

expoqa[®]26

MADRID 26th, 27th & 28th May

expoqa.eu

HI, I'M ŽIVKOVIĆ ČEDOMIR

SENIOR QA ENGINEER (MENTOR & LEAD)

In my current role as a Senior QA Engineer (Mentor & Lead), I am passionate about **software testing and quality improvement**. My focus is on gaining a deep **understanding of user needs** and ensuring **quality across all layers** of an application – from **API, Frontend, and Database, to Automation, Gateway, ESB, and ERP systems**. I have strong expertise in analyzing application communication and traffic between endpoints to ensure **reliability and performance**.



QUALITY ACROSS ALL LAYERS

Ensuring quality across **API, Frontend, Database, Automation, Gateway, ESB, and ERP systems**.



DEEP UNDERSTANDING OF USER NEEDS

Focused on gaining a deep understanding of **user needs** and delivering reliable, high-quality solutions.



APPLICATION COMMUNICATION EXPERT

Strong expertise in analyzing application communication and traffic between endpoints to ensure **reliability and performance**.



MENTOR & LEAD

Mentoring QA engineers, leading by example, and **driving quality culture** across teams.



COMMITTED TO **QUALITY**. DRIVEN BY **CURIOSITY**. FOCUSED ON **IMPACT**.



LET'S CONNECT



LinkedIn



From >_ **CONSOLE** to **CONTRACT:**

ETHICAL API HACKING & DEBUGGING
THAT WINS



PRACTICAL
API TESTING



DEVTOOLS
TRICKS



A TRUE
ENDPOINT-HACKING
STORY



THAT LED TO A
CLIENT WIN.



>_ What you'll learn:

1 Design focused API tests

Design focused API tests (requests, schemas, status codes, edge cases) that increase coverage and reduce flaky UI dependencies.

POST /api/v1/users

```
{
  "name": "Cedomir",
  "email": "cedo@example.com",
  "role": "user"
}
```

✓ Status codes
200 / 400 / 401 / 404

✓ Schema validation
request & response

✓ Edge cases
empty, large, null,
special chars, limits



Better coverage • Fewer flaky UI tests • Faster feedback

2 Use browser DevTools

Use browser DevTools (Console, Network, Application) to discover hidden API calls, replay traffic, and extract payloads for automated tests.

Name	Method	Status	Type
feed	GET	200	xhr
update-settings	POST	200	xhr
notifications	GET	200	xhr
analytics	POST	204	fetch

Headers Payload Response

```
{
  "limit": 20,
  "cursor": "eyJpZCI6MTIz",
  "filters": {
    "type": "all"
  }
}
```

Copy as cURL

Discover → Replay → Extract → Automate

3 Apply ethical "hacking" checks

Apply basic ethical "hacking" checks on endpoints: input fuzzing, parameter tampering, authorization checks, and response analysis (without destructive testing).



Input fuzzing
"1 OR 1=1 --"
"../../../../etc/passwd"



Parameter tampering
id=123 → id=124
role=user → role=admin



Authorization checks
with token vs. without token
user A vs. user B



Response analysis
status codes, error handling,
sensitive data exposure



Ethical
Responsible
Non-destructive

4 Convert findings into automated checks

Convert manual findings into automated checks (Postman, examples) and meaningful bug reports.

GET /api/v1/users/123

Send

```
pm.test("Status code is 200", function () {
  pm.response.to.have.status(200);
});

pm.test("Schema - name exists", function () {
  var json = pm.response.json();
  pm.expect(json).to.have.property("name");
});

pm.test("No unexpected fields", function () {
  pm.expect(json).to.not.have.property("password");
});
```

🚨 Bug report

Summary
Unauthorized access via user ID

Steps to reproduce
1. Login as User A
2. Call GET /api/v1/users/123
3. Change ID to another user
4. Observe response

Expected result
Should return 403
Actual result
Returns 200 and user data

Impact
High - user data exposure
Attachments
Request/response, screenshots



Postman Tests → Automated Checks → Actionable Bugs

5 Use common sense to triage issues

Adopt 'common sense' heuristics for triaging issues quickly (how to prioritise, when to escalate to security, when to write regression tests).



