ISSN 2337-6805

ANALISIS KEAMANAN APLIKASI ANDROID XYZ MENGGUNAKAN METODE OWASP API TOP 10 2023

SECURITY ANALYSIS OF THE XYZ ANDROID APPLICATION USING THE OWASP API TOP 10 METHODOLOGY (2023)

Roni Reza Abdullah[1], Andi Suprianto[2], Riadi Marta Dinata[3]
[1, 2, 3] Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
ronireza105@gmail.com[1], andi.suprianto@ymail.com[2], riadimrt@gmail.com[3]

ABSTRAKSI
Application Programming Interface (API) adalah elemen penting dalam pengembangan aplikasi. API target utama penyerangan karena mengekspos data sensitif. Penetration Testing suatu langkah pencegahan penting untuk mengidentifikasi kelemahan serta kebocoran data yang mungkin disebabkan oleh API. Open Web Application Security Project (OWASP) API Top 10 2023 merupakan standar pengujian keamanan API. Hasil pengujian kerentanan banyak terjadi pada Broken Object LevelAuthorization (BOLA) dampaknya yaitu berupa perubahan, pengungkapan dan penghapusan data, cara perbaikannya yaitu merubah ID objek menjadi Universally Unique Identifier (UUID).
Kata Kunci : Application Programming Interface (API), Broken Object Level Authorization (BOLA), Open Web Application Security Project (OWASP), Identifier (ID), Universally Unique Identifier (UUID).

ABSTRACT
Application Programming Interface (API) is an important element in application development. APIs are prime targets for attacks because they expose sensitive data. Penetration Testing is an important preventive measure to identify weaknesses and data leaks that may be caused by APIs. Open Web Application Security Project (OWASP) API Top 10 2023 is an API security testing standard. The results of testing many vulnerabilities occur in Broken Object Level Authorization (BOLA), the impact is in the form of changes, disclosure and deletion of data, the way to fix it is to change the object ID to a Universally Unique Identifier (UUID).
Keywords : *Application Programming Interface (API), Broken Object Level Authorization (BOLA), Open Web Application Security Project (OWASP), Identifier (ID), Universally Unique Identifier (UUID).*

1. PENDAHULUAN

Android merupakan sistem operasi yang dikembangkan untuk perangkat mobile yang berbasis linux seperti telepon pintar dan komputer tablet. Seiring perkembangan teknologi informasi yang semakin maju, Android menjadi OS yang paling banyak digunakan di antara sekian banyak pilihan sistem operasi untuk perangkat mobile. Sifatnya yang open source memudahkan pengembang untuk membuat aplikasi Android sehingga dengan mudah para pengembang untuk menciptakan dan memodifikasi aplikasi atau fitur – fitur yang belum ada pada sistem operasi Android sesuai dengan keinginan mereka sendiri.

Application programming interface (API) merupakan teknologi yang dipakai untuk memfasilitasi pertukaran data antara dua aplikasi perangkat lunak atau lebih. Dengan adanya API ini, maka memudahkan programmer untuk "membongkar" suatu software, kemudian dapat dikembangkan atau diintegrasikan dengan perangkat lunak yang lain. API dapat dikatakan sebagai penghubung suatu aplikasi dengan aplikasi lainnya yang memungkinkan programmer menggunakan sistem function. Dalam dunia bisnis, peran API sangat diperlukan untuk memberikan sarana sebagai penerapan dalam berbisnis.

Open Web Application Security Project (OWASP) merupakan organisasi nirlaba di Amerika Serikat yang resmi secara daring pada bulan Desember 2001. OWASP adalah komunitas terbuka yang didedikasikan untuk memungkinkan organisasi memahami, mengembangkan, memperoleh, mengoperasikan, dan memelihara aplikasi yang dapat dipercaya dari aspek keamanan. OWASP API TOP 10 2023 merupakan 10 kategori kerentanan pada API yang diterbitkan pada tahun 2023. API merupakan elemen dasar dari inovasi di dunia yang digerakkan oleh aplikasi saat ini adalah API. Mulai dari bank, ritel, dan transportasi hingga IoT, kendaraan

ISSN 2337-6805

otonom, dan kota pintar, API merupakan bagian penting dari aplikasi seluler, SaaS, dan modern serta dapat ditemukan di aplikasi yang berhadapan langsung dengan pelanggan, yang berhadapan langsung dengan mitra, dan aplikasi internal. Pada dasarnya, API mengekspos logika aplikasi dan data sensitif seperti Personally Identifiable Informatian (PII) dan karena itu semakin menjadi target penyerang. Tanpa API yang aman, inovasi yang cepat tidak mungkin dilakukan.

