



Enhancing API Security through LLM

A Novel Approach for Detecting BOLA Vulnerabilities

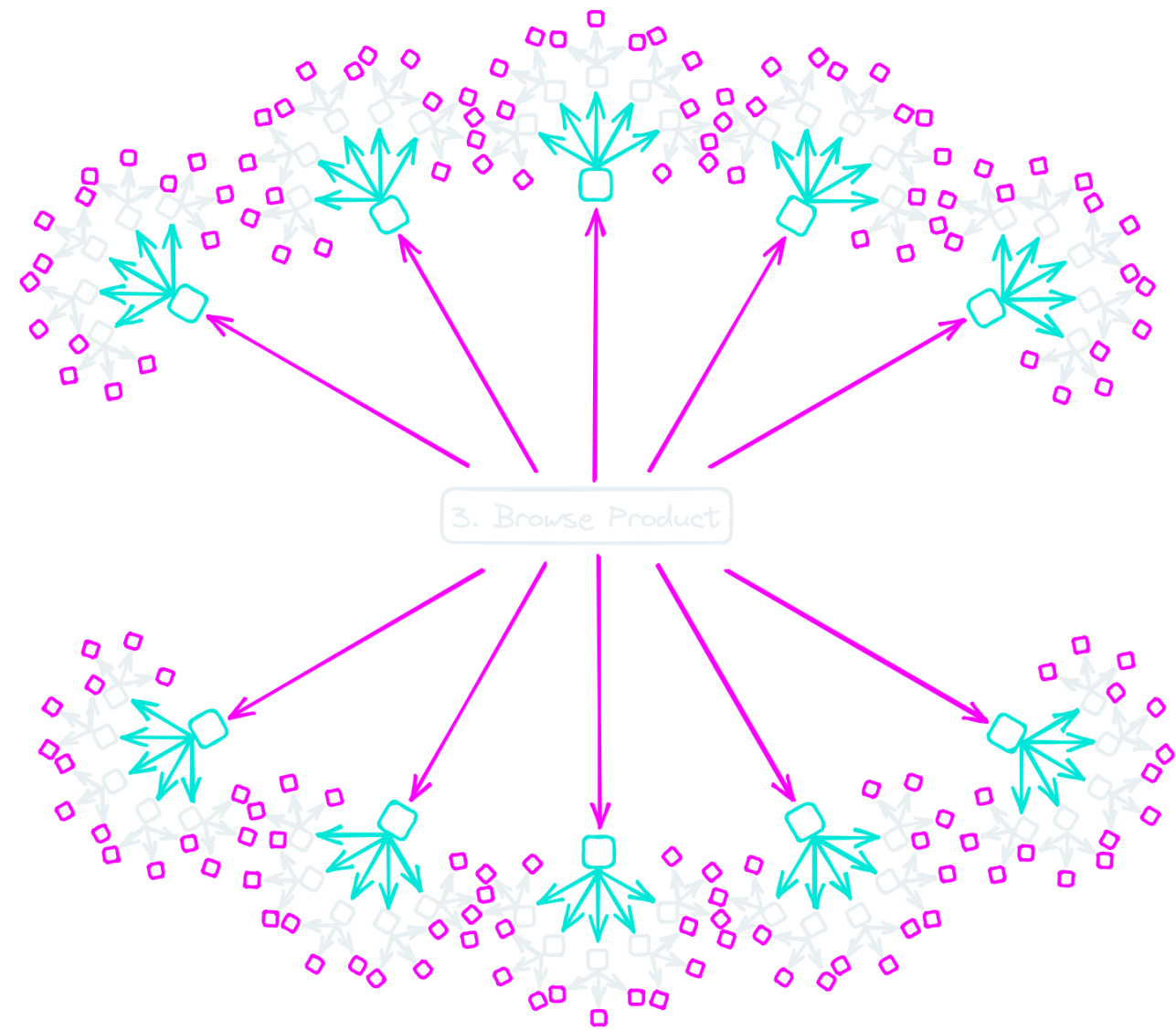
Alessio Dalla Piazza | CTO & Co-Founder Equixly

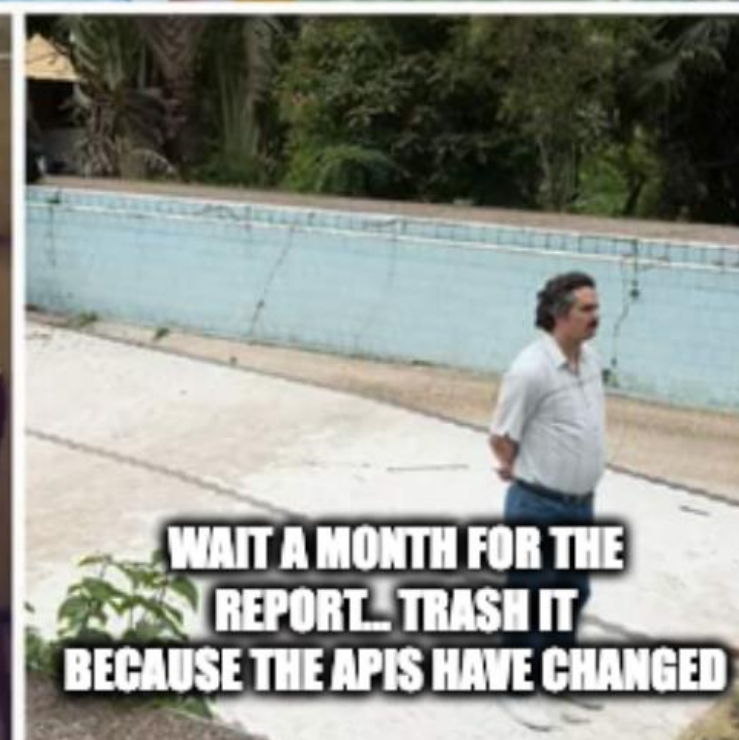
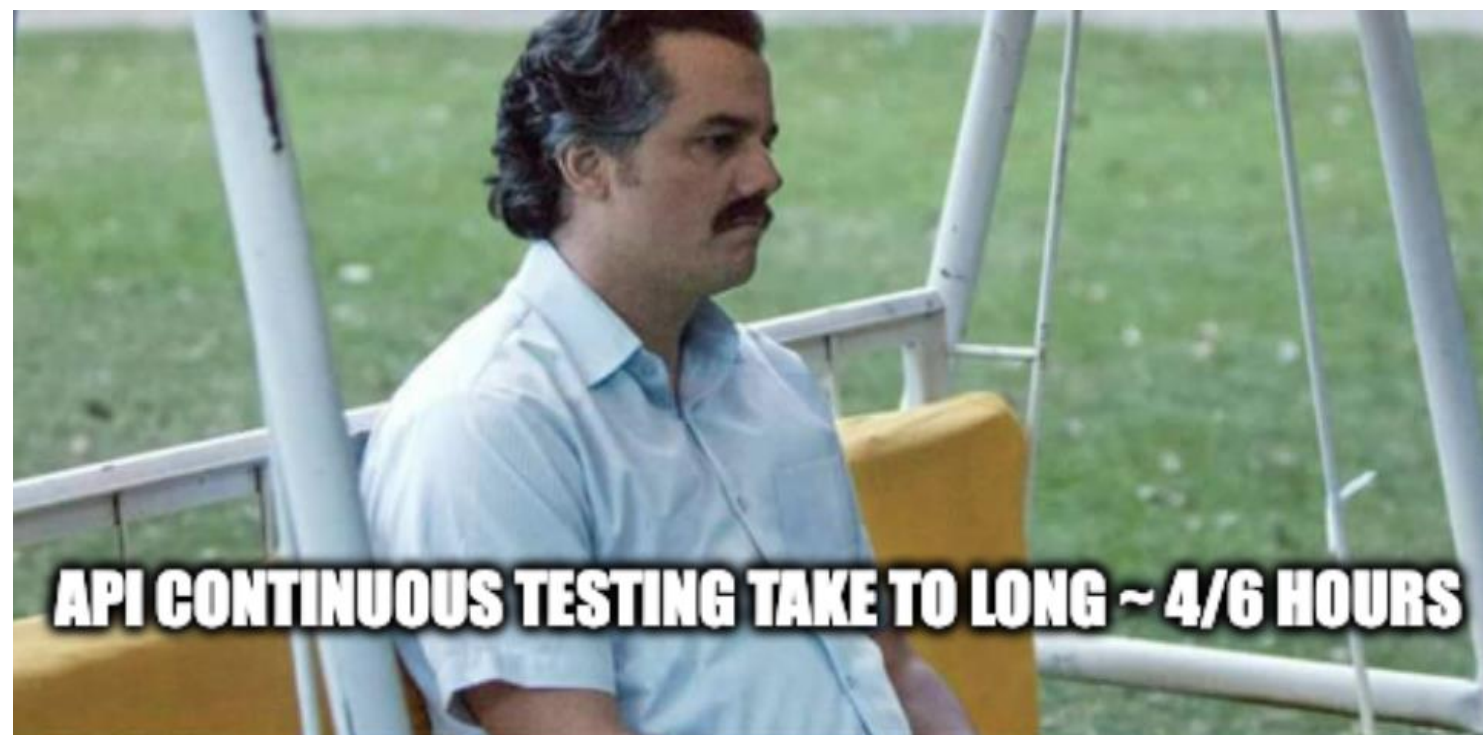
- Inspired by the [RBT4](#) forum
- Cybersecurity Consulting (10+ years)
- Passion for breaking things.
CVEs (Apple Safari, VMWare, IBM Websphere, Docker...)
- Co-Founder at Equixly
AI-Powered API Security Testing Platform



