INTRO

Enhancing API Security through LLM

A Novel Approach for Detecting BOLA Vulnerabilities

Alessio Dalla Piazza - Equixly

OWASP Italy @ Security Summit 2024 – Milan, 21st March

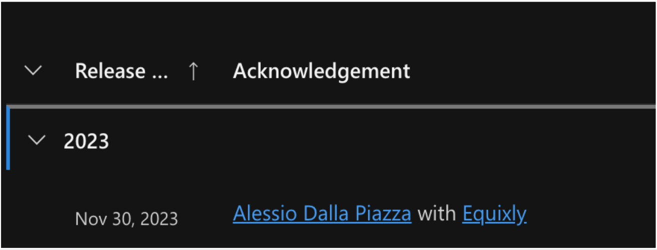
AGENDA

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

equixly

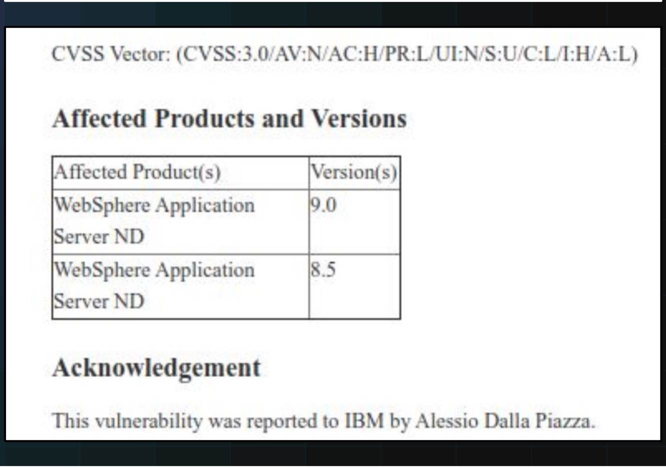
$ whoami – ALESSIO DALLA PIAZZA

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



2023

Nov 30, 2023 Alessio Dalla Piazza with Equixly

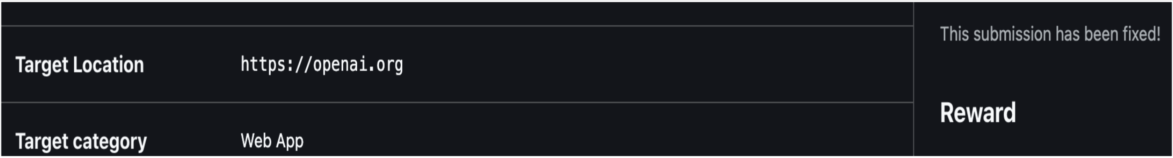

CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L)

Affected Products and Versions

Affected Product(s)	Version(s)
WebSphere Application Server ND	9.0
WebSphere Application Server ND	8.5

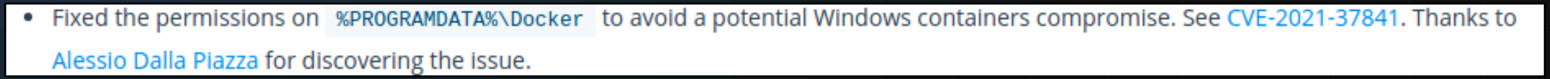
Acknowledgement

This vulnerability was reported to IBM by Alessio Dalla Piazza.


Target Location	https://openai.org
Target category	Web App

This submission has been fixed!