Prioritise

- Impact on users
- Data sensitivity
- Ease of exploitation
- Frequency / reach



Escalate to Security

- Auth bypass
- Data exposure
- Privilege escalation
- Injection risks



Write Regression Tests

- Fixed bugs
- Critical flows
- Edge cases
- Prevention for future



Rule of thumb:

High impact + Easy to exploit + Sensitive data = Escalate
Fixed issue that can break again = Automate



Think like a tester. Inspect like a developer. Act like a professional.

Build quality. Protect users. Deliver value. >_

“HOW ONE API CALL TOOK ME TO A MOVIE PREMIERE”

CURIOSITY, ETHICS, AND ACCIDENTAL ADVENTURES IN *CYBERSECURITY*



CURIOSITY

Questioning everything



ETHICS

Doing the right thing, always



API EXPLORATION

Finding paths others don't see



REAL IMPACT

Turning a discovery into an opportunity

```
GET /api/v1/movies
Host: api.app.local
Authorization: Bearer ***
Accept: application/json
```



```
{
  "status": 200,
  "success": true,
  "data": {
    "access": "granted",
    "result": "unexpected"
  }
}
```

```
POST /api/v1/booking
Content-Type: application/json
Body: { ... }
Response: 201 Created
```



ONE ENDPOINT. ONE DISCOVERY.
ONE UNEXPECTED INVITATION.

THE PHONE CALL

 He says,

“LISTEN...
SOMETHING IS **OFF**
WITH THIS WEBSITE
I'M WORKING ON.

 QA IS **ASLEEP**,

 DEVELOPMENT HAS
DISAPPEARED INTO THE **WOODS**,

 AND THE WHOLE THING
FEELS... **CURSED**.

 SOMETHING IS WRONG.
I NEED TO FIND **THE TRUTH**.



SUSPICIOUS BEHAVIOR. HIDDEN ISSUES. ONE MISSION.



INVESTIGATE



ANALYZE TRAFFIC



REVERSE & TEST



RESTORE QUALITY

"SHURE I WILL
TAKE A QUICK
LOOK"

*THE MOST
DANGEROUS
SENTENCE IN
TECH*



Quick look.
Should be
quick...

"THE API STARTED OVERSHARING"

```
$ api_explorer --target https://cursed-website.com/api
```

```
Connected. Enumerating endpoints...
```

```
21:42:01 GET /api/user ✓  
21:42:03 GET /api/user/profile ✓  
21:42:05 GET /api/user/wallet ✓  
21:42:07 GET /api/wallet/operations ✓  
21:42:10 GET /api/tokens ✓  
21:42:12 GET /api/tokens/generate ✓  
21:42:15 GET /api/rewards ✓  
21:42:17 GET /api/admin/panel ✓  
21:42:19 GET /api/internal/config ✓  
21:42:21 GET /api/backup/database ✓  
21:42:23 GET /api/_
```

! WARNING

Sensitive data exposure detected.
Multiple critical vulnerabilities found.
Access control: NONE

! USER DATA

```
id: 84219  
name: John Doe  
email: john.doe@mail.com  
phone: +381 60 123 4567  
address: Belgrade, Serbia  
...
```

! WALLET OPERATIONS

```
id: 948571  
type: withdrawal  
amount: 1250.00  
currency: USD  
status: completed  
...
```

! TOKENS

```
access_token:  
eyJhbGciOiJIUzI1NiIs...  
refresh_token:  
def50200ac4b...  
...
```

! REWARD SYSTEM

```
user_id: 84219  
points: 98540  
tier: VIP  
rewards_claimed: 12  
...
```

OVERSHARING

THE API

"BRO... THIS SITE
IS BASICALLY A
PIÑATA."

“
IF YOU BREATHE
ON IT,
CANDY FALLS OUT.”



BEAUTIFUL OUTSIDE.
EMPTY INSIDE.
BUGS EVERYWHERE.



"CURIOSITY WITHOUT ETHICS IS JUST EXPLOITATION"



SECURITY REPORT

Executive Summary

Scope

Methodology

Findings

Vulnerabilities

Impact

Recommendations

Timeline

Appendix

CONFIDENTIAL

Prepared for:
Client

Date:
May 18, 2024

Executive Summary

During the engagement, multiple security vulnerabilities were identified within the API endpoints. These issues could allow unauthorized access to sensitive data, financial operations, and administrative functionality. Detailed findings and recommendations are provided in this report.