1. \$ whoami
2. Continuous API Active Testing
3. Shift Left Practices
4. OWASP API Top 10: Business Logic
5. Understanding BOLA Vulnerabilities
6. Challenges in Automating API Testing
7. Interpreting API Requests-Abstraction
8. Interpreting Results with LLMs
9. Challenges of Working with LLMs

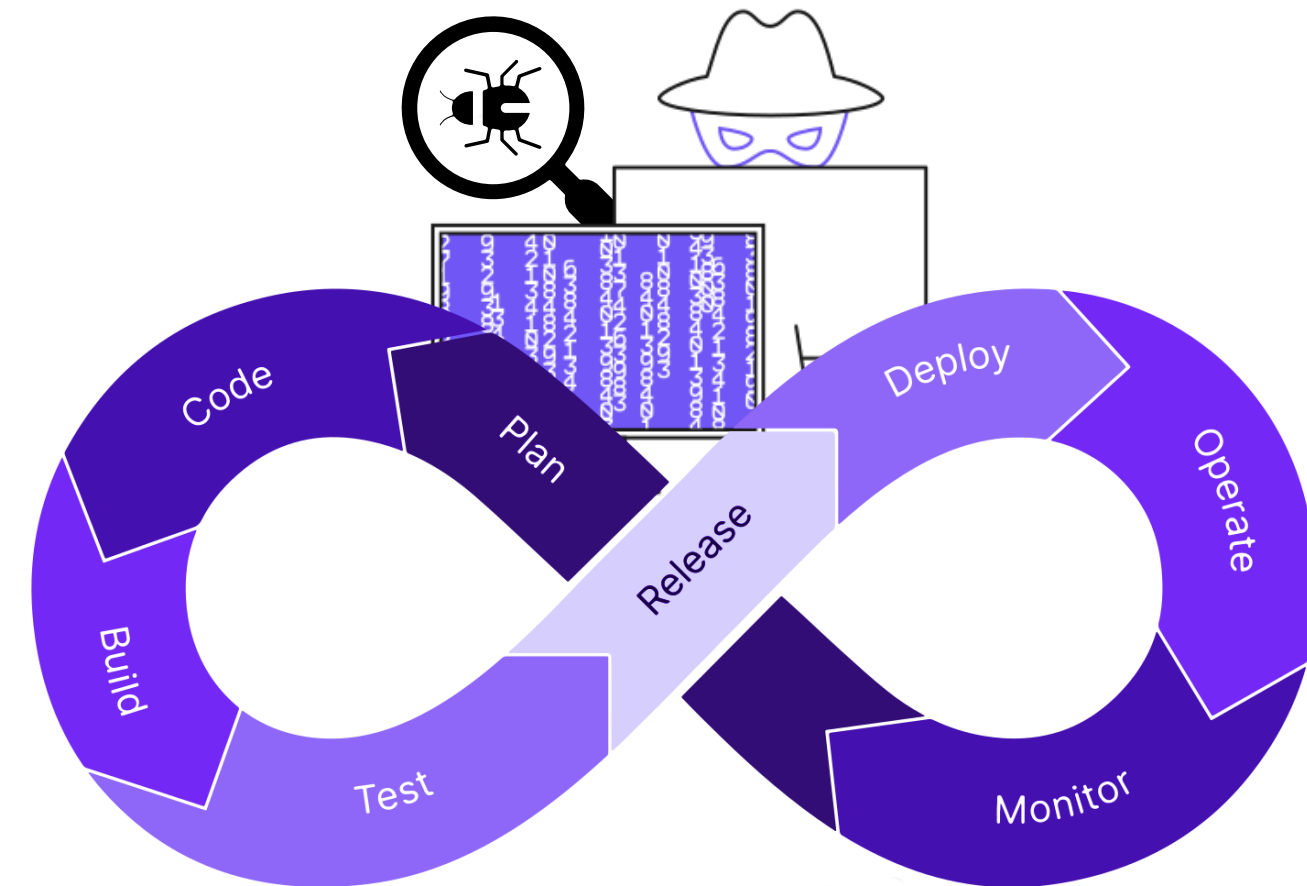
- Proactive Security
- Automated Testing integrated with CI/CD
- Evolves tests with your API changes
- Immediate Feedback - insights for remediation of issues