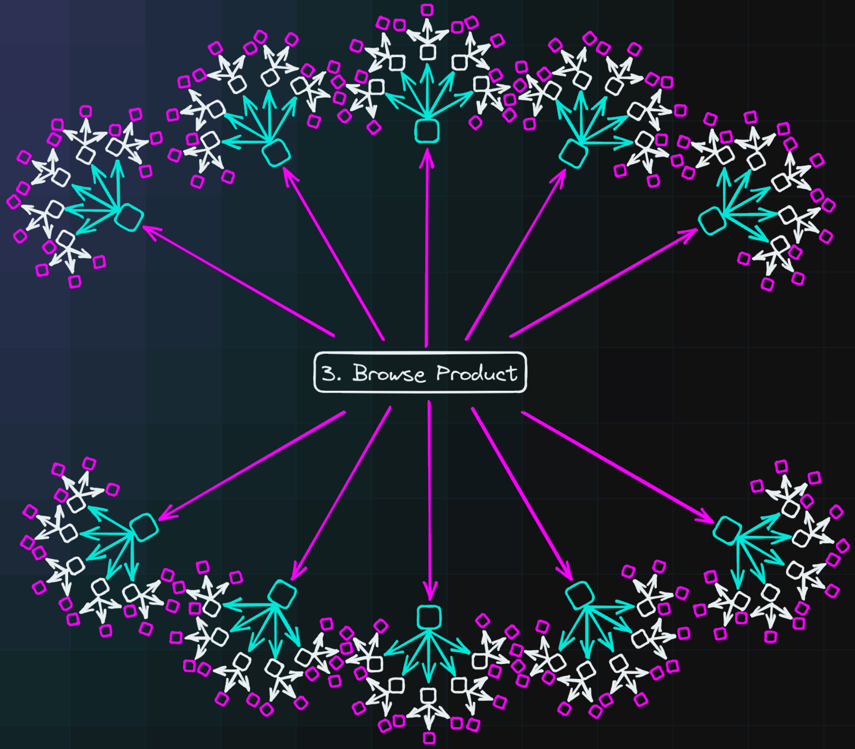
Reward


- Fixed the permissions on `%PROGRAMDATA%\Docker` to avoid a potential Windows containers compromise. See CVE-2021-37841. Thanks to Alessio Dalla Piazza for discovering the issue.

