CONFIDENTIAL

Vulnerability Assessment & Penetration Testing

Technical Report

Information Systems — crAPI (Lab)

Client	crAPI (Lab)
Target	http://127.0.0.1:8888
Asset type	API
Testing approach	Grey-box
Standards	OWASP API Security Top 10 2023
Overall risk	**Critical**
Report version	1.1
Report date	September 29, 2026
Prepared by	Muhammad Faqih

Table of Contents

List of Figures **3**

List of Tables **5**

1 Scope of Work **6**

1.1 Methodology 6

1.2 Standards and Frameworks 7

1.2.1 API (OWASP API Security Top 10 2023) 7

1.3 List of Assets 7

2 Summary of Vulnerabilities **8**

3 Findings on API **12**

3.1 crAPI Identity Service (http://127.0.0.1:8888/identity) 12

3.1.1 Broken Authentication (API2) – JWT Signature Not Verified — Authentication Bypass 12

3.1.2 Broken Authentication (API2) – Bypassable Brute-Force Protection on Password Reset OTP 16

3.1.3 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Vehicle Location 18

3.1.4 Unrestricted Resource Consumption (API4) – Unrestricted Resource Consumption — No Login Rate Limiting 21

3.1.5 Improper Inventory Management (API9) – Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live 23

3.1.6 Broken Object Property Level Authorization (API3) – Mass Assignment on User Registration 25

3.1.7 Broken Object Level Authorization (API1) – Missing Authentication Check on Vehicle Location (Unauthenticated Access) 27

3.1.8 Broken Authentication (API2) – Password Reset OTP Per-Session Lockout 29

3.2 crAPI Workshop Service (http://127.0.0.1:8888/workshop) 31

3.2.1 Server Side Request Forgery (API7) – Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover 31

3.2.2 Broken Function Level Authorization (API5) – Unauthenticated Access to Order Details 35

3.2.3 Broken Function Level Authorization (API5) – Broken Function Level Authorization — Management Endpoint Exposes All Users 38

3.2.4 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Mechanic Reports 40

3.2.5 Unsafe Consumption of APIs (API10) – Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic 42

3.2.6 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Order Return 44

3.2.7 Broken Object Level Authorization (API1) – Missing Authentication Check on Mechanic Report (Unauthenticated Access) 46

3.2.8 Unrestricted Access to Sensitive Business Flows (API6) – Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected) 48

3.3 crAPI Community Service (http://127.0.0.1:8888/community) 50

3.3.1 Security Misconfiguration (API8) – NoSQL Injection on Coupon Validation 50

3.3.2 Security Misconfiguration (API8) – Coupon Validation with Normal String Input 52

4 Summary of Recommendations **54**

5 Conclusion **56**

6 Attachments **57**

List of Figures

Figure 1 - Vulnerability Assessment and Penetration Testing Methodology 6
Figure 2 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - normal: token sah, akun sendiri 13
Figure 3 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - proses: susun token alg:none 13
Figure 4 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - eksploitasi: token alg:none diterima 14
Figure 5 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - proses: tamper RS256, signature lama 14
Figure 6 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - dampak: token tampered diterima, CIA 15
Figure 7 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: meminta OTP reset password 17
Figure 8 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: satu percobaan OTP salah 17
Figure 9 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Dampak: forget-password me-reset lockout, memungkinkan ATO 17
Figure 10 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888 (Grey-box) - Dashboard crAPI menampilkan peta lokasi kendaraan (browser) 19
Figure 11 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Normal flow: lokasi kendaraan sendiri 19
Figure 12 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Eksploitasi: UUID korban mengembalikan lokasi + email korban 20
Figure 13 - Unrestricted Resource Consumption — No Login Rate Limiting (API4) - http://127.0.0.1:8888/identity/api/auth/login (Login) (Grey-box) - satu login gagal 22
Figure 14 - Unrestricted Resource Consumption — No Login Rate Limiting (API4) - http://127.0.0.1:8888/identity/api/auth/login (Login) (Grey-box) - 20 percobaan, tanpa rate limiting 22
Figure 15 - Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live (API9) - http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy) (Grey-box) - versi saat ini v3 24
Figure 16 - Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live (API9) - http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy) (Grey-box) - versi lama v2 masih hidup 24
Figure 17 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Normal flow: registrasi standar 25
Figure 18 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Percobaan: sisipkan field privileged role/isAdmin 26
Figure 19 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Hasil: role tetap user, kontrol efektif 26
Figure 20 - Missing Authentication Check on Vehicle Location (Unauthenticated Access) (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Normal flow: lokasi kendaraan sendiri dengan token 27

Figure 21 - Missing Authentication Check on Vehicle Location (Unauthenticated Access) (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Percobaan ditolak: tanpa token -> 401 28
Figure 22 - Password Reset OTP Per-Session Lockout (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: satu percobaan OTP salah 29
Figure 23 - Password Reset OTP Per-Session Lockout (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Percobaan ditolak: lockout memicu pada percobaan ke-10 30
Figure 24 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888 (Grey-box) - Dashboard crAPI dengan fitur 'Contact Mechanic' (browser) 32
Figure 25 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - normal: server mem-fetch mechanic API 32
Figure 26 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - SSRF membaca inbox MailHog internal (45 email) 33
Figure 27 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - panen OTP korban via SSRF 33
Figure 28 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - reset password korban dgn OTP panen 34
Figure 29 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - login sebagai korban — Account Takeover 34
Figure 30 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888 (Grey-box) - Halaman Past Orders crAPI dengan 'Order Details' (browser) 36
Figure 31 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details) (Grey-box) - Normal flow: permintaan order ber-autentikasi 36
Figure 32 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details) (Grey-box) - Eksploitasi: tanpa autentikasi, PII bocor 37
Figure 33 - Broken Function Level Authorization — Management Endpoint Exposes All Users (API5) - http://127.0.0.1:8888/workshop/api/management/users/all (User Management) (Grey-box) - normal: hanya akun sendiri 39
Figure 34 - Broken Function Level Authorization — Management Endpoint Exposes All Users (API5) - http://127.0.0.1:8888/workshop/api/management/users/all (User Management) (Grey-box) - eksploitasi: dump PII semua user 39
Figure 35 - Broken Object Level Authorization (IDOR) on Mechanic Reports (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Normal flow: referensi report_id=1 41
Figure 36 - Broken Object Level Authorization (IDOR) on Mechanic Reports (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Eksploitasi: report_id=2 membocorkan data pemilik lain 41
Figure 37 - Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic (API10) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - mengonsumsi mechanic API 43
Figure 38 - Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic (API10) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - respons upstream mentah dipantulkan 43

Figure 39 - Broken Object Level Authorization (IDOR) on Order Return (API1) - http://127.0.0.1:8888 (Grey-box) - Halaman Past Orders crAPI dengan aksi 'Return' (browser) 44
Figure 40 - Broken Object Level Authorization (IDOR) on Order Return (API1) - http://127.0.0.1:8888/workshop/api/shop/orders/return_order?order_id={id} (Return Order) (Grey-box) - Percobaan ditolak: retur order milik user lain -> 403 45
Figure 41 - Missing Authentication Check on Mechanic Report (Unauthenticated Access) (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Normal flow: report dengan token valid 46
Figure 42 - Missing Authentication Check on Mechanic Report (Unauthenticated Access) (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Percobaan ditolak: tanpa token -> 401 47
Figure 43 - Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected) (API6) - http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim) (Grey-box) - klaim kupon pertama berhasil 48
Figure 44 - Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected) (API6) - http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim) (Grey-box) - replay ditolak .. 49
Figure 45 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Normal flow: kode kupon string valid 51
Figure 46 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Eksploitasi: operator $ne membocorkan kupon valid 51
Figure 47 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Dampak: $gt juga membocorkan kupon, injeksi terkonfirmasi 51
Figure 48 - Coupon Validation with Normal String Input (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Normal flow: kode kupon valid diterima 52
Figure 49 - Coupon Validation with Normal String Input (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Kontrol: kode string tak dikenal ditolak 53

List of Tables

Table 1 - Penetration Testing Approaches 6
Table 2 - OWASP API Security Top 10 2023 Categories 7
Table 3 - List of Assets 7
Table 4 - Vulnerability Summary – crAPI Identity Service 8
Table 5 - Vulnerability Summary – crAPI Workshop Service 9
Table 6 - Vulnerability Summary – crAPI Community Service 10

1 Scope of Work

1.1 Methodology

The methodology used in this vulnerability assessment and penetration test is described below.

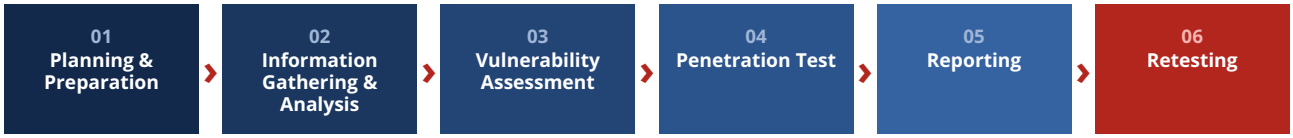


Figure 1 - Vulnerability Assessment and Penetration Testing Methodology

1. **Planning and understanding the target system and supporting applications.** Understanding the target system, supporting applications, public and internal IP addresses, operating systems (OS), databases, and application topology within the relevant work unit, through interviews or the documentation provided.
2. **Conducting the vulnerability assessment.** Assessing vulnerabilities and identifying security weaknesses within the scope of the system and its supporting network infrastructure, including web applications, operating systems, databases, and networks.
3. **Performing penetration testing based on the assessment results.** Exploitation aims to prove that the security gaps or vulnerabilities found exist, and to assess their level of risk and impact on the company's applications, information, and business reputation.
4. **Reporting and discussing results with Team crAPI (Lab).** Preparing the report and discussing the penetration test results and recommendations for improvement, and reaching a mutual agreement on reducing the existing security gaps. Recommendations are based on the standards and frameworks used in the test.
5. **Retesting the implemented improvements.** Retesting the improvements implemented to ensure that security gaps and risks have been effectively reduced.

The testing approaches used in penetration testing are black-box, grey-box and white-box:

Table 1 - Penetration Testing Approaches

Approach	Description	This engagement
Black-box	Conducted without any prior information or knowledge about the target. Testing uses only a list of IP addresses or domains, without detailed knowledge of the system profile or application topology.	—
Grey-box	Conducted with some information and knowledge about the target, including user access to web applications or servers but without full access rights. Testing is still limited by firewall filtering or a WAF (Web Application Firewall).	✔ Applied
White-box	Conducted with comprehensive information about the target, such as the application topology, test user IDs, internal network access, and the IP addresses of the target and users, without any firewall or WAF filtering.	—

1.2 Standards and Frameworks

Findings in this report are classified against the following standards and frameworks: **OWASP API Security Top 10 2023**.

1.2.1 API (OWASP API Security Top 10 2023)

The OWASP API Security Top 10 (2023) lists the most critical security risks specific to APIs. Reference: https://owasp.org/API-Security/editions/2023/en/0x11-t10/

Table 2 - OWASP API Security Top 10 2023 Categories

ID	Category
API1:2023	Broken Object Level Authorization
API2:2023	Broken Authentication
API3:2023	Broken Object Property Level Authorization
API4:2023	Unrestricted Resource Consumption
API5:2023	Broken Function Level Authorization
API6:2023	Unrestricted Access to Sensitive Business Flows
API7:2023	Server Side Request Forgery
API8:2023	Security Misconfiguration
API9:2023	Improper Inventory Management
API10:2023	Unsafe Consumption of APIs

1.3 List of Assets

The scope of security testing and penetration testing for the crAPI (Lab) web application is as follows:

Table 3 - List of Assets

No	Name	URL	Type	Status
1	**crAPI Identity Service**	`http://127.0.0.1:8888/identity`	API	FAIL
2	**crAPI Workshop Service**	`http://127.0.0.1:8888/workshop`	API	FAIL
3	**crAPI Community Service**	`http://127.0.0.1:8888/community`	API	FAIL

Status legend: **PASS** — no vulnerability found **FAIL** — vulnerability found

2 Summary of Vulnerabilities

Testing of the crAPI (Lab) web application identified **11 vulnerabilities**: **2 Critical**, **3 High** and **6 Medium**; in addition, **7 tested scenarios** did not result in a vulnerability (PASS).

2	3	6	0	0	7
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL	PASS

crAPI Identity Service

http://127.0.0.1:8888/identity · API · 5 vulnerabilities, 3 PASS

Table 4 - Vulnerability Summary – crAPI Identity Service

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
1	**Broken Authentication (API2) – JWT Signature Not Verified — Authentication Bypass** API2:2023 Broken Authentication	Critical	9.8	Yes	Verifikasi tanda tangan JWT dengan kunci publik RS256 pada setiap request; tolak alg:none dan allow-list algoritma.
2	**Broken Authentication (API2) – Bypassable Brute-Force Protection on Password Reset OTP** API2:2023 Broken Authentication	High	7.4	Yes	Terapkan lockout persisten per akun serta rate-limit/CAPTCHA pada forget-password; gunakan OTP lebih panjang.
3	**Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Vehicle Location** API1:2023 Broken Object Level Authorization	Medium	6.5	Yes	Verifikasi kepemilikan kendaraan terhadap user terautentikasi sebelum mengembalikan lokasi.
4	**Unrestricted Resource Consumption (API4) – Unrestricted Resource Consumption — No Login Rate Limiting** API4:2023 Unrestricted Resource Consumption	Medium	6.5	Yes	Terapkan rate limiting dan lockout pada login; tambahkan CAPTCHA/anti-automasi.
5	**Improper Inventory Management (API9) – Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live** API9:2023 Improper Inventory Management	Medium	5.3	Yes	Nonaktifkan versi API usang (v2) dan kelola inventaris endpoint yang aktif.

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
6	**Broken Object Property Level Authorization (API3) – Mass Assignment on User Registration** API3:2023 Broken Object Property Level Authorization	PASS	—	—	Pertahankan allow-list field yang boleh diset klien saat registrasi.
7	**Broken Object Level Authorization (API1) – Missing Authentication Check on Vehicle Location (Unauthenticated Access)** API1:2023 Broken Object Level Authorization	PASS	—	—	Pertahankan autentikasi wajib; tambahkan juga pemeriksaan kepemilikan objek (lihat temuan FAIL terkait).
8	**Broken Authentication (API2) – Password Reset OTP Per-Session Lockout** API2:2023 Broken Authentication	PASS	—	—	Jadikan lockout persisten per akun agar tak dapat di-reset lewat permintaan OTP baru (lihat temuan FAIL terkait).

crAPI Workshop Service

http://127.0.0.1:8888/workshop · API · 5 vulnerabilities, 3 PASS

Table 5 - Vulnerability Summary – crAPI Workshop Service

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
9	**Server Side Request Forgery (API7) – Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover** API7:2023 Server Side Request Forgery	Critical	9.6	Yes	Allow-list endpoint mekanik; blokir host internal (mailhog/identity); segmentasi layanan internal; jangan pantulkan respons upstream.
10	**Broken Function Level Authorization (API5) – Unauthenticated Access to Order Details** API5:2023 Broken Function Level Authorization API1:2023 Broken Object Level Authorization	High	7.5	Yes	Wajibkan autentikasi dan verifikasi kepemilikan order; gunakan identifier non-sekuensial (UUID).
11	**Broken Function Level Authorization (API5) – Broken Function Level Authorization — Management Endpoint Exposes All Users** API5:2023 Broken Function Level Authorization API3:2023 Broken Object Property Level Authorization	Medium	6.5	Yes	Terapkan otorisasi berbasis peran di sisi server pada semua endpoint manajemen.

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
12	**Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Mechanic Reports** API1:2023 Broken Object Level Authorization API3:2023 Broken Object Property Level Authorization	Medium	6.5	Yes	Verifikasi report yang diminta milik pemanggil; gunakan UUID dan minimalkan field yang dikembalikan.
13	**Unsafe Consumption of APIs (API10) – Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic** API10:2023 Unsafe Consumption of APIs	Medium	5.4	Yes	Validasi & sanitasi respons API upstream; batasi tujuan upstream ke allow-list tepercaya.
14	**Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Order Return** API1:2023 Broken Object Level Authorization	PASS	—	—	Pertahankan pemeriksaan kepemilikan pada aksi retur.
15	**Broken Object Level Authorization (API1) – Missing Authentication Check on Mechanic Report (Unauthenticated Access)** API1:2023 Broken Object Level Authorization	PASS	—	—	Pertahankan autentikasi wajib; tambahkan juga pemeriksaan kepemilikan objek (lihat temuan FAIL terkait).
16	**Unrestricted Access to Sensitive Business Flows (API6) – Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected)** API6:2023 Unrestricted Access to Sensitive Business Flows	PASS	—	—	Klaim kupon yang sama dua kali ditolak ('already claimed'); batas per-user ditegakkan.

crAPI Community Service

http://127.0.0.1:8888/community · API · 1 vulnerability, 1 PASS

Table 6 - Vulnerability Summary – crAPI Community Service

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
17	**Security Misconfiguration (API8) – NoSQL Injection on Coupon Validation** API8:2023 Security Misconfiguration	High	7.1	Yes	Paksa coupon_code menjadi string dan tolak objek/operator; validasi skema input.

No	Vulnerability	Severity	CVSS	Exploited	Recommendation
18	**Security Misconfiguration (API8) – Coupon Validation with Normal String Input** API8:2023 Security Misconfiguration	PASS	—	—	Terapkan pemaksaan tipe string dan tolak operator/objek (lihat temuan FAIL terkait).

References used for every finding: OWASP API Security Top 10 2023, Bugcrowd VRT, CWE 4.0, CVSS v3.1.

3 Findings on API

3.1 crAPI Identity Service (http://127.0.0.1:8888/identity)

3.1.1 Broken Authentication (API2) – JWT Signature Not Verified — Authentication Bypass

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Critical	9.8 / 10	Yes	CWE-347

Standard mapping	**API2:2023** Broken Authentication (OWASP API Security Top 10 2023)
Impact rating	Critical
Bugcrowd VRT	P1 - Broken Authentication and Session Management (VRT 2.1)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`
Affected feature / URL	http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan broken authentication pada layanan identity crAPI: JSON Web Token (JWT) diterima tanpa memverifikasi tanda tangannya. Token yang dibuat dengan header alg:none (tanpa tanda tangan) diterima, dan token RS256 sah yang payload-nya diubah tanpa ditandatangani ulang juga diterima. Karena tanda tangan tidak pernah divalidasi, penyerang dapat memalsukan token untuk pengguna mana pun dan menaikkan klaim role menjadi admin.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk mengambil alih akun mana pun tanpa kredensial. Saat pengujian, tim memalsukan token berisi identitas korban dan role=admin lalu mengakses data akun korban, sehingga merusak Confidentiality dan Integrity dari model autentikasi.

RECOMMENDATION

1. Verifikasi tanda tangan JWT dengan kunci publik RS256 milik server pada setiap request.
2. Tolak eksplisit algoritma alg:none dan terapkan allow-list algoritma (hanya RS256).
3. Gunakan pustaka JWT matang dengan verifikasi wajib serta validasi klaim exp, iss, dan aud.

REFERENCES

- VRT 2.1 - Broken Authentication and Session Management
- https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
- https://cwe.mitre.org/data/definitions/347.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication)

a. Tim login dan menggunakan token RS256 sah miliknya sendiri (ditampilkan utuh) untuk mengakses dashboard-nya; server hanya mengembalikan akun attacker (id=8).