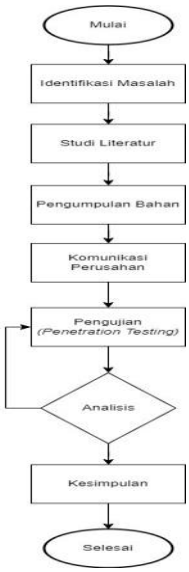
Keamanan API berfokus pada strategi dan solusi untuk memahami dan mengurangi kerentanan unik dan risiko keamanan API. Oleh karna itu, dengan adanya api sebagai penghubung didalam applikasi android maka harus dilakukan pengujian keamanan demi mendapatkan aplikasi yang aman dari pencurin data ataupun kerusakan pada aplikasi.

Permasalahan yang di jadikan Objek penelitian ini adalah sebagai berikut : Mengapa pengujian kerentanan API menggunakan metode OWASP API TOP 10 2023 ?; Bagaimana cara mengetahui kerentanan terbanyak pada aplikasi android yang masuk kedalam kategori OWASP API TOP 10 2023?; Bagaimana cara mengetahui penyebab kerentanan pada kategori OWASP API TOP 10 yang banyak terjadi?.

2. METODOLOGI PENELITIAN

Alur Penelitian

Untuk Memulai Penelitian yang akan dilakukan, maka ada beberapa tahap yang harus di lakukan, dapat di lihat pada gambar di bawah ini:



Gambar Alur penelitian

Pada Gambar Alur penelitian menunjukan alur penelitian yang akan di lakukan, berikut adalah deskripsi dari gambar berikut:

Identifikasi Masalah

Berdasarkan pengalaman API sangat rentan atas kebocoran data di karenakan mengekspos logika aplikasi dan data sensitif, maka membuat peneliti tertarik untuk menjadikan API sebagai objek penelitian ini.

Studi Literatur

Studi Literatur adalah cara untuk mengumpulkan data atau sumber yang berhubungan dengan objek penelitian API, Penetration Testing, Vulnerabilty, OWASP API TOP 10 2023, yang didapat dari berbagai sumber media, jurnal, buku, catatan dan laporan.

Pengumpulan Kebutuhan

Pengumpulan bahan dilakukan karena agar proses pengujian dapat berjalan dengan lancar, bahan yang harus dikumpulkan yaitu.

- Aplikasi android sebagai objek penelitian
- Burpsuite sebagai alat penangkap request pada saat aplikasi berjalan
- Memuplay sebagai emulator untuk menjalakan aplikasi android
- Adb, Cmd dan bash sebagai alat untuk import dan push certificate burpsuite ke dalam system emulator.
- Sqlmap sebagai alat bantu untuk mengeksekusi kerentanan sql injection.

Komunikasi Perusahan

Dalam proses ini adalah mencari perusahan yang mengizinkan untuk dilakukan penetration testing pada aplikasi yang berjalan menggunakan API serta menentukan waktu untuk memulai pengujian dan objek penelitian.

Pengujian

Penetration Testing (Pentest) merupakan proses menemukan celah keamanan dalam sebuah sebuah sistem yang sudah di tentukan.

Analisis

Analisi Merupakan kegiatan untuk memeriksa data dari hasil pengujian untuk menentukan sesuai golongan yang sudah di tentukan jika tidak sesuai dengan ketentuan,maka objek peneliatan harus diulang kembali dan jika sudah sesuai dengan metode yang sudah digunakan proses analisis sudah selesai.

ISSN 2337-6805

Kesimpulan

Berdasarkan hasil analisis maka dapat ditarik kesimpulan atas kerentanan yanng paling banyak didapatkan pada objek penelitia

Alat dan Bahan Penelitian

Alat Penelitian

Pada penelitian berikut ini akan digunakan perangkat lunakdan keras sebagai berikut:

Perangkat keras

Pada penelitian yang di lakukan, ada apun perangkat keras(hardware) yaitu :

- Komputer

Spesifikasi komputer yang digunakan untuk melakukan penelitian ini adalah

- CPU CORE i7
- RAM 12
- SSD 500 GB

Perangkat Lunak

Pada penelitian yang dilakukan, Adapun perangkat lunak (Software) yaitu :

- Burpsuite
- Memu (Android Emulator)
- Sqlmap
- Android Debug Bridge
- Command Prompt
- Windows Subsystem for Linux (WSL)

Bahan Penelitian

Bahan penelitian yang akan digunakan oleh penulis diantara lain:

