E-ISSN : 2986-5360

Identifikasi Kerentanan Terhadap Serangan Slot Backdoor Pada Website di Indonesia Dengan Menggunakan Metode OSINT

Miftahul Fadli Mutaqin[1], Doddy Ferdiansyah[2]

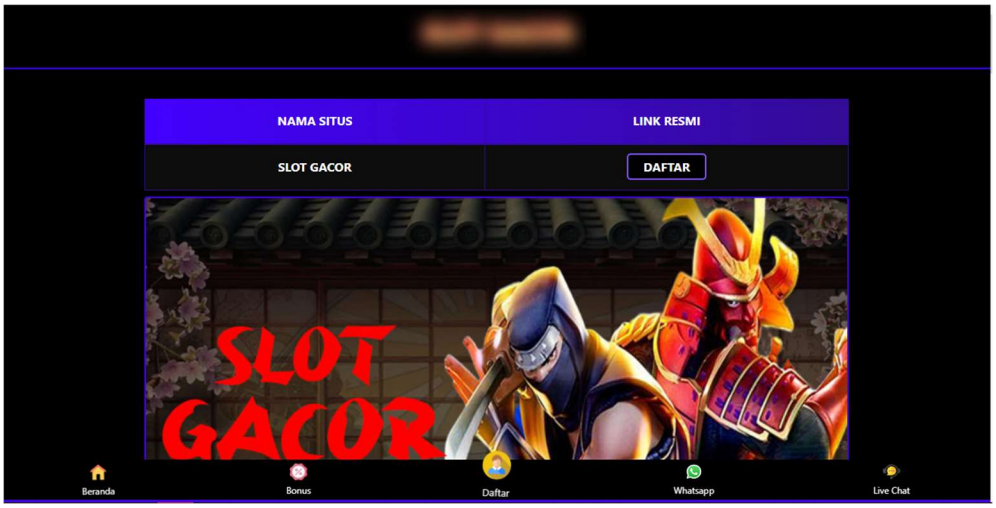
[1,2] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Pasundan
Jln. Dr. Setiabudhi no. 193 Bandung, Jawa Barat
[1]miftah.4ma@mail.unpas.ac.id, [2]doddy@unpas.ac.id

Abstrak- Kejadian yang berhubungan dengan peretasan dan kebocoran data di dunia siber semakin meningkat. Kejadian ini tercatat bahwa dalam kuartal II tahun 2022, kasus-kasus kebocaran data di Indonesia melonjak sampai 143%. Beberapa kasus yang terjadi tidak hanya dari sektor perdagangan digital (*e-commerce*), tetapi terjadi juga pada sektor pendidikan, industri, sampai dengan pemerintahan. Hal ini tidak lepas dari sistem yang kurang aman, baik dalam pengembangannya atau pemeliharannya. Salah satu kasus yang diangkat dalam penelitian ini adalah maraknya website-website di Indonesia yang diretas oleh hacker dengan mengubah halaman website tersebut menjadi halaman website ilegal (judi atau slot). Sehingga tujuan dari penelitian ini adalah untuk mengidentifikasi kerentanan (*vulnerability*) yang terjadi pada website yang terkena peretasan dengan menggunakan metode *Open Source Intelligent* (OSINT).

Index Terms- Peretasan, Keamanan Siber, Kebocoran Data, *Information Gathering*, Peretasan web, *vulnerability*.