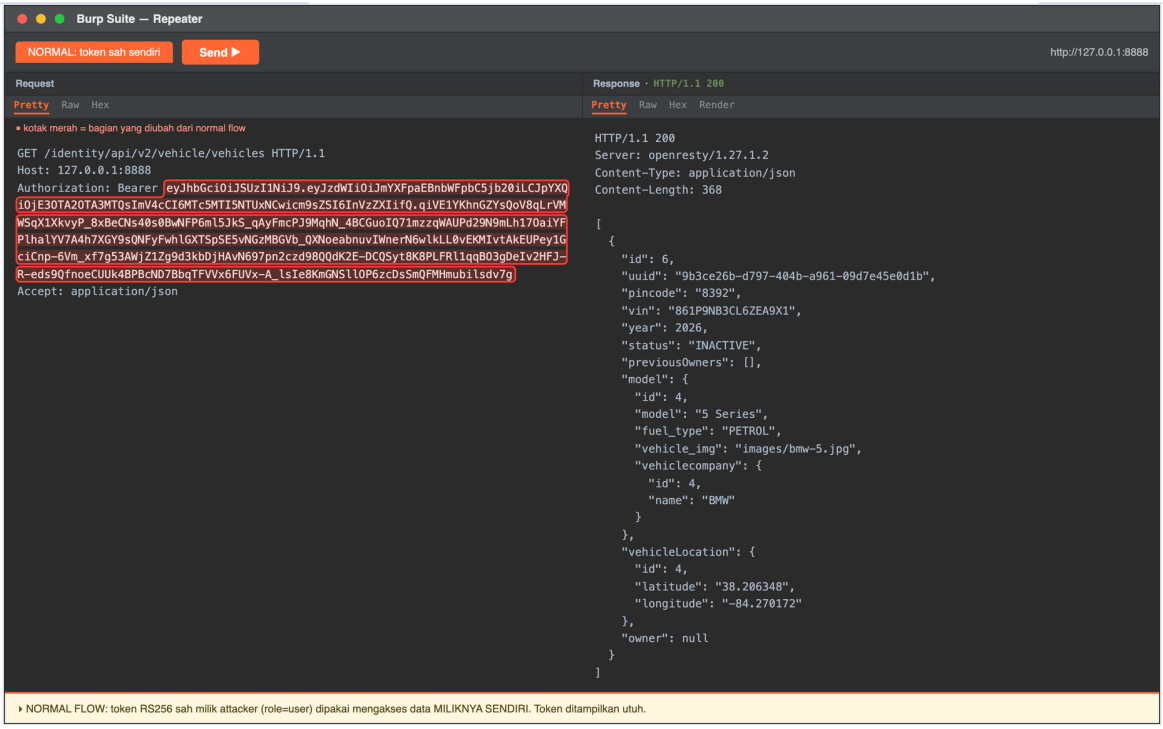


Figure 2 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - normal: token sah, akun sendiri

b. Tim mendekode JWT (base64url header dan payload), mengubah algoritma menjadi "none" dengan signature kosong, menetapkan role=admin dan sub=admin@example.com (menyamar sebagai administrator), lalu menyusun ulang token palsu secara lengkap (ditampilkan utuh, tanpa dipotong).

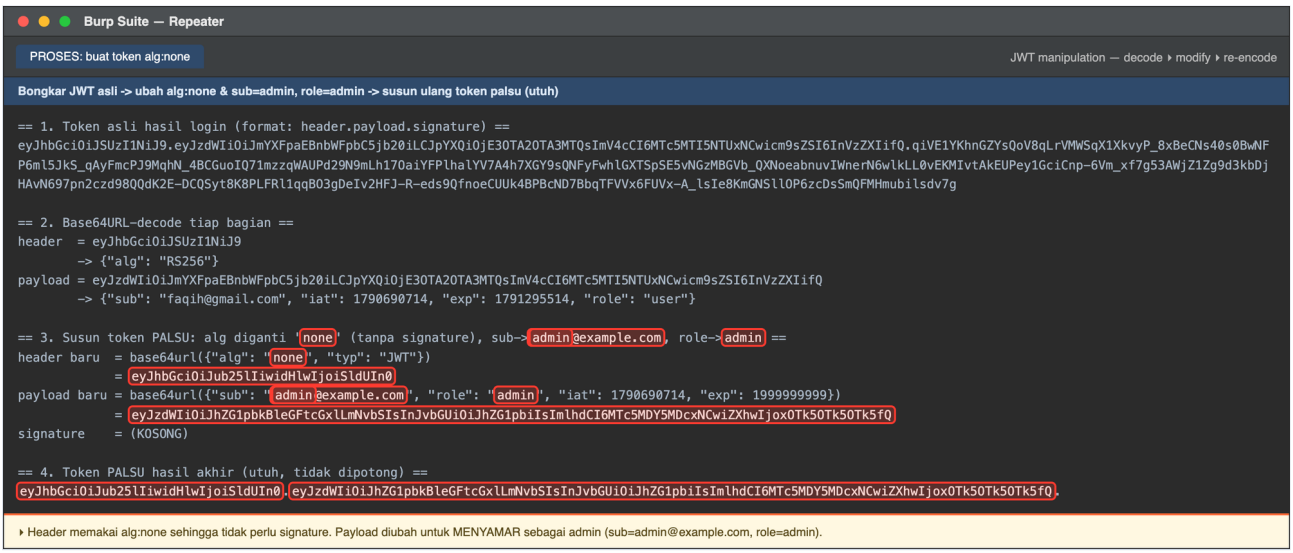


Figure 3 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - proses: susun token alg:none

c. Tim mengirim token palsu alg:none; server menerimanya dan mengembalikan akun ADMIN (id=5, ROLE_ADMIN).

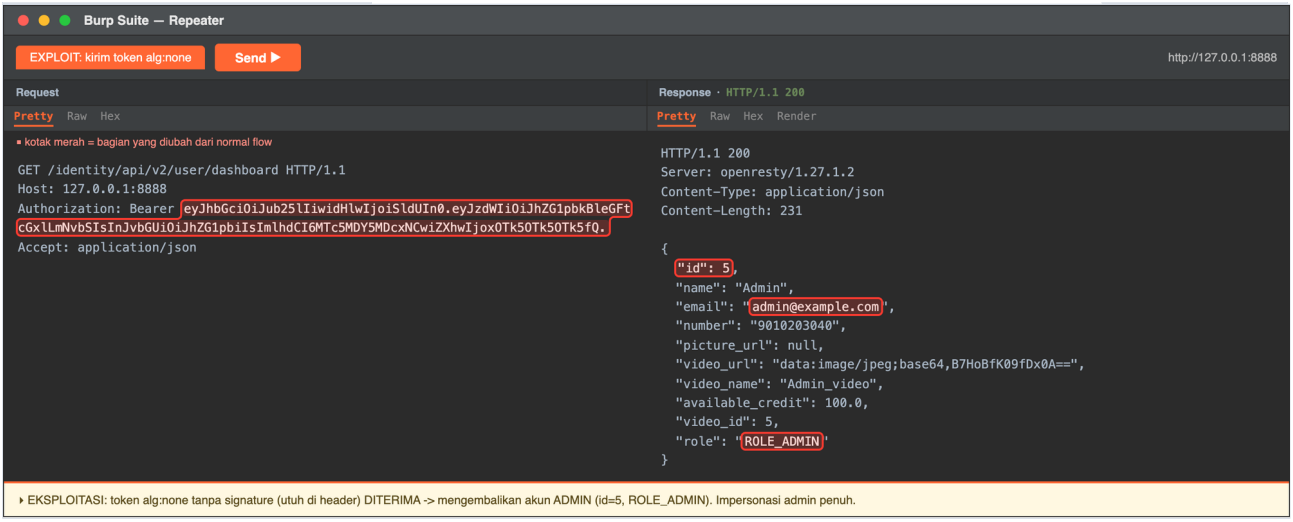


Figure 4 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - eksploitasi: token alg:none diterima

d. Tim mengambil token RS256 sah, mengedit payload menjadi role=admin dan sub=admin@example.com, lalu memasang kembali signature ASLI tanpa menandatangani ulang, menghasilkan token tampered yang lengkap (ditampilkan utuh).

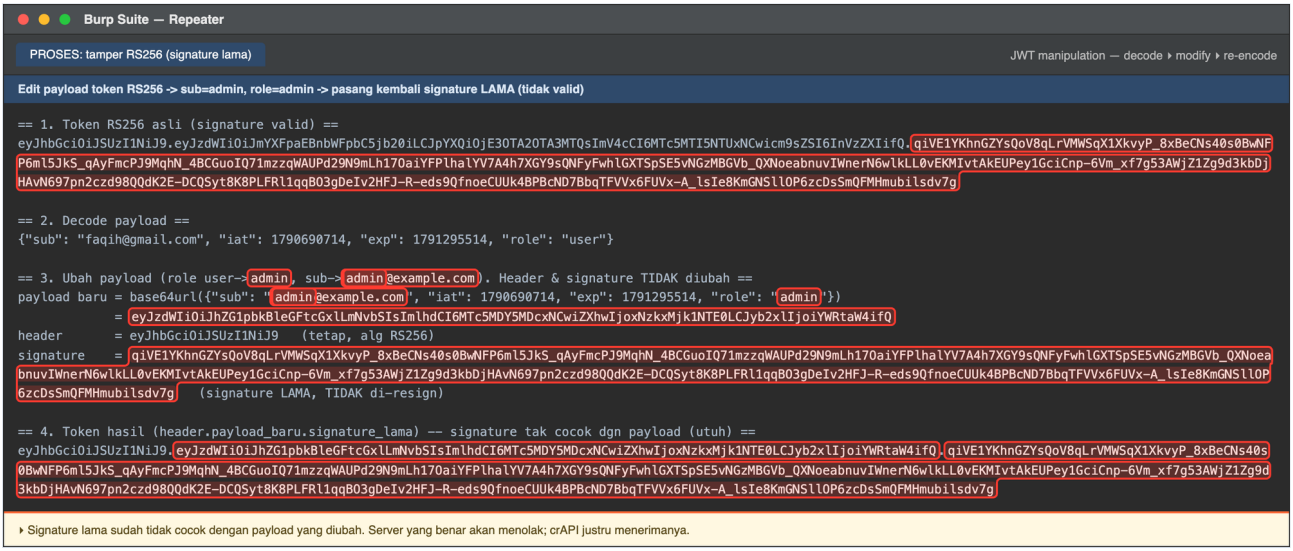


Figure 5 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - proses: tamper RS256, signature lama

e. Tim mengirim token RS256 tampered; server tetap membalas HTTP 200 berisi data korban, membuktikan signature tidak diverifikasi (Confidentiality + Integrity).

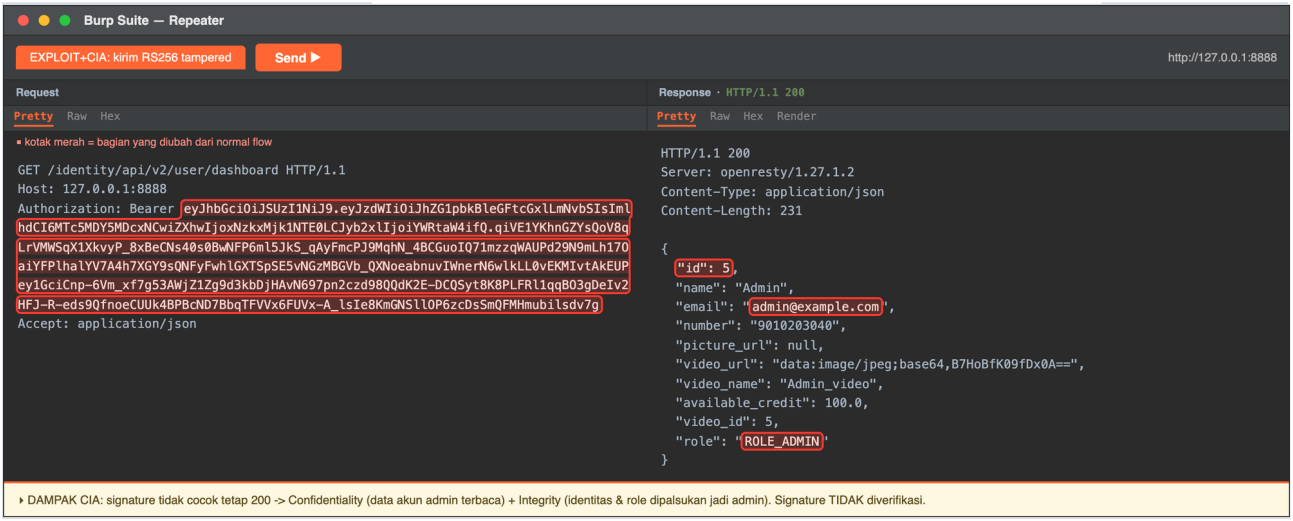


Figure 6 - JWT Signature Not Verified — Authentication Bypass (API2) - http://127.0.0.1:8888/identity/api/v2/user/dashboard (JWT Authentication) (Grey-box) - dampak: token tampered diterima, CIA

3.1.2 Broken Authentication (API2) – Bypassable Brute-Force Protection on Password Reset OTP

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
High	7.4 / 10	Yes	CWE-307

Standard mapping	**API2:2023** Broken Authentication (OWASP API Security Top 10 2023)
Impact rating	**Medium**
Bugcrowd VRT	P2 - Broken Authentication and Session Management (VRT 2.4)
CVSS vector	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`
Affected feature / URL	http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan proteksi brute-force yang lemah pada alur reset password. Endpoint verifikasi OTP mengunci setelah 9 percobaan salah per sesi OTP, tetapi counter ini ter-reset setiap kali forget-password dipanggil, dan forget-password sendiri tidak di-rate-limit maupun ber-CAPTCHA. Proteksi dengan demikian dapat dilewati dengan pola siklus terhadap OTP 4-digit.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk mengambil alih akun mana pun yang emailnya diketahui. Karena OTP hanya 4 digit (10.000 kombinasi) dan tiap siklus memberi 9 tebakan tanpa hambatan atas OTP baru, penyerang terotomasi dapat mereset password korban (Confidentiality + Integrity).

RECOMMENDATION

1. Terapkan lockout persisten per akun yang tidak ter-reset oleh permintaan OTP baru.
2. Rate-limit dan tambahkan CAPTCHA/anti-automasi pada endpoint forget-password.
3. Gunakan OTP minimal 6 digit dengan masa berlaku singkat dan invalidasi setelah kegagalan kumulatif.

REFERENCES

- VRT 2.4 - Broken Authentication and Session Management
- https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
- https://cwe.mitre.org/data/definitions/307.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP)

a. Tim memicu reset password dengan memanggil forget-password untuk email korban; server membalas HTTP 200 (normal flow).

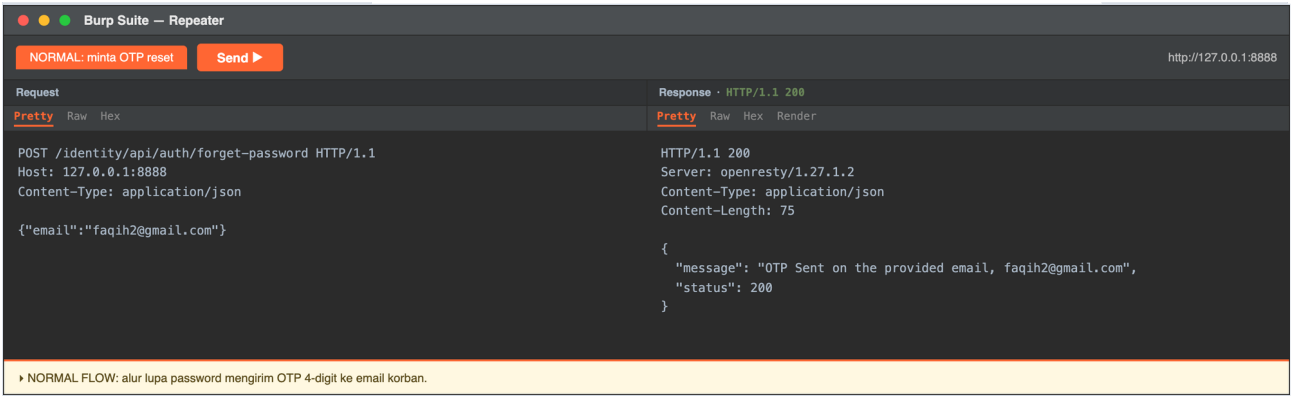


Figure 7 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: meminta OTP reset password

b. Tim mengirim satu OTP salah ke check-otp; server membalas Invalid OTP (satu percobaan normal).

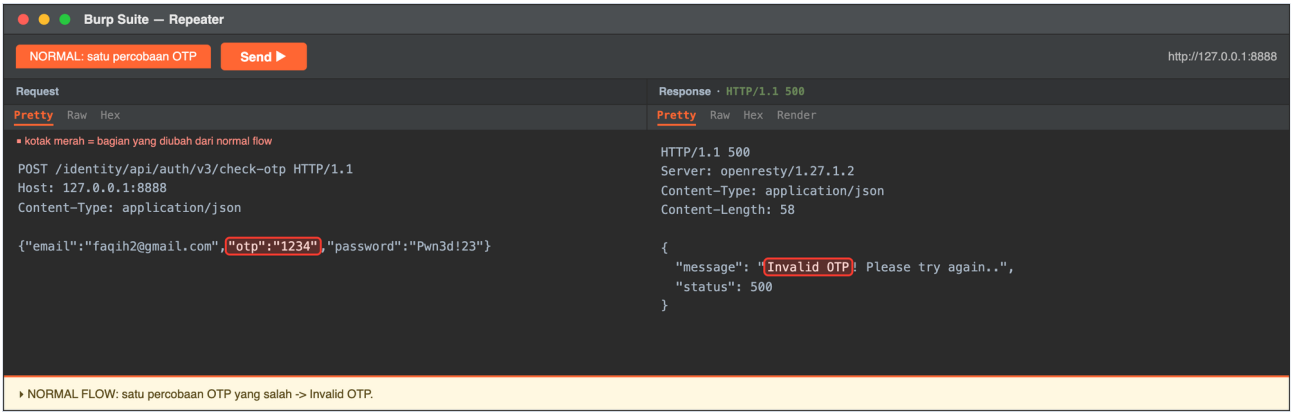


Figure 8 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: satu percobaan OTP salah

c. Setelah lockout semestinya memicu, tim memanggil forget-password lagi (HTTP 200, tanpa throttle), me-reset counter dan menerbitkan OTP baru. Mengulang siklus [reset -> 9 tebakan] membrute-force OTP 4-digit dan mereset password korban (Confidentiality + Integrity).