OWASP® Clusit SECURITY SUMMIT ASTREA

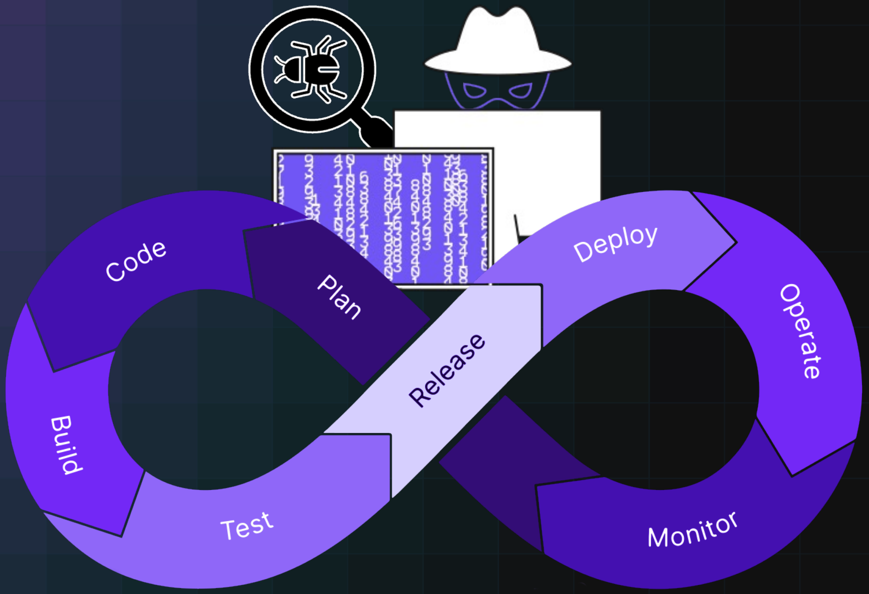
CONTINUOUS API PENETRATION TESTING

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



SHIFT-LEFT PRACTICES

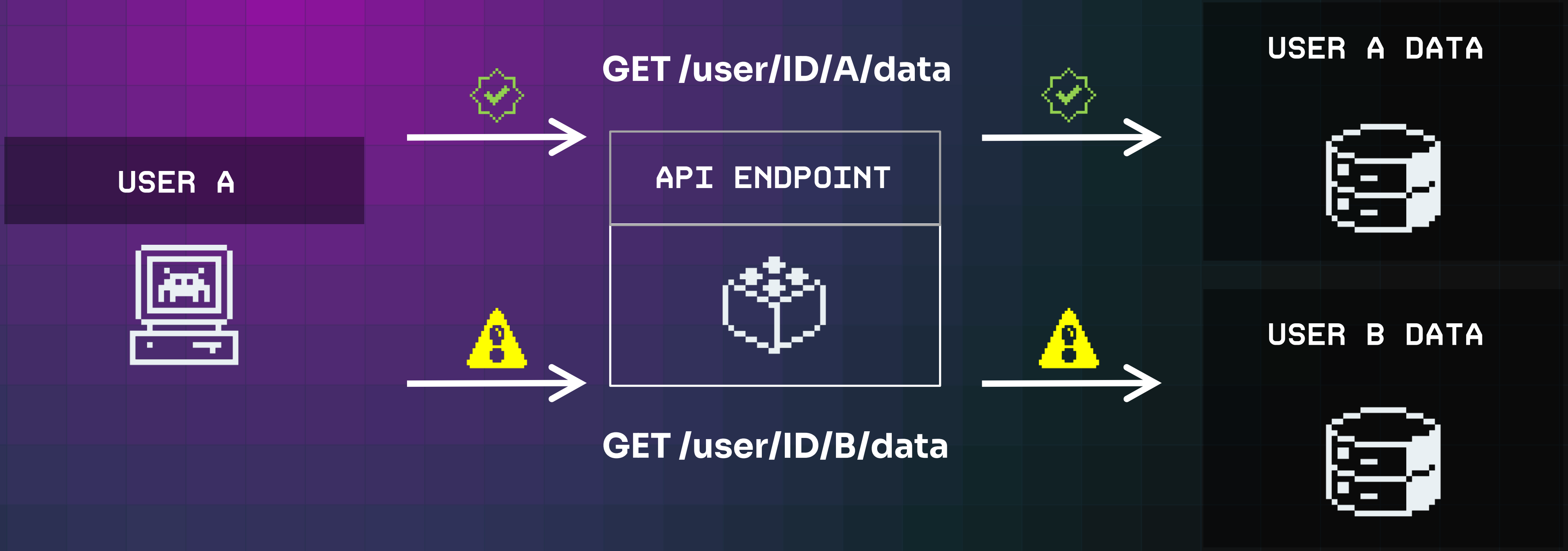
- **Integrate Early** – minimize risks
- **Continuous Evaluation** – test from Staging/QA
- **Cost-Effective** – fixing issues early cuts down the cost and time



OWASP API TOP 10: BUSINESS LOGIC

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

UNDERSTANDING BOLA VULNERABILITIES

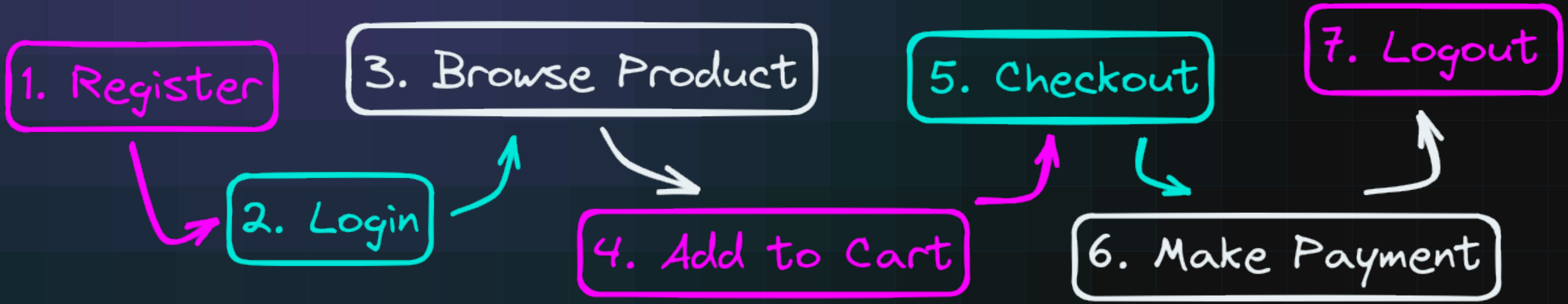


Users can substitute the ID of their own resource in the API call with an ID of a resource belonging to another user.