Objek penelitian

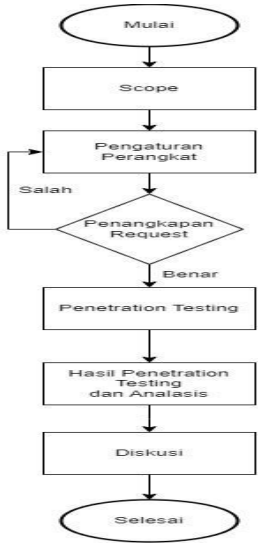
Objek penilitian ini merupakan aplikasi android yang setiap requestnya menggunakan API. terlihat pada path setiap proses yang di jalankan/API/

Data Hasil pengujian

Data yang di makssud adalah data yang didapat dari dokumentasi setelah proses penetration testing selesai di lakukan pada objek penelitian.

Alur Pengujian

Dalam melakukan pengujian atau penetration testing pada aplikasi android yang berfokus pada API , Memiliki beberapa rangkaian tahapan seperti yang ada di bawah ini:



Gambar Diagram alur pengujian

Pada Gambar Diagram alur pengujian menujukan alur pengujian yang akan di lakukan,berikut adalah deskripsi dari gambar di atas :

Scope

Batasan yang sudah disepakati oleh peneliti dengan pemilik aplikasi yaitu hanya melakukan pentest pada aplikasi android. Pentest yang berjalan pada fitur yang menggunakan API dan menjaga kerahasian yang bersifat sensitif atas kerentanan yang didapat dari hasil pentest.

Pengaturan perangkat

Pengaturan perangkat yang di maksud adalah pengaturan proxy yang berisi ip perangkat dan port yang agar terhubung dengan emulator, serta melakukan import certificate burpusite kedalam system android menggunakan adb.

Penangkapan request

Merupakan cara pencegatan setiap proses yang di jalakan oleh aplikasi, untuk penentuan bahwa burpsuite berhasil terkoneksi atau tidak yaitu dengan cara masuk ke burpsuite lalu klik intercept agar off setelah itu membuka browser ataupun aplikasi jika tetap berjalan dan burpsuite berhasil menangkap request yang terlihat pada history maka dikatakan bahwa burpsuite berhasil mendapatkan request aplikasi, tetapi jika aplikasi tidak bisa terbuka dan web mendapatkan respon failed to connect maka pengaturan perangkat harus di lakukan kembali agar mendapatkan request setiap proses aplikasi android.

Penetration Testing

Merupakan pegujian tarhadap keamanan pada sistem serta mendokumentasikan kerentanan yang didapat dari hasil pentest tersebut. Pengujian mengunakan dua metode yaitu :

- Grey Box

  Pengujian grey box merupakan tingkatan dari pengujian blac kbox dikarenakan pentest grey box mengetahui sebagian

ISSN 2337-6805

struktur dari aplikasi. serta grey box melakukan pentest pada fitur setelah melakukan proses login.

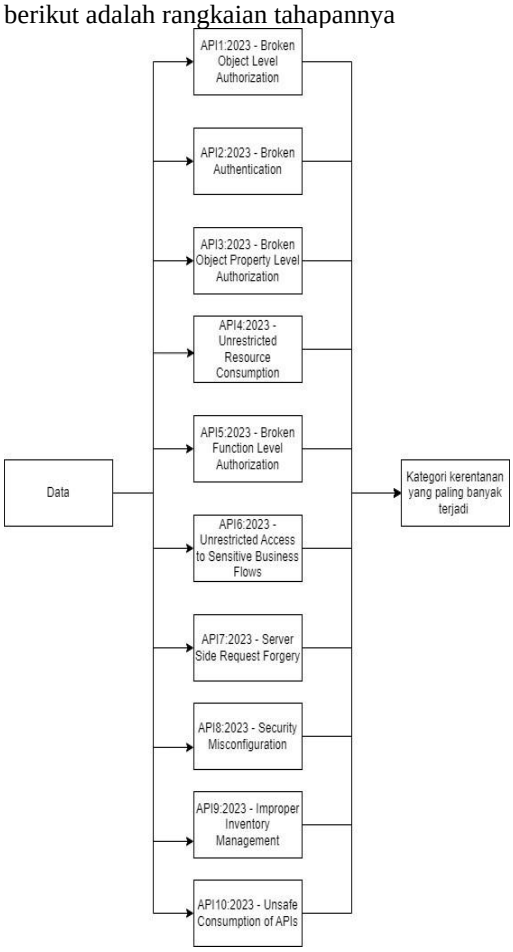
- Black Box
  Pentest black box merupakan pengujian yang di lakukan tanpa mengetahui struktur dari aplikasi, dan pengujian black box hanya mendapatkan aplikasi ataupun URL tanpa ada data informasi terkait dengan aplikasi ataupun sistem jaringan yang digunakan..