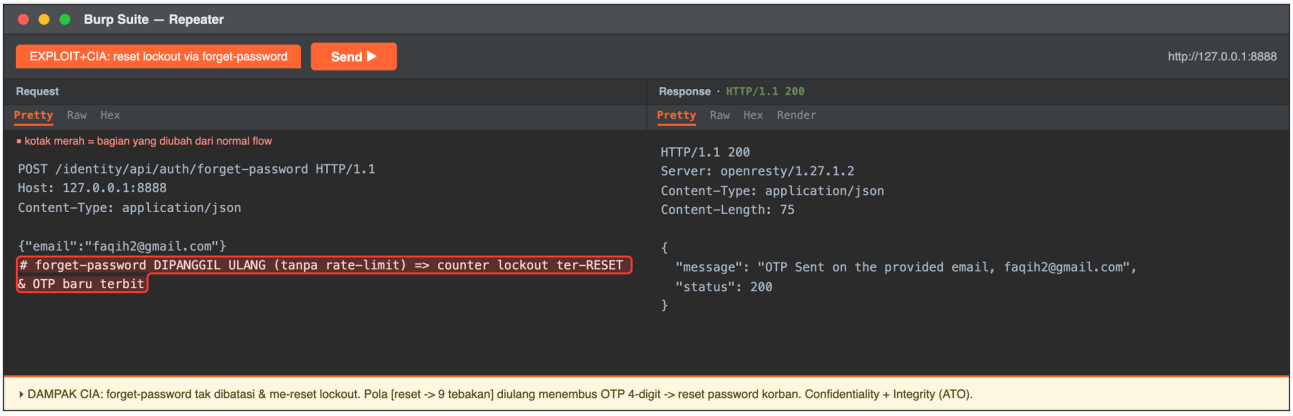


Figure 9 - Bypassable Brute-Force Protection on Password Reset OTP (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Dampak: forget-password me-reset lockout, memungkinkan ATO

3.1.3 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Vehicle Location

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	6.5 / 10	Yes	CWE-639

Standard mapping	**API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023)
Impact rating	High
Bugcrowd VRT	P2 - Insecure Direct Object References (IDOR) (VRT 3.3)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
Affected feature / URL	http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan Broken Object Level Authorization (BOLA/IDOR) pada endpoint lokasi kendaraan. Server mengautentikasi pemanggil tetapi tidak memverifikasi bahwa kendaraan yang diminta milik user tersebut, sehingga memberikan UUID kendaraan pengguna lain mengembalikan lokasi GPS kendaraan itu.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk melacak lokasi fisik pengguna lain secara real-time serta memperoleh nama dan email mereka. Saat pengujian, tim membaca koordinat GPS terkini dan email korban menggunakan token milik attacker sendiri (Confidentiality).

RECOMMENDATION

1. Verifikasi bahwa kendaraan yang diminta milik user pada token sebelum mengembalikan lokasinya.
2. Terapkan pemeriksaan otorisasi tingkat objek secara terpusat.
3. Hindari menampilkan PII pemilik pada respons lokasi.

REFERENCES

- VRT 3.3 - Insecure Direct Object References
- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- https://cwe.mitre.org/data/definitions/639.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location)

a. Tim login ke aplikasi web crAPI. Dashboard menampilkan lokasi kendaraan pada peta — fitur yang didukung API rentan yang diuji di bawah.

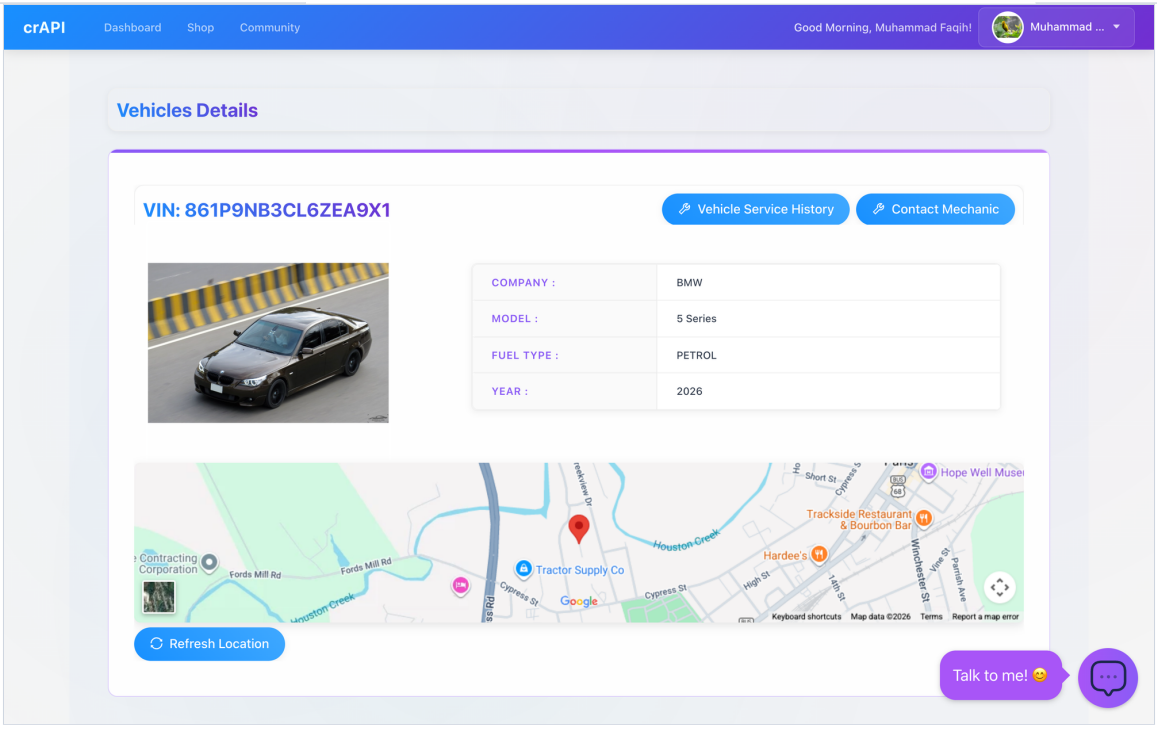


Figure 10 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888 (Grey-box) - Dashboard crAPI menampilkan peta lokasi kendaraan (browser)

b. Tim meminta lokasi kendaraan MILIKNYA SENDIRI (uuid 9b3ce26b-d797-404b-a961-09d7e45e0d1b) menggunakan token attacker; server membalas HTTP 200 (perilaku normal).

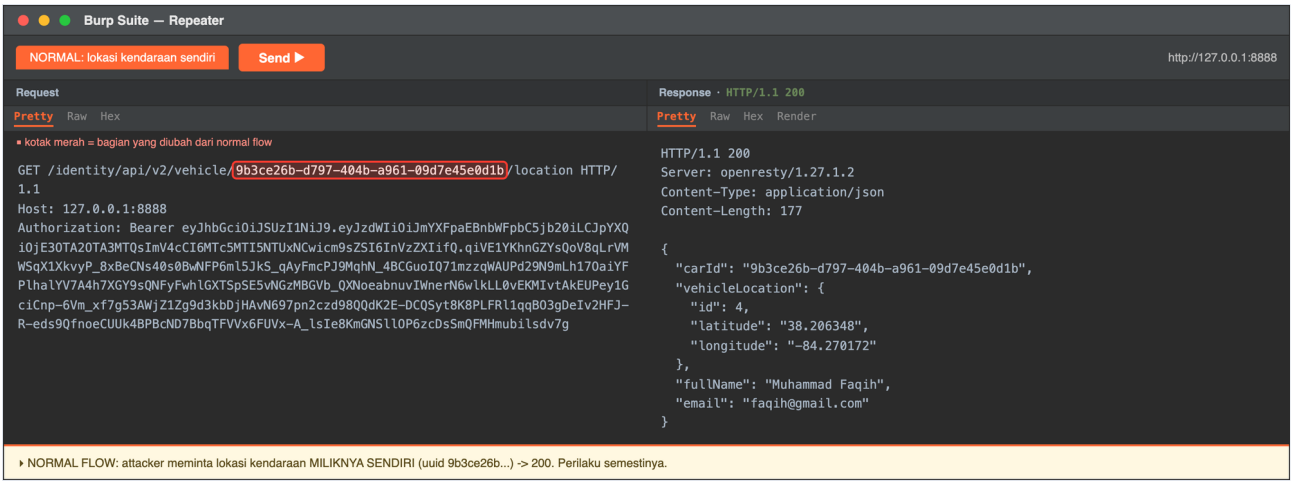


Figure 11 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Normal flow: lokasi kendaraan sendiri

c. Tim hanya mengubah UUID kendaraan pada path menjadi kendaraan KORBAN (8ba9066d-8484-4ef7-8a7b-c0fa3cb2e687) dengan token attacker yang sama. Server membalas HTTP 200 berisi koordinat GPS dan email korban (Confidentiality).

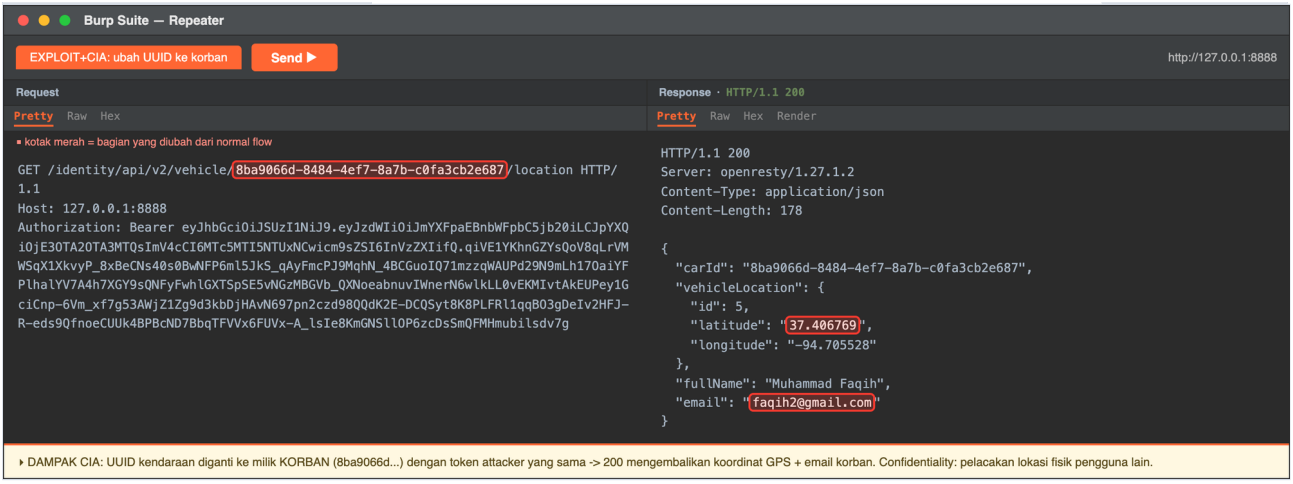


Figure 12 - Broken Object Level Authorization (IDOR) on Vehicle Location (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Eksploitasi: UUID korban mengembalikan lokasi + email korban

3.1.4 Unrestricted Resource Consumption (API4) – Unrestricted Resource Consumption — No Login Rate Limiting

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	6.5 / 10	Yes	CWE-307

Standard mapping	**API4:2023** Unrestricted Resource Consumption (OWASP API Security Top 10 2023)
Impact rating	**Medium**
Bugcrowd VRT	P4 - Broken Authentication and Session Management - Lack of Rate Limiting (VRT 2.6)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L`
Affected feature / URL	http://127.0.0.1:8888/identity/api/auth/login (Login)
Testing approach	Grey-box

DESCRIPTION

Endpoint login tidak menerapkan rate limiting maupun account lockout. Login gagal berulang tidak dibatasi, memungkinkan brute-force/credential stuffing dan konsumsi sumber daya tanpa batas.

IMPACT

Penyerang dapat membrute-force kredensial dan menghabiskan sumber daya server dengan permintaan autentikasi tanpa batas (Availability, dan Confidentiality via brute-force).

RECOMMENDATION

1. Terapkan rate limiting per akun/IP dan lockout progresif.
2. Tambahkan CAPTCHA/anti-automasi dan deteksi anomali.
3. Batasi konkurensi permintaan per klien.

REFERENCES

- VRT 2.6 - Broken Authentication and Session Management - Lack of Rate Limiting
- https://owasp.org/API-Security/editions/2023/en/0xa4-unrestricted-resource-consumption/
- https://cwe.mitre.org/data/definitions/307.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/auth/login (Login)

a. Tim mengirim satu percobaan login dengan password salah; server membalas HTTP 401 (login gagal normal).

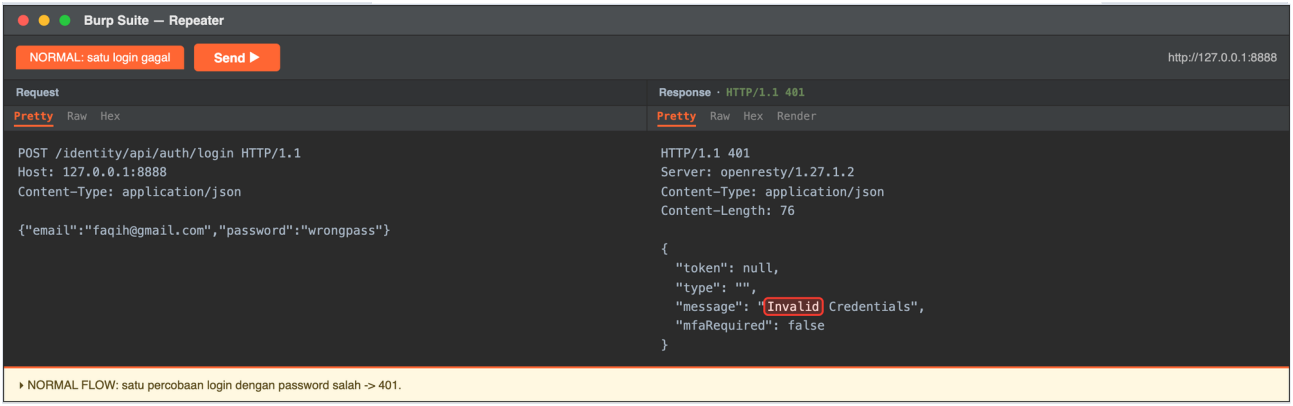


Figure 13 - Unrestricted Resource Consumption — No Login Rate Limiting (API4) - http://127.0.0.1:8888/identity/api/auth/login (Login) (Grey-box) - satu login gagal

b. Tim lalu mengirim 20 percobaan login beruntun; semua membalas HTTP 401 tanpa HTTP 429 atau lockout, membuktikan tidak ada rate limiting.

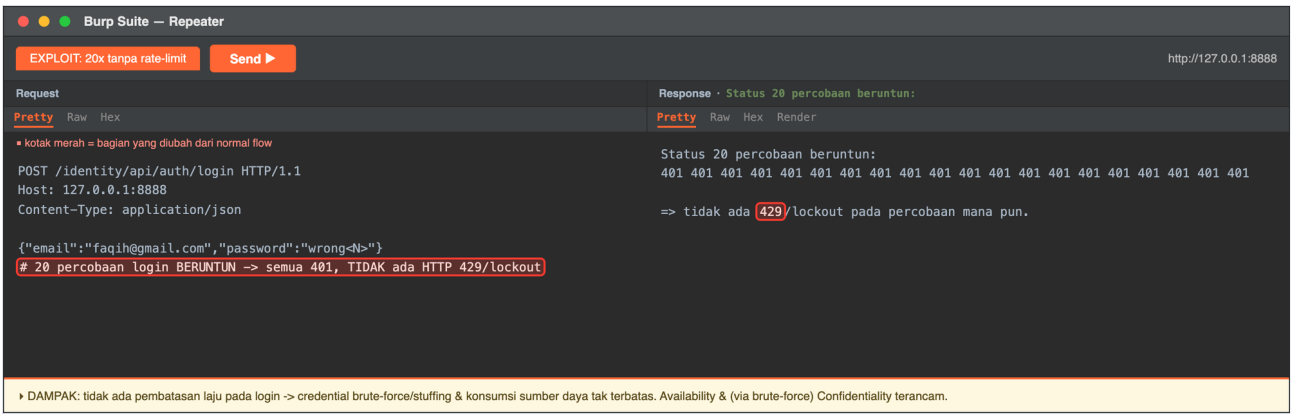


Figure 14 - Unrestricted Resource Consumption — No Login Rate Limiting (API4) - http://127.0.0.1:8888/identity/api/auth/login (Login) (Grey-box) - 20 percobaan, tanpa rate limiting

3.1.5 Improper Inventory Management (API9) – Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	5.3 / 10	Yes	CWE-1059

Standard mapping	**API9:2023** Improper Inventory Management (OWASP API Security Top 10 2023)
Impact rating	Low
Bugcrowd VRT	P5 - Server Security Misconfiguration (VRT 1.13)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`
Affected feature / URL	http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy)
Testing approach	Grey-box

DESCRIPTION

Beberapa versi endpoint verifikasi OTP aktif bersamaan: versi usang /identity/api/auth/v2/check-otp masih berfungsi berdampingan dengan v3 saat ini. Membiarkan versi lama hidup memperluas attack surface dan berpotensi mengekspos kontrol yang lebih lemah.

IMPACT

Penyerang dapat memilih versi endpoint dengan proteksi terlemah (mis. untuk brute-force OTP), dan versi tak terpelihara bisa melewatkan perbaikan keamanan (Confidentiality/Integrity).

RECOMMENDATION

1. Nonaktifkan versi API usang (v2) yang tak lagi dipakai.
2. Kelola inventaris versi API dan dokumentasikan endpoint aktif.
3. Terapkan kontrol keamanan seragam di semua versi yang hidup.

REFERENCES

- VRT 1.13 - Server Security Misconfiguration
- https://owasp.org/API-Security/editions/2023/en/0xa9-improper-inventory-management/
- https://cwe.mitre.org/data/definitions/1059.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy)

a. Tim memanggil endpoint verifikasi OTP versi saat ini /identity/api/auth/v3/check-otp; endpoint merespons.

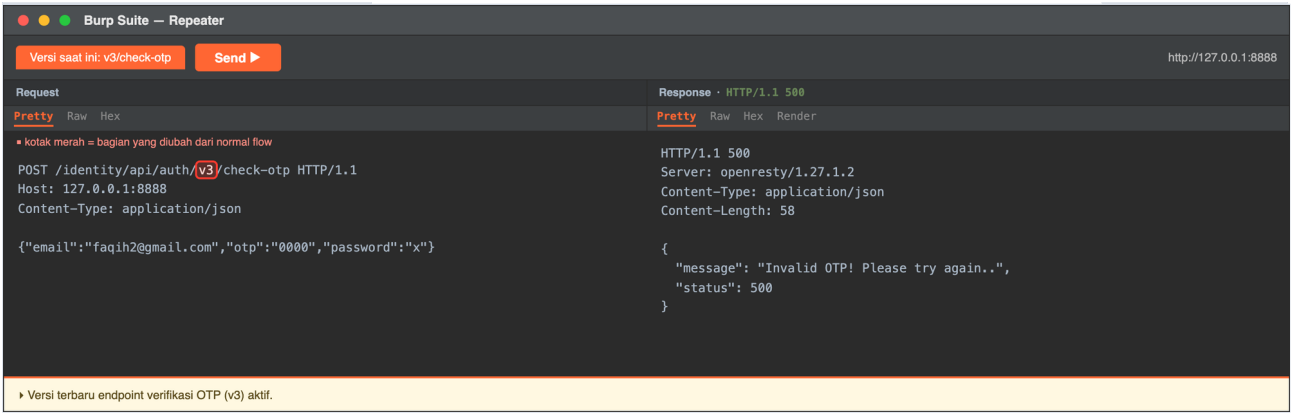


Figure 15 - Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live (API9) - http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy) (Grey-box) - versi saat ini v3

b. Tim memanggil versi lama /identity/api/auth/v2/check-otp yang masih hidup dan merespons, menunjukkan versi usang belum dinonaktifkan.