equixly

CHALLENGES IN AUTOMATING API TESTING

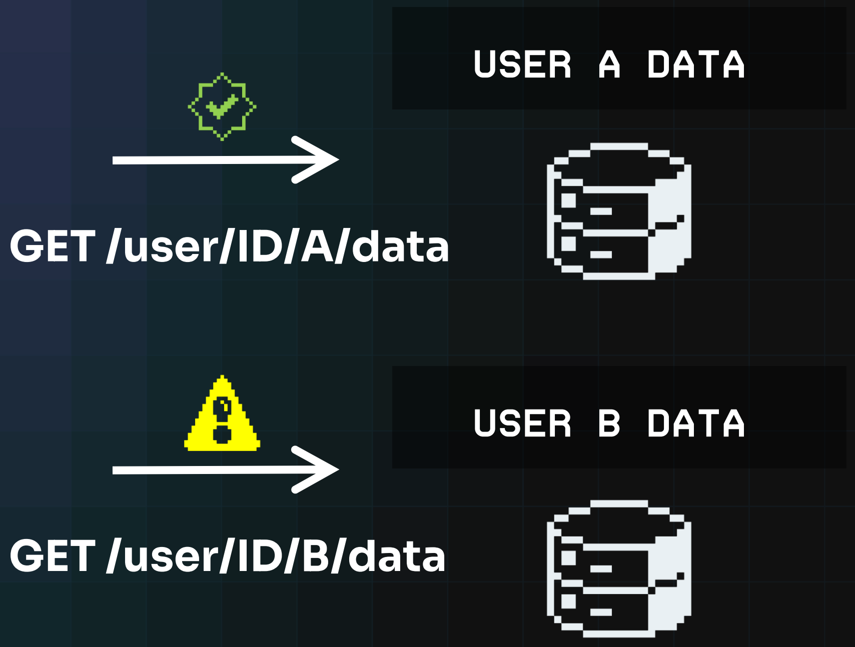
- **Spec Reliance** – flawed API documentation.
- **Business Logic**
- **Complex Auth** – intricate authentication methods.
- **Data Dependencies**
- **Multi-API Vulnerability**



equixly

INTERPRETING API REQUEST - ABSTRACTION

- **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.