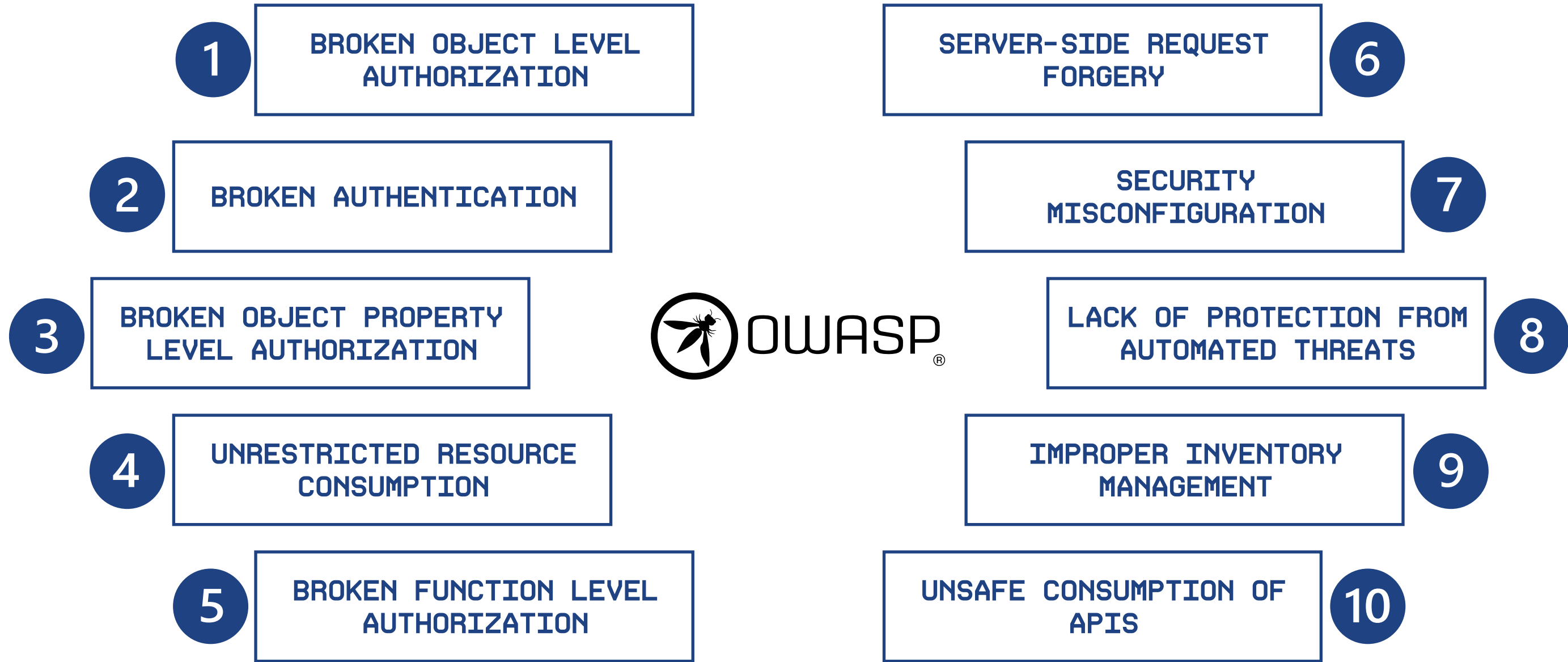


SHIFT-LEFT PRACTICES

- Integrate Early - minimize risks
- Continuous Evaluation - test from Staging/QA
- Cost-Effective - fixing issues early cuts down the cost and time



OWASP API TOP 10



- 1 BROKEN OBJECT LEVEL AUTHORIZATION
- 2 BROKEN AUTHENTICATION
- 3 BROKEN OBJECT PROPERTY LEVEL AUTHORIZATION
- 4 UNRESTRICTED RESOURCE CONSUMPTION
- 5 BROKEN FUNCTION LEVEL AUTHORIZATION
- 6 SERVER-SIDE REQUEST FORGERY
- 7 SECURITY MISCONFIGURATION
- 8 LACK OF PROTECTION FROM AUTOMATED THREATS
- 9 IMPROPER INVENTORY MANAGEMENT
- 10 UNSAFE CONSUMPTION OF APIS

- Lack of Operation Sequence Awareness – API operation in isolation
- Dependency Handling – cannot capture the dependencies between API Operation
- Insufficient Understanding of API Logic – random fuzz
- Context Aware Parameter Inference – Smart Fuzz
- Error Message Interpretation – Adapt on responses

- ~ 35%:
- Manual Authentication
- No distinction from “*false*” 200 OK
- No dependencies
- Most of resolved requests don’t require parameters

The screenshot shows the ZAP 2.15.0 interface. The top panel displays a request details view for a GET request to `http://127.0.0.1:5656/microservicebola/documents/10`. The request headers are visible, including `user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:125.0) Gecko/20100101 Firefox/125.0` and a Bearer token in the `Authorization` header.

The bottom panel shows a history table with the following data:

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/app.mopub.com/we...	200	OK	11 ms	36 bytes	Low		JSON
11	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/community/forum	200	OK	4 ms	373 bytes	Low		JSON
15	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/crowdsignal/createt...	200	OK	7 ms	62 bytes	Low		JSON
19	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/docs/index.html	200	OK	4 ms	3,728 bytes	Medium		Script
22	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/documents/10	200	OK	3 ms	137 bytes	Low		JSON
24	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/evilsite/api/manage...	200	OK	9 ms	25 bytes	Low		JSON
33	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/gql.reddit.com/subr...	200	OK	4 ms	97 bytes	Low		JSON
36	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord...	200	OK	4 ms	752 bytes	Low		JSON
40	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/orderenumeration/g...	200	OK	6 ms	125 bytes	Low		JSON
42	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/orderenumeration/or...	200	OK	4 ms	1,789 bytes	Low		JSON
43	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/paginated/payout?pa...	200	OK	4 ms	49 bytes	Low		JSON
47	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/pandao/api/addorder	200	OK	4 ms	38 bytes	Low		JSON
50	Manual	6/13/24, 12:44:18 PM	GET	http://127.0.0.1:5656/microservicebola/pandao/api/order/10	200	OK	3 ms	241 bytes	Low		JSON
21	Manual	6/13/24, 12:44:18 PM	POST	http://127.0.0.1:5656/microservicebola/documents	201	Created	4 ms	259 bytes	Low		JSON

- 100%:
- Auto Authentication
- Distinction from “*false*”
200 OK
- Dependencies Handling

```

→ bola_evilsite_get_companyid[200|✓] → bola_mopub_get_mopub_list_orders[200|✓] → bola_evilsite_get_companydata[200|✓] → bola_crowdsig
INFO[15691] ■ bola_crowdsignal_add_team_member - POST /microservicebola/crowdsignal/addteammember
INFO[15691] ■ bola_crowdsignal_create_team - POST /microservicebola/crowdsignal/createteam
INFO[15691] ■ bola_crowdsignal_get_user_info - GET /microservicebola/crowdsignal/userinfo/{TEAMID}/{USERID}
INFO[15691] ■ bola_docs - GET /microservicebola/docs/index.html
INFO[15691] ■ bola_evilsite_get_companydata - GET /microservicebola/evilsite/api/managements/v1/companies/{company_id}/accounts
INFO[15691] ■ bola_evilsite_get_companyid - GET /microservicebola/evilsite/api/managements/v1/companies
INFO[15691] ■ bola_forum_create-document - POST /microservicebola/documents
INFO[15691] ■ bola_forum_get-document - GET /microservicebola/documents/{document_id}
INFO[15691] ■ bola_forum_list-post - GET /microservicebola/community/forum
INFO[15691] ■ bola_login_user - POST /microservicebola/login
INFO[15691] ■ bola_logout - GET /microservicebola/logout
INFO[15691] ■ bola_mopub_create_order - POST /microservicebola/app.mopub.com/web-client/api/orders/create
INFO[15691] ■ bola_mopub_get_mopub_list_orders - GET /microservicebola/app.mopub.com/web-client/api/orders/stats/query/{order_id}
INFO[15691] ■ bola_nordvpn_nordorderlist - POST /microservicebola/nordvpn/api/v1/orders
INFO[15691] ■ bola_orderenumeration_gettransaction - POST /microservicebola/orderenumeration/gettransaction
INFO[15691] ■ bola_orderenumeration_orders - GET /microservicebola/orderenumeration/orders
INFO[15691] ■ bola_pagination_consumer - GET /microservicebola/paginated/payout/{user_id}
INFO[15691] ■ bola_pagination_producer - GET /microservicebola/paginated/payout
INFO[15691] ■ bola_pandao_add_order - POST /microservicebola/pandao/api/addorder
INFO[15691] ■ bola_pandao_list_order - GET /microservicebola/pandao/api/order/{order_id}
INFO[15691] ■ bola_reddit_get_subreddit_names - GET /microservicebola/gql.reddit.com/subreddits
INFO[15691] ■ bola_reddit_subreddits_moderator_logs - POST /microservicebola/gql.reddit.com
INFO[15691] ■ bola_register - POST /microservicebola/register
INFO[15691] ■ bola_vehicle_get_vehicle - GET /microservicebola/vehicle/user/{UUID}
INFO[15691] ■ =====
INFO[15691] Stats - coverage: 100.00%, reached: 100.00%, attempted: 100.00%