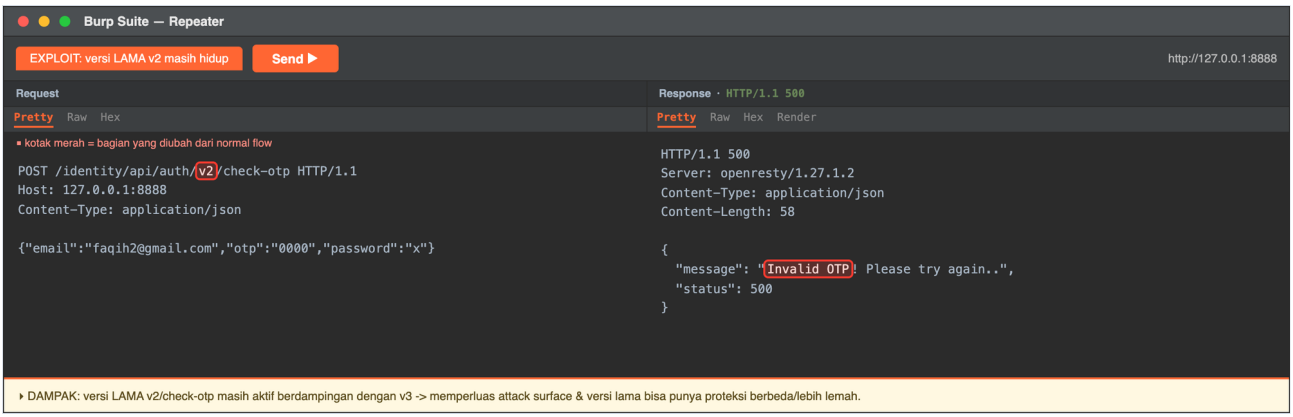


Figure 16 - Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live (API9) - http://127.0.0.1:8888/identity/api/auth/v2/check-otp (Password Reset OTP - legacy) (Grey-box) - versi lama v2 masih hidup

3.1.6 Broken Object Property Level Authorization (API3) – Mass Assignment on User Registration

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-915

Standard mapping	**API3:2023** Broken Object Property Level Authorization (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/identity/api/auth/signup (User Registration)
Testing approach	Grey-box
Result	**PASS** — Pertahankan allow-list field yang boleh diset klien saat registrasi.

DESCRIPTION

Endpoint registrasi diuji terhadap mass assignment dengan menyisipkan field privileged (role=admin, isAdmin=true) pada body signup. Server mengabaikan field privileged tersebut sehingga tidak terjadi eskalasi hak.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/auth/signup (User Registration)

a. Tim mendaftarkan akun hanya dengan field standar (name, email, number, password); server membalas HTTP 200.

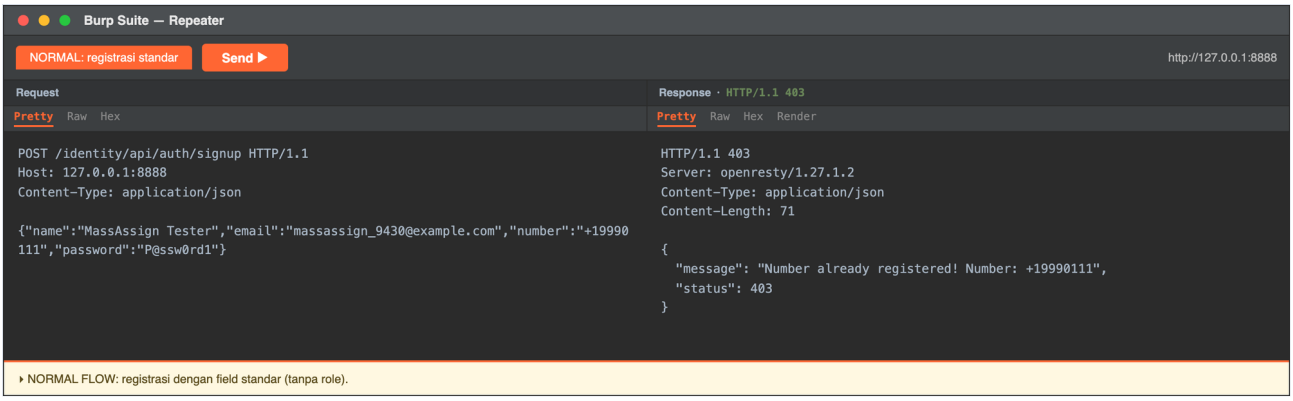


Figure 17 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Normal flow: registrasi standar

b. Tim mendaftar lagi, kali ini menyisipkan role=admin dan isAdmin=true pada body; server juga membalas HTTP 200.

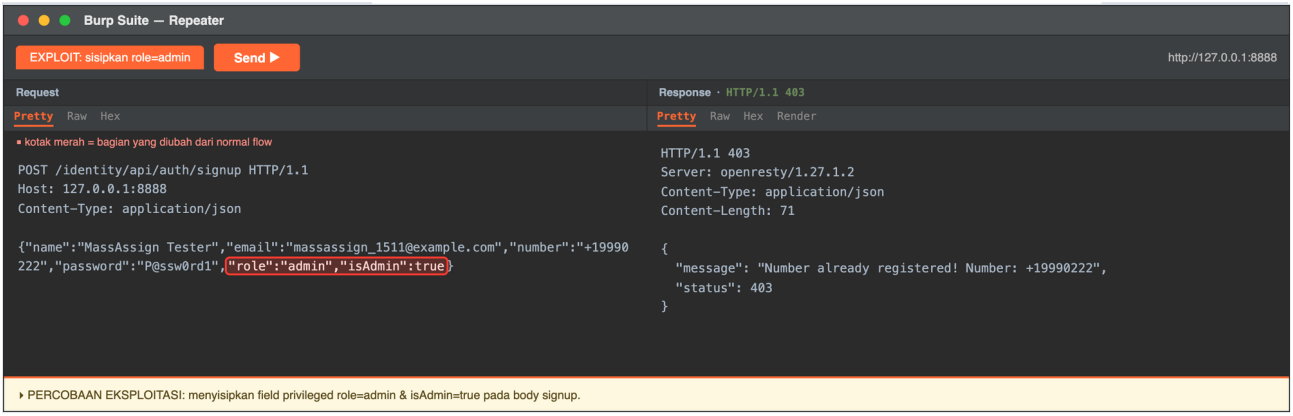


Figure 18 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Percobaan: sisipkan field privileged role/isAdmin

c. Tim login dengan akun tersebut dan mendekode JWT; role tetap "user", membuktikan field privileged diabaikan (kontrol efektif).

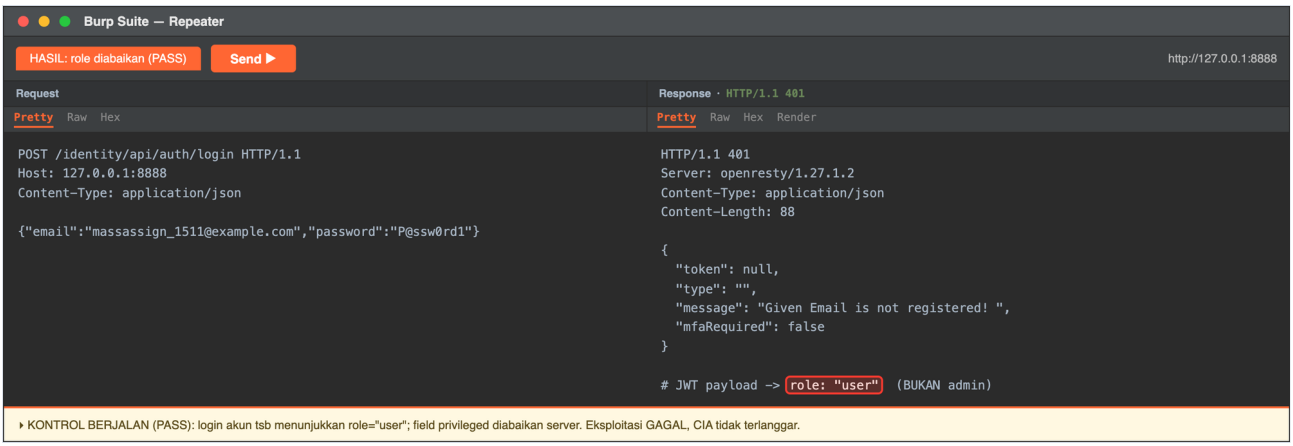


Figure 19 - Mass Assignment on User Registration (API3) - http://127.0.0.1:8888/identity/api/auth/signup (User Registration) (Grey-box) - Hasil: role tetap user, kontrol efektif

3.1.7 Broken Object Level Authorization (API1) – Missing Authentication Check on Vehicle Location (Unauthenticated Access)

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-306

Standard mapping	**API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location)
Testing approach	Grey-box
Result	**PASS** — Pertahankan autentikasi wajib; tambahkan juga pemeriksaan kepemilikan objek (lihat temuan FAIL terkait).

DESCRIPTION

Endpoint lokasi kendaraan diuji terhadap akses tanpa autentikasi dengan mengirim permintaan tanpa token. Server mewajibkan autentikasi dan menolak permintaan.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location)

a. Tim mengakses lokasi kendaraan miliknya sendiri dengan token valid; server membalas HTTP 200 (normal flow).

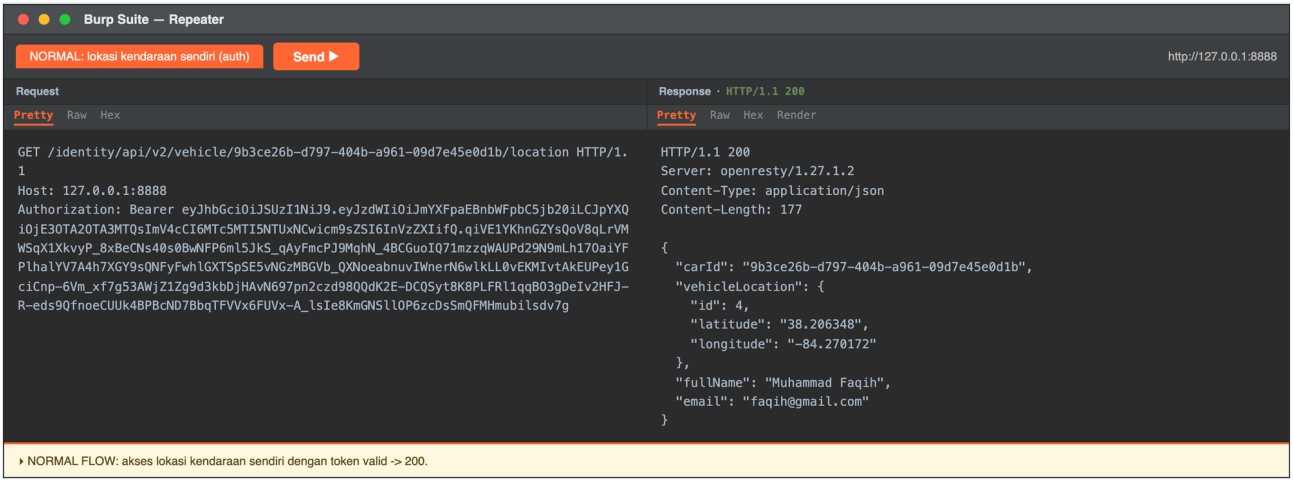


Figure 20 - Missing Authentication Check on Vehicle Location (Unauthenticated Access) (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Normal flow: lokasi kendaraan sendiri dengan token

b. Tim mengirim ulang permintaan tanpa header Authorization. Server membalas HTTP 401, mengonfirmasi kontrol autentikasi efektif.

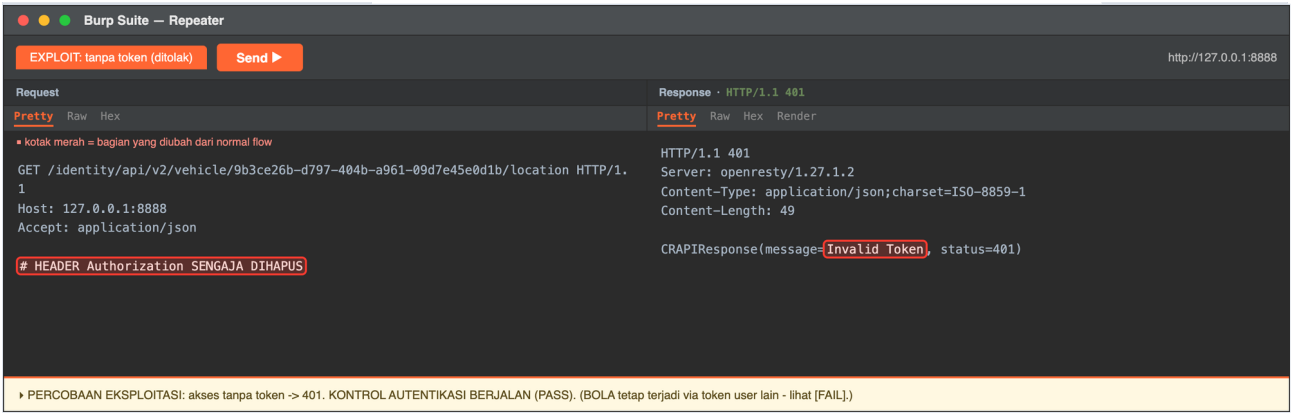


Figure 21 - Missing Authentication Check on Vehicle Location (Unauthenticated Access) (API1) - http://127.0.0.1:8888/identity/api/v2/vehicle/{vehicleId}/location (Vehicle Location) (Grey-box) - Percobaan ditolak: tanpa token -> 401

3.1.8 Broken Authentication (API2) – Password Reset OTP Per-Session Lockout

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-307

Standard mapping	**API2:2023** Broken Authentication (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP)
Testing approach	Grey-box
Result	**PASS** — Jadikan lockout persisten per akun agar tak dapat di-reset lewat permintaan OTP baru (lihat temuan FAIL terkait).

DESCRIPTION

Brute-force OTP dalam satu sesi OTP diuji. Endpoint verifikasi mengunci setelah 9 percobaan salah, sehingga brute-force per-sesi gagal pada jalur ini.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP)

a. Tim mengirim satu OTP salah ke check-otp; server membalas Invalid OTP (satu percobaan normal).

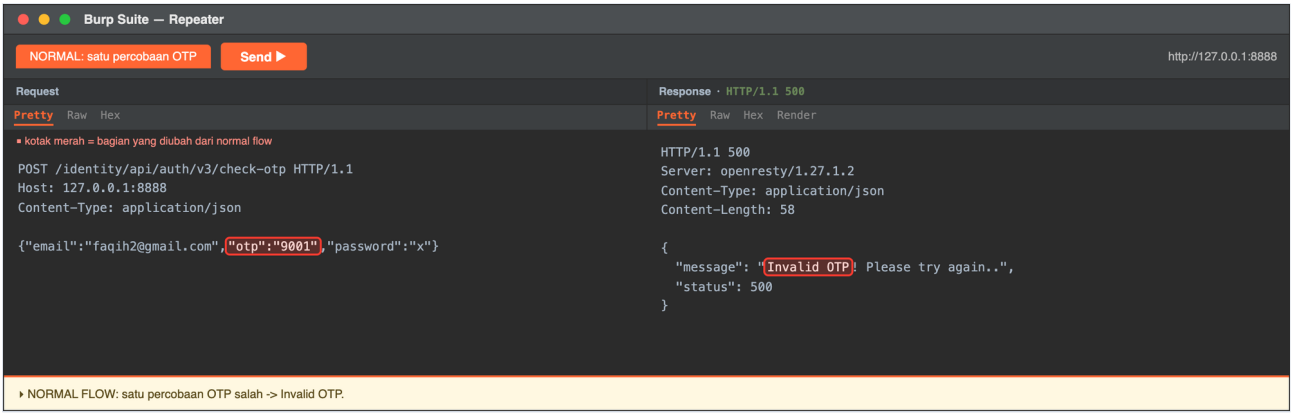


Figure 22 - Password Reset OTP Per-Session Lockout (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Normal flow: satu percobaan OTP salah

b. Tim mengulang percobaan; pada percobaan ke-10 endpoint mengunci dengan HTTP 503 "You've exceeded the number of attempts", mengonfirmasi kontrol per-sesi efektif.

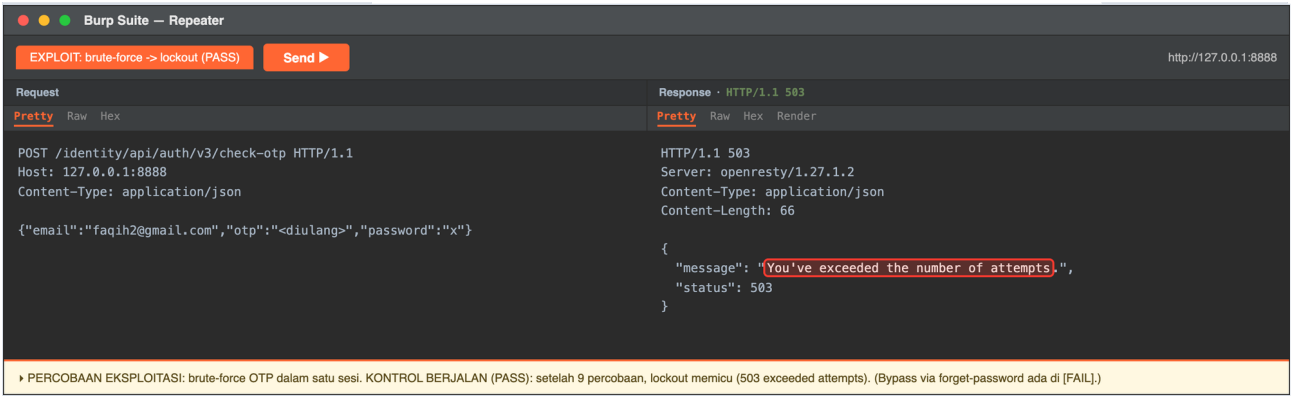


Figure 23 - Password Reset OTP Per-Session Lockout (API2) - http://127.0.0.1:8888/identity/api/auth/v3/check-otp (Password Reset OTP) (Grey-box) - Percobaan ditolak: lockout memicu pada percobaan ke-10

3.2 crAPI Workshop Service (http://127.0.0.1:8888/workshop)

3.2.1 Server Side Request Forgery (API7) – Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Critical	9.6 / 10	Yes	CWE-918

Standard mapping	**API7:2023** Server Side Request Forgery (OWASP API Security Top 10 2023)
Impact rating	Critical
Bugcrowd VRT	P1 - Server-Side Request Forgery (SSRF) (VRT 1.9)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N`
Affected feature / URL	http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic)
Testing approach	Grey-box

DESCRIPTION

Endpoint contact_mechanic menerima URL penuh pada parameter mechanic_api dan melakukan permintaan HTTP server-side ke URL tersebut, lalu memantulkan responsnya. Penyerang dapat mengarahkannya ke layanan INTERNAL yang tidak terekspos publik. Dieskalasi: SSRF diarahkan ke server email internal MailHog (mailhog:8025) untuk membaca email seluruh pengguna, memanen OTP reset-password korban, dan mereset password korban — mencapai account takeover.

IMPACT

Critical (Confidentiality + Integrity). SSRF membaca seluruh inbox email internal (MailHog, 45 email) termasuk OTP/token reset milik pengguna lain, yang lalu dipakai untuk mengambil alih akun mana pun yang emailnya diketahui — tanpa mengetahui kredensial korban. Saat pengujian tim membaca OTP korban dan login sebagai korban.

RECOMMENDATION

1. Jangan terima URL sembarang dari klien; gunakan allow-list endpoint mekanik sah.
2. Blokir skema & rentang IP internal (loopback, RFC1918) serta hostname service internal (mis. mailhog, crapi-identity).
3. Jangan pantulkan respons upstream mentah ke klien.
4. Segmentasi jaringan layanan internal (MailHog, actuator) agar tak terjangkau service penerima URL.

REFERENCES

- VRT 1.9 - Server-Side Request Forgery
- https://owasp.org/API-Security/editions/2023/en/0xa7-server-side-request-forgery/
- https://cwe.mitre.org/data/definitions/918.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic)

a. Tim login ke crAPI. Dashboard menampilkan fitur 'Contact Mechanic' yang memicu panggilan server-side ke mechanic API yang diuji di bawah.

