



## Security Summit Roma 19 giugno 2024



#### Alessio Dalla Piazza | CTO & Co-Founder Equixly









#### \$ whoami - ALESSIO DALLA PIAZZA

- Inspired by the <u>RBT4</u> forum
- Cybersecurity Consulting (10+ years)
- Passion for breaking things. CVEs (Apple Safari, VMWare, IBM Websphere, Docker...)

2

Co-Founder at Equixly AI-Powered API Security Testing Platform











#### AGENDA

1.	\$ whoami	6.	Challeng
2.	Continuous API Active Testing	7.	Interpre
3.	Shift Left Practices	8.	Interpre

- 4. OWASP API Top 10: Business Logic 9. Challe
- 5. Understanding BOLA Vulnerabilities



nges in Automating API Testing

reting API Requests-Abstraction

reting Results with LLMs

9. Challenges of Working with LLMs





## 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









### CONTINUOUS API PENETRATION TESTING



# API CONTINUOUS TESTING TAKE TO LONG ~ 4/6 HOURS

# ENGAGE ONE-SHOT PENETRATION TEST









#### 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









#### OWASP API TOP 10: BUSINESS LOGIC









## LIMITATION OF EXISTING TOOLS IN RESTFUL API

- 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







#### ZED ATTACK PROXY - ZAP COVERAGE

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

	Untitled Session - ZAP 2.15.0				
Standard Mode 🗸 🗋 🖨 🖬 💼 💼 🏶 📲 🛋 📼 🗈	∃ 🗖 🗖 🖬 🖬 🖶 纋 🖓   👄 🕨 🕨 🗡 🔗 💢	IIII 🐀 📼 🛛 🔮	•		
Sites 🕂	✓ ♀ Quick Start	ester 🛨			
	Header: Text     >       Body: Text     >				
<ul> <li>Contexts</li> <li>Default Context</li> <li>Sites</li> </ul>	GET http://127.0.0.1:5656/microservicebola/docu host: 127.0.0.1:5656 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64 pragma: no-cache cache-control: no-cache accept: application/json content-length: 0 Authorization: Bearer eyJhbGci0iJIUzI1NiISInR5c eyJlbWFpbCI6InVzZXIxQGV4YW1wbGUuY29tIiwiZXhwIjo	uments/10 HTTP/1. ; x64; rv:125.0) cCI6IkpXVCJ9. pxNzE4NTM0NTY3LCJ	1 Gecko/201 J1c2VySUQiO	l00101 Firefox/125.0 DjIsInV1aWQiOiI11ZDc0Y1	<sup>-</sup> QwYS0zMjViLTQxYjE
🗮 History 🔍 Search 📑 Alerts 📄 Output 📼 Progr	ress 🔸				
Staten → Netts → Staten → Netts					
ID Source Req. Timestamp Method	URL C	Code \land Reason	RTT Size R	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 bv	/tes 🂫 Low	ISON
11 🍓 Manual 6/13/24, 12:44:18 PM GET http://	//127.0.0.1:5656/microservicebola/community/forum	200 OK	4 ms 373 b	ovtes 💫 Low	ISON
15 🍓 Manual 6/13/24, 12:44:18 PM POST http://	//127.0.0.1:5656/microservicebola/crowdsignal/createt	200 OK	7 ms 62 bv	/tes P Low	ISON
19 🥮 Manual 6/13/24 12:44:18 PM CET http:/	//127.0.0.1.5656/microservicebola/docs/index.html	200 OK	4 ms 3 728	8 bytes 🕒 Medium	Script
22 Manual 6/13/24 12:44:18 PM CET http:	,, 12, 101011.5050, merosen neebola, accs, maeximum				201101
	//127.0.0.1.5656/microservicebola/documents/10	200 OK	3 ms 137 h	ovtes Plow	ISON
24 4 Manual 6/13/24, 12:44:18 PM GET http:/	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/ani/manage</pre>	200 OK	3 ms 137 b 9 ms 25 by	bytes P Low	JSON
24 Manual 6/13/24, 12:44:18 PM GET http: 33 Manual 6/13/24 12:44:18 PM GET http:	//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/ggl.reddit.com/subr	200 OK 200 OK 200 OK	3 ms 137 b 9 ms 25 by 4 ms 97 by	ytes PLow /tes PLow	JSON JSON JSON