Hasil Pengujian

Hasil pengujian merupakan, dokumentasi dari hasil pentest yang dilakukan secara black box dan grey box.

Alur Analisis

Untuk melakukan analisis, data yang diperlukan merupakan hasil dari penetration testing, yang akan di kelompokan kedalam kategori kerentanan yang terdapat pada OWASP API Top 10 2023, dikarenakan OWASP API Top 10 2023 fokus pada resiko teratas dan sering terjadi, serta menjadi standar industri yang diakui dan diikuti oleh banyak organisasi dan profesional keamanan dan Relevansi dengan Perkembangan Terbaru. berikut adalah rangkaian tahapannya



Gambar Alur Analisis dan pengelompokan

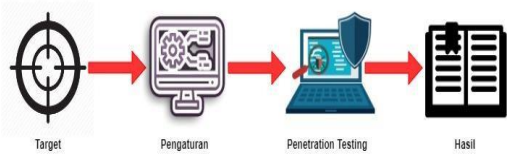
Pada Gambar Alur Analisis dan pengelompokan menunjukan alur analisis yang akan di lakukan untuk mengelompokan kerentanan berdasarkan kategori OWASP API TOP 10 2023, serta mengetahui categori kerentanan yang paling banyak terjadi pada aplikasi tersebut. berikut adalah diskripsi dari gambar diatas :

- Data
  Merupakan hasil keselurahan dari penetration testing pada objek dengan jenis pengujian Black Box dan Grey Box.
- Pengelompokan
  Pengelompokan di lakukan berdasarkan dokumentasi yang didapat dari hasil penetration testing, lalu dikelompokan kedalam kategori kerentanan yang sesuai dengan OWASP API TOP 10 2023, untuk menentukan pengelompokan kategori kerentanan tersebut OWASP API TOP 10 2023 sudah memberikan deskripsi kerentanan dan referensi agar lebih mudah untuk menentukan kategori kerentanan tersebut.
- Analisis
  Hasil dari pengelompokan kategori kerentanan yang masuk kedalam OWASP API Top 10 2023 akan membuktikan kategori kerentanan paling banyak terjadi pada objek penelitian tersebut, dengan adanya hal tersebut maka dapat mengetahui penyebab kategori kerentanan tersebut sering terjadi.

3. HASIL DAN PEMBAHASAN

Pengujian

Sebelum Melakukan Penetration testing, ada beberapa tahap yang harus di lakukan yaitu:



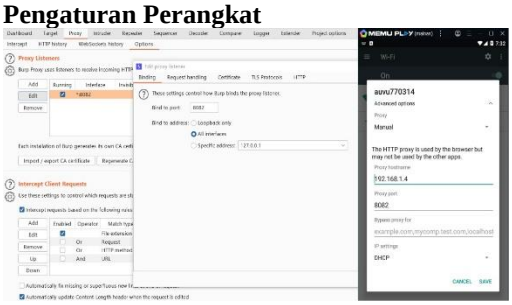
Gambar Tahap pengujian

Gambar Tahap pengujian merupakan tahapan dalam melakukan pengujian yaitu mengetahui target yang akan di uji, pengaturan dilakukan agar burpsuite dapat menangkap semua request pada saat aplikasi berjalan, Jika burpusite berhasil mendapatkan request maka penetration testing pada target dapat di lakukan, untuk mendapatkan hasil berupa jenis dan jumlah kerentanan yang terdapat pada target.

Proses dalam pengaturan antara burpuite dengan perangkat dapat dilihat berikut ini serta pengujian yang dilakukan pada target.