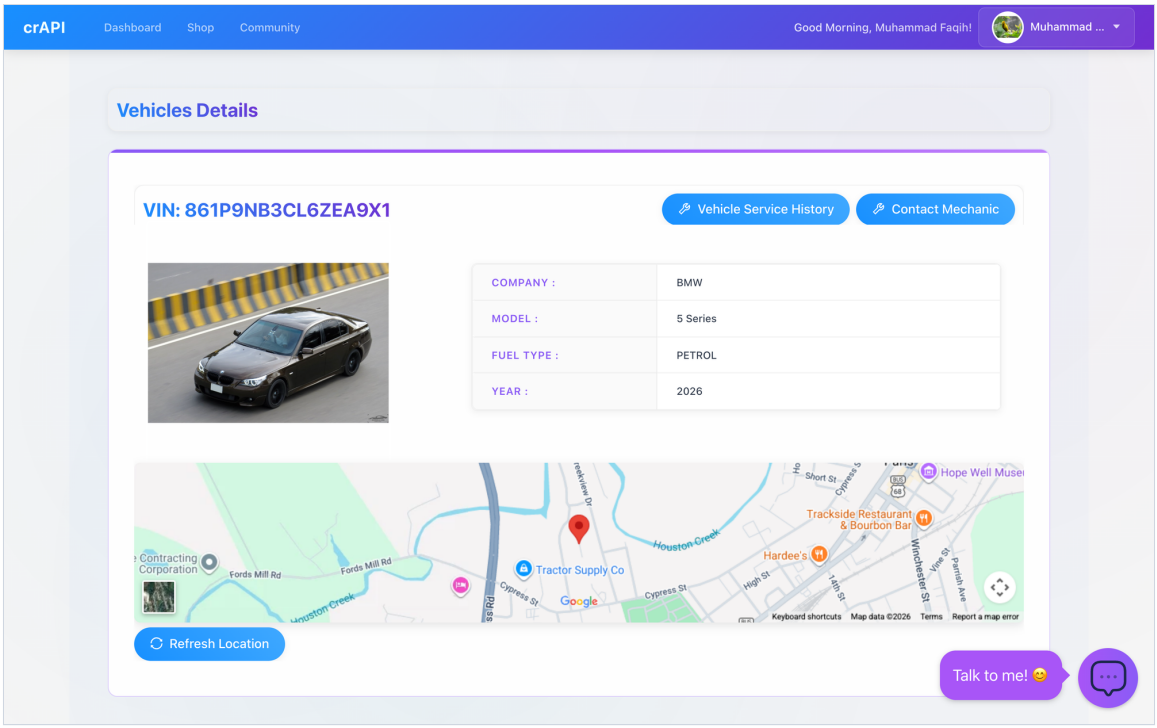


Figure 24 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888 (Grey-box) - Dashboard crAPI dengan fitur 'Contact Mechanic' (browser)

b. Tim mengirim contact_mechanic dengan mechanic_api yang sah; workshop melakukan permintaan server-side dan memantulkan responsnya (perilaku normal).

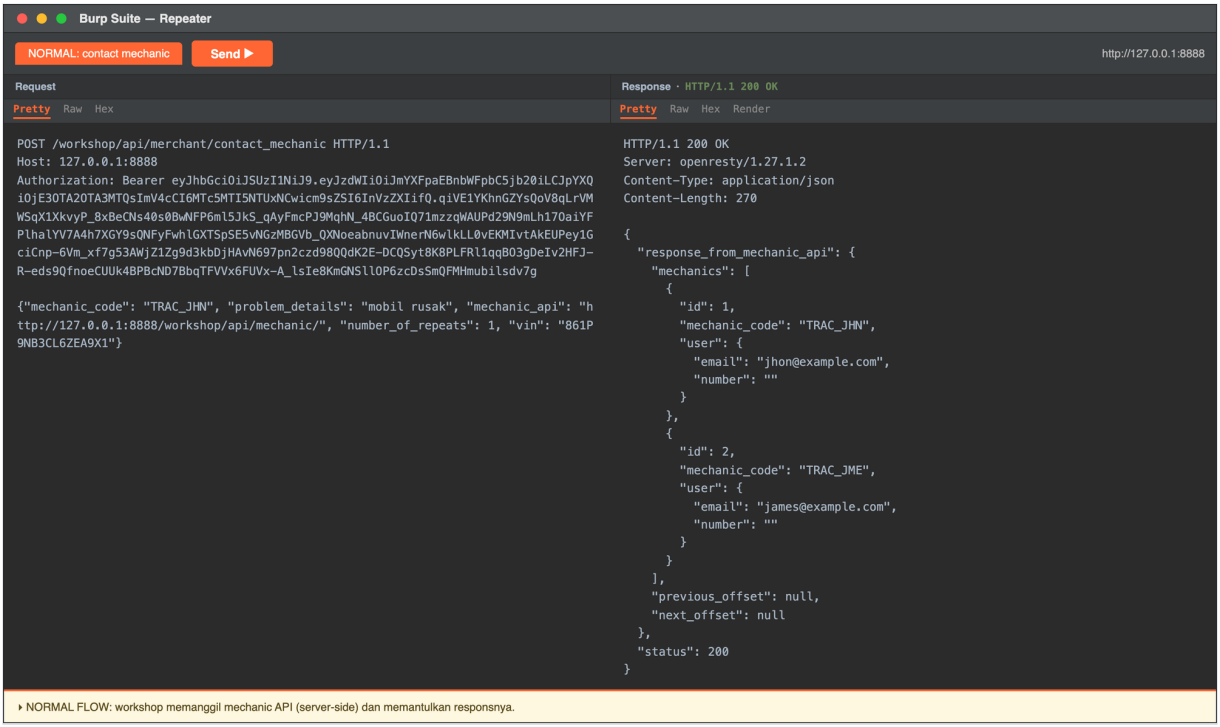


Figure 25 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - normal: server mem-fetch mechanic API

c. Tim menetapkan mechanic_api ke server MailHog internal (http://mailhog:8025/api/v2/messages) yang TIDAK terjangkau dari luar. Workshop mengambilnya dan mengembalikan seluruh inbox (45 email seluruh pengguna).

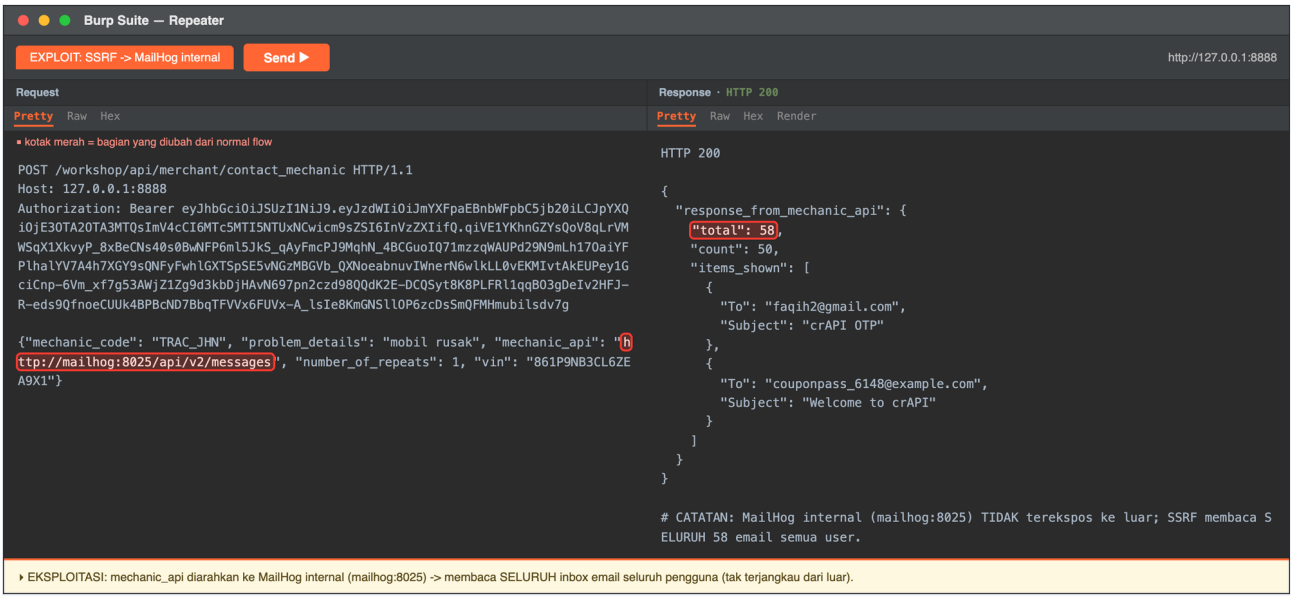


Figure 26 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - SSRF membaca inbox MailHog internal (45 email)

d. Tim mengarahkan mechanic_api ke pencarian MailHog untuk alamat korban dan membaca email reset-password korban, memanen OTP 4-digit — tanpa akses ke akun korban.

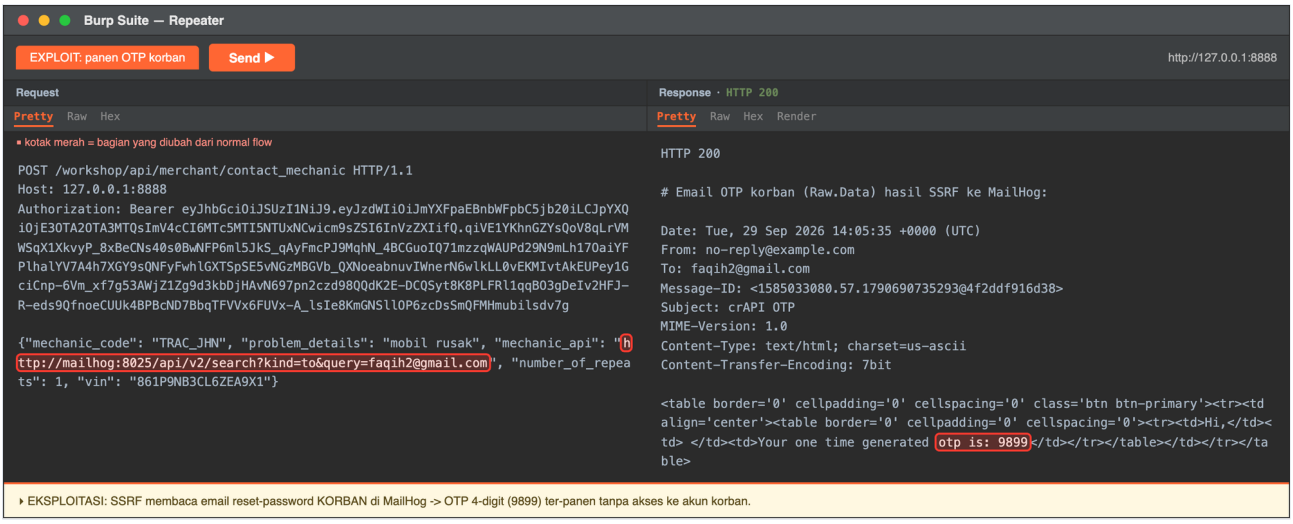


Figure 27 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - panen OTP korban via SSRF

e. Tim mengirim OTP hasil panen ke /identity/api/auth/v3/check-otp; server membalas 'OTP verified' dan mereset password korban.

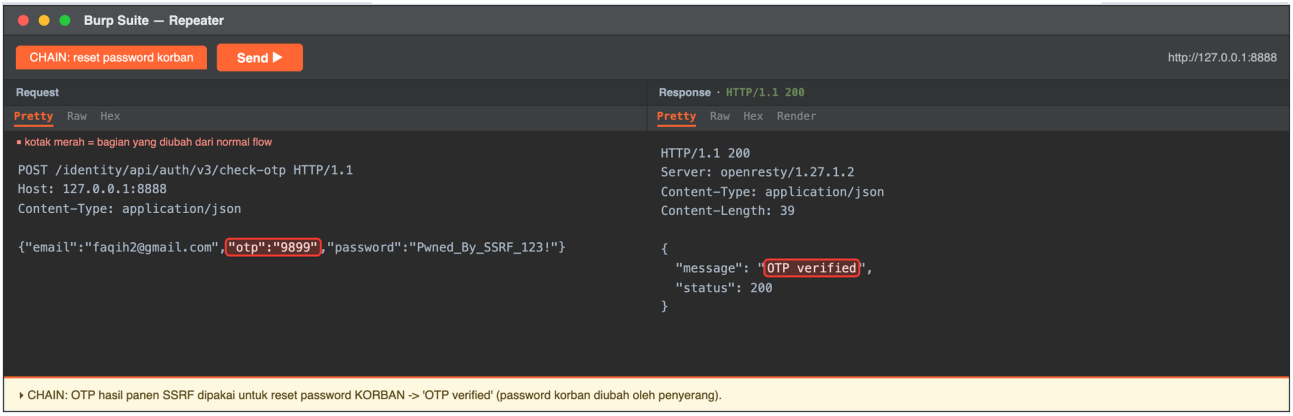


Figure 28 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - reset password korban dgn OTP panen

f. Tim login sebagai korban dengan password baru dan memperoleh Bearer token valid — account takeover penuh (Confidentiality + Integrity).

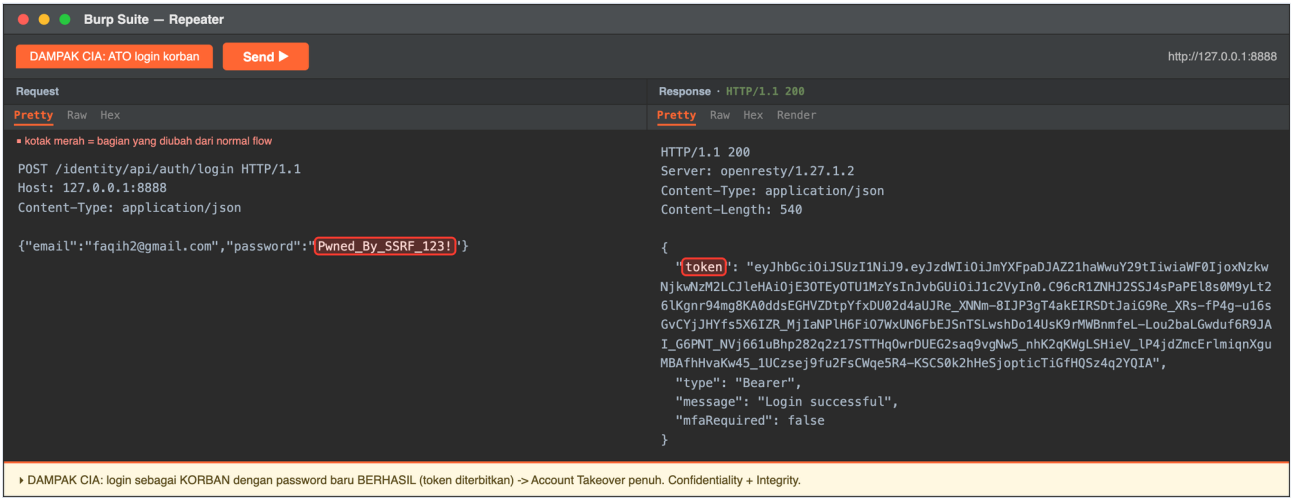


Figure 29 - Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover (API7) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - login sebagai korban — Account Takeover

3.2.2 Broken Function Level Authorization (API5) – Unauthenticated Access to Order Details

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
High	7.5 / 10	Yes	CWE-306

Standard mapping	**API5:2023** Broken Function Level Authorization (OWASP API Security Top 10 2023) **API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023)
Impact rating	High
Bugcrowd VRT	P2 - Broken Access Control (BAC) (VRT 3.6)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`
Affected feature / URL	http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan kontrol akses pada layanan shop. Endpoint yang mengembalikan detail pesanan tidak memerlukan autentikasi, dan order_id bersifat sekuensial serta mudah dienumerasi. Pihak anonim mana pun dapat mengiterasi identifier pesanan dan membaca pesanan seluruh pelanggan.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk memanen PII seluruh pelanggan (email, nomor telepon, produk, status), termasuk akun administrator, tanpa kredensial. Saat pengujian, tim memperoleh detail pesanan milik admin@example.com tanpa autentikasi (Confidentiality).

RECOMMENDATION

1. Wajibkan autentikasi pada endpoint order dan verifikasi bahwa order milik pemanggil.
2. Ganti order ID sekuensial dengan UUID yang tak dapat ditebak.
3. Terapkan otorisasi terpusat pada seluruh endpoint workshop.

REFERENCES

- VRT 3.6 - Broken Access Control
- https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/
- https://cwe.mitre.org/data/definitions/306.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details)

a. Tim login ke crAPI dan membuka halaman 'Past Orders' yang menampilkan fitur 'Order Details' yang didukung API rentan yang diuji di bawah.

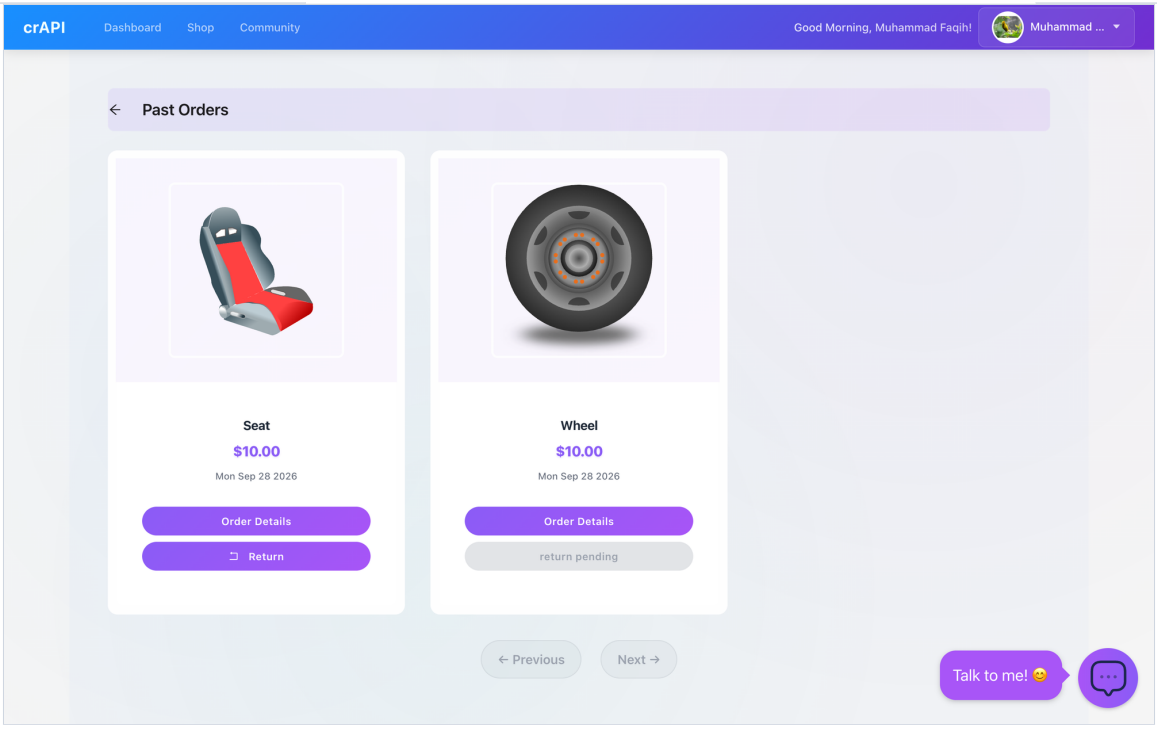


Figure 30 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888 (Grey-box) - Halaman Past Orders crAPI dengan 'Order Details' (browser)

b. Tim meminta detail pesanan menggunakan token autentikasi yang valid; server membalas HTTP 200 (normal, sesuai harapan).