```

demo.equixly.com/projects/7b859cac-26c1-4434-b279-272aaa834055/scans/bd72907f-4c0b-4463-be6e-926064b8ba6c?pageSize=48#authorization-matrix

BOLA / Scans / Scan Detail

Dashboard Scans Issues Inventory Settings

General Issues 4 Authorization Matrix HTTP History Inventory Settings

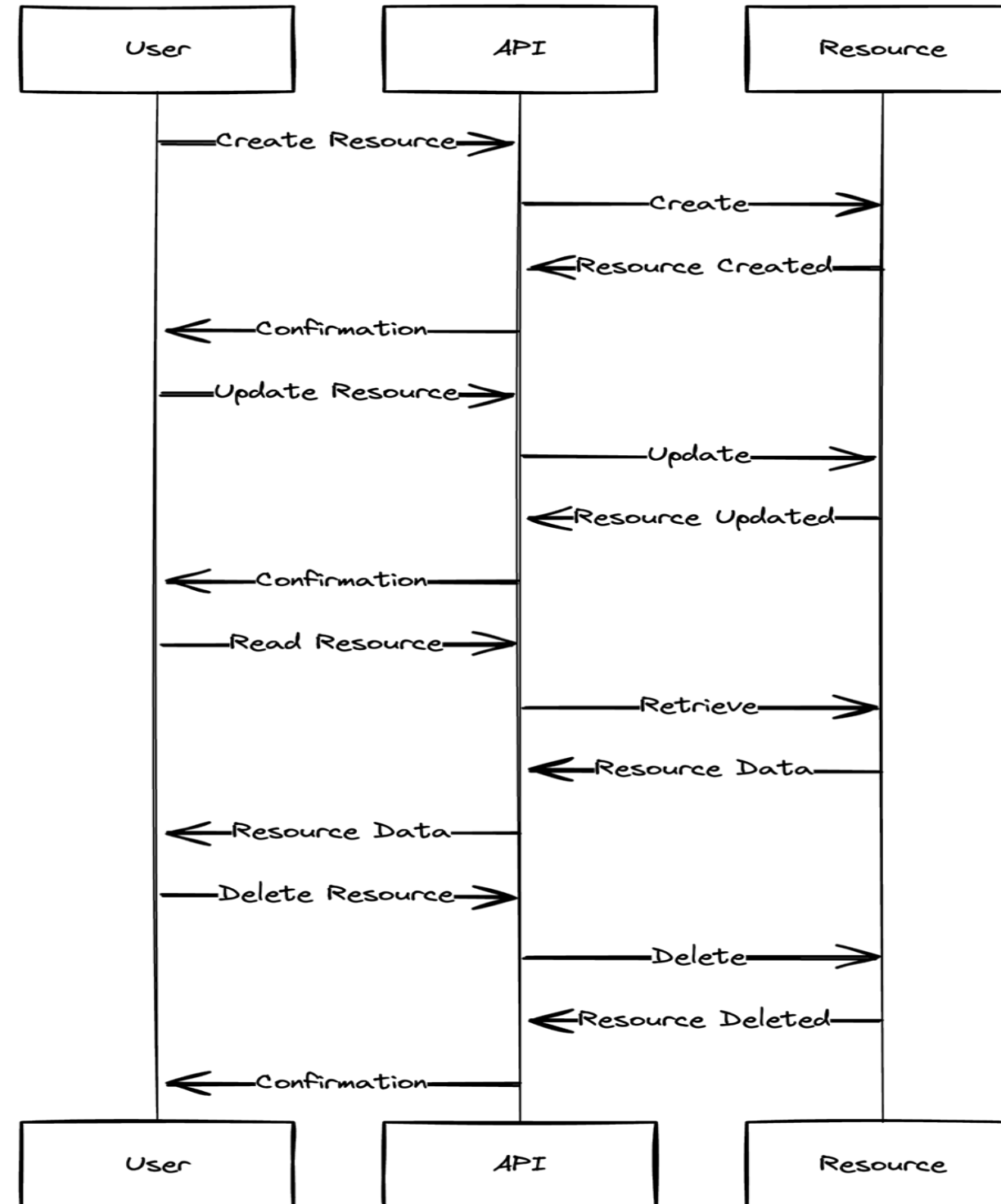
PDF Report

Method	Path	Endpoint	Category	User1	Anonymous
GET	/microservicebola/vehicle/user/{UUID}		read	✓	–
POST	/microservicebola/register		register	–	✓
GET	/microservicebola/pandao/api/order/{order_id}		read	✓	–
POST	/microservicebola/pandao/api/addorder		create	✓	–
GET	/microservicebola/paginated/payout/{user_id}		read	✓	–
GET	/microservicebola/paginated/payout		read	✓	–
GET	/microservicebola/orderenumeration/orders		read	✓	–
POST	/microservicebola/orderenumeration/gettransaction		read	✓	–
POST	/microservicebola/nordvpn/api/v1/orders		read	–	✓
GET	/microservicebola/logout		logout	✓	–
POST	/microservicebola/login		login	✓	✓
GET	/microservicebola/gql.reddit.com/subreddits		read	✓	–
POST	/microservicebola/gql.reddit.com		read	✓	–
GET	/microservicebola/evilsite/api/managements/v1/companies/{company_id}/accounts		read	✓	–
GET	/microservicebola/evilsite/api/managements/v1/companies		read	✓	–
GET	/microservicebola/documents/{document_id}		read	✓	–
POST	/microservicebola/documents		create	✓	–
GET	/microservicebola/docs/index.html		read	–	✓
GET	/microservicebola/crowdsignal/userinfo/{TEAMID}/{USERID}		read	✓	–
POST	/microservicebola/crowdsignal/createteam		create	✓	–
POST	/microservicebola/crowdsignal/addteammember		create	✓	–
GET	/microservicebola/community/forum		read	✓	–
GET	/microservicebola/app.mopub.com/web-client/api/orders/stats/query/{order_id}		read	✓	–
POST	/microservicebola/app.mopub.com/web-client/api/orders/create		create	✓	–