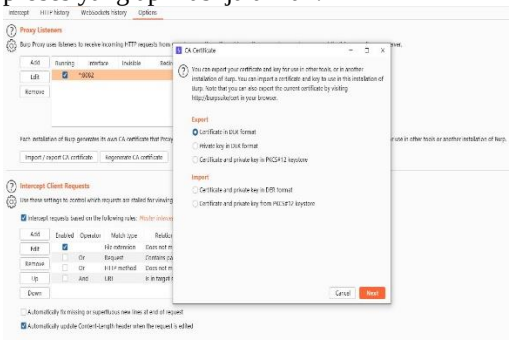
ISSN 2337-6805

Pengaturan Perangkat



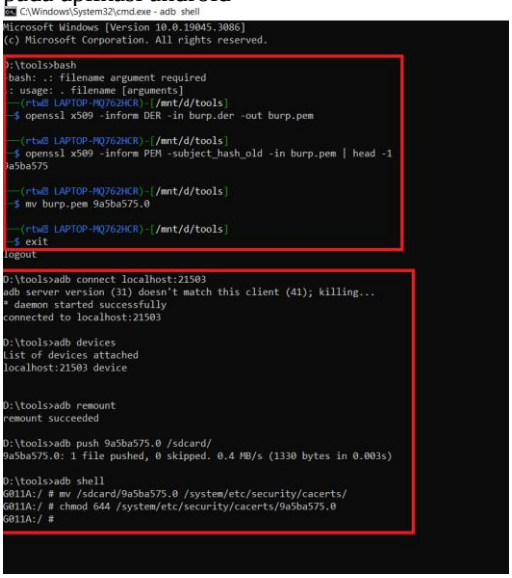
Gambar Proxy

Pada gambar Proxy menunjukan pengaturan proxy dari Burpsuite ke emulator yang berguna untuk mengoneksikan setiap proses yang aplikasi jalankan.



Gambar Import Sertifikat

Pada gambar Import Sertifikat menunjukan proses import sertifkat pada burpsuite yang akan di gunakan sebagai izin koneksi akses pada aplikasi android



Gambar Push sertifikat

Pada gambar Push sertifikat menunjukan perubahan extension (EXT) pada sertifikat burpsuite, memindahkan sertifikat lalu memberikan hak akses agar dapat mengakses serta memodifikasi file sesuai yang diinginkan. Bash linux berfunsgi sebagai konversi sertifikat dari DER menjadi PEM di karenakan android menginginkan sertifikat dalam format PEM, dan Mencetak hash nama subjek sertifikat menggunakan algoritme lama seperti yang digunakan oleh OpenSSL sebelum versi 1.0.0. subject_hash_old nilai yang ditambahkan dengan .0 dibagain belakang. Berikut adalah comment yang di gunakan pada bash

$ openssl x509 -inform DER -in burp.der -out burp.pem (untuk merubah ext dari der menjadi pem)

$ openssl x509 -inform PEM -subject_hash_old -in burp.pem | head -1 (untuk mendaparkan has pada sertifikat yang sudah di rubah .pem)

$ mv burp.pem 9a5ba575.0 (merubah burp.pem menjadi has yang didapat)

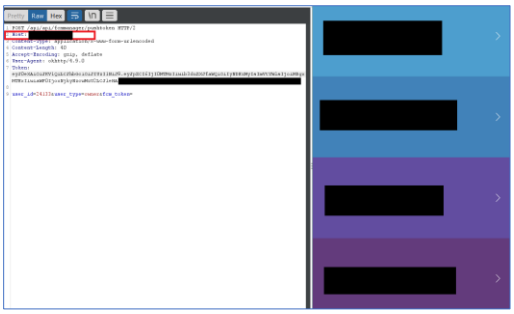
Cmd berfungsi untuk menjalankan perintanh adb yang akan memasang kembali ke file system dan push cert yang sudah di hash ke dalam perangkat android serta mengatur hak akses agar dapat mengakses file yang diinginkan.

$ adb remount (Mengubah partisi sistem pada perangkat Android dari mode hanya baca (read-only) menjadi mode tulis-baca (read-write))

$ adb push 9a5ba575.0 /sdcard/ (Untuk memindahkan file dari pc kedalam penyimpanan device)

mv /sdcard/9a5ba575.0 /system/etc/security/cacerts/ (untuk memindakan lokasi file)

chmod 644 /system/etc/security/cacerts/9a5ba575.0 (Untuk memberikan akses)



Gambar Pengaturan selesai

Pada Gambar Pengaturan selesai menunjukan bahwa burpsuite berhasil menangkap request aplikasi, bahwa terlihat pada pada tambilan burpsuite dengan host yang didapat saat aplikasi dijalankan, host tersebut merupakan milik aplikasi tersebut, yang berarti bawah pengaturan berhasil.