I. PENDAHULUAN

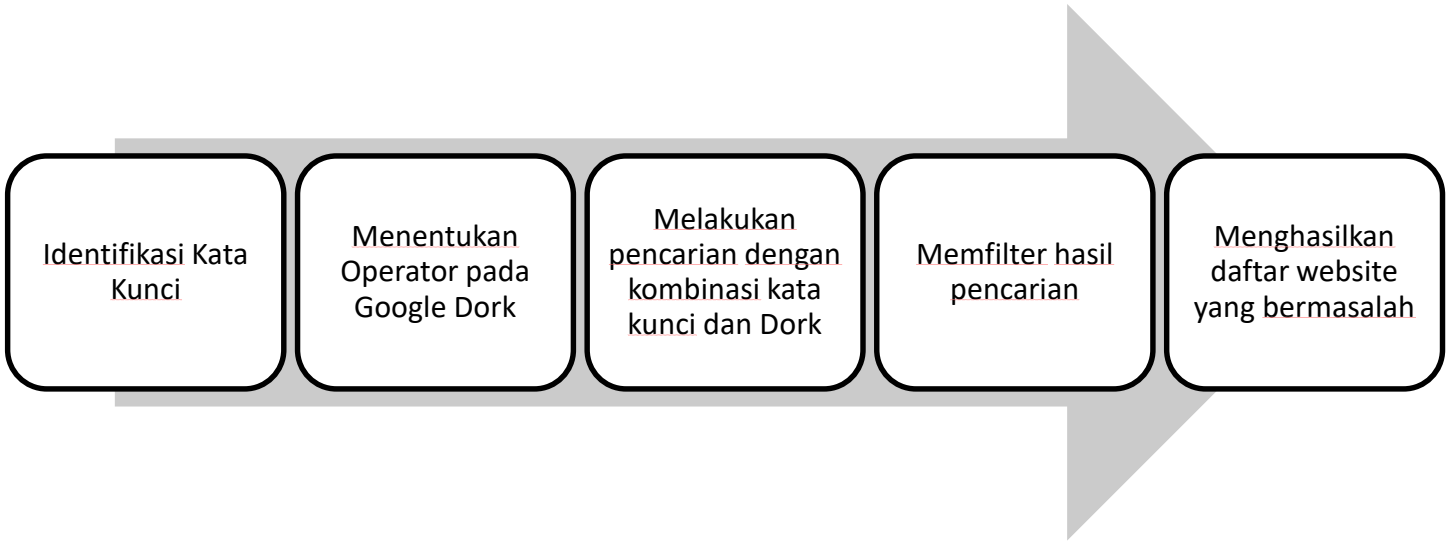
Saat ini, keamanan siber sedang menjadi perhatian utama diseluruh dunia. Maraknya serangan-serangan siber dan konten-konten illegal atau sensitive yang tersedia di internet menambah perhatian khusus bagi seluruh perusahaan terutama di Indonesia. Keamanan siber sendiri tidak hanya berdiri sendiri. Keamanan siber mencakup berbagai macam praktik, alat, dan konsep yang terkait erat dengan keamanan teknologi informasi dan operasional. Keamanan siber memiliki ciri khas dalam hal penggunaan teknologi informasi secara ofensif untuk menyerang musuh [1]. Oleh karena itu untuk melindungi data pribadi dan sistem informasi seperti jaringan, komputer, aplikasi, database, dll harus dilakukan dengan prosedur yang baik dan teratur. Sebagian besar perusahaan hanya mengandalkan firewall dan antivirus untuk melindungi sistem diperusahannya, padahal masih banyak teknik dan konsep yang perlu diterapkan untuk meningkatkan postur keamanan siber yang baik [2]. Beberapa penyebab terjadinya serangan di dunia siber dapat terjadi dari malicious software atau *malware*, *hacker* atau *cracker*, *cyber* teroris, dan *spionage*. Akibatnya, dari sumber serangan tadi dapat mengakibatkan beberapa serangan seperti menginject *script* sql atau disebut dengan sql *injection*, meretas *password* yang lemah atau disebut dengan *password guessing*, memanfaatkan celah keamanan atau bug pada sistem operasi atau aplikasi yang belum di *patch/update*, sampai dengan menelusuri file atau direktori yang tidak diamankan dengan menggunakan *google dork* [3]. Aplikasi Web sensitif terhadap ancaman keamanan informasi karena informasi yang memadai yang diperolehnya dari pengguna [10]. Selama sebuah sistem terhubung ke jaringan dan internet, semua ancaman diatas sangat mungkin terjadi. Salah satu kasus yang sangat trending saat ini di Indonesia adalah maraknya serangan terhadap website dengan menginject halaman web melalui *backdoor* dari website judi *online* atau slot. Contoh halaman web yang sudah terkena serangan backdoor ini seperti digambarkan pada gambar 1. Oleh karena itu, penelitian menghasilkan identifikasi website-website yang terkena serangan *backdoor* dan melakukan penilaian terhadap kelemahan (*vulnerability*) pada lingkungan website tersebut. Dalam kasus ini, mengambil tempat kasusnya di salah satu perguruan tinggi swasta XYZ di Indonesia.



Gambar 1. Tampilan halaman web judi *online* / slot

II. METODE PENELITIAN

Dari kasus-kasus yang sudah dijelaskan pada bagian pendahuluan, serangan *backdoor* ini merupakan serangan yang berbahaya dan saat ini terjadi sangat massif di seluruh website di Indonesia. Bagi pemilik *top level domain* (TLD) ac.id, perlu perhatian lebih pada web mereka. TLD atau top level domain dipegang dan dikendalikan oleh *Internet Corporation for Assigned Names and Numbers* (ICANN) dan dikatakan bahwa sampai dengan 12 Februari 2019 ada 1.584 TLD diseluruh dunia [4]. Karena serangan ini bersifat massif, banyak website-website perguruan tinggi baik negeri maupun swasta terkena jenis serangan backdoor ini. Beberapa halaman web mereka berubah tampilan menjadi halaman web judi online/slot. Untuk mengidentifikasi website-website apa saja di Indonesia yang sudah terkena serangan ini, dalam penelitian ini akan menggunakan metode *Open Source Intelligent* (OSINT) untuk melakukan pengumpulan data (information gathering). Langkah-langkah dalam menerapkan Metode penelitian berdasarkan *Open Source Intelligent* (OSINT) ini dijelaskan pada gambar 2.