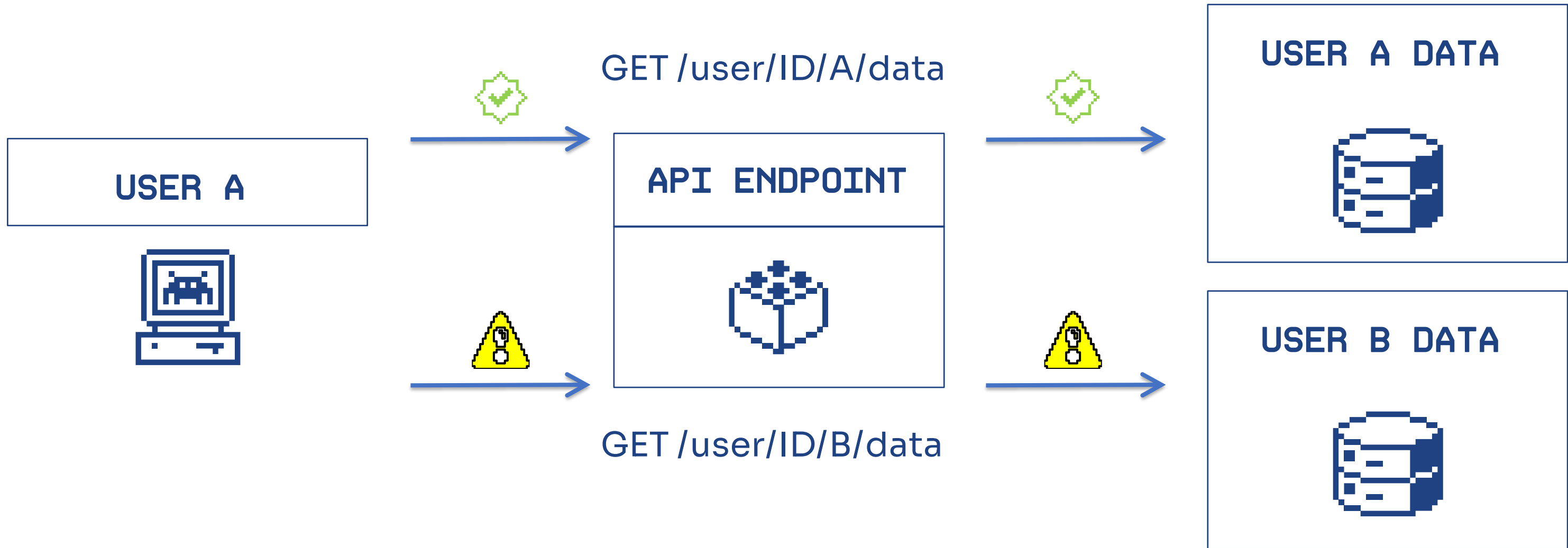
- Coverage Alone is Not Enough
- Context-Agnostic Testing – miss state dependent vulnerabilities
- Resource Lifecycle Abstraction – track the resources, owner and their states

UNDERSTANDING BUSINESS LOGIC

- Example of Resource Tracking
 - Finite State Machine (FSM)



EXAMPLE BOLA VULNERABILITIES



Users can substitute the ID of their own resource in the API call with an ID of a resource belonging to another user.

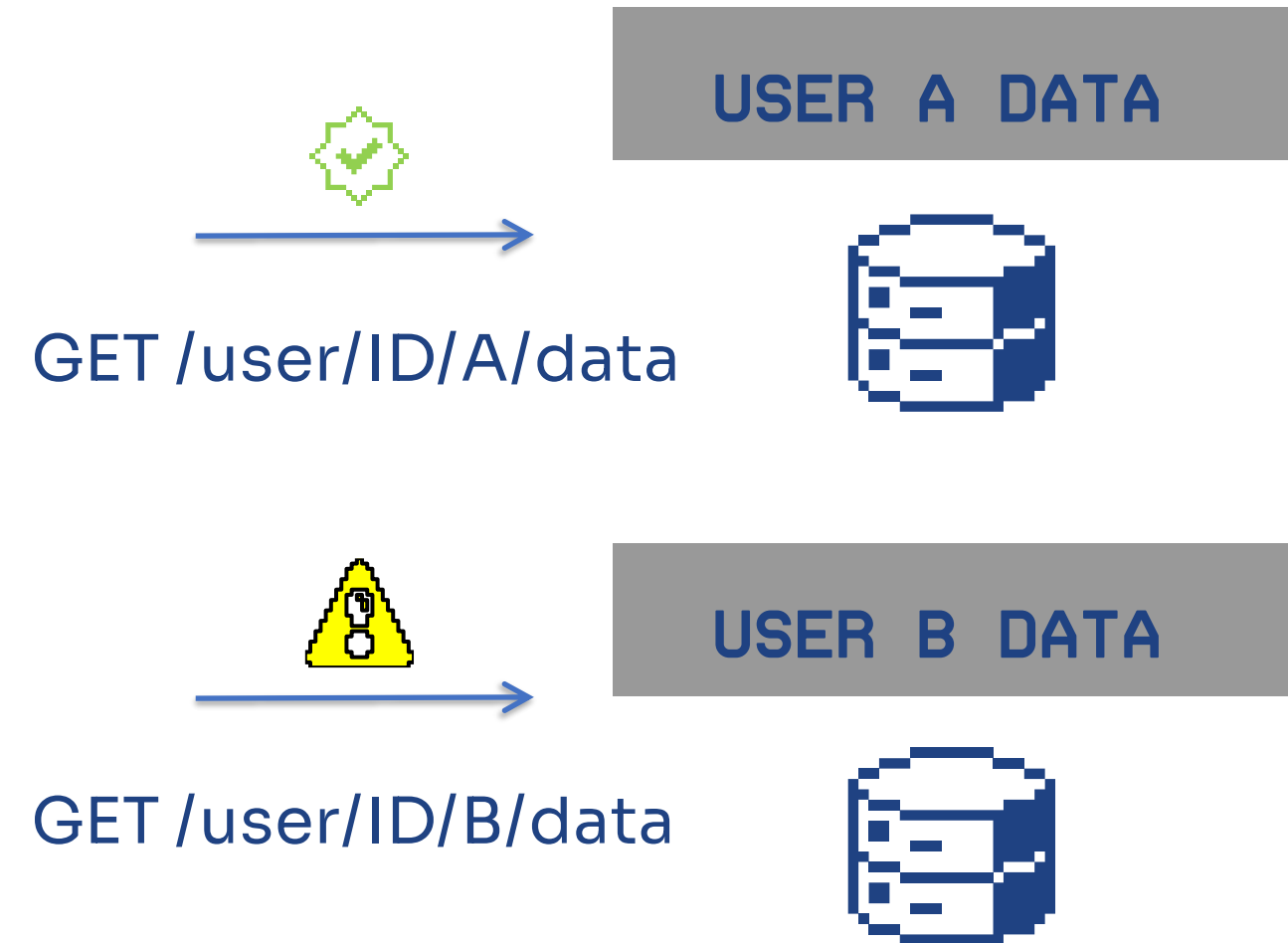
- Spec Reliance - flawed API documentation.
- Business Logic
- Complex Auth - intricate authentication methods.
- Data Dependencies
- Multi-API Vulnerability



User Role Distinction - User A's resources cannot be accessed by others.