24 @ Manual 6/13/24, 12:44:18 PM GET http: 33 @ Manual 6/13/24, 12:44:18 PM GET http: 36 @ Manual 6/13/24, 12:44:18 PM POST http:	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/norr/ypn/api/y1/ord</pre>	200 OK 200 OK 200 OK 200 OK	3 ms 3,720 3 ms 137 b 9 ms 25 by 4 ms 97 by 4 ms 752 b	ytes P Low ytes P Low	JSON JSON JSON JSON
24 @ Manual 6/13/24, 12:44:18 PM GET http: 33 @ Manual 6/13/24, 12:44:18 PM GET http: 36 @ Manual 6/13/24, 12:44:18 PM POST http: 40 @ Manual 6/13/24, 12:44:18 PM POST http:	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderputeration/g</pre>	200 OK 200 OK 200 OK 200 OK 200 OK	3 ms         137 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b	bytes     P Low       ytes     P Low       ytes     P Low       ytes     D Low       bytes     Low	JSON JSON JSON JSON
22         Manual 6/13/24, 12:44:18 PM         GET         http://discrete           24         Manual 6/13/24, 12:44:18 PM         GET         http://discrete           33         Manual 6/13/24, 12:44:18 PM         GET         http://discrete           36         Manual 6/13/24, 12:44:18 PM         POST         http://discrete           40         Manual 6/13/24, 12:44:18 PM         POST         http://discrete           42         Manual 6/13/24, 12:44:18 PM         CET         http://discrete	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderenumeration/g //127.0.0.1:5656/microservicebola/orderenumeration/g</pre>	200 OK 200 OK 200 OK 200 OK 200 OK	3 ms         137 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b	Pytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       oytes     Py Low       oytes     Py Low       oytes     Py Low	JSON JSON JSON JSON JSON
22         Manual 6/13/24, 12:44:18 PM         GET         http://discourse           24         Manual 6/13/24, 12:44:18 PM         GET         http://discourse           33         Manual 6/13/24, 12:44:18 PM         GET         http://discourse           36         Manual 6/13/24, 12:44:18 PM         POST         http://discourse           40         Manual 6/13/24, 12:44:18 PM         POST         http://discourse           42         Manual 6/13/24, 12:44:18 PM         GET         http://discourse           43         Manual 6/13/24, 12:44:18 PM         GET         http://discourse	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderenumeration/g //127.0.0.1:5656/microservicebola/orderenumeration/or //127.0.0.1:5656/microservicebola/norderenumeration/or</pre>	200 OK 200 OK 200 OK 200 OK 200 OK 200 OK	3 ms         137 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b           4 ms         1,789           4 ms         1,789	Pytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       oytes     Py Low	JSON JSON JSON JSON JSON JSON
22       Manual 6/13/24, 12:44:18 PM       GET       http://discussion.pdf         24       Manual 6/13/24, 12:44:18 PM       GET       http://discussion.pdf         33       Manual 6/13/24, 12:44:18 PM       GET       http://discussion.pdf         36       Manual 6/13/24, 12:44:18 PM       POST       http://discussion.pdf         40       Manual 6/13/24, 12:44:18 PM       POST       http://discussion.pdf         42       Manual 6/13/24, 12:44:18 PM       GET       http://discussion.pdf         43       Manual 6/13/24, 12:44:18 PM       GET       http://discussion.pdf         