Penetration Testing

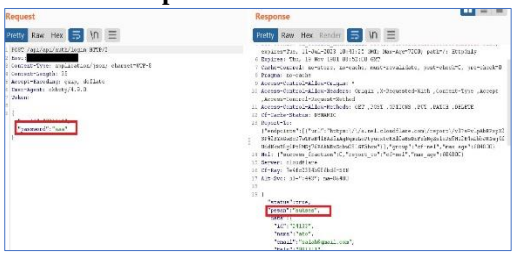
Merupakan tahapan untuk menemukan celah keamanan pada objek penelitan, berikut adalah proses yang di lakukan :

ISSN 2337-6805

Black box

Black Box testing yang akan di lakukan merupakan pencarian keamanan tanpa melakukan login terlebih dahulu. Berikut adalah celah keamanan yang didapat:

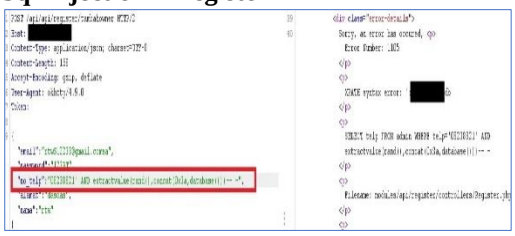
Permits weak passwords.



Gambar Permits weak passwords.

Gambar Permits weak passwords merupakan hasil dari pengujian dengan kerentenan dalam pembuatan user, aplikasi mengizinkan pengunaan password yang sangat lemah (dalam lingkarkan merah menunjukan bawah "password":"aaaa".

Sql Injection – Register



Gambar Sql Injection – Register

Gambar Sql Injection – Register merupakan hasil dari pengujian dengan kerentenan Sql Injection yang didapat merupakan eror-based dengan pemangilan database dan payload yang digunakan dalah ' AND extractvalue(rand(),concat(0x3a,database()))--"

Improper Input Validation

Gambar Input Validation

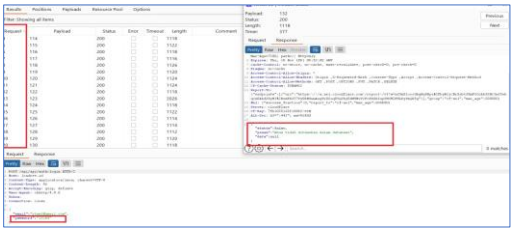
Gambar Input Validation merupakan hasil dari pengujian dengan kerentenan Input validation (<h1>{{9*9}}) yang di lakukan yaitu pada inputan nomer hp, saat input melalui aplikasi secara langsung dilarang, tetapi melalui burp suite dizinkan, dan pendaftaran akun berhasildi buat.

Sql Injection – Login

Gambar Sql injection – Login

Gambar Sql injection – Login merupakan hasil dari pengujian dengan kerentenan Sql injection yang di lakukan pada fitur login yaitu eror based dengan pemangilan nama database, Payload yang digunakan ' AND extractvalue(rand(),concat(0x3a,database()))--

No Rate limit



Gambar No Rate Limit

Gambar No Rate Limit merupakan hasil dari pengujian dengan kerentanan No Rate Limit, merupakan serangan secara paksa dengan cara menebak (Brute Force) pada form login yang bermaksud untuk menebak password.

Hasil Penetration Testing

Hasil dari penetration testing yang di lakukan pada target yang sudah di tentukan mendapatkan jenis-jenis kerentanan dan jumlah dari kerentanan yang di dapatkan , berikut adalah hasil kerentanan yang di dapat :

Tabel Hasil Penetration Testing

No	Jenis Pengujian	Jenis kerentanan	Jumlah
1	Black Box	Permits weak password	1
		Improper Input Validation	1
		Sql Injection	2
		No Rate Limit	1
2	Grey Box	IDOR	15
		No Confirmation of Password	1
		Account Take Over	1
		Sql Injection	8
		Unrestricted File Upload	1
Total Kerentanan			**31**

Pada Tabel Hasil Penetration Testing menunjukan jenis kerentanan serta jumlah disetiap kerentanan yang didapat dari hasil penetration testing yang dilakukan pada target yang sudah ditentukan, dengan jenis pengujian black box dan grey box mendapatkan 31 kerentanan yang di dapat cukup banyak terutama pada jenis pengujian grey box di karenakan lebih banyak fitur maka dari hal tersebut akan mendapatkan banyak request yang didapat untuk dilakukan penetration testing.

ISSN 2337-6805

Hasil kerentanan inilah yang akan dikelompokan bedasarkan kategori kerentanan pada OWASP API TOP 10 2023 untuk mengetahui jenis kerentanan yang paling banyak terjadi pada objek tersebut.

Pengelompokan dan Analisis

Pengelompokan dilakukan berdasarkan data hasil pengujian yang akan di masukan kedalam kategori kerentanan OWASP API TOP 10 2023 untuk mengetahui kerentanan yang paling banyak terjadi.