USER A DATA

GET /user/ID/A/data

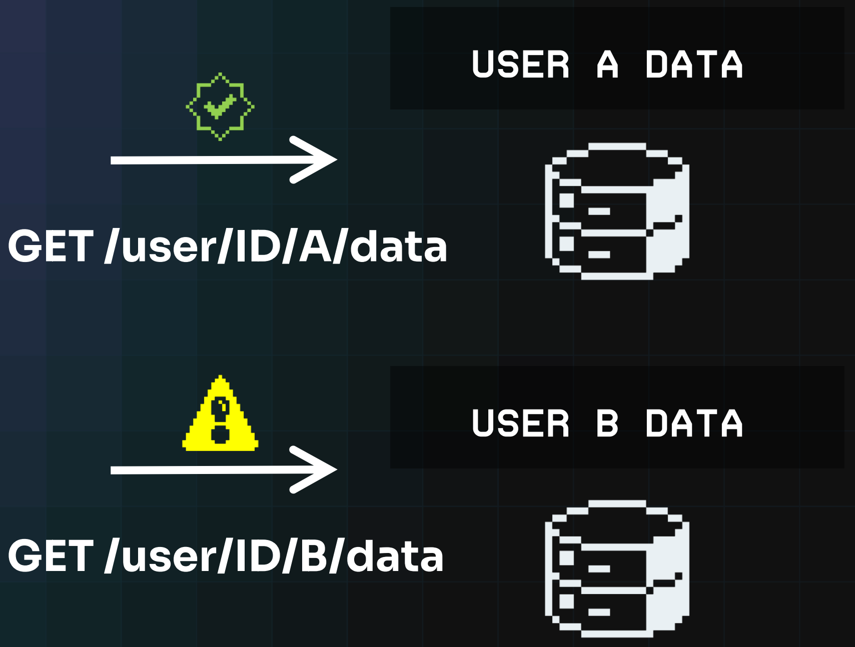
USER B DATA

GET /user/ID/B/data

equixly

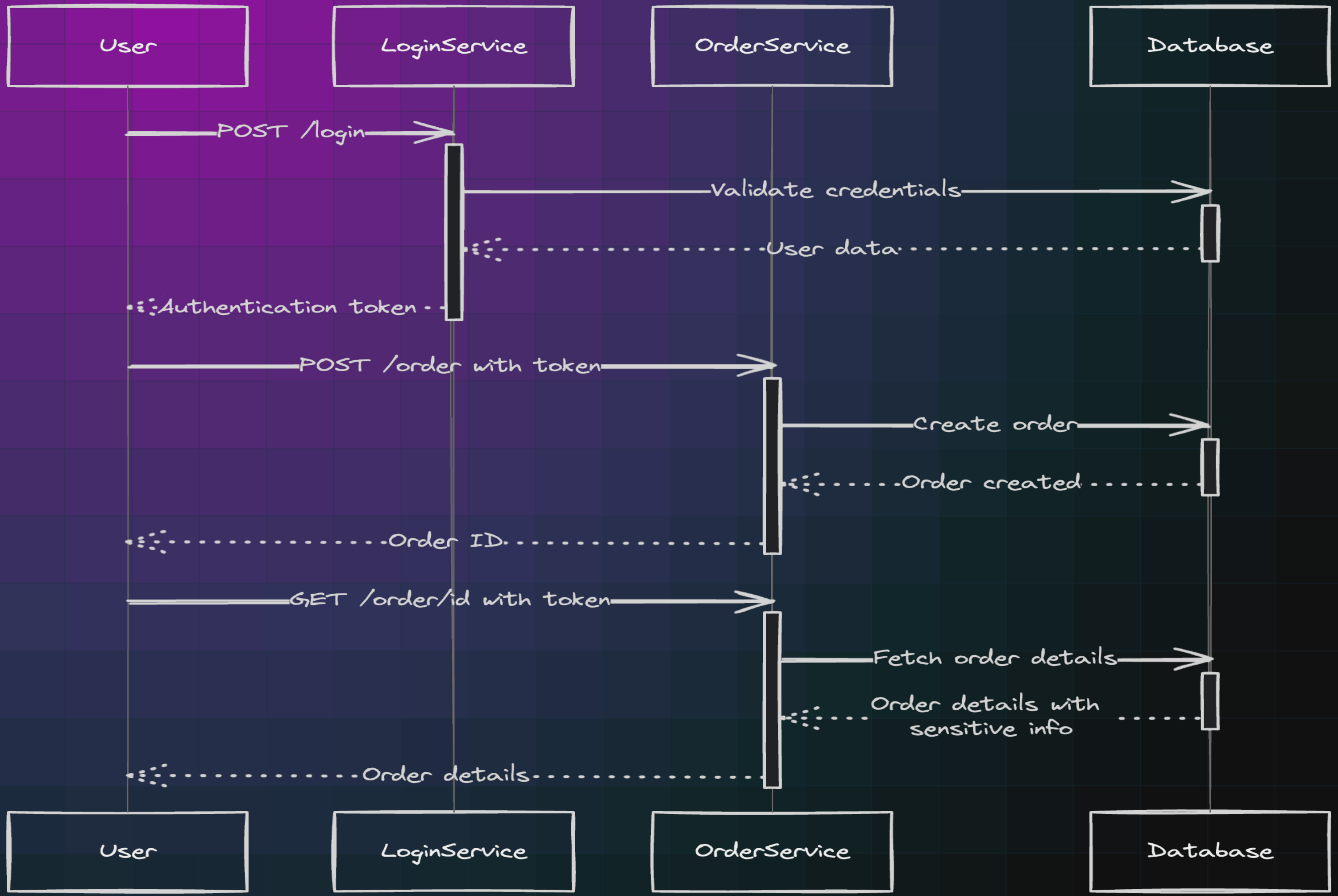
INTERPRETING API REQUEST - ABSTRACTION

- **Testing Scenarios** - tested unauthorized access by different roles
- **Response Analysis** - never trust developers