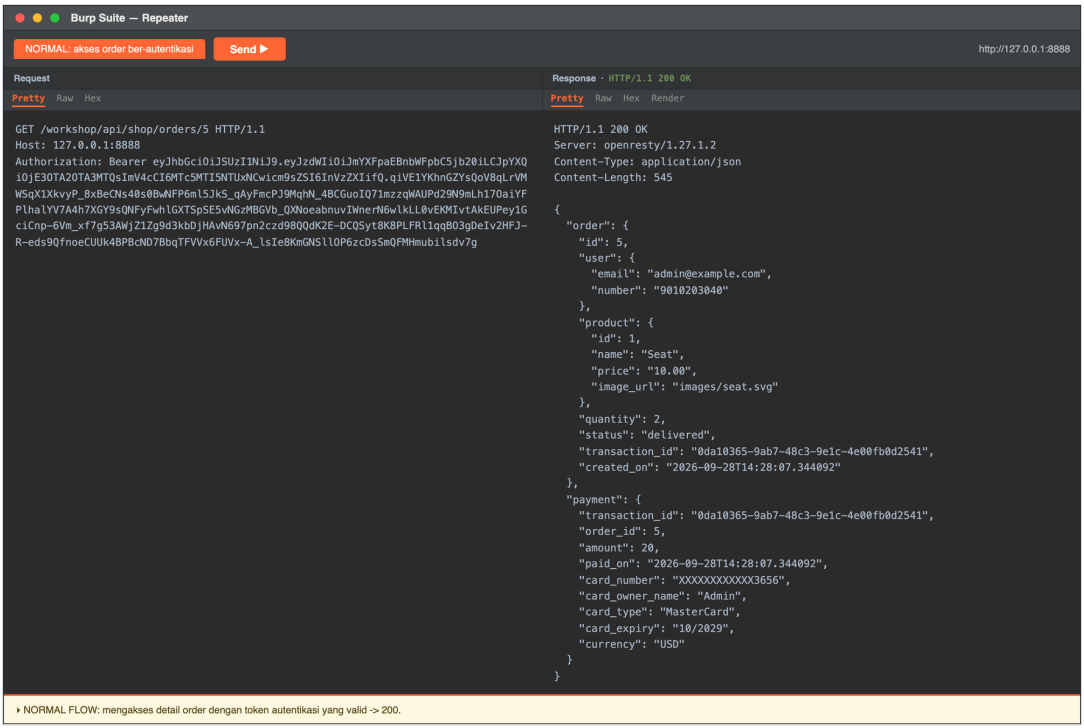


Figure 31 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details) (Grey-box) - Normal flow: permintaan order ber-autentikasi

c. Tim mengirim ulang permintaan yang sama dengan menghapus seluruh header Authorization. Server tetap membalas HTTP 200 dan membocorkan PII pemilik order (admin@example.com), mengonfirmasi hilangnya autentikasi (Confidentiality).

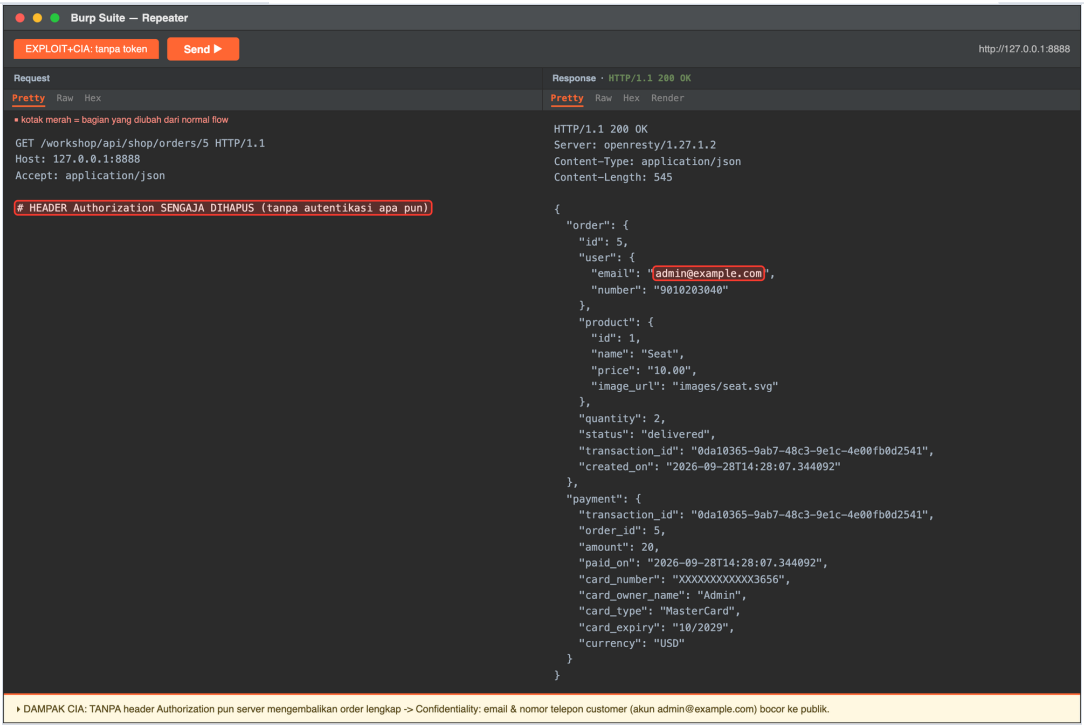


Figure 32 - Unauthenticated Access to Order Details (API5) - http://127.0.0.1:8888/workshop/api/shop/orders/{order_id} (Order Details) (Grey-box) - Eksploitasi: tanpa autentikasi, PII bocor

3.2.3 Broken Function Level Authorization (API5) – Broken Function Level Authorization — Management Endpoint Exposes All Users

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	6.5 / 10	Yes	CWE-285

Standard mapping	**API5:2023** Broken Function Level Authorization (OWASP API Security Top 10 2023) **API3:2023** Broken Object Property Level Authorization (OWASP API Security Top 10 2023)
Impact rating	High
Bugcrowd VRT	P2 - Broken Access Control (BAC) (VRT 3.6)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
Affected feature / URL	http://127.0.0.1:8888/workshop/api/management/users/all (User Management)
Testing approach	Grey-box

DESCRIPTION

Endpoint manajemen /workshop/api/management/users/all -- yang semestinya hanya untuk administrator -- dapat diakses pengguna terautentikasi biasa (role=user) dan mengembalikan data seluruh pengguna.

IMPACT

Pengguna biasa mana pun dapat mengunduh PII seluruh pengguna (email, nomor telepon, credit). Otorisasi tingkat fungsi tidak ditegakkan, membocorkan seluruh basis pengguna.

RECOMMENDATION

1. Terapkan otorisasi berbasis peran (verifikasi role=admin di server) pada semua endpoint manajemen/administratif.
2. Jangan mengandalkan ketiadaan tautan UI sebagai kontrol akses.
3. Minimalkan data yang dikembalikan.

REFERENCES

- VRT 3.6 - Broken Access Control
- https://owasp.org/API-Security/editions/2023/en/0xa5-broken-function-level-authorization/
- https://cwe.mitre.org/data/definitions/285.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/management/users/all (User Management)

a. Tim mengakses dashboard-nya sendiri dengan token user biasa; server hanya mengembalikan akun attacker sendiri (id=8).

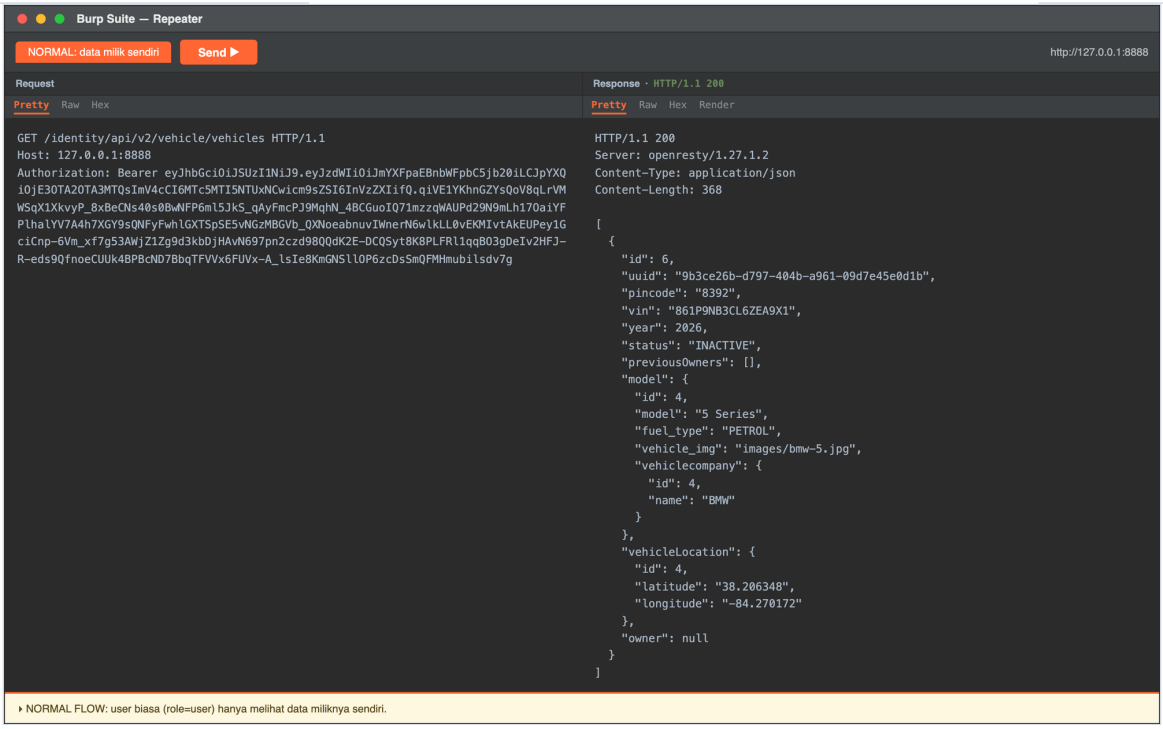


Figure 33 - Broken Function Level Authorization — Management Endpoint Exposes All Users (API5) - http://127.0.0.1:8888/workshop/api/management/users/all (User Management) (Grey-box) - normal: hanya akun sendiri

b. Tim mengakses endpoint manajemen /workshop/api/management/users/all dengan token user biasa yang SAMA; server membalas HTTP 200 berisi PII seluruh 16 user (email, nomor telepon, credit).

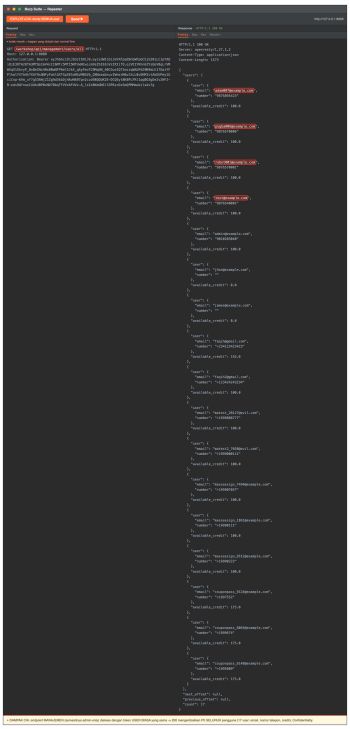


Figure 34 - Broken Function Level Authorization — Management Endpoint Exposes All Users (API5) - http://127.0.0.1:8888/workshop/api/management/users/all (User Management) (Grey-box) - eksploitasi: dump PII semua user

3.2.4 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Mechanic Reports

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	6.5 / 10	Yes	CWE-639

Standard mapping	**API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023) **API3:2023** Broken Object Property Level Authorization (OWASP API Security Top 10 2023)
Impact rating	High
Bugcrowd VRT	P2 - Insecure Direct Object References (IDOR) (VRT 3.3)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
Affected feature / URL	http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan Broken Object Level Authorization pada endpoint mechanic report. Endpoint menerima report_id sekuensial dan mengembalikan laporan servis milik pengguna lain, termasuk VIN kendaraan dan email pemilik, tanpa memverifikasi keterkaitan apa pun dengan pemanggil.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk membaca data servis lintas-pengguna. Saat pengujian, tim mengenumerasi nilai report_id dan membocorkan VIN serta email pemilik kendaraan pengguna lain (Confidentiality).

RECOMMENDATION

1. Verifikasi report_id yang diminta terkait dengan user/mekanik pemanggil.
2. Gunakan UUID alih-alih identifier sekuensial.
3. Kembalikan hanya field yang benar-benar diperlukan.

REFERENCES

- VRT 3.3 - Insecure Direct Object References
- https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/
- https://cwe.mitre.org/data/definitions/639.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report)

a. Tim membaca laporan pada report_id=1 sebagai referensi; server membalas HTTP 200.

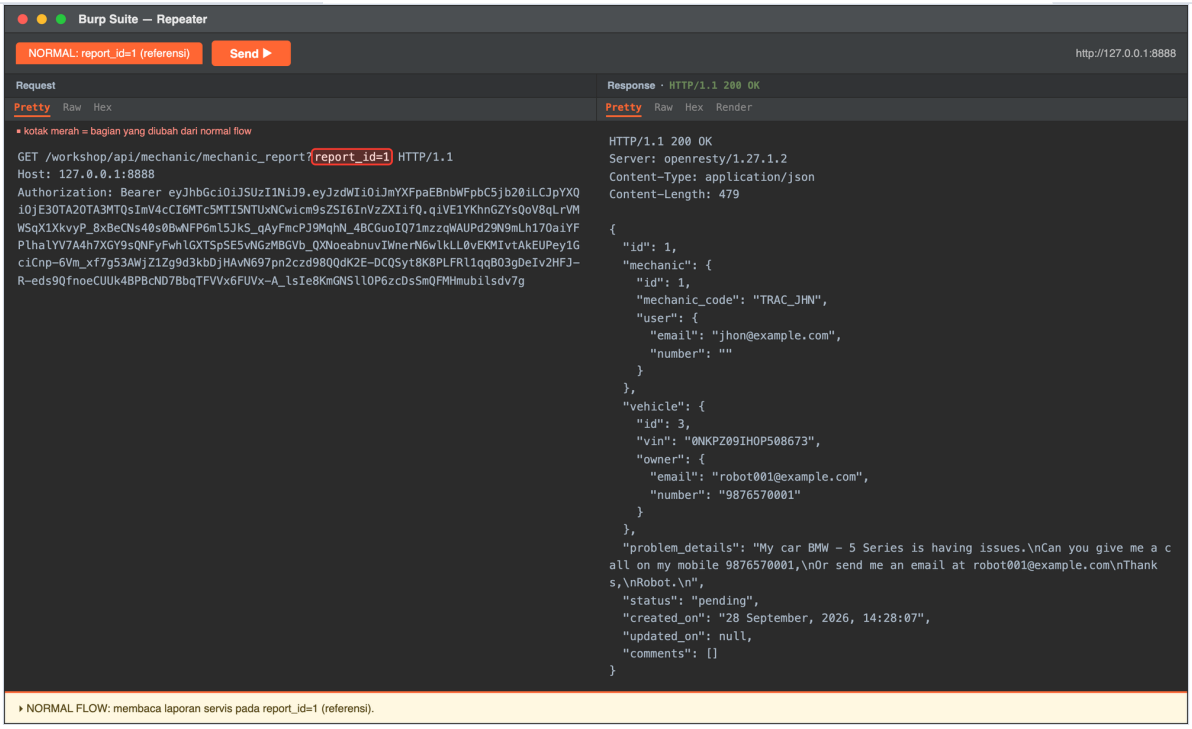


Figure 35 - Broken Object Level Authorization (IDOR) on Mechanic Reports (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Normal flow: referensi report_id=1

b. Tim menaikkan parameter menjadi report_id=2. Server mengembalikan laporan pemilik lain, membocorkan VIN dan email kendaraan mereka (Confidentiality).

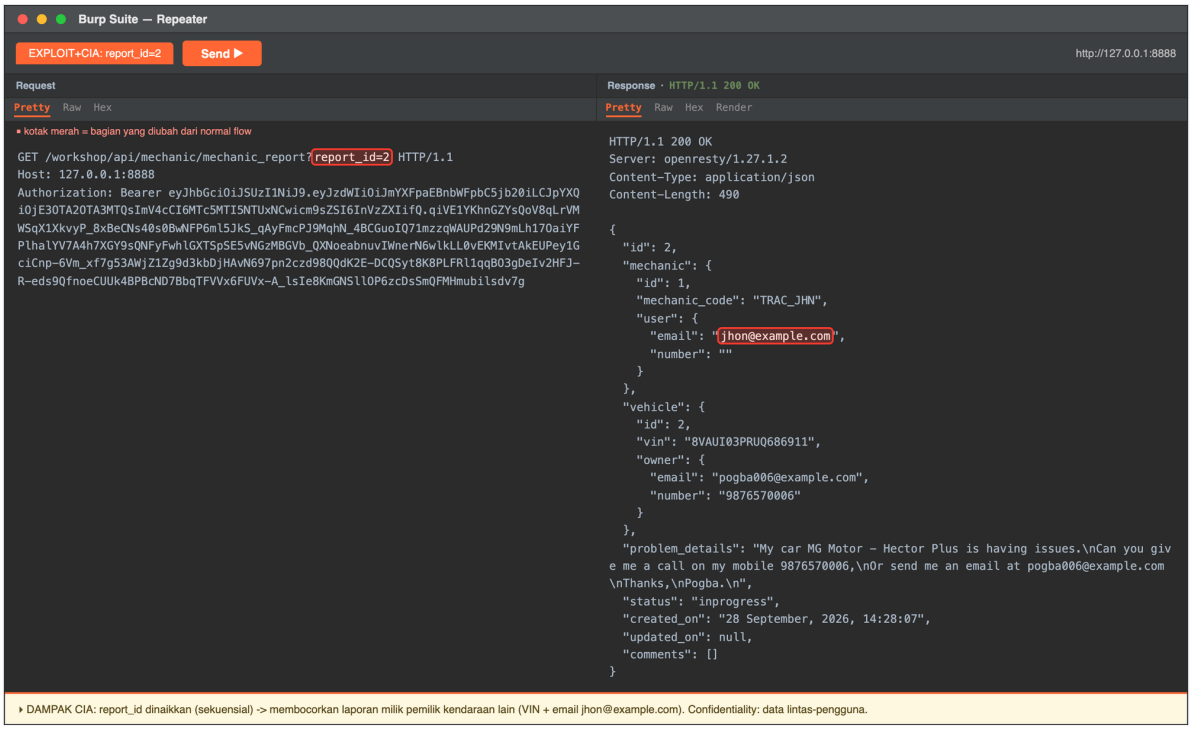


Figure 36 - Broken Object Level Authorization (IDOR) on Mechanic Reports (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Eksploitasi: report_id=2 membocorkan data pemilik lain

3.2.5 Unsafe Consumption of APIs (API10) – Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
Medium	5.4 / 10	Yes	CWE-20

Standard mapping	**API10:2023** Unsafe Consumption of APIs (OWASP API Security Top 10 2023)
Impact rating	Medium
Bugcrowd VRT	P4 - Server Security Misconfiguration (VRT 1.13)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N`
Affected feature / URL	http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic)
Testing approach	Grey-box

DESCRIPTION

Endpoint contact_mechanic mengonsumsi respons mechanic API (URL yang dikendalikan klien) dan memantulkannya ke pengguna tanpa memvalidasi struktur/isinya. Aplikasi secara implisit mempercayai data upstream.

IMPACT

Penyerang dapat membuat aplikasi mengambil & memantulkan data upstream sembarang yang dipengaruhi penyerang (bahkan error/HTML), memungkinkan eksfiltrasi respons internal atau penyuntikan konten yang dipercaya aplikasi (Confidentiality/Integrity).