47       Manual 6/13/24, 12:44:18 PM       CET       http://discussion.pdf	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderenumeration/g //127.0.0.1:5656/microservicebola/orderenumeration/or //127.0.0.1:5656/microservicebola/paginated/payout?pa //127.0.0.1:5656/microservicebola/paginated/payout?pa</pre>	200 OK 200 OK 200 OK 200 OK 200 OK 200 OK 200 OK	3 ms         3,726           3 ms         137 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b           4 ms         1,789           4 ms         49 by           4 ms         49 by	Pytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       oytes     Py Low	JSON JSON JSON JSON JSON JSON JSON
22       Manual 6/13/24, 12:44:18 PM       GET       http://discourses/action	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderenumeration/g //127.0.0.1:5656/microservicebola/paginated/payout?pa //127.0.0.1:5656/microservicebola/paginated/payout?pa //127.0.0.1:5656/microservicebola/paginated/payout?pa</pre>	200 OK	3 ms         3,72 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b           4 ms         1,789           4 ms         49 by           4 ms         38 by	Poytes     Pu Low       ytes     Pu Low       ytes     Pu Low       ytes     Pu Low       poytes     Pu Low       ytes     Pu Low       ytes     Pu Low       ytes     Pu Low       ytes     Pu Low	JSON JSON JSON JSON JSON JSON JSON JSON
22       Manual 6/13/24, 12:44:18 PM       GET       http:,         24       Manual 6/13/24, 12:44:18 PM       GET       http:,         33       Manual 6/13/24, 12:44:18 PM       GET       http:,         36       Manual 6/13/24, 12:44:18 PM       POST       http:,         40       Manual 6/13/24, 12:44:18 PM       POST       http:,         42       Manual 6/13/24, 12:44:18 PM       GET       http:,         43       Manual 6/13/24, 12:44:18 PM       GET       http:,         47       Manual 6/13/24, 12:44:18 PM       GET       http:,         50       Manual 6/13/24, 12:44:18 PM       GET       http:,         21       Manual 6/13/24, 12:44:18 PM       GET       http:,         50       Manual 6/13/24, 12:44:18 PM       GET       http:,         21       Manual 6/13/24, 12:44:18 PM       GET       http:,         50       Manual 6/13/24, 12:44:18 PM       GET       <	<pre>//127.0.0.1:5656/microservicebola/documents/10 //127.0.0.1:5656/microservicebola/evilsite/api/manage //127.0.0.1:5656/microservicebola/gql.reddit.com/subr //127.0.0.1:5656/microservicebola/nordvpn/api/v1/ord //127.0.0.1:5656/microservicebola/orderenumeration/g //127.0.0.1:5656/microservicebola/orderenumeration/or //127.0.0.1:5656/microservicebola/paginated/payout?pa //127.0.0.1:5656/microservicebola/pandao/api/addorder //127.0.0.1:5656/microservicebola/pandao/api/order/10 //127.0.0.1:5656/microservicebola/documents/</pre>	200 OK           200 OK	3 ms         3,72 b           9 ms         25 by           4 ms         97 by           4 ms         752 b           6 ms         125 b           4 ms         1,789           4 ms         49 by           4 ms         38 by           3 ms         241 b	Pytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       pytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       ytes     Py Low       pytes     Py Low	JSON JSON JSON JSON JSON JSON JSON JSON