Analisis dilakukan berdasarkan hasil yang didapat dari pengelompokan yaitukategori OWASP API TOP 10 2023 yang paling banyak terjadi. Maka akan di lakukan pembahasan yang berisi sebab terjadinya kerenatanan tersebut serta memberikan informasi atau saran untuk dilakukan perbaikan.

Pengelompokan

Data hasil dari penetration testing yang sudah dilakukan akan dikelompokan berdasarkan OWASP API TOP 10 2023 untuk mengetahui kategori kerentanan yang paling banyak terjadi, berikut adalah data pengelompokan :

Tabel Pengelompokan data

No	OWASP API TOP 10 2023	Kerentanan hasil dari pentest	tatus	Jumlah Kerentanan	Total
1	API1:2023 - BrokenObject LevelAuthorization	Insecure direct object reference	FAIL	15	16
		Account Take Over		1	
2	API2:2023 - Broken Authentication	Permits weak Passwords	FAIL	1	2
		No Confirmation Of Password		1	
3	API3:2023 - Broken Object Property Level Authorization		PASS	0	0
4	API4:2023 - Unrestricted Resource Consumption	No Rate Limit	FAIL	1	1
5	API5:2023 - Broken Function Level Authorization		PASS	0	0
6	API6:2023 -Unrestricted Access to Sensitive BusinessFlows		PASS	0	0
7	API7:2023 - Server Side Request Forgery		PASS	0	0
8	API8:2023 - Security Misconfiguration		PASS	0	0
9	API9:2023 – Improper Inventory Management		PASS	0	0
10	API10:2023 - Unsafe Consumption of APIs	Sql Injection	FAIL	10	12
		Input Validation		1	
		Unrestricted File Upload		1	

Pada Tabel Pengelompokan data menunjukan tabel pengelompokan berikut adalah diskripsi dari tabel diatas:

- Kategori kerenantanan owasp api top 10 2023 merupakanketegori kerentanan yang terdapat pada.
- Kerentanan hasil dari pentest merupakan kerentanan yangdi dapat dari penetration testing.
- Status terdapat 2 status yaitu fail berarti terdapat kerentanan dan pass yang berarti tidak ditemukankerentanan
- Jumlah kerentanan jumlah kerentanan di ambil dari hasil penetration testing
- Total diambil dari jumlah kerentanan yang terdapat pada setiap kategori owasp api top 10 2023.

Analisis

Berdasarkan hasil dari pegelompokan kategori kerentanan API1:2023 Broken Object Level Authorization menjadi kerentanan yang paling banyak terjadi, yaitu dengan kerentanan jenis IDOR berjumlah 15 kerentanan dan account take over jumlah 1 kerentanan,
berikut adalah pembahasanya:

- IDOR : Kerentanan ini masuk kedalam kategori Owasp API1:2023 - Broken Object Level Authorization di karenakan penyerang dapat mengeksploitasi pada titik akhir api yang rentan terhadap otorisasi tingkat objek yang rusak dengan merubah ID objek yang terdapat pada permintaan. Akses mengakitbatkan pengungkapan data, kehilangan data ataupun merubah data ke pihak yang tidak berwenang.
- Account Take Over : Kerentanan ini masuk dalam ketegori Owasp API1:2023 Broken Object Level Authorization di karenakan penyerang dapat mengeksploitasi pada titik akhir api yang rentan terhadap otorisasi tingkat objek yang rusak dengan merubah ID objek yang terdapat pada permintaan. Dalam keadaan tertentu, akses tidak sah ke objek dapat menyebabkan pengambilalihan akun secara penuh.

Karna ketegori kerentanan API1:2023 Broken Object Level Authorization di akibatkan otorisasi tingkat objek yang rusak dengan cara merubah ID objek maka perbaikan untuk meminimalisir adanya kerentananan tersebut yaitu :

- Validasi dan Otorisasi di Sisi Server:
  Pastikan bahwa setiap permintaan yang mengandung token atau ID objek diverifikasi di sisi server sebelum mengizinkan akses. Verifikasi bahwa token yang diberikan sah dan memiliki izin untuk mengakses objek tertentu
- Gunakan Indeks untuk Referensi Objek
  Merubah ID objek yang digunakan menjadi ID acak atau Universal Unique Identifier (UUID) sebagai referensi objek. ID yang acak atau UUID tidak mengikuti pola yang mudah diprediksi dan lebih sulit untuk ditebak oleh penyerang.
- Lakukan Pengujian Keamanan
  Melakukan Pengujian keamanan secara menyeluruh, termasuk pengujian Penetration Testing dan pengujian kerentanan secara berkala.hal tersebut dilakukan untuk menemukan celah dalam

ISSN 2337-6805

sistem serta memastikan bahwa tingkat keamanan tetap konsisten dan berjalan dengan baik seiring waktu.