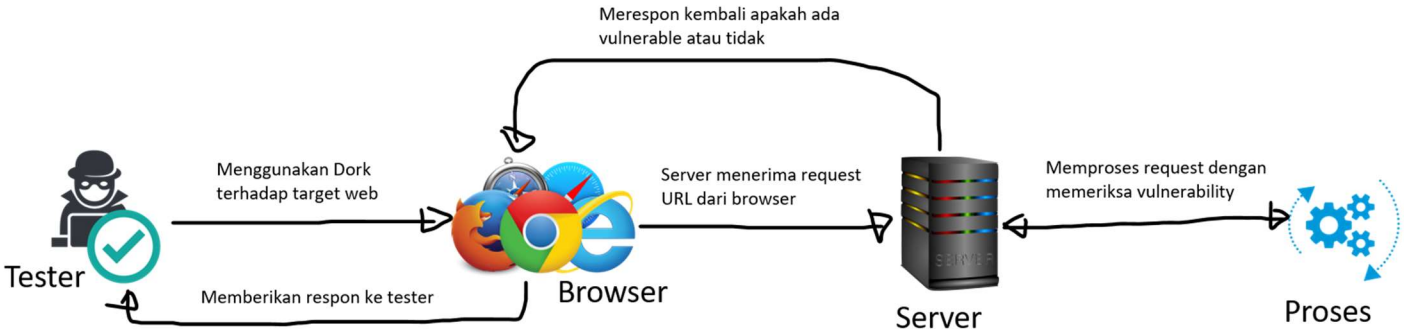


Gambar 2. Metode Penelitian dengan Menggunakan OSINT

I. HASIL DAN PEMBAHASAN

Open source intelligence memberikan pengetahuan khusus kepada pengguna agar mereka dapat menggunakannya dalam tindakan dan proses pengambilan keputusan. Karena domain publik merupakan platform yang cocok untuk menyebarkan informasi, berbagai aktor dalam domain ini berusaha untuk memberikan dampak pada informasi, sehingga sulit untuk mengevaluasi, membandingkan, dan menganalisis. Yang juga menarik untuk dicatat di sini adalah bahwa sampai saat ini, tidak ada catatan konkrit mengenai penggunaan pertama kali dari open source intelligence [5]. Untuk teknik pengumpulan informasi yang digunakan dalam OSINT menggunakan

Google Dork, Dimana menurut Joao Rafael G.E, dkk., mengatakan bahwa Dork merupakan string yang digunakan untuk melakukan *Google Hacking* dalam fase passive *recognition* dalam *Open Source Intelligence*. Namun, *Google Hacking Database* berisi jumlah atribut yang lebih sedikit, semuanya dengan nilai tekstual, yang membuatnya tidak mungkin untuk menerapkan teknik *machine learning*. Salah satu cara untuk memperkaya *Google Hacking Database* dengan atribut adalah dengan pemrosesan bahasa Natural dan transformasi nilai tekstual menjadi numerik, mengubah karakter Dorks menjadi ASCII. Jadi, tujuannya adalah untuk menerapkan pemrosesan bahasa alami untuk memperkaya *Google Hacking Database* dengan atribut dan mengubah nilai tekstualnya menjadi ASCII, untuk memungkinkan penerapan teknik Machine Learning [6]. Selain itu, *Google Dork* juga dapat digunakan untuk mencari informasi aplikasi apa saja yang tingkat pertahanannya rendah [7]. Proses dari *Google Dork* dapat dilihat pada gambar 3.



Gambar 3. Proses menemukan *vulnerability* pada website dengan *Google Dork*

Dimana dalam proses pencarian vulnerability dengan menggunakan *google dork* ini, penguji hanya memanfaatkan operator dasar dan operator lanjutan yang akan diinput melalui kolom pencarian di google pada sebuah browser. Kemudian operator dasar dan operator lanjutan tersebut dikirim ke server dan akan di proses. Informasi yang dihasilkan apakah ada vulnerability atau tidak akan di kirim ke *browser* dan *browser* akan menampilkan hasil pencarian berdasarkan operator dasar dan operator lanjutan yang digunakan.
Untuk operator dasar dan operator lanjutan yang digunakan dalam *Google Dork* sangat banyak dan beragam [8]. Beberapa contoh operator dasar yang umum digunakan dalam *google dork* dapat dilihat pada tabel 1.