Risk Level

HIGH

Critical Findings

7
Require immediate attention

Total Findings

15
Across 9 endpoints

Tested Endpoints

23
In scope

Top Vulnerabilities

- CRITICAL** Broken Object Level Authorization (BOLA)
- CRITICAL** Insecure Direct Object Reference (IDOR)
- HIGH** Sensitive Data Exposure
- HIGH** Insecure Token Generation
- MEDIUM** Missing Rate Limiting

Impact

- Unauthorized access to user data
- Financial operations manipulation
- Account takeover risk
- Data confidentiality breach

Conclusion

The issues identified pose a significant risk to the confidentiality, integrity, and availability of the application and its data. Immediate remediation is strongly recommended.

"REPORT"



"TWO DAYS OF SILENCE"



AND THEN... NOTHING.

Two days of silence.
Two days of imagining everything from



INBOX

Inbox

Sent

Drafts

Archive

Trash

Search...



Your inbox is empty.
Nothing to see here... yet.

Settings

New message... |



Send

Last communication received: May 15, 2026 • 2 Days Ago



"CAN YOU COME TO LONDON TO DISCUSS?"

- AMAZING!
- INCREDIBLE!



Can you come to London to discuss?

Looking forward to your reply.



ONE SMALL PROBLEM:

I NEED A VISA.



PROCESSING TIME

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

AND THE VISA NEEDS ONE MONTH.

SO I OFFER MILAN INSTEAD.

BECAUSE IF YOU CAN'T HAVE LONDON, AT LEAST YOU CAN HAVE GOOD PASTA.



PROBLEM: VISA TAKES 1 MONTH



SOLUTION: MEET IN MILAN INSTEAD



RESULT: GREAT CONVERSATIONS & EVEN BETTER PASTA

LET'S MAKE IT HAPPEN!



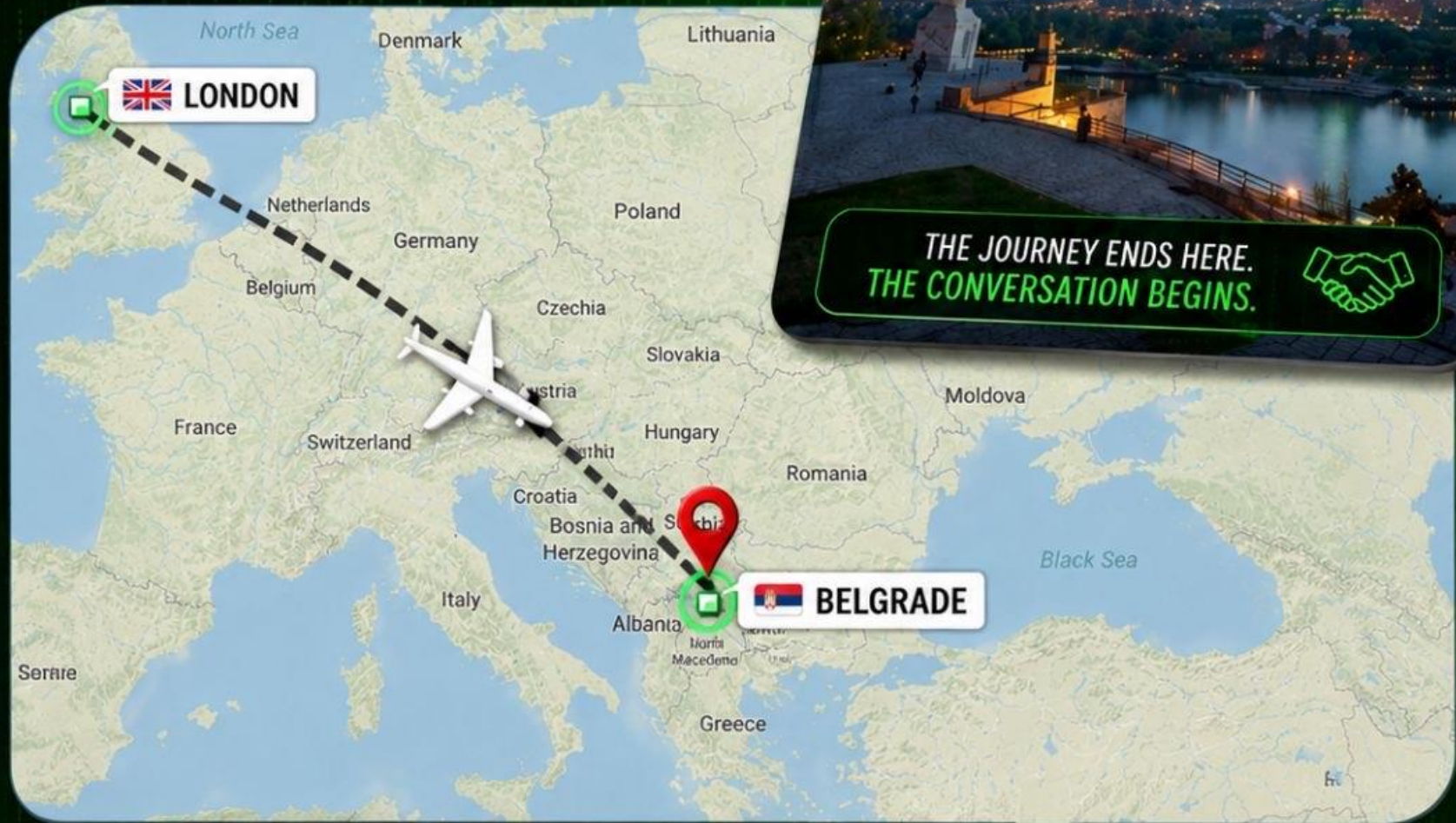
“NO. I’LL COME TO YOU.”