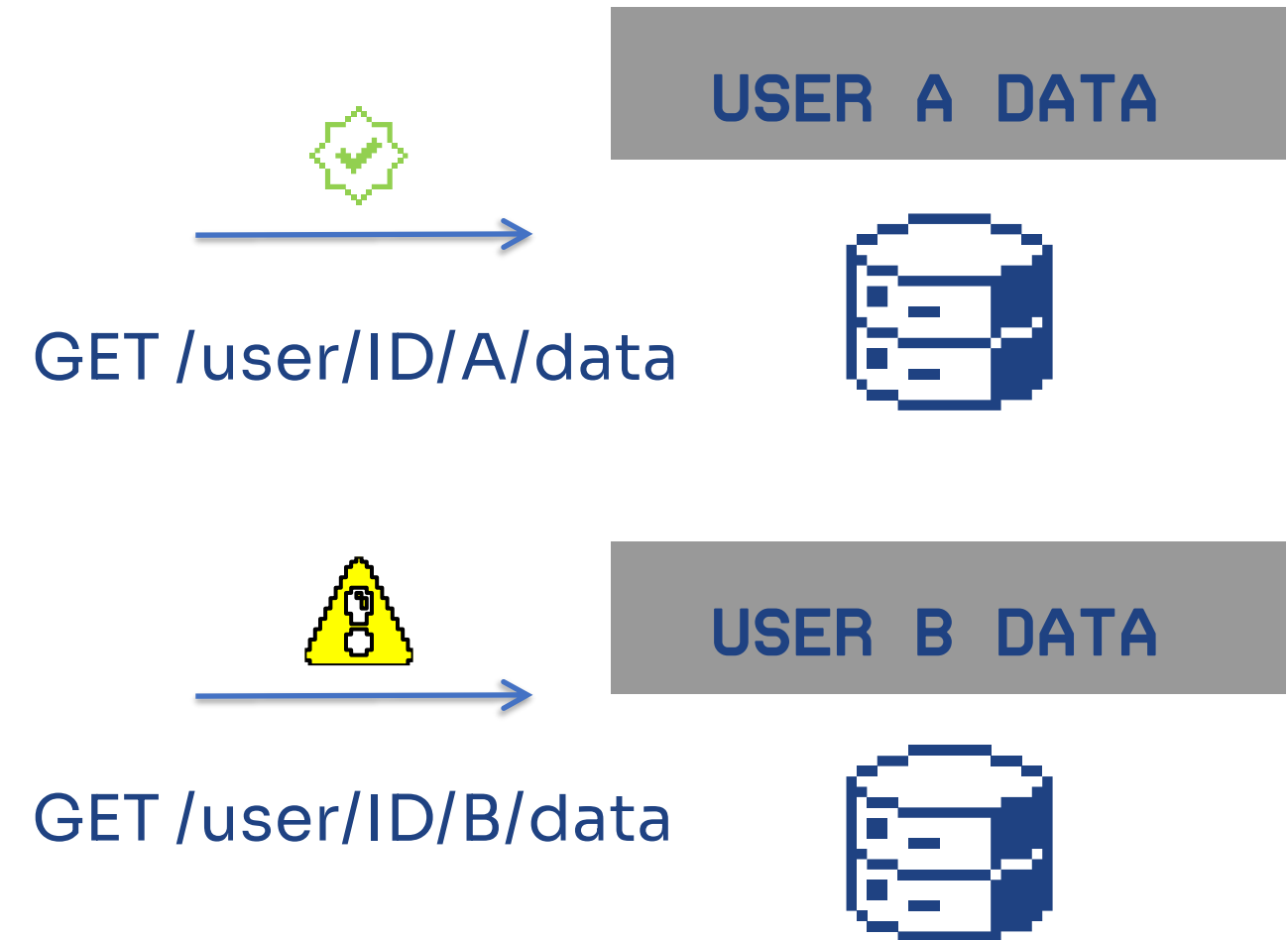
Access Verification - READ operations do not retrieve unauthorized resources.

Resource Tracking - CREATE operations are tagged and tracked.