#### equi∷ly

#### equixly API SECURITY COVERAGE

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

→ bola_evils	ite_get_companyid[200  $\checkmark$ ] $\rightarrow$ bola_mopub_g
INF0[15691]	■ bola_crowdsignal_add_team_member -
INF0[15691]	bola_crowdsignal_create_team - POST
INF0[15691]	bola_crowdsignal_get_user_info - GE
INF0[15691]	bola_docs - GET /microservicebola/d
INF0[15691]	bola_evilsite_get_companydata - GET
INF0[15691]	bola_evilsite_get_companyid - GET /
INF0[15691]	bola_forum_create-document - POST /
INF0[15691]	bola_forum_get-document - GET /micr
INF0[15691]	bola_forum_list-post - GET /microse
INF0[15691]	bola_login_user - POST /microservice
INF0[15691]	<ul> <li>bola_logout - GET /microservicebola</li> </ul>
INF0[15691]	bola_mopub_create_order - POST /mic
INF0[15691]	■ bola_mopub_get_mopub_list_orders -
INF0[15691]	bola_nordvpn_nordorderlist - POST /i
INF0[15691]	bola_orderenumeration_gettransaction
INF0[15691]	bola_orderenumeration_orders - GET ,
INF0[15691]	bola_pagination_consumer - GET /mic
INF0[15691]	bola_pagination_producer - GET /mic
INF0[15691]	bola_pandao_add_order - POST /micros
INF0[15691]	bola_pandao_list_order - GET /micros
INF0[15691]	bola_reddit_get_subreddit_names - G
INF0[15691]	bola_reddit_subreddits_moderator_lo
INF0[15691]	bola_register - POST /microserviceb
INF0[15691]	bola_vehicle_get_vehicle - GET /mic
INF0[15691]	
INF0[15691]	Stats - coverage: 100.00%, reached: 100



```
et_mopub_list_orders[200|√] → bola_evilsite_get_companydata[200|√] → bola_crowdsig
POST /microservicebola/crowdsignal/addteammember
/microservicebola/crowdsignal/createteam
  /microservicebola/crowdsignal/userinfo/{TEAMID}/{USERID}
/microservicebola/evilsite/api/managements/v1/companies/{company_id}/accounts
microservicebola/evilsite/api/managements/v1/companies
nicroservicebola/documents
oservicebola/documents/{document_id}
rvicebola/community/forum
ebola/login
/logout
roservicebola/app.mopub.com/web-client/api/orders/create
GET /microservicebola/app.mopub.com/web-client/api/orders/stats/query/{order_id}
microservicebola/nordvpn/api/v1/orders
  - POST /microservicebola/orderenumeration/gettransaction
/microservicebola/orderenumeration/orders
roservicebola/paginated/payout/{user_id}
roservicebola/paginated/payout
servicebola/pandao/api/addorder
servicebola/pandao/api/order/{order_id}
ET /microservicebola/gql.reddit.com/subreddits
gs - POST /microservicebola/gql.reddit.com
ola/register
roservicebola/vehicle/user/{UUID}
```

.00%, attempted: 100.00%





### equixly API SECURITY COVERAGE

÷	$\rightarrow$ C	ට් 🎧 🖙 demo.equixly.com/projects/7b859cac-26c1-4434-b279-272aaa834055/scans/bd72907f-4c0b-4463-be6e-926064b8ba6c?pageSize=48#a	utho
x	BOLA	/ Scans / Scan Detail	
	Genera	al Issues 4 Authorization Matrix HTTP History Inventory Settings	
	Metho	od Path	
	All		
	GET	/microservicebola/vehicle/user/{UUID}	
	POST	/microservicebola/register	
	GET	/microservicebola/pandao/api/order/{order_id}	
	POST	/microservicebola/pandao/api/addorder	
	GET	/microservicebola/paginated/payout/{user_id}	
<b>o</b>	GET	/microservicebola/paginated/payout	
000	GET	/microservicebola/orderenumeration/orders	
	POST	/microservicebola/orderenumeration/gettransaction	
	POST	/microservicebola/nordvpn/api/v1/orders	
	GET	/microservicebola/logout	
	POST	/microservicebola/login	
	GET	/microservicebola/gql.reddit.com/subreddits	
	POST	/microservicebola/gql.reddit.com	
	GET	/microservicebola/evilsite/api/managements/v1/companies/{company_id}/accounts	
	GET	/microservicebola/evilsite/api/managements/v1/companies	
	GET	/microservicebola/documents/{document_id}	
	POST	/microservicebola/documents	
	GET	/microservicebola/docs/index.html	
	GET	/microservicebola/crowdsignal/userinfo/{TEAMID)/{USERID}	
	POST	/microservicebola/crowdsignal/createteam	
	POST	/microservicebola/crowdsignal/addteammember	
	GET	/microservicebola/community/forum	
	GET	/microservicebola/app.mopub.com/web-client/api/orders/stats/query/{order_id}	
	POST	/microservicebola/app.mopub.com/web-client/api/orders/create	



ition-matrix	ବ୍	\$ 	۵ 🔞	X	-	<b>D</b>		:
		Dashb	oard Sca	ans Issu	ies Ir	nventory	Setti	ngs
							enort	
							eport	
read			/					
register						~		
read			1					
create			/					
read			/					
read			/					
read			/					
read			/					
read						~		
logout			1					
login			1			~		
read			1					
read			/					
read			/					
read			/					
read			/					
create			/					
read						~		
read			/					
create			/					
create								
read			/					
read			/					
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



GET/user/ID/B/data

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











#### CHALLENGES IN AUTOMATING API TESTING

- Spec Reliance flawed API
   Data Dep documentation.
- Business Logic
- Complex Auth intricate authentication methods.