Tabel 1. Operator Google – Operator Dasar

Operator Dasar	Deskripsi
+	Operator ini akan memastikan kata yang di cari
-	Operator ini akan mengabaikan kata yang di cari
~	Operator ini akan memasukkan unsur sinonim (google secara default menggunakan ~)
*	Operator ini disebut wildcard, dimana dia akan menyesuaikan semua kata atau kalimat
“	Operator ini akan mencari kata atau kalimat yang sama persis
|	Sama dengan operator OR
OR	Operator ini akan mengembalikan hasil yang berhubungan dengan X atau Y
AND	Operator ini akan mengembalikan hasil yang berhubungan dengan X dan Y (google secara default menggunakan AND)

Sedangkan untuk contoh operator lanjutan yang dapat digunakan dalam pencarian dengan *google dork* dapat dilihat pada tabel 2.

Tabel 2. Operator Google – Operator Lanjutan

Operator Lanjutan	Deskripsi
intext	Menghasilkan halaman yang berisi kata (atau kata-kata) tertentu di suatu tempat di konten.
intitle	Menghasilkan halaman dengan kata (atau beberapa kata) tertentu di judulnya
inurl	Menghasilkan halaman dengan kata (atau beberapa kata) tertentu di URL.
allintext	Mirip dengan "intext", tetapi hanya hasil yang berisi semua kata yang ditentukan di suatu tempat di halaman yang akan dikembalikan.
allintitle	Mirip dengan "intitle", tetapi hanya hasil yang berisi semua kata yang ditentukan dalam tag judul yang akan ditampilkan.
allinurl	Mirip dengan "inurl", tetapi hanya hasil yang berisi semua kata yang ditentukan di URL yang akan ditampilkan.
cache	Mengembalikan cache dari halaman web
Define	Menampilkan arti kata dalam hasil seperti di SERP.
Link	Menghasilkan halaman yang tertaut ke domain atau URL tertentu.
site	Hanya menghasilkan website yang spesifik
Filetype	Menghasilkan jenie file tertentu seperti PDF, DOC, TXT, PPT, dll

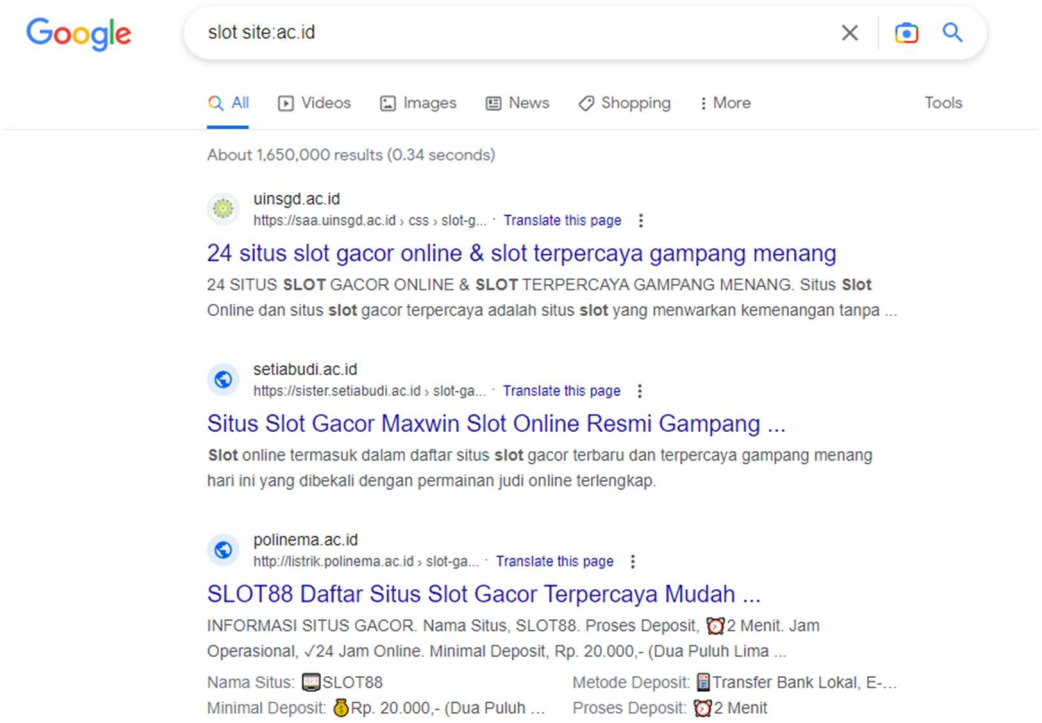
Operator-operator diatas memiliki persyaratan saat penggunaannya. Ada yang bisa digabungkan dengan operator lain, ada juga yang tidak bisa digabungkan. Dalam penelitian ini, kasus yang menjadi objek adalah situs-situs web yang terkena serangan backdoor situs judi *online*/slot. Situs-situs yang akan dicari memiliki limitasi sebagai berikut :