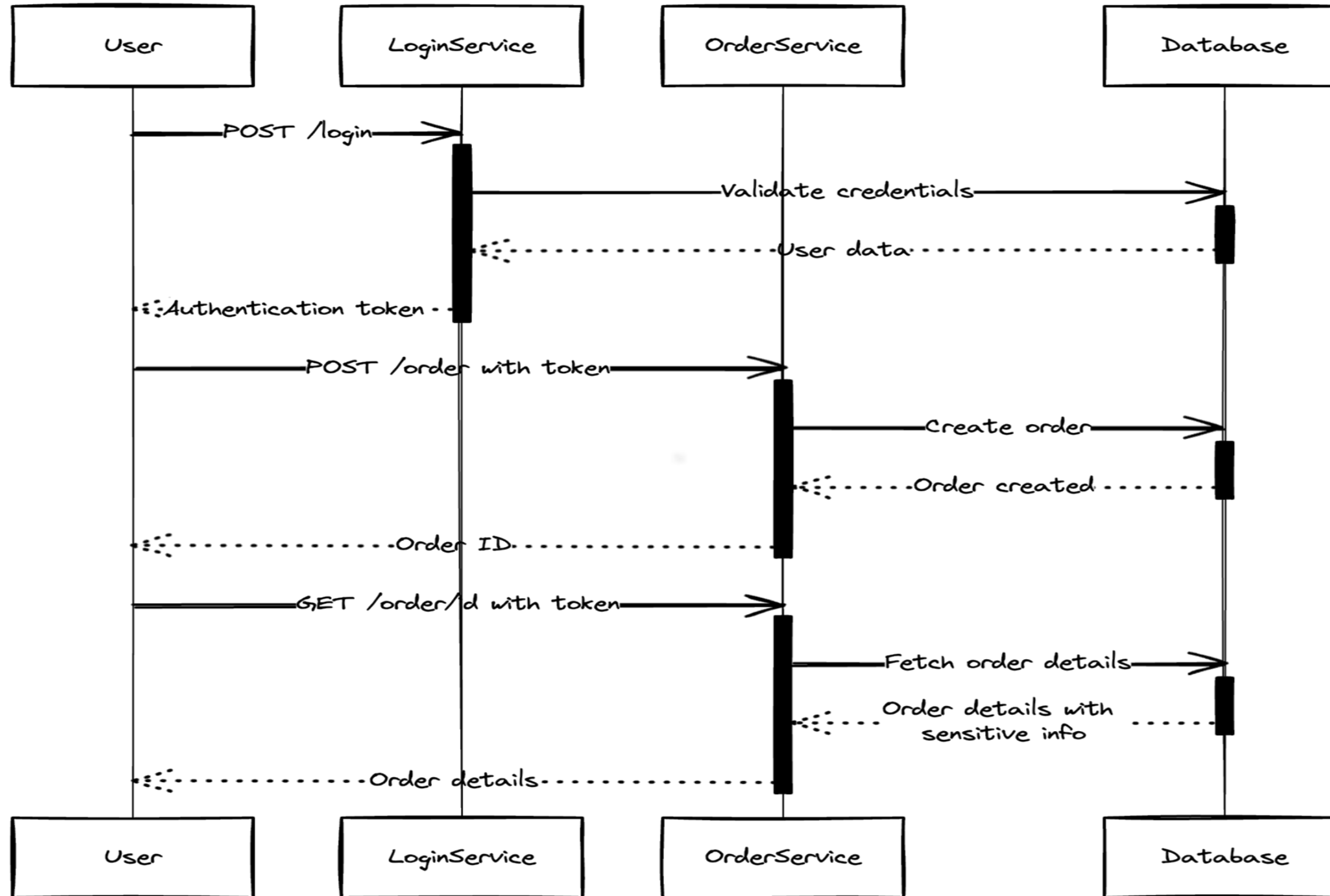


Testing Scenarios - tested unauthorized access by different roles

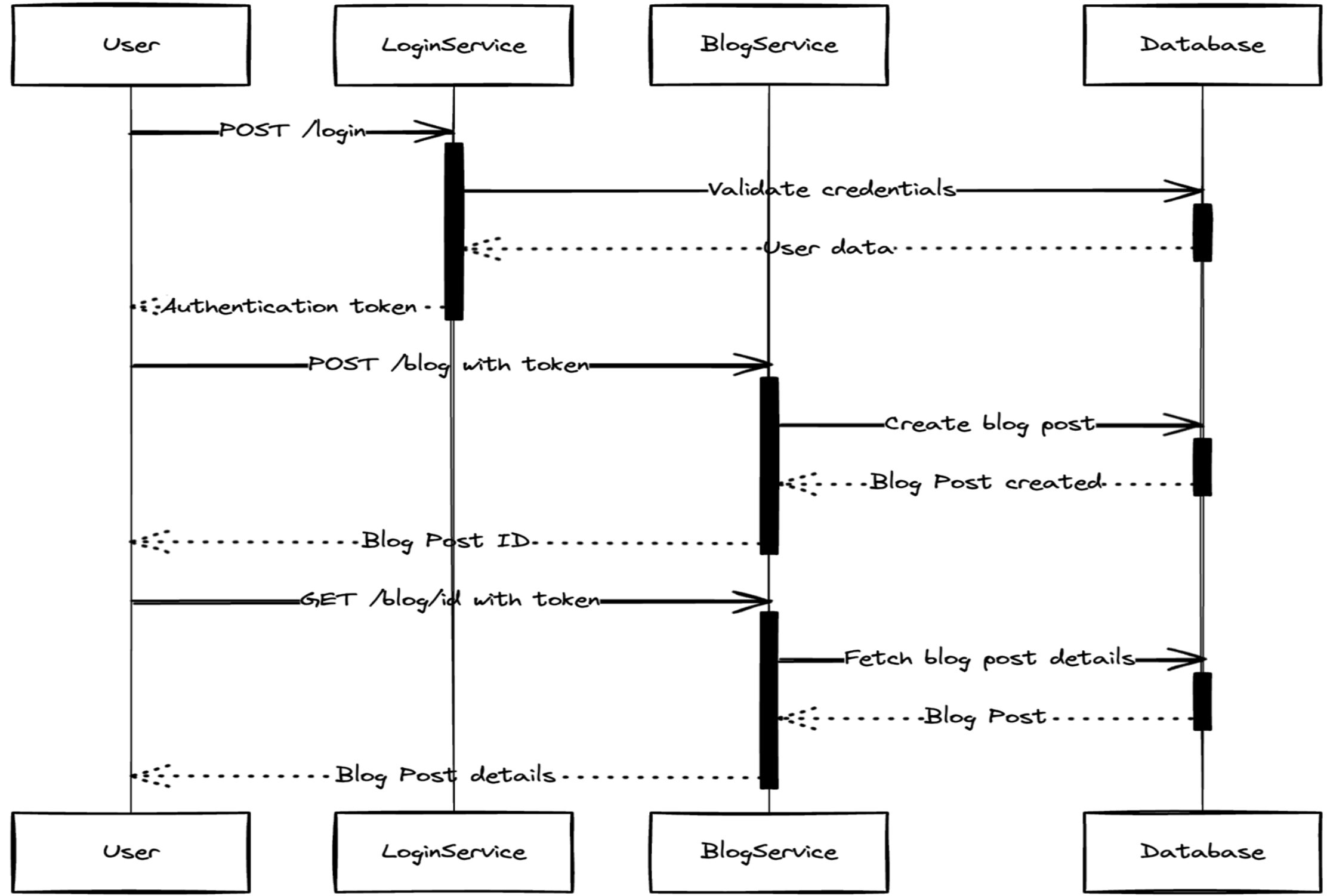
Response Analysis - never trust developers



INTERPRETING API REQUEST - ABSTRACTION

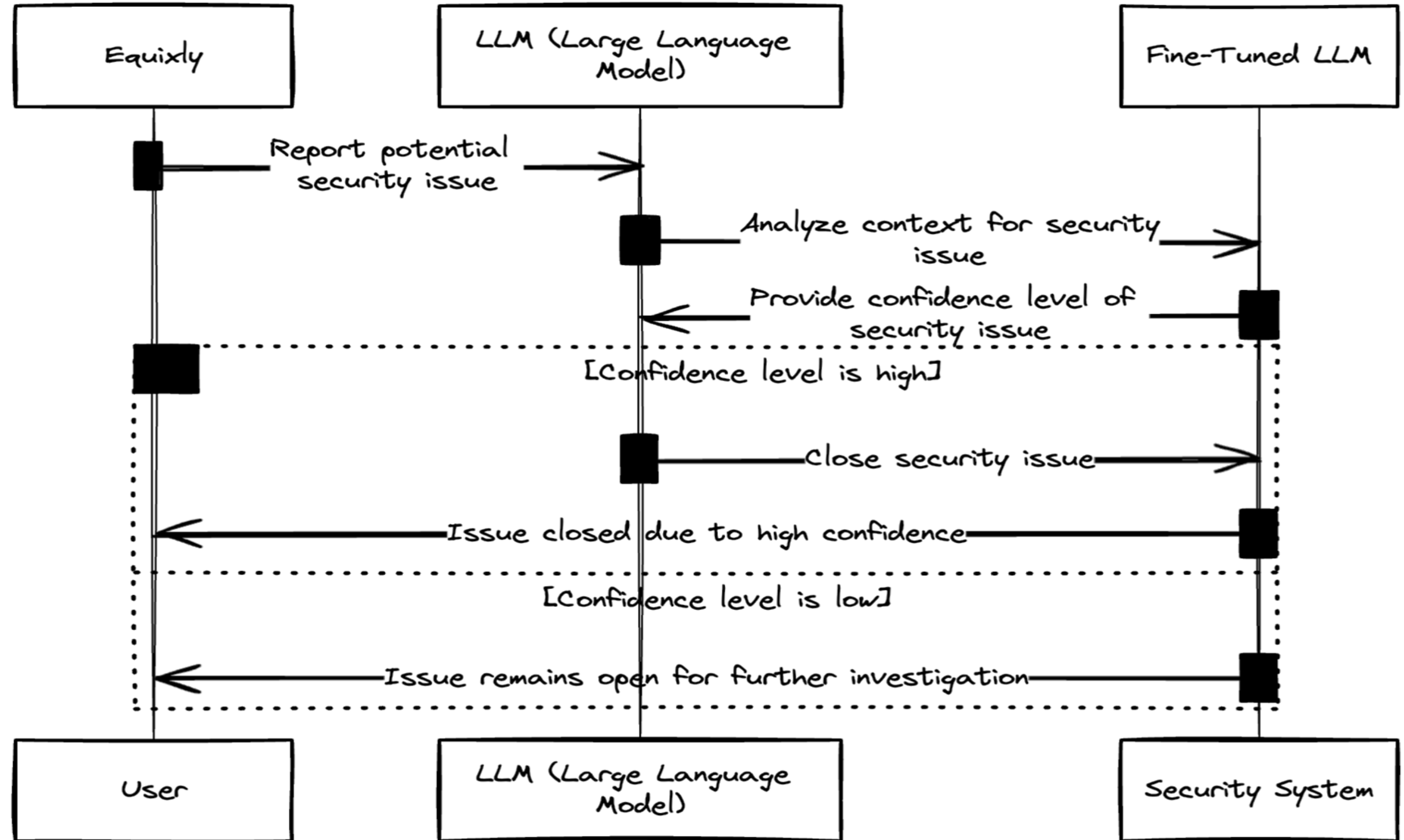


CONTEXT AWARENESS



CONTEXT AWARENESS

- Automated Security Triage
- Confidence Assessment
- Resolution Path



BOLA / Scans / Scan Detail / Issue Detail

Dashboard Scans Issues Inventory Settings

Issue Detail Exclude

Broken Object-Level Authorization NEW

Authentication

API	Severity	Confidence
GET /microservicebola/pandao/api/order/{order_id}	High	Certain

OWASP	CWE	CVSS
API-2023	639	6.5

Description

BOLA occurs when an application fails to implement adequate authorization checks at the object level, allowing users to access or manipulate resources they should not have access to.