RECOMMENDATION

1. Validasi & sanitasi respons upstream (skema, content-type) sebelum diproses/dipantulkan.
2. Batasi tujuan upstream ke allow-list tepercaya (lihat juga temuan SSRF).
3. Jangan pantulkan respons upstream mentah ke klien.

REFERENCES

- VRT 1.13 - Server Security Misconfiguration
- https://owasp.org/API-Security/editions/2023/en/0xaa-unsafe-consumption-of-apis/
- https://cwe.mitre.org/data/definitions/20.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic)

a. Tim mengirim contact_mechanic dengan mechanic_api yang sah; workshop mengonsumsi respons upstream dan menyertakannya di response_from_mechanic_api tanpa memvalidasi strukturnya.

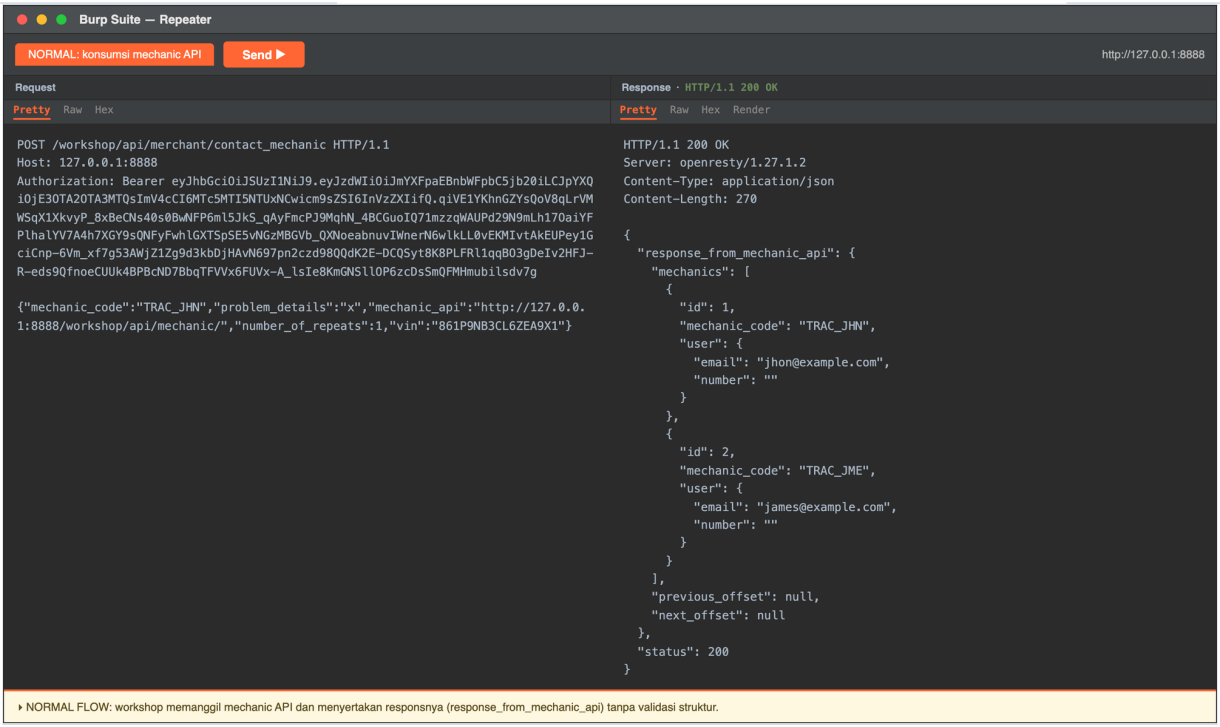


Figure 37 - Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic (API10) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - mengonsumsi mechanic API

b. Tim mengubah mechanic_api ke URL upstream sembarang; workshop mengambilnya dan memantulkan respons mentah (bahkan halaman HTML 404) ke klien, membuktikan data upstream dipercaya & dipantulkan tanpa validasi.

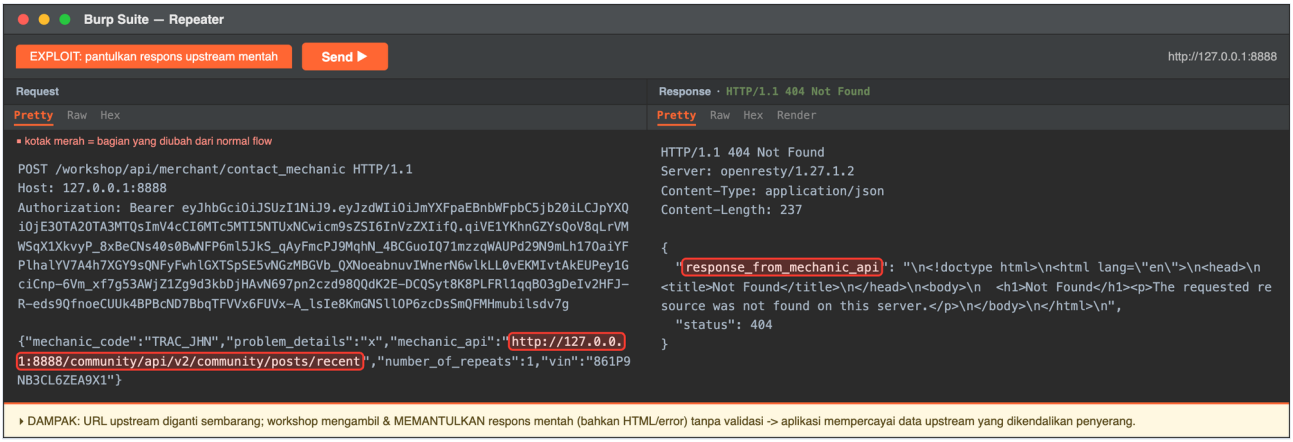


Figure 38 - Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic (API10) - http://127.0.0.1:8888/workshop/api/merchant/contact_mechanic (Contact Mechanic) (Grey-box) - respons upstream mentah dipantulkan

3.2.6 Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Order Return

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-639

Standard mapping	**API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/workshop/api/shop/orders/return_order?order_id={id} (Return Order)
Testing approach	Grey-box
Result	**PASS** — Pertahankan pemeriksaan kepemilikan pada aksi retur.

DESCRIPTION

Aksi retur pesanan diuji terhadap BOLA dengan mencoba meretur pesanan milik pengguna lain. Server menegakkan otorisasi kepemilikan dan menolak permintaan.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/shop/orders/return_order?order_id={id} (Return Order)

a. Tim login ke crAPI dan membuka 'Past Orders' yang menyediakan aksi 'Return' untuk pesanan milik user — alur yang diuji di bawah.

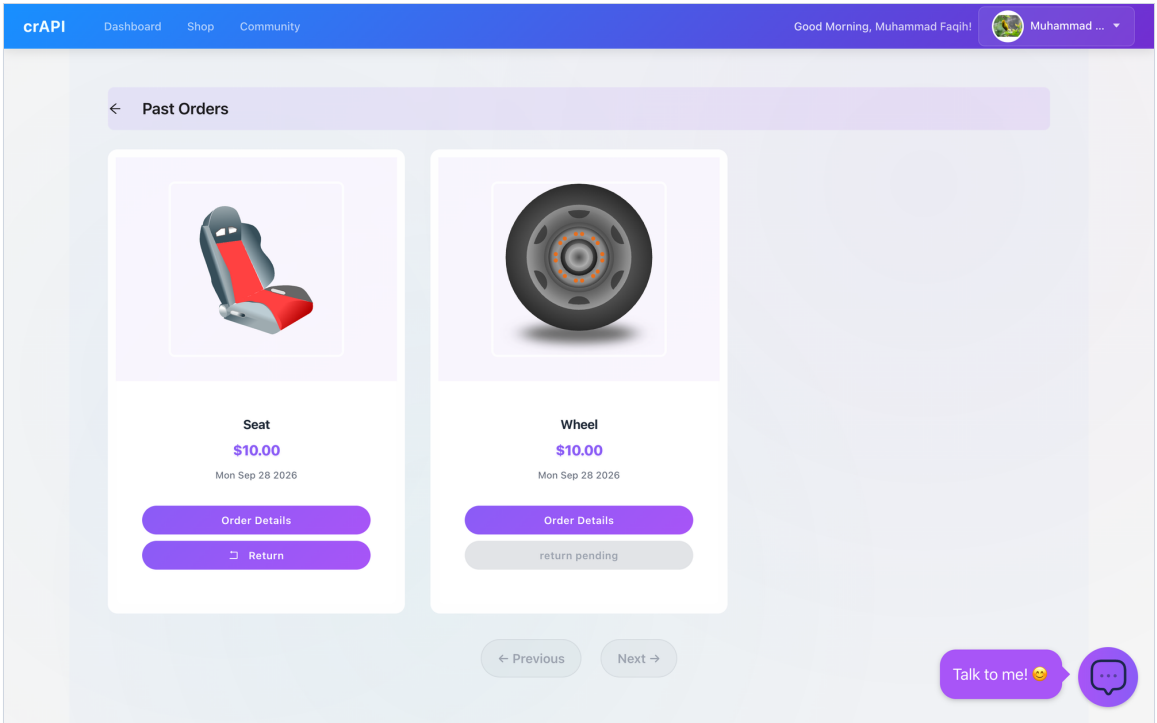


Figure 39 - Broken Object Level Authorization (IDOR) on Order Return (API1) - http://127.0.0.1:8888 (Grey-box) - Halaman Past Orders crAPI dengan aksi 'Return' (browser)

b. Tim mencoba memproses retur untuk order_id=1 yang bukan milik attacker. Server membalas HTTP 403 "You are not allowed to access this resource!", mengonfirmasi kontrol efektif.

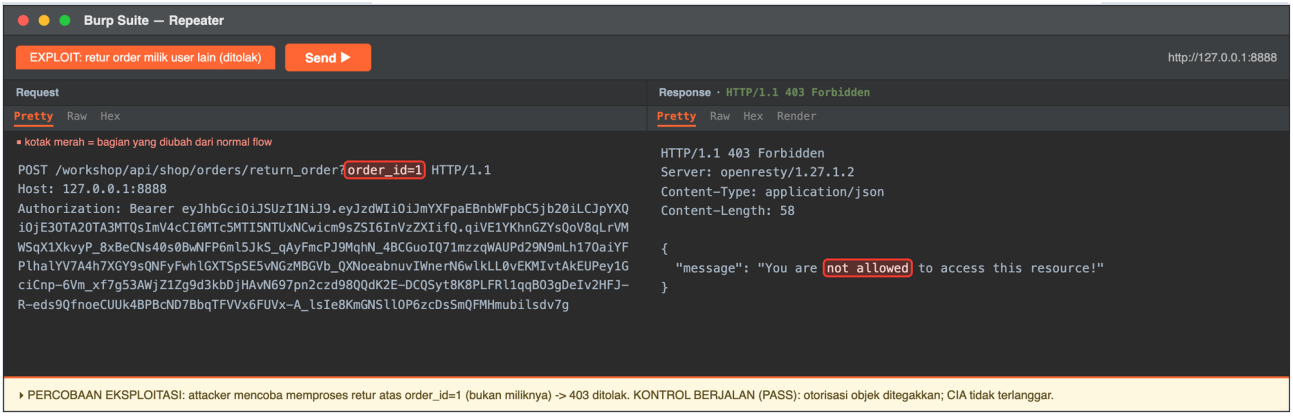


Figure 40 - Broken Object Level Authorization (IDOR) on Order Return (API1) - http://127.0.0.1:8888/workshop/api/shop/orders/return_order?order_id={id} (Return Order) (Grey-box) - Percobaan ditolak: retur order milik user lain -> 403

3.2.7 Broken Object Level Authorization (API1) – Missing Authentication Check on Mechanic Report (Unauthenticated Access)

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-306

Standard mapping	**API1:2023** Broken Object Level Authorization (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report)
Testing approach	Grey-box
Result	**PASS** — Pertahankan autentikasi wajib; tambahkan juga pemeriksaan kepemilikan objek (lihat temuan FAIL terkait).

DESCRIPTION

Endpoint mechanic report diuji terhadap akses tanpa autentikasi. Server mewajibkan autentikasi dan menolak permintaan tanpa token.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report)

a. Tim membaca sebuah mechanic report dengan token valid; server membalas HTTP 200 (normal flow).

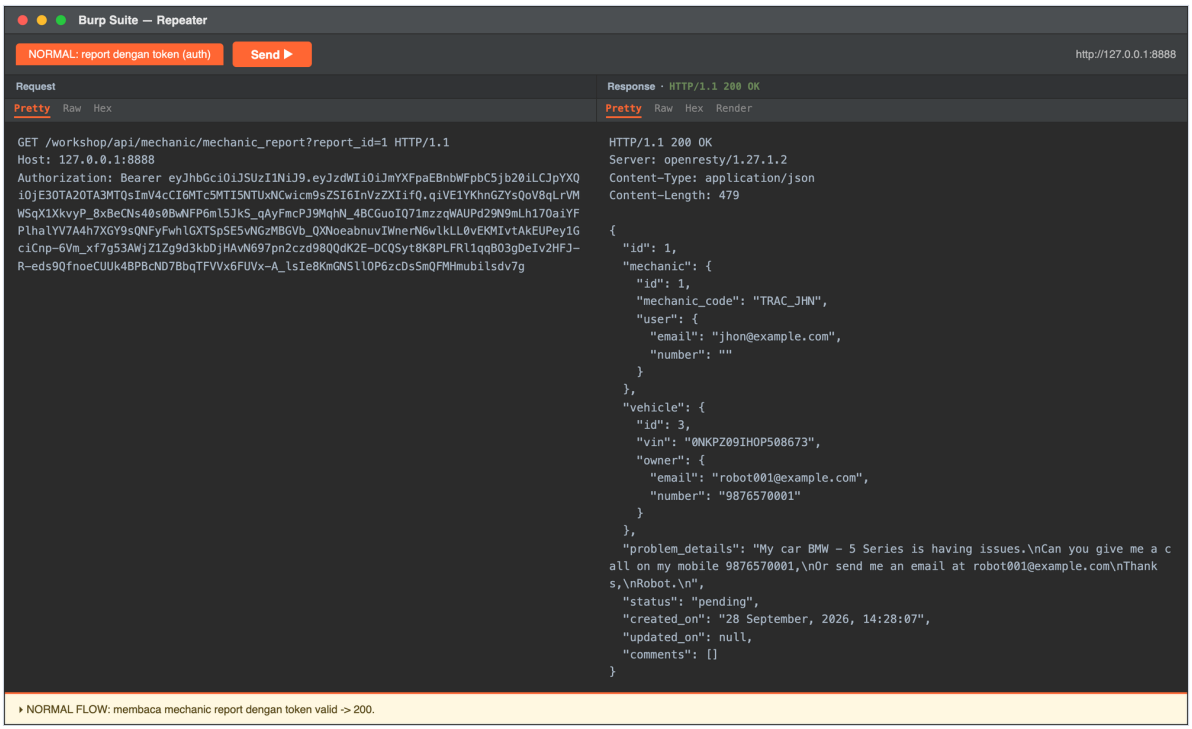


Figure 41 - Missing Authentication Check on Mechanic Report (Unauthenticated Access) (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Normal flow: report dengan token valid

b. Tim mengirim ulang permintaan tanpa header Authorization. Server membalas HTTP 401, mengonfirmasi kontrol autentikasi efektif.

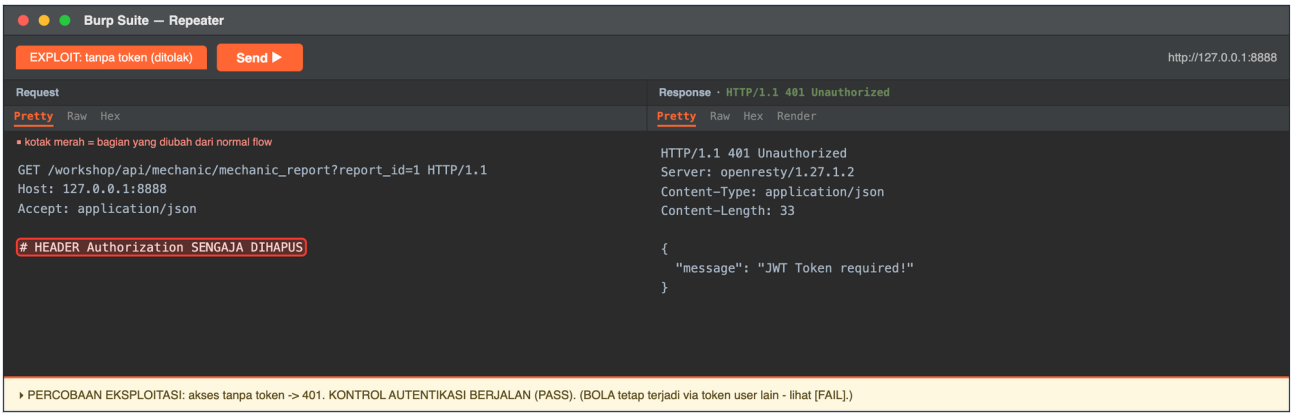


Figure 42 - Missing Authentication Check on Mechanic Report (Unauthenticated Access) (API1) - http://127.0.0.1:8888/workshop/api/mechanic/mechanic_report?report_id={id} (Mechanic Report) (Grey-box) - Percobaan ditolak: tanpa token -> 401

3.2.8 Unrestricted Access to Sensitive Business Flows (API6) – Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected)

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-837

Standard mapping	**API6:2023** Unrestricted Access to Sensitive Business Flows (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim)
Testing approach	Grey-box
Result	**PASS** — Klaim kupon yang sama dua kali ditolak ('already claimed'); batas per-user ditegakkan.

DESCRIPTION

Tim menguji apakah alur bisnis sensitif klaim kupon (yang menambah saldo) dapat disalahgunakan dengan me-replay kupon yang sama. Server menegakkan batas klaim per-user dan menolak replay.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim)

a. Dengan akun baru, tim mengklaim kupon TRAC075 untuk pertama kali; berhasil dan menambah saldo akun.

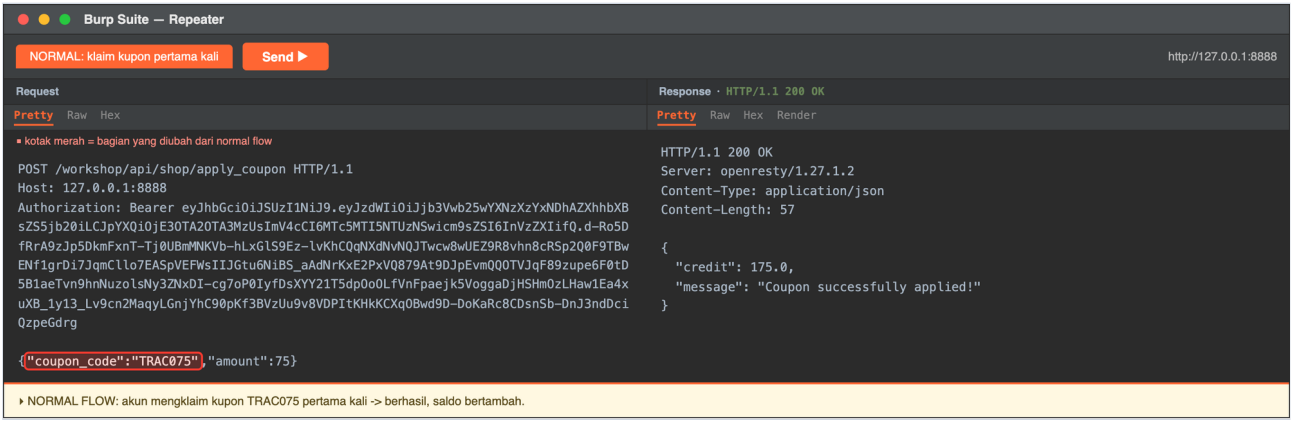


Figure 43 - Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected) (API6) - http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim) (Grey-box) - klaim kupon pertama berhasil

b. Tim mencoba mengklaim kupon yang sama lagi; server menolak dengan 'already claimed', menunjukkan alur bisnis dibatasi per user.