Data Dependencies

Multi-API Vulnerability







## INTERPRETING API REQUEST - ABSTRACTION

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

Access Verification - <u>READ</u> operations do not retrieve unauthorized resources.

Resource Tracking - <u>CREATE</u> operations are tagged and tracked.









## INTERPRETING API REQUEST - ABSTRACTION

**Testing Scenarios - tested unauthorized** access by different roles

Response Analysis – never trust developers





GET/user/ID/A/data



**USER A DATA** 



#### GET/user/ID/B/data







#### INTERPRETING API REQUEST - ABSTRACTION









#### CONTEXT AWARENESS









### CONTEXT AWARENESS









#### EQUIXLY - ISSUE DETAILS

<pre>state bases</pre>	BOLA / Scans / Scan Detail / Issue D	etail				
Broken Object-Level Authorization   Authentication   Apl   Severity   Confidence   Image: Severity   Owase   Cve   Cve   Cve   Cve   Cve   Cve   Cve   Description   Bob Access why should not have access to:   Brow more   Femediation   Cve   Cve <td>Issue Detail</td> <td></td> <td></td> <td></td> <td></td> <td></td>	Issue Detail					
API Severity Confidence   Import Service bola/pandaolapilorder/(order_id) Import Service bola/pandaolapilorder/(order_id) Import Service bola/pandaolapilorder/(order_id)   OWASP OVE CVES   Import Service bola/pandaolapilorder/(order_id) Import Service bola/pandaolapilorder/(order_id) Import Service bola/pandaolapilorder/(order_id)   Description Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Show more Show more Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Femediation Stress for Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Show more Stress for Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Femediation Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Show more Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Femediation Import Service bola/pandaolapilorder/id Import Service bola/pandaolapilorder/id   Show more Import Service bola/pandaolapilorder/id	Broken Object-Level A Authentication	uthorization		NEW		
Image: Severe Sever	ΑΡΙ	Severity	Confidence			
Owasp Owe Oves     Owasp Owe        Owasp Owe        Owasp Owe              Owasp Owe <td>GET 7 /microservicebola/pandao/api/order/{</td> <td>order_id}</td> <td>Certain</td> <td></td> <td></td> <td>POST /mi</td>	GET 7 /microservicebola/pandao/api/order/{	order_id}	Certain			POST /mi
APR2023 697 65     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   AP call   Implement access control mechanisms   Show access to data belonging to other users, strengthen access control mechanisms   Show more   Ap call   Implement access control mechanisms   Show 200   Implement access control mechanisms   <	OWASP	CWE	CVSS			
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       Fost / Interoservicebolalgendoa/apiloadourier         2       Fost / Interoservicebolalgendoa/apiloadourier         3       Scotter: Type: application/sion         3       Section: Zoon         4)       Tote (Interoservicebolalgendoa/apiloadourier/IA4         3       Scotter: Type: application/sion         4)       Thereare the collagendoa/apilorder/IA4         5       Scotter: Type: application/sion         3       Scotter: Type: application/sion         4       Scotter: Type: application/sion         5       Scotter: Type: application/sion         5       Scotter: Type: application/sion         4       Stotus: 200         7       Stotus: 200         9       "easily-Sequence-Namespace: 11c814df-4dd2-4f8a-bf29-c6e6b6b358:ad         7	API1:2023	639	6.5			POST /microserv
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  I _ DOIT _ /microservicebolal/pandao/apl/addorder 2 _ POST _ /microservicebolal/pandao/apl/addorder 3 _ DOIT _ /microservicebolal/pandao/apl/addo	Description					
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  I POST /microservicebola/padiao/api/addorder  C Post /microservicebola/padiao/api/addorder  C Post /microservicebola/padiao/api/addorder/ C Post /microservicebola/padi	BOLA occurs when an application fails	to implement adequate authorization	n checks at the object level, allowing users to access	s or manipulate		GET /microservi