1. Hanya situs-situs di Indonesia
2. Hanya situs pemerintahan, Lembaga perguruan tinggi, dan Lembaga Pendidikan dasar dan menengah

Maka skenario pencarian dengan menggunakan google dork adalah sebagai berikut.
Dork :

1. slot site:ac.id
2. slot site:go.id
3. slot site:sch.id

Dari metode OSINT, langkah-langkah *google dork*, dan limitasi pencarian yang sudah ditentukan pada bagian sebelumnya, sekarang akan dilakukan proses pencarian berdasarkan limitasi tersebut dengan menggunakan web browser dan search enginee dari google. Dork pertama yang digunakan adalah "slot site:ac.id". hasil pencarian dari dork tersebut adalah 1.650.000 dimana hasil yang didapatkan dapat dilihat pada gambar 4 dan untuk contoh halaman situs yang sudah terkena backdoor judi online/slot dapat dilihat pada gambar 5.

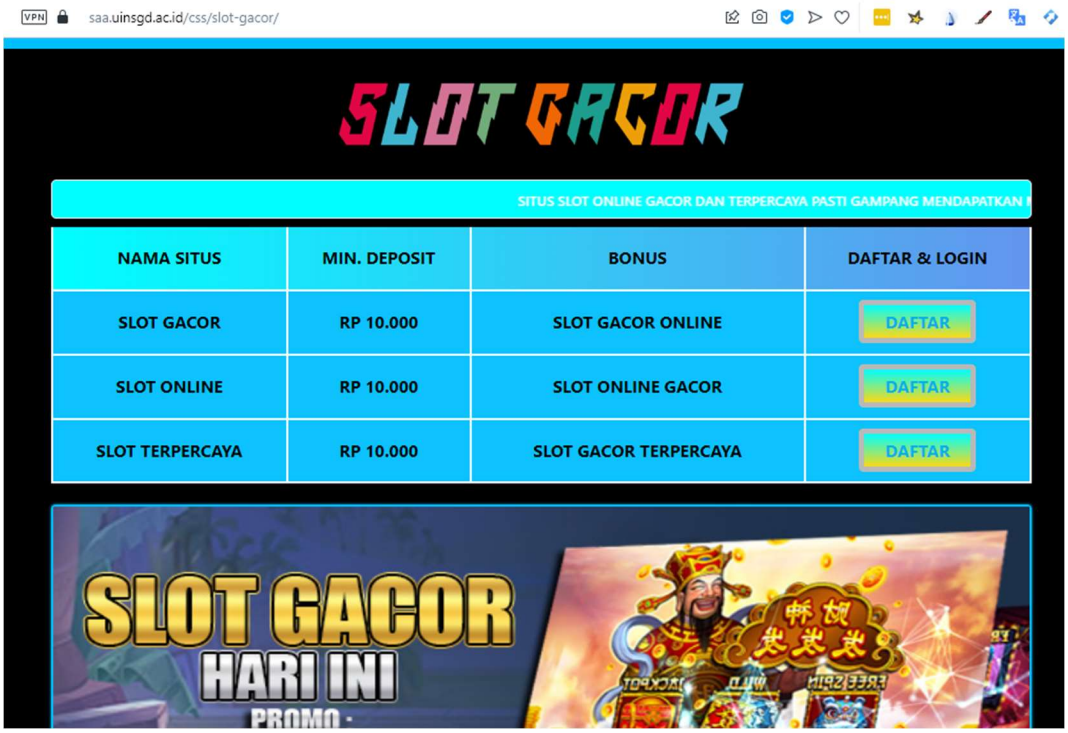


Gambar 4. Hasil pencarian dengan dork “slot site:ac.id”

Gambar 4 diatas menampilkan hasil pencarian dari search engine google dengan menggunakan teknik google dork “slot site:ac.id” sebesar 1.650.000 situs. Perintah google dork “slot site:ac.id” memiliki arti sebagai berikut :