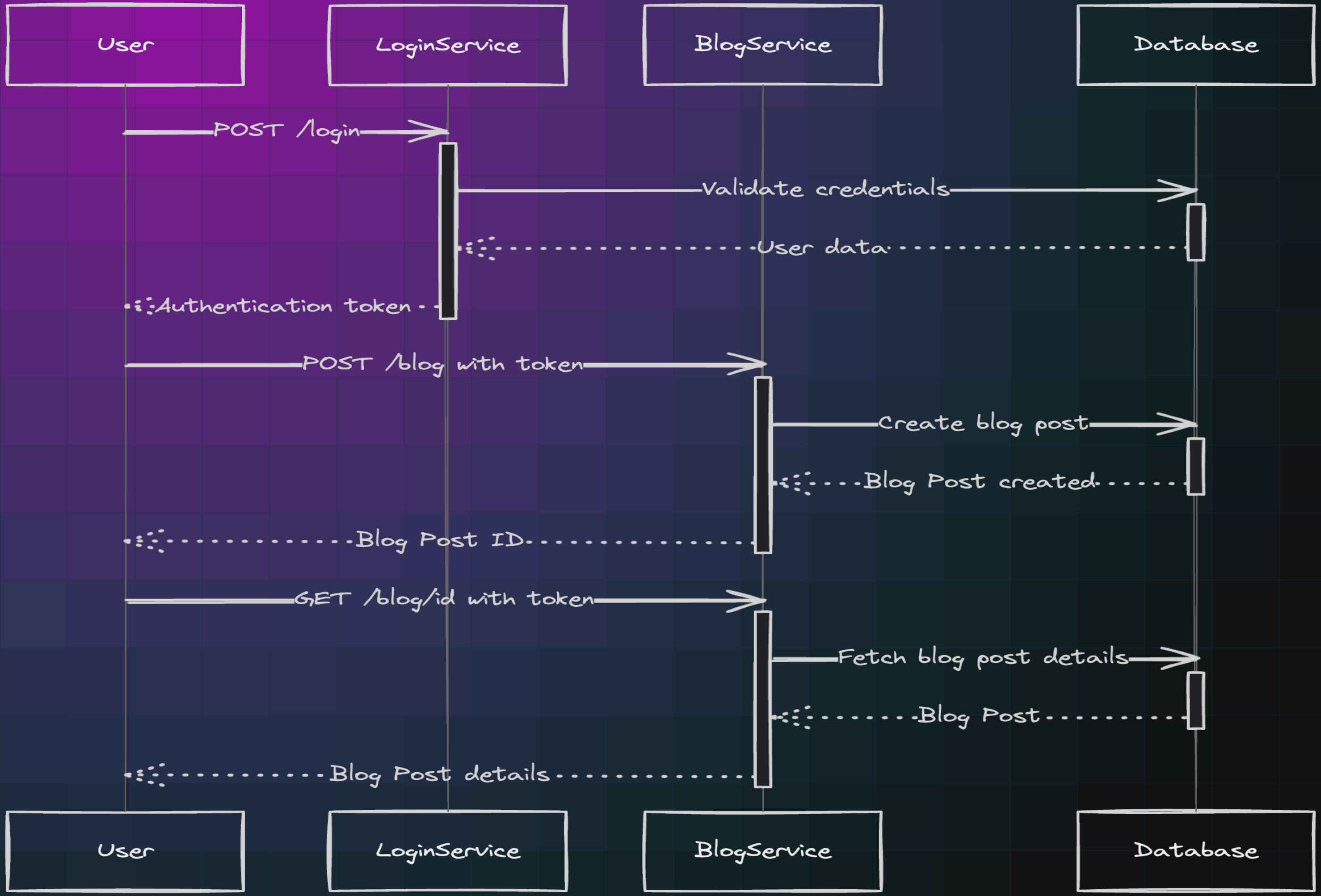
OWASP® Clusit

INTERPRETING API REQUEST - ABSTRACTION



equixly

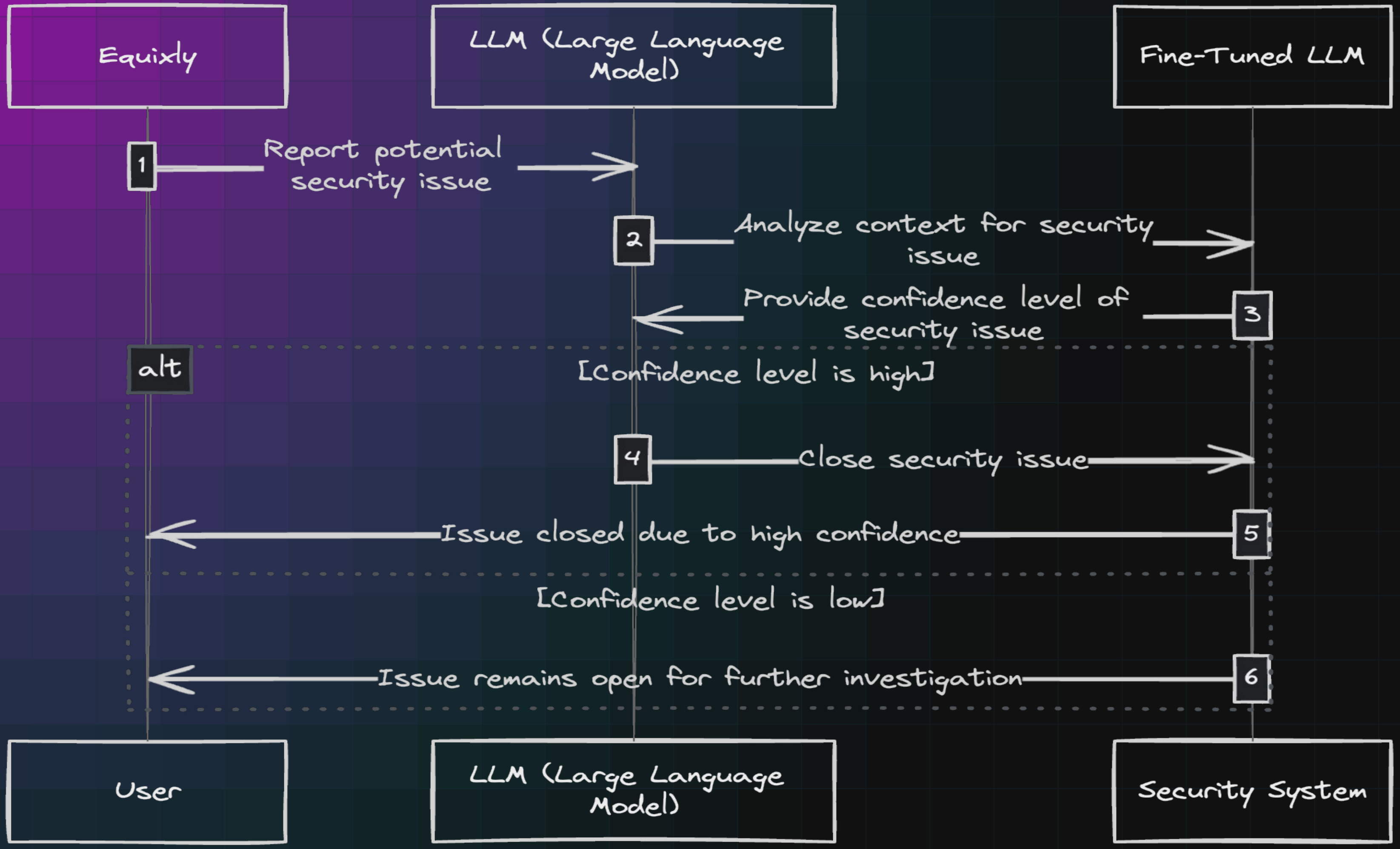
CONTEXT AWARENESS



OWASP® Clusit SECURITY SUMMIT ASTREA

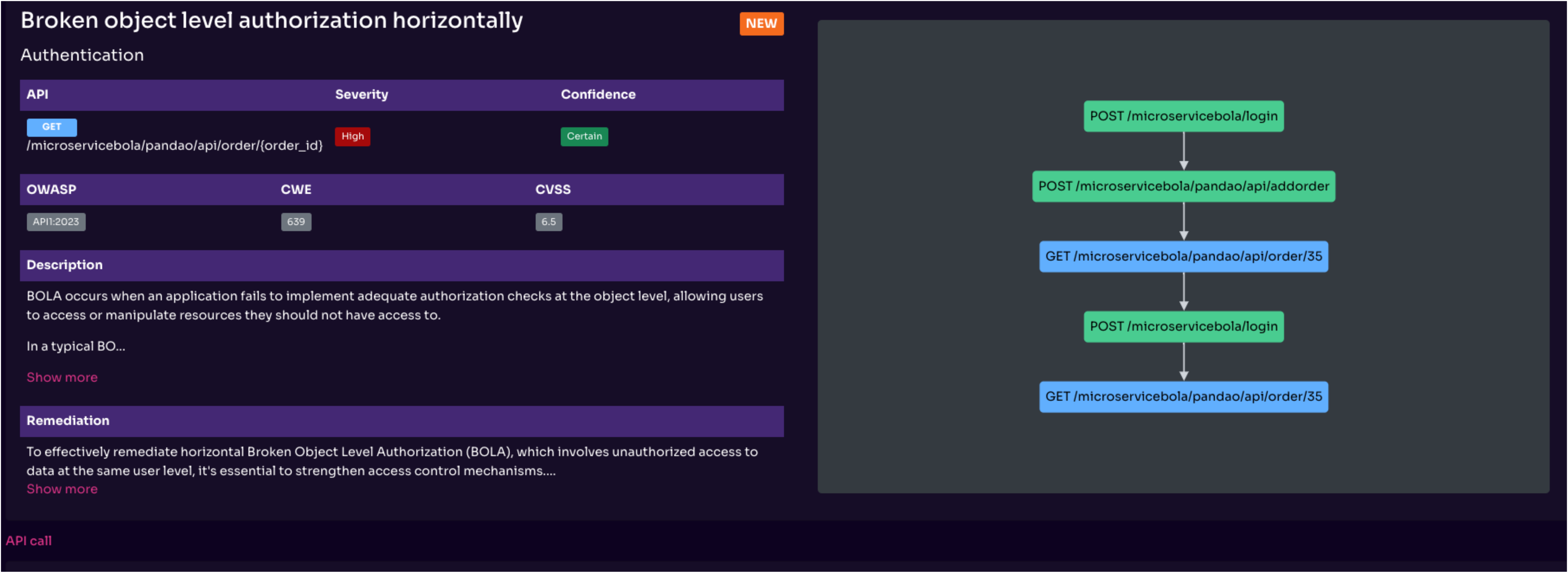
CONTEXT AWARENESS

- Automated Security Triage
- Confidence Assessment
- Resolution Path



Equixly
LLM (Large Language Model)
Fine-Tuned LLM
1
Report potential security issue
2
Analyze context for security issue
3
Provide confidence level of security issue
alt
[Confidence level is high]
4