In a typical BOL...

[Show more](#)

Remediation

To effectively remediate horizontal Broken Object Level Authorization on Enumeration resource, which involves unauthorized access to data belonging to other users, strengthen access control mechanisms...

[Show more](#)

API call

1	POST /microservicebola/login	Status: 200
2	POST /microservicebola/pandao/api/addorder	Status: 200
3	GET /microservicebola/pandao/api/order/144	Status: 200
4	GET /microservicebola/pandao/api/order/143	Status: 200

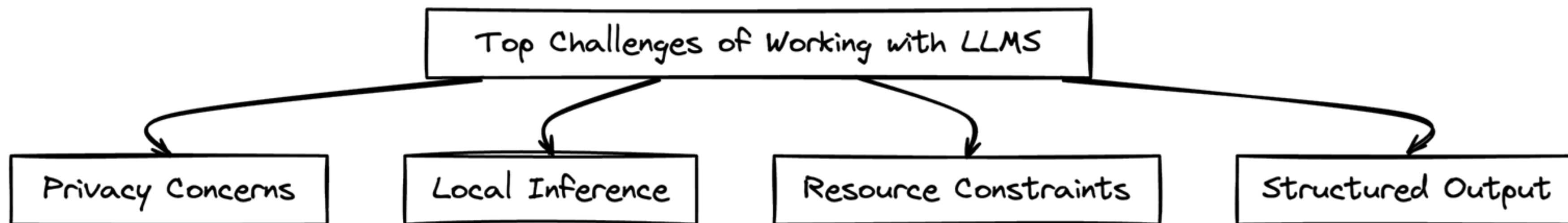
Request **Response**

```

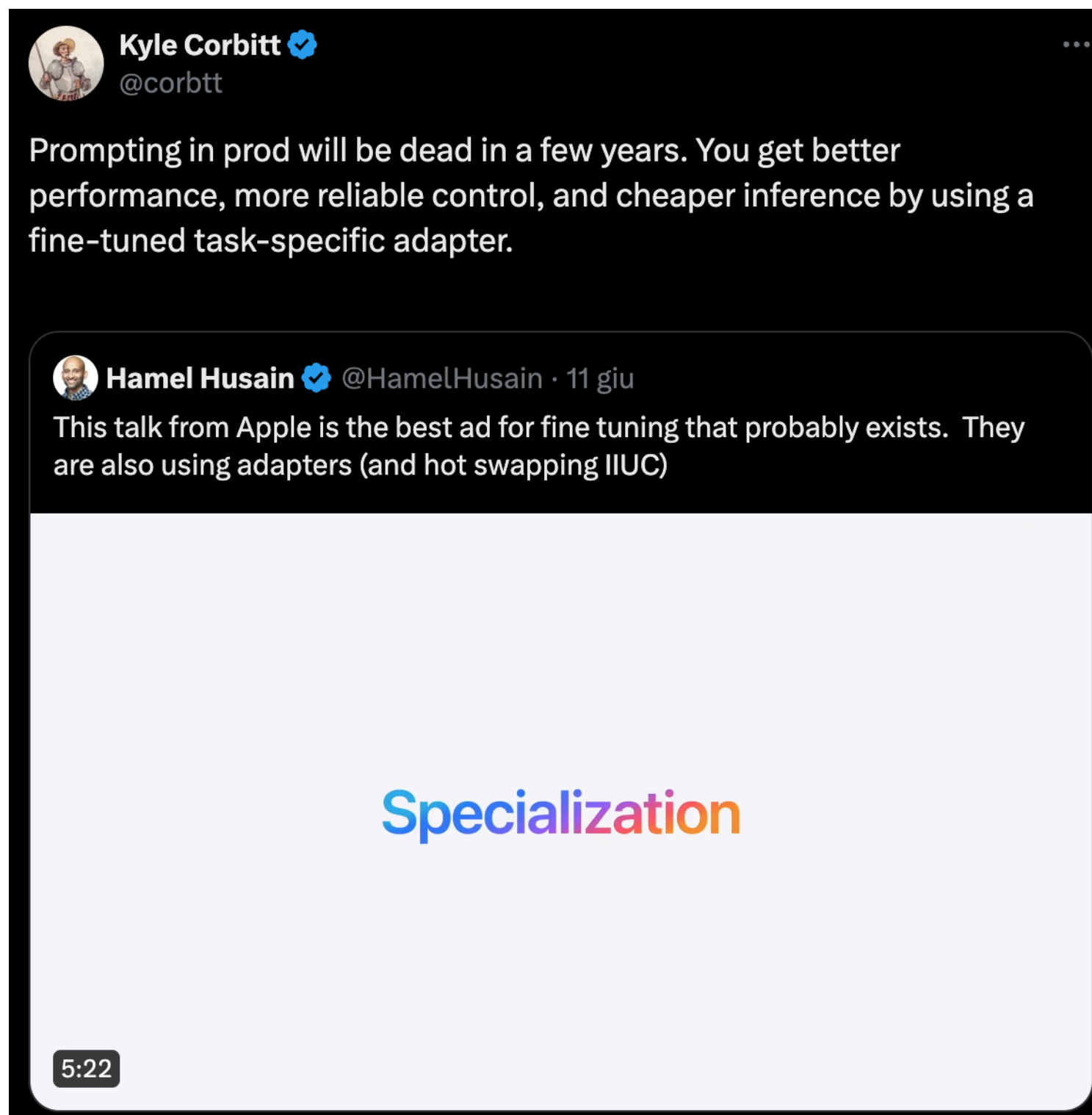
1 POST /microservicebola/login HTTP/1.1
2 Host: local.equixly.com:5656
3 Content-Type: application/json
4 User-Agent: Equixly/1.0 (API Security; ML-powered Testing)
5 X-Equixly-Auth-Profile: User1
6 X-Equixly-Sequence-Namespace: 11c814df-d4d2-4f8a-bf29-c6e6b6853e3d
7
8 {
9   "email": "user1@example.com",
10  "password": "password"
11 }
    
```


Reason

The resource identified as `order_id` is considered vulnerable. It should be protected and only accessible to authorized users. Public access to this resource could lead to unauthorized access and data breaches. The confidence level provided by the Equixly LLM model is **98.90%**, strongly indicating that this resource is indeed vulnerable and requires appropriate security measures.




- Fine Tuning



Kyle Corbitt 
@corbtt

Prompting in prod will be dead in a few years. You get better performance, more reliable control, and cheaper inference by using a fine-tuned task-specific adapter.

Hamel Husain  @HamelHusain · 11 giu

This talk from Apple is the best ad for fine tuning that probably exists. They are also using adapters (and hot swapping IUC)

Specialization

5:22

THANK YOU & QA

June 19th, 2024

Meet our team at

**Security
Summit**

Rome

Auditorium Della Tecnica

equixly