BELGRADE

- ✓ HE FLIES TO **BELGRADE**.
- ✓ TO MEET ME **PERSONALLY**.

HE SAID. HE DID.
NOW WE MEET.



THE JOURNEY ENDS HERE.
THE CONVERSATION BEGINS.



FROM MESSAGE TO MEETING.



FROM DISTANCE TO **CONNECTION.**





AND NOT ONLY THAT —
**HE INVITES ME TO
MEET HIM**
AT THE PREMIERE OF
HIS NEW MOVIE.



LADIES AND GENTLEMEN...

I WENT FROM

INSPECTING API ENDPOINTS
WITH A GLASS OF WINE
TO WALKING A RED CARPET
WITH A MAN WHOSE
API HAD TRUST ISSUES.



TRY EXPLAINING THAT
CAREER PATH TO
YOUR PARENTS.



INSPECTING API
ENDPOINTS



INVITED TO THE
MOVIE PREMIERE



WALKING THE
RED CARPET



WITH A MAN WHOSE
API HAD TRUST ISSUES



"BUT HERE 'S THE
REAL MESSAGE
BEHIND THE
HUMOR"



Curiosity
opened
the door.

Integrity
kept it
open.





"SOMETIMES
OPPORTUNITIES
DON'T KNOCK...
THEY LEAK
THROUGH AN API"

</>



FROM CODE TO RED CARPET
THE JOURNEY IS UNPREDICTABLE.
MAKE IT MEANINGFUL.

user@system:~\$ █



SO STAY CURIOUS.

Keep asking questions. Keep exploring.
The best discoveries start with curiosity.



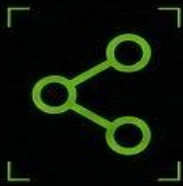
STAY ETHICAL.

With great access comes great responsibility.
Build trust. Protect it. Earn it.



AND ALWAYS BE READY —

Opportunities don't come with a warning.
Be prepared. Be adaptable. Be you.



BECAUSE YOU NEVER KNOW WHEN
A SUMMER NIGHT, A FRIEND'S FRUSTRATION,
AND ONE TINY ENDPOINT.
MIGHT LEAD YOU TO THE PREMIERE
OF A MOVIE YOU DIDN'T EVEN KNOW
EXISTED THAT MORNING.

> THANK YOU. █



CONTACT DETAILS

LET'S CONNECT.



zivkovic.cedomir@gmail.com



+381 64 160 45 93



TRUST IS EARNED.
CONTACT IS THE FIRST STEP.



SCAN TO SAVE
CONTACT



expoqa[®]26

MADRID 26th, 27th & 28th May

Thank you for attending

expoqa.eu