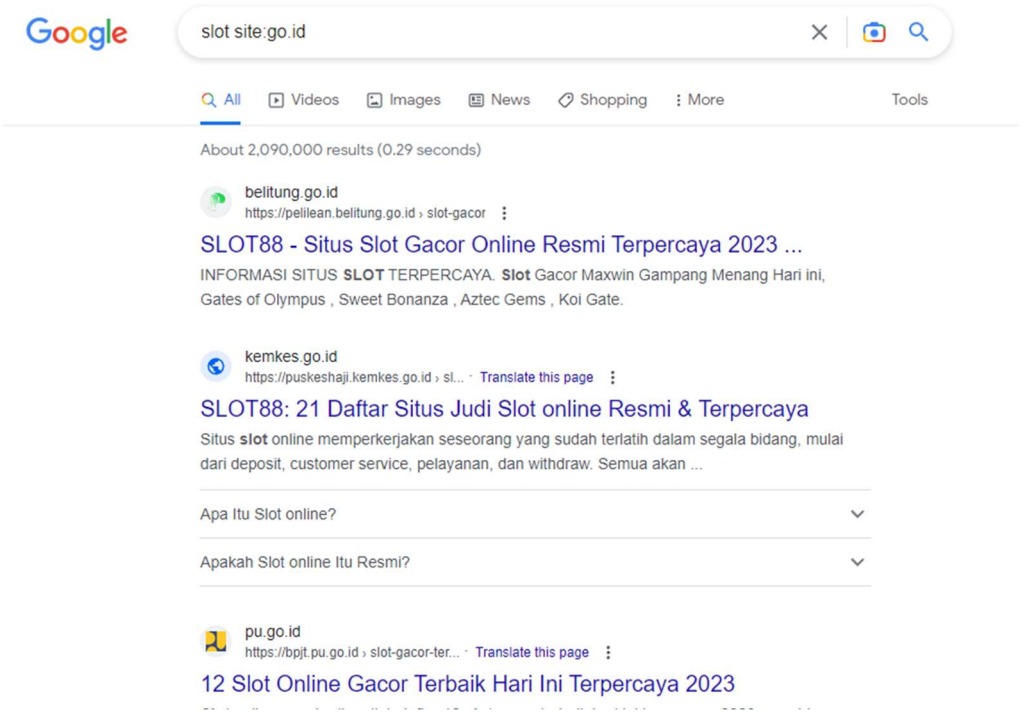
- Slot : merupakan kata kunci (keyword) yang akan di cari oleh search engine pada seluruh website yang terindex.
- Site:ac.id : merupakan filtering terhadap situs-situs yang hanya memiliki TLD ac.id saja. Selain itu diabaikan.

Sehingga ketika dork diatas dieksekusi, maka search engine akan mencari seluruh situs yang memiliki TLD ac.id dan didalam situs tersebut mengandung kata slot. Maka hasil yang ditampilkan oleh search engine seperti gambar 4.



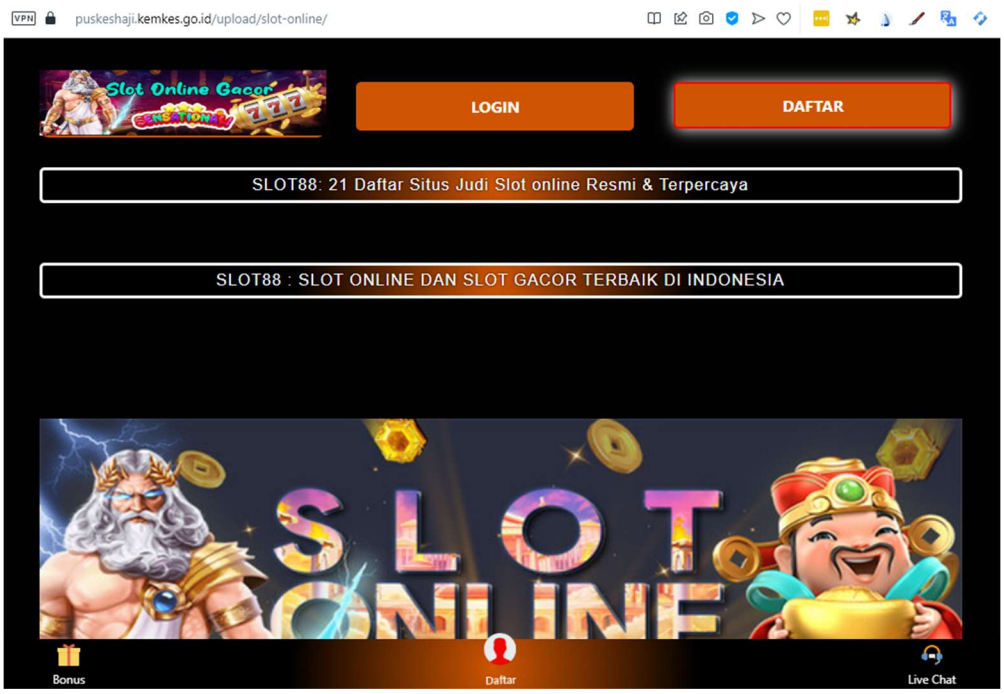
Gambar 5. Tampilan situs yang terkena backdoor judi online/slot di domain ac.id