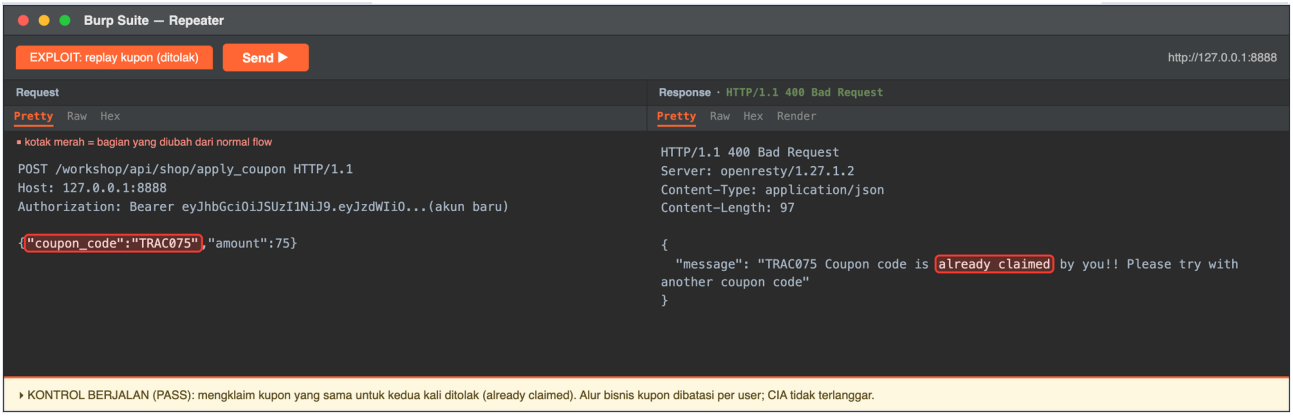


Figure 44 - Unrestricted Access to Sensitive Business Flow — Coupon Claim (Replay Protected) (API6) - http://127.0.0.1:8888/workshop/api/shop/apply_coupon (Coupon Claim) (Grey-box) - replay ditolak

3.3 crAPI Community Service (http://127.0.0.1:8888/community)

3.3.1 Security Misconfiguration (API8) – NoSQL Injection on Coupon Validation

SEVERITY	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS
High	7.1 / 10	Yes	CWE-943

Standard mapping	**API8:2023** Security Misconfiguration (OWASP API Security Top 10 2023)
Impact rating	High
Bugcrowd VRT	P1 - Server-Side Injection (VRT 1.12)
CVSS vector	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N`
Affected feature / URL	http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation)
Testing approach	Grey-box

DESCRIPTION

Ditemukan kerentanan NoSQL injection pada endpoint validasi kupon. Nilai JSON coupon_code diteruskan langsung ke query MongoDB tanpa pemaksaan tipe, sehingga memberikan operator query (mis. {" ne":"x"} atau {" gt":""}) mencocokkan kupon apa pun tanpa mengetahui kodenya.

IMPACT

Penyerang dapat memanfaatkan kerentanan ini untuk membocorkan kode kupon valid beserta nilainya dan melewati validasi kupon demi diskon ilegal. Saat pengujian, tim memperoleh kupon valid tanpa mengetahui kodenya (Confidentiality + Integrity).

RECOMMENDATION

1. Paksa coupon_code menjadi tipe string sebelum query; tolak objek dan operator.
2. Gunakan query yang di-parameter/sanitasi dan aktifkan validasi skema input.
3. Terapkan pengerasan input yang sama pada query berbasis MongoDB lainnya.

REFERENCES

- VRT 1.12 - Server-Side Injection
- https://owasp.org/API-Security/editions/2023/en/0xa8-security-misconfiguration/
- https://cwe.mitre.org/data/definitions/943.html
- https://bugcrowd.com/vulnerability-rating-taxonomy

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation)

a. Tim mengirim kode kupon sebagai string biasa yang sudah diketahui (TRAC075); server membalas HTTP 200 (penggunaan normal).

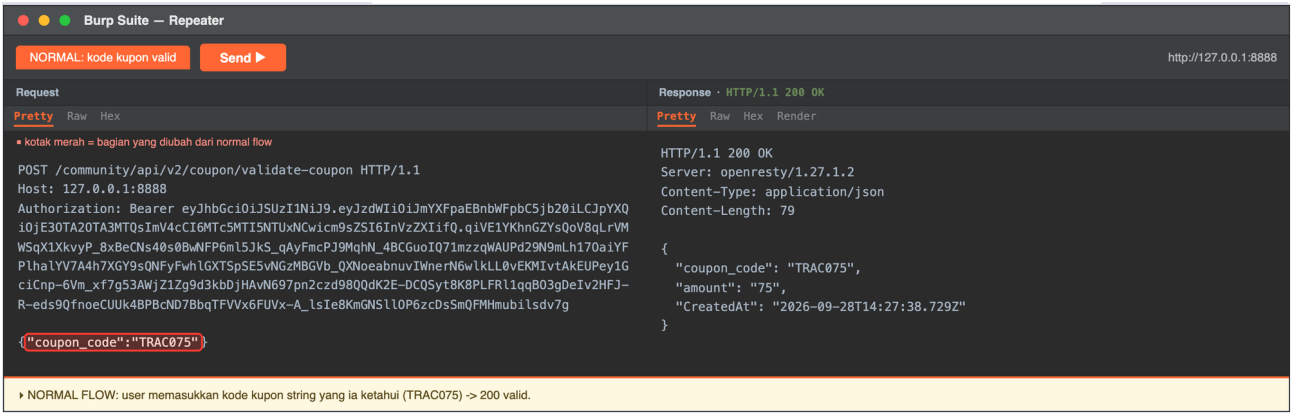


Figure 45 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Normal flow: kode kupon string valid

b. Tim mengganti coupon_code dengan operator NoSQL {"$ne":"x"}. Server mengembalikan kupon valid tanpa tim mengetahui kodenya.

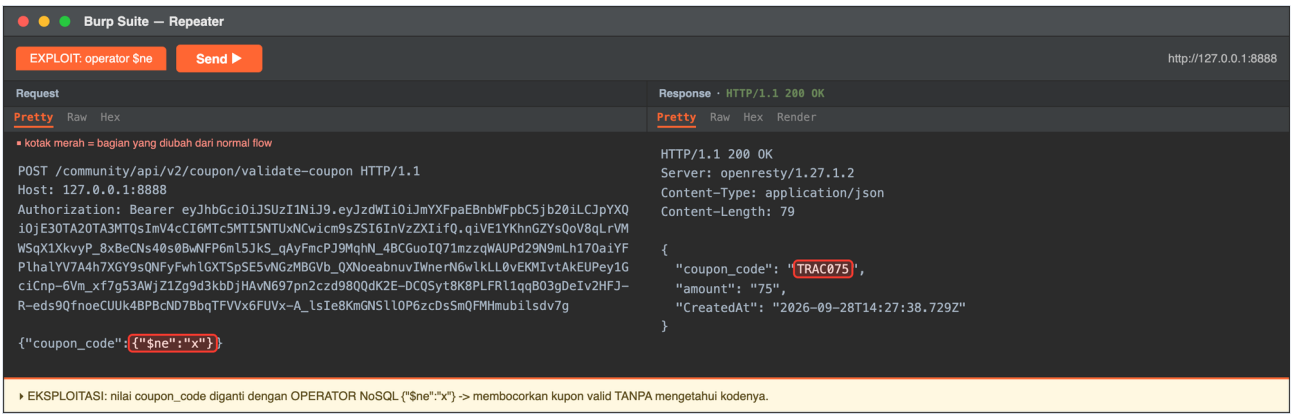


Figure 46 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Eksploitasi: operator $ne membocorkan kupon valid

c. Tim menggunakan operator {"$gt":""} yang juga mengembalikan kupon valid, mengonfirmasi NoSQL injection (Confidentiality + Integrity).

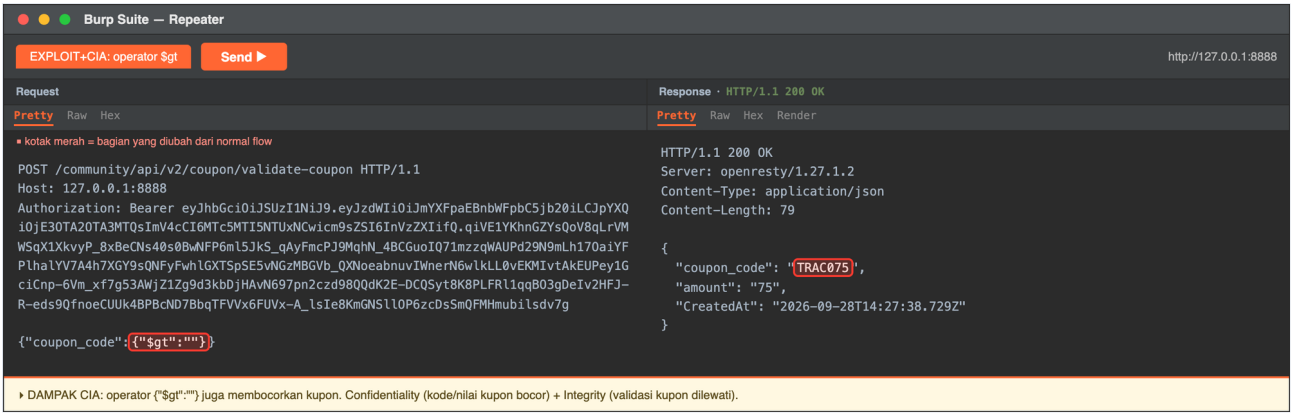


Figure 47 - NoSQL Injection on Coupon Validation (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Dampak: $gt juga membocorkan kupon, injeksi terkonfirmasi

3.3.2 Security Misconfiguration (API8) – Coupon Validation with Normal String Input

RESULT	CVSS V3.1 BASE SCORE	EXPLOITED	WEAKNESS TESTED
PASS	—	No	CWE-943

Standard mapping	**API8:2023** Security Misconfiguration (OWASP API Security Top 10 2023)
Affected feature / URL	http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation)
Testing approach	Grey-box
Result	**PASS** — Terapkan pemaksaan tipe string dan tolak operator/objek (lihat temuan FAIL terkait).

DESCRIPTION

Validasi kupon diuji dengan input string biasa (kode valid dan kode tak dikenal), tanpa operator NoSQL. Kode valid diterima dan kode tak dikenal ditolak sebagaimana mestinya.

EVIDENCE

URL Terdampak: http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation)

a. Tim mengirim kode kupon string valid (TRAC075); server membalas HTTP 200 (normal flow).

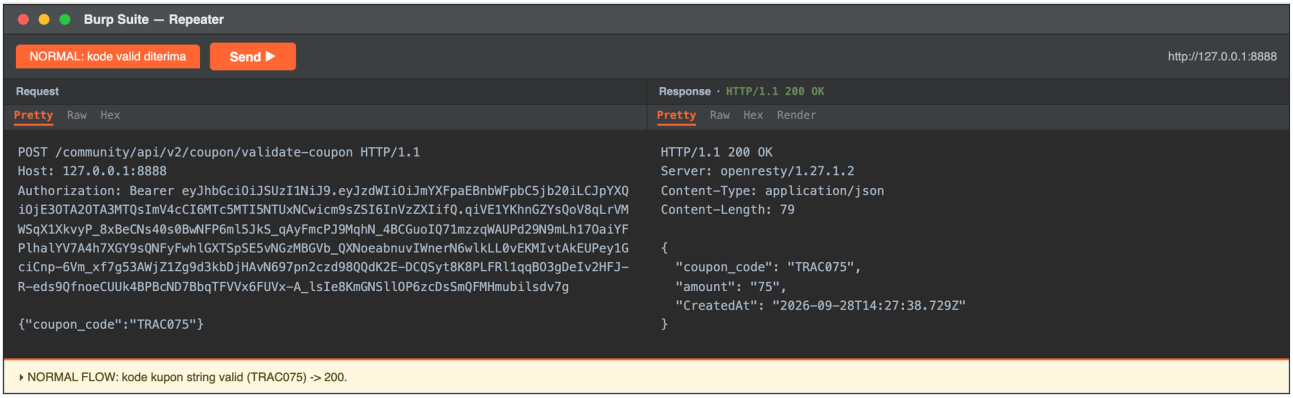


Figure 48 - Coupon Validation with Normal String Input (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Normal flow: kode kupon valid diterima

b. Tim mengirim kode string tak dikenal (INVALID_RANDOM_XYZ) yang ditolak, mengonfirmasi validasi input normal berjalan.

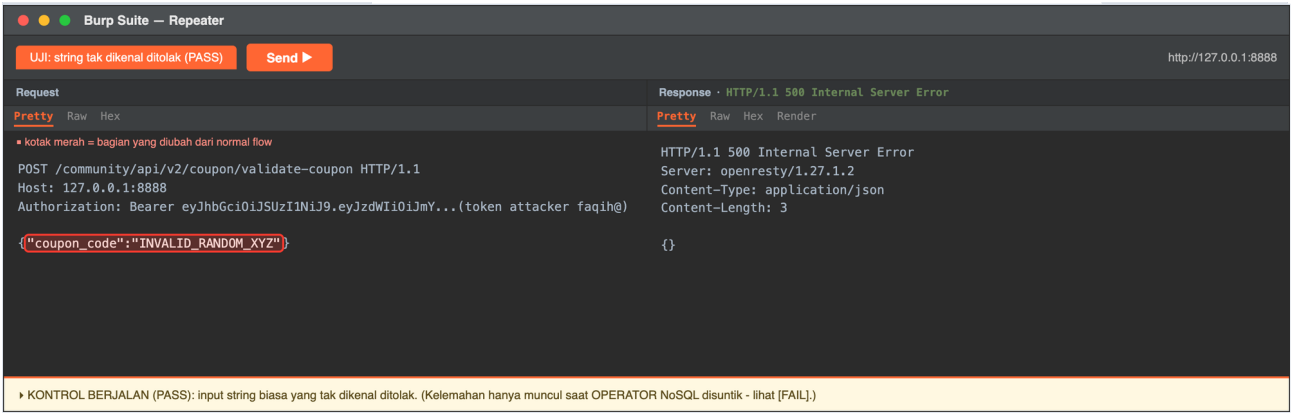


Figure 49 - Coupon Validation with Normal String Input (API8) - http://127.0.0.1:8888/community/api/v2/coupon/validate-coupon (Coupon Validation) (Grey-box) - Kontrol: kode string tak dikenal ditolak

4 Summary of Recommendations

Berdasarkan pemeriksaan tim, ditemukan beberapa kerentanan pada aplikasi crAPI yang dapat dieksploitasi untuk membocorkan data sensitif dan mengambil alih akun pengguna. Kami merekomendasikan tindakan berikut, diurutkan berdasarkan tingkat keparahan.

Broken Authentication (API2) – JWT Signature Not Verified — Authentication Bypass — **Critical**

1. Verifikasi tanda tangan JWT dengan kunci publik RS256 milik server pada setiap request.
2. Tolak eksplisit algoritma alg:none dan terapkan allow-list algoritma (hanya RS256).
3. Gunakan pustaka JWT matang dengan verifikasi wajib serta validasi klaim exp, iss, dan aud.

Server Side Request Forgery (API7) – Server-Side Request Forgery (SSRF) via Contact Mechanic → Internal MailHog → Account Takeover — **Critical**

1. Jangan terima URL sembarang dari klien; gunakan allow-list endpoint mekanik sah.
2. Blokir skema & rentang IP internal (loopback, RFC1918) serta hostname service internal (mis. mailhog, crapi-identity).
3. Jangan pantulkan respons upstream mentah ke klien.
4. Segmentasi jaringan layanan internal (MailHog, actuator) agar tak terjangkau service penerima URL.

Broken Function Level Authorization (API5) – Unauthenticated Access to Order Details — **High**

1. Wajibkan autentikasi pada endpoint order dan verifikasi bahwa order milik pemanggil.
2. Ganti order ID sekuensial dengan UUID yang tak dapat ditebak.
3. Terapkan otorisasi terpusat pada seluruh endpoint workshop.

Broken Authentication (API2) – Bypassable Brute-Force Protection on Password Reset OTP — **High**

1. Terapkan lockout persisten per akun yang tidak ter-reset oleh permintaan OTP baru.
2. Rate-limit dan tambahkan CAPTCHA/anti-automasi pada endpoint forget-password.
3. Gunakan OTP minimal 6 digit dengan masa berlaku singkat dan invalidasi setelah kegagalan kumulatif.

Security Misconfiguration (API8) – NoSQL Injection on Coupon Validation — **High**

1. Paksa coupon_code menjadi tipe string sebelum query; tolak objek dan operator.
2. Gunakan query yang di-parameter/sanitasi dan aktifkan validasi skema input.
3. Terapkan pengerasan input yang sama pada query berbasis MongoDB lainnya.

Broken Function Level Authorization (API5) – Broken Function Level Authorization — Management Endpoint Exposes All Users — **Medium**

1. Terapkan otorisasi berbasis peran (verifikasi role=admin di server) pada semua endpoint manajemen/administratif.
2. Jangan mengandalkan ketiadaan tautan UI sebagai kontrol akses.
3. Minimalkan data yang dikembalikan.

Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Mechanic Reports	Medium

1. Verifikasi report_id yang diminta terkait dengan user/mekanik pemanggil.
2. Gunakan UUID alih-alih identifier sekuensial.
3. Kembalikan hanya field yang benar-benar diperlukan.

Broken Object Level Authorization (API1) – Broken Object Level Authorization (IDOR) on Vehicle Location	Medium

1. Verifikasi bahwa kendaraan yang diminta milik user pada token sebelum mengembalikan lokasinya.
2. Terapkan pemeriksaan otorisasi tingkat objek secara terpusat.
3. Hindari menampilkan PII pemilik pada respons lokasi.

Unrestricted Resource Consumption (API4) – Unrestricted Resource Consumption — No Login Rate Limiting	Medium

1. Terapkan rate limiting per akun/IP dan lockout progresif.
2. Tambahkan CAPTCHA/anti-automasi dan deteksi anomali.
3. Batasi konkurensi permintaan per klien.

Unsafe Consumption of APIs (API10) – Unsafe Consumption of APIs — Unvalidated Upstream Response in Contact Mechanic	Medium

1. Validasi & sanitasi respons upstream (skema, content-type) sebelum diproses/dipantulkan.
2. Batasi tujuan upstream ke allow-list tepercaya (lihat juga temuan SSRF).
3. Jangan pantulkan respons upstream mentah ke klien.

Improper Inventory Management (API9) – Improper Inventory Management — Deprecated OTP Endpoint (v2) Still Live	Medium

1. Nonaktifkan versi API usang (v2) yang tak lagi dipakai.
2. Kelola inventaris versi API dan dokumentasikan endpoint aktif.
3. Terapkan kontrol keamanan seragam di semua versi yang hidup.

5 Conclusion

OVERALL RISK RATING

Critical

Berdasarkan penilaian tim, aplikasi crAPI dinilai **tidak aman**: broken authentication (tanda tangan JWT tidak diverifikasi) memungkinkan pengambilalihan akun penuh, dan sejumlah masalah kontrol akses, SSRF, injeksi, konsumsi sumber daya, inventaris, serta unsafe consumption membocorkan data pelanggan. Perbaikan atas temuan yang berhasil dieksploitasi wajib dilakukan sebelum penggunaan produksi.

6 Attachments

Attachment	Description