bisa dibuat. Subdomain takeover ini bagi pemilik web secara jelas bisa terlihat dari panel domain/hosting/ DNS manajemen. Sementara bagi orang umum bisa melakukan analisis dari hasil pencarian atau menemukan data sub domain di halaman yang terindex di mesin pecari dan dengan tool online seperti sub domain finder.

5. Kesimpulan

Penelitian ini menggunakan sampel data hasil pencarian Google dalam 24 jam terakhir dilakukan dalam waktu maksimal 81 hari. Proses pengumpulan data menggunakan tool online apify.com untuk proses sracpping /crawling data. Diperoleh data sebanyak 7.604 konten (445 domain) diretas dalam 81 hari, pada domain go.id dan 3.576 ac.id (252 domain) yang diretas dalam 43 hari.

Ruang lingkup data yang diambil terbatas pada domain dengan TLD ac.id dan go.id dengan batasan pecarian maksimal 100 data konten terindex perhari yang masuk dalam hasil pencarian SERP (*Search Engine Result Page*). Dari sampel data ini tersebut diperkirakan terjadi peretasan web antara 5-6 institusi yang berbeda dalam setiap hari baik di institusi kampus ataupun pemerintah. Analisi data ini dikelompokan jadi 4 jenis. Untuk Domain go.id ada kasus Reflected XSS in search 3.418 (45%), Invisible backlink 621 (8%), konten retas 3.431 (45%) dan sub domain 134 (2%). Untuk Domain ac.id ada kasus : Reflected XSS in search 1.209 (34%), Invisible backlink 1.348 (38%), konten retas 931 (26%) sub domain 88 (2%).

Penelitian ini terbatas anilisis jenis keamaman web pada peretasan konten perjudian. Penelitian belum dilakukan sampai analisasis terhadap web yang mengalami masalah keamanan, mencari penyebab, respon penangganan dan sumber peretasan.

6. Kontribusi Penulis

Imam Suharjo : akuisisi data, validasi data, analisis data, naskah publikasi **Putry Wahyu Setyaningsih:** dokumentasi, akuisisi data, labeling data, draft publikasi.

7. Declaration of Competing Interest

Penulis dengan ini menyatakan bahwa tidak ada masalah dan konflik kepentingan dalam pengumpulan data, pelaksanaan, maupun publikasi laporan ini.

8. Referensi

Aji, B. B. (2023.). Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website. *csecurity*, 25–29.

apify.com. (2023, 11). *Google Search Videos Scraper - www.apify.com*. Retrieved from apify.com: https://www.apify.com

Arghire, I. (2020). *SEO Spam Dominated Website Infections in 2019: Report*. Retrieved from securityweek.com: https://www.securityweek.com/seo-spam-dominated-website-infections-2019-report/

Farizi, M. (2020). Pengelompokan Spam Botnet Dengan Metode Fuzzy Hashing. *Jurnal TELEMATIKA MKOM Vol.12 No.1 Maret 2020*.

kominfo.go.id. (2022). *50% Situs Pemerintah Diserang Hacker!* Retrieved from www.kominfo.go.id: https://www.kominfo.go.id/content/detail/1493/50-persen-situs-pemerintah-diserang-hacker/0/berita

ISSN 2502-3357 (*Online*)
Imam Suharjo, dkk./TEKNOLOGI 14 (1) 2024 61-70 ISSN 2503-0477 (*Print*)

Mi, X. (2019). Resident Evil: Understanding Residential IP Proxy as a Dark Service. *IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. , doi: 10.1109/SP.2019.00011*, 1185-1201. Retrieved from https://doi.org/10.1109/SP.2019.00011

Murphy, D. T. (2021). Plugins to Detect Vulnerable Plugins: An Empirical Assessment of the Security Scanner Plugins for WordPress. *IEEE/ACIS 19th International Conference on Software Engineering Research*, https://ieeexplore.ieee.org/document/9509274/.

Nguyen, V.-L. (2019). Web attacks: defeating monetisation attempts. *Network Security Vol. 2019, No. 5*.

Petkova. (2019). Security's Leaks In Seo Spamming. Knowledge. *International Journal, 35(3) Retrieved from http://ikm.mk/ojs/index.php/kij/article/view/1721* , 987–991. Retrieved from http://ikm.mk/ojs/index.php/kij/article/view/1721

Putri, N. I. (2021). Strategi Dan Peningkatan Keamanan Pada Komputasi Awan, . *J-SIKA Vol. 3 No. 01 (2021)*.

Rahman, R. U. (2020). Classification of Spamming Attacks to Blogging Websites and Their Security Techniques. In *Encyclopedia of Criminal Activities and the Deep Web, Financial Fraud, Identity Theft, and Social Manipulation Through Social Media* (pp. https://www.irma-international.org/viewtitle/248089/?isxn=9781522597155).

www.statista.com. (2023, 10 26). *Daily spam volume worldwide 2020-2021*. Retrieved from www.statista.com.

Yunjia Wang, d. (2021). Data Analytics and Assessment (CyberSA), An Empirical Study: Automated Subdomain Takeover Threat Detection . *International Conference on Cyber Situational Awareness*.