Dork kedua yang digunakan adalah “slot site:go.id”. hasil pencarian dari dork tersebut adalah 2.090.000 lebih banyak dari dork pertama. Dimana hasil yang didapatkan dapat dilihat pada gambar 6 dan untuk contoh halaman situs yang sudah terkena *backdoor* judi online/slot dapat dilihat pada gambar 7.



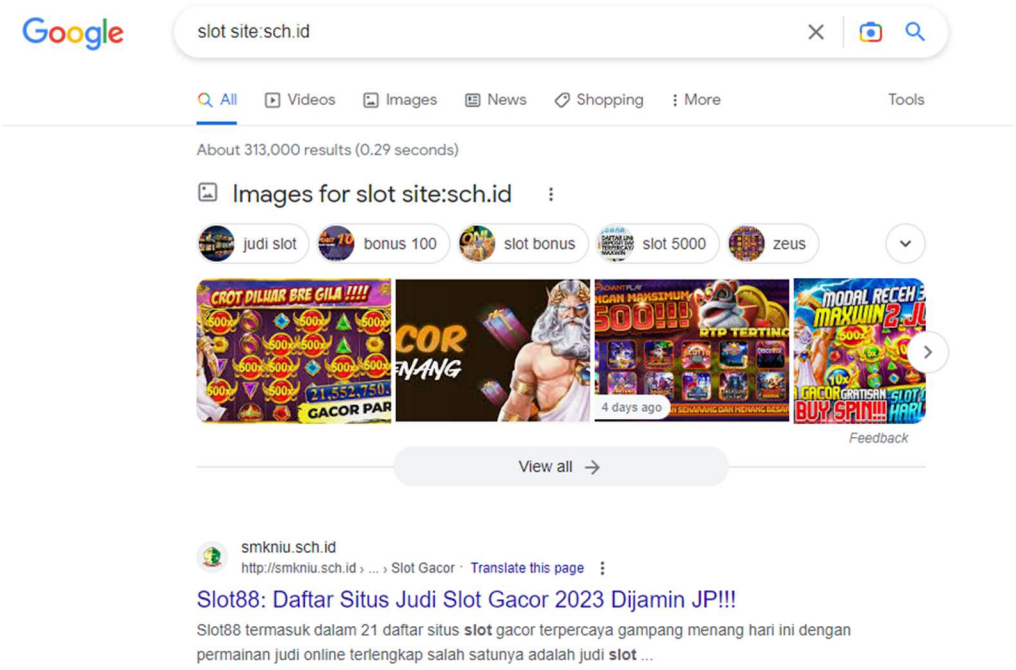
Gambar 6. Hasil pencarian dengan dork “slot site:go.id”

Cara ini sama seperti yang dilakukan pada tahap sebelumnya di gambar 4, tetapi objek penelusuran TLD yang berbeda karena disini menggunakan go.id dimana TLD go.id digunakan untuk situs-situs pemerintah Indonesia. Hasil dari perintah google dork “slot site:go.id” lebih banyak dibandingkan dengan ac.id. hasilnya dapat dilihat pada gambar 6.



Gambar 7. Tampilan situs yang terkena *backdoor* judi online/slot di domain go.id

Dork ketiga yang digunakan adalah “slot site:sch.id”. hasil pencarian dari dork tersebut adalah 313.000 lebih sedikit dari dork pertama dan dork kedua. Dimana hasil yang didapatkan dapat dilihat pada gambar 8 dan untuk contoh halaman situs yang sudah terkena backdoor judi online/slot dapat dilihat pada gambar 9.



Gambar 8. Hasil pencarian dengan dork “slot site:sch.id”

Gambar 8 menunjukkan hasil pencarian dengan menggunakan dork ketiga yaitu “slot site:sch.id”. Ternyata untuk TLD sch.id, sangat sedikit terjadi serangan slot yaitu hanya sebesar 313.000 situs.

Gambar 9. Tampilan situs yang terkena *backdoor* judi online/slot di domain sch.id

Dari hasil pencarian dengan menggunakan kata kunci “slot” dan dork yang digunakan adalah “site” terhadap domain ac.id, go.id, dan sch.id, maka hasil tersebut dapat dirangkum pada tabel 3.