4. SIMPULAN

Berdasarkan hasil pengujian pada objek penelitian berfokus pada api, peneliti menarik kesimpulan sebagai berikut:

1. Owasp api top 10 2023 terbukti efektif dijadikan sebagai standar keamanan untuk melakukan penetration testing. dikarenakan mencakup kerentanan dan lebih fleksibel.
2. Semua kerentanan yang didapat dari hasil penetration testing pada objek tersebut, dapat dikelompokan kedalam kategori OWASP API Top 10 2023 berdasarkan attack vector.
3. Kerentanan otorisasi dan injection cukup banyak terjadi pada api, yang menyebabkan penyerang dapat mengakses data sensitif tau melakukan tidak sah.
4. Pada OWASP API Top 10 2023 Broken Object Level Authorization menjadi top 1, pernyataan tersebut sesuai dengan hasil kerentanan yang terjadi pada objek penelitian.

Saran

Berdasarkan hasil pengujian dan analisis yang telah dilakukan, API1:2023 - Broken Object Level Authorization menjadi pembahasan karna paling banyak terjadi kerentanan. saran dari peneliti untuk kerentanan dalamkategori API1:2023 - Broken Object Level Authorization sebagai berikut :

1. Melakukan validasi antara token dengan objek id
2. merubah ID objek menjadi UUID.
3. Melakukan penetration testing sebelum api digunakan sebagai penghubung antar aplikasi
4. Melakukan penetration testing untuk keseluruhan aplikasi

5. DAFTAR PUSTAKA

Adinugroho, N. B., Hendradi, P., & Sasongko, D. (2022). Analisis Keamanan E-Learning Menggunakan Open Web Application Security Project (Owasp) (Studi Kasus Moca Unimma). Jurnal Informatika, 22(2), 132–138.

Alviansyah, F. A., & Ramadhani, E. (2021). Implementasi Dynamic Application Security Testing pada Aplikasi Berbasis Android. Automata, 2(1), 1–6.

Ardian, A. (2021). Perancangan Aplikasi Pengolah Data Siswa Berbasis Android (Studi Kasus : Mis Nurul Huda Labuhan Batu Selatan). Journal of Computer Science and Information Systems (JCoInS), 2(2), 113–123.

Erbeliza, S. (2023). Analisis Keamanan Aplikasi Mobile Commerce Menggunakan Mobile Security Framework (Mobsf) dan Owasp Mobile Application Security Testing Guide (Mastg).

Hasanuddin, Asgar, H., & Hartono, B. (2022). Rancang Bangun Rest Api Aplikasi Weshare Sebagai Upaya Mempermudah Pelayanan Donasi Kemanusiaan. Jurnal Informatika Teknologi Dan Sains, 4(1), 8–14.

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. Sudo Jurnal Teknik Informatika, 1(4),171–177.

Hermawan, R. (2021). Teknik Uji Penetrasi Web Server Menggunakan SQL Injection dengan SQLmap di Kalilinux. STRING (Satuan Tulisan Riset Dan Inovasi Teknologi), 6(2), 210.

Indera, R., Budiono, A., & Hediyanto, U. Y. K. S. (2023). Vulnerability Assessment Pada Situs Web KPPM FRI Dengan Burp Suite dan Intruder. E-Proceeding of Engineering, 10(2), 1623.

Irawan, B., & Rosyani, P. (2022). Perancangan Aplikasi Pengenalan Kebudayaan dan Pariwisata Kabupaten Cianjur Berbasis Android. TIN: Terapan Informatika Nusantara, 2(8), 521–526.

Ma'rufi, M., & Asnawi, M. F. (2021). Algoritma Evolusi Genetika Sebagai Fungsi Optimasi. JURNAL DEVICE, 11(1), 25–33.

Saputri, F., & Umam, H. (2023). Analisis Perbandingan Static Routing Dan Dynamic Routing Pada Lab Akademi Komunitas Darussalam. JURNAL ADMINISTRASI JARINGAN KOMPUTER, 1(1), 1–13.

Siregar, R. R., Nasution, K., & Haramaini, T. (2021). Aplikasi Ujian Online Untuk Siswa Sekolah Menengah Pertama Dengan Menggunakan Metode Rational Unified Process (RUP). Jurnal Minfo Polgan, 10(1), 33–41.

Yalon, E., Shkedy, I., & Silva, P. (2023). OWASP API Security Project.