Close security issue
5
Issue closed due to high confidence
[Confidence level is low]
6
Issue remains open for further investigation
User
LLM (Large Language Model)
Security System

EQUIXLY – ISSUE DETAILS



Broken object level authorization horizontally

NEW

Authentication

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

OWASP	CWE	CVSS
API1:2023	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 BO...

Show more

Remediation

To effectively remediate horizontal Broken Object Level Authorization (BOLA), which involves unauthorized access to data at the same user level, it's essential to strengthen access control mechanisms....

Show more

POST /microservicebola/login

POST /microservicebola/pandao/api/addorder

GET /microservicebola/pandao/api/order/35

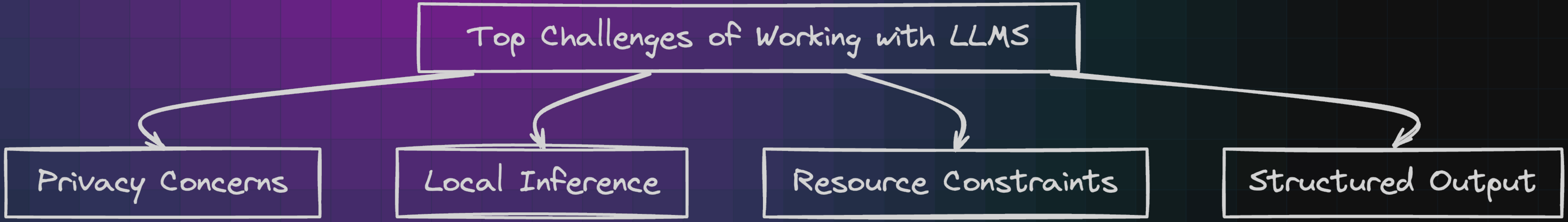
POST /microservicebola/login

GET /microservicebola/pandao/api/order/35

API call

equixly

CHALLENGES OF WORKING WITH LLMS


Top Challenges of Working with LLMS

Privacy Concerns

Local Inference

Resource Constraints

Structured Output

OWASP® Clusit SECURITY SUMMIT ASTREA

THANK YOU & QA