Tabel 3. Hasil pencarian dengan 3 dork

Dork	Hasil
Slot site:ac.id	1.650.000 halaman situs
Slot site:go.id	2.090.000 halaman situs
Slot site:sch.id	313.000 halaman situs

II. KESIMPULAN

Menggunakan Google dork untuk mengambil informasi rahasia dan pribadi. Tingkat lanjut string pencarian yang disebut kueri Google dork yang digunakan untuk menemukan informasi sensitive [9]. Terbukti dari hasil pencarian yang sudah dilakukan menghasilkan informasi yang sangat luar biasa, bahkan dapat menemukan jenis ancaman yang menyerang sebuat website.
Dari hasil yang sudah dijelaskan pada bagian sebelumnya, 3 domain yaitu ac.id, go.id, dan sch.id sebagian besar terkena serangan backdoor judi online/slot secara masif. Hal ini dapat dilihat dari hasil untuk domain Lembaga pemerintah yang menjadi peringkat pertama yaitu sebanyak 2.090.000 halaman situs yang terkena serangan. Menyusul yang kedua dari Lembaga perguruan tinggi sebesar 1.650.000 halaman situs, dan yang terakhir yaitu Lembaga Pendidikan dasar dan menengah sebesar 313.000 halaman situs. Tentunya dari hasil ini sangat memprihatinkan karena sebegitu besar halaman-halaman situs yang terkena serangan backdoor dan sampai detik ini serangan masih berkelanjutan dan belum berakhir. Perlu kesigapan dan respon yang cepat dari pengurus IT di masing-masing organisasi atau Lembaga, terutama Lembaga perguruan tinggi, Lembaga pemerintah dan Lembaga Pendidikan dasar dan menengah untuk dengan cepat melakukan investigasi dan mitigas jika website mereka terkena serangan ini. Setelah itu sesegera mungkin melakukan pemulihan terhadap halaman situs yang sudah terkena serangan backdoor ini.

Untuk penelitian berikutnya dari hasil ini dapat dilakukan dari beberapa hal, misalkan :

1. Berapa jumlah seluruh domain di Indonesia yang terkena serangan ini?
2. Melalui celah mana si “attacker” menyerang website tersebut?
3. Bagaimana threat modeling yang bisa dibuat terhadap kasus ini?
4. Bagaimana cara mitigasi dan recovery terhadap serangan backdoor ini?

Sehingga jika semua penelitian diatas dilakukan, maka output dari penelitian ini dapat lebih bermanfaat dan memberikan rekomendasi pencegahan serta menginkatkan awareness keamanan bagi seluruh organisasi dan Lembaga baik di pemerintah atau swasta.

REFERENCES

[1] G. Darko, “Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model”, in *International Journal of Applied Sciences & Development*, vol. 1, 2022.

[2] K. B. Yash, M. Udit, “Technical Security Known as Cyber Security: A Review”, in *Journal of Computer Technology & Applications,* vol. 13, issue 3, 2022.

[3] W. M. Annas, A. Adnan, F. Shoaib, A. Irfan, A. N. Naeem, I. Kashif, “Cyber threats : taxonomy, impact, policies, and way forward”, in KSII Transactions on Internet and Information Systems, vol. 16, No. 7, 2022

[4] O.M. Enrique, “Dot-Science Top Level Domain: academic websites or dumpsites?”, in Scientometrics, 2021.

[5] I. Tomislav, D. Tomislav, “Open Source Intelligence (OSINT): Issues and Trends”, in *INFuture2019:Knowledge in the Digital Age.*, 2020.

[6] R.G.E. Joao, J. S. MRenato, R. Marcio, “oogle Hacking Database Attributes Enrichment and Conversion to Enable the Application of Machine Learning Techniques,” *Research Square.*, 2022.

[7] S. Biswas, M. M. H. K. Sajal, T. Afrin, T. Bhuiyan, M. M. Hassan,” A Study on Remote Code Execution Vulnerability in Web Applications”, in International Conference on Cyber Security and Computer Science, 2018

[8] J. P. Mayurkumar, “Google Dorks : Advance Searching Technique”, in ResearchGate, 2019.

[9] B.J. Santhosh Kumar, B.R. Pushpa,” A Method for Information Grabbing, Bypassing Security and Detecting Web Application Vulnerabilities”, in International Journal of Engineering & Technology, 2018

[10] Md Haris Uddin Sharif,” Web Attacks Analysis and Mitigation Techniques”, in International Journal of Engineering Research & Technology, 2022