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  I POST /microservicebola/pandao/api/addorder Status: 200  C POST /microservicebola/pandao/api/addorder Status: 200  C microservicebola/pandao/api/addorder/I44 Status: 200  C microservicebola/pandao/api/addorder/I44 Status: 200  C microservicebola/pandao/api/odder/I44 Status: 200  C microservicebola/pandao/api/odde	In a typical BOI					
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         2       POST         2       POST         3       OET         3       OET         3       OET         4       OET         9       "maintorservicebola/apil/addorder/144         5       X-Equixty-1.00 (API Security; ML-powered Testing)         5       X-Equixty-2.00         4       OET         9       "maintorservicebola/apil/addorder/144         5       X-Equixty-Auth-Profile: User1         6       X-Equixty-Sequence-Hamespace: 11c814df-d4d2-4f8a-bf29-c6e6b6853e3d         7       "maint": "user1@example.com",         9       "maint": "user1@example.com",         10       "password": "password": "password"	Show more					GET /microservi
Memodiation         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/Togin         2       POST /microservicebola/pandao/apl/addorder         3       Gett /microservicebola/pandao/apl/addorder/I44         3       status: 200         4       Gett /microservicebola/pandao/apl/order/I43         9       "mail": "userl@examplecom",         9       "mail": "userl@examplecom",         1       "massword": "password": "pa	Descent of states					
API call          1       POST       /microservicebola/login         2       POST       /microservicebola/login HTTP/1.1         2       POST       /microservicebola/login HTTP/1.1         2       POST       /microservicebola/login HTTP/1.1         3       GET       /microservicebola/login dado/api/order/144         Status: 200       Status: 200         4       GET       /microservicebola/login dado/api/order/144         Status: 200       %	To effectively remediate horizontal Bro belonging to other users, strengthen a Show more	ken Object Level Authorization on En ccess control mechanisms	umeration resource, which involves unauthorized ad	ccess to data		
1       POST /microservicebola/login         Status: 200       1         2       POST /microservicebola/pandao/api/addorder         3       Status: 200         3       OET /microservicebola/pandao/api/order/144         status: 200       5         4       OET /microservicebola/pandao/api/order/143         status: 200       7         6       {         9       "email": "userl@example.com", 10         9       "email": "userl@example.com", 10         10       "password": "password": "password"	API call					
2       POST /microservicebola/login HTTP/1.1         2       POST /microservicebola/pandao/api/addorder         3       Status: 200         3       CET /microservicebola/pandao/api/order/144         5       X-Equixly-Auth-Profile: User1         6       X-Equixly-Sequence-Namespace: 11c814df-d4d2-4f8a-bf29-c6e6b6853e3d         7       8 {         9       "email": "userl@example.com",         10       "password": "password": "password"	POST /microservicebola/login			Request O Response		
3       GET /microservicebola/pandao/api/order/144         Status: 200       5         4       GET /microservicebola/pandao/api/order/143         5       X=Equixly=Sequence=Namespace:         1       >	2 POST /microservicebola/pandao/ap/ Status: 200	/addorder	1 2 3 4	<ol> <li>POST /microservicebola/login HTTP</li> <li>Host: local.equixly.com:5656</li> <li>Content-Type: application/json</li> <li>User-Agent: Equixly/1.0 (API Secu</li> </ol>	/1.1 rity; ML-powered Testing)	
4       GET       /microservicebola/pandao/api/order/143       8 {         9       "email": "user1@example.com",         10       "password": "password"         11       }	3 GET /microservicebola/pandao/api Status: 200	lorder/144	5	5 X-Equixly-Auth-Profile: User1 5 X-Equixly-Sequence-Namespace: 11c 7	814df-d4d2-4f8a-bf29-c6e6b6853e	3d
	4 GET /microservicebola/pandao/ap Status: 200	/order/143	8 9 10 11	<pre>&gt; {     "email": "user1@example.com", ) "password": "password" L }</pre>		

#### 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.











#### CHALLENGES OF WORKING WITH LLMS









#### CHALLENGES OF WORKING WITH LLMS

#### **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 IIUC)

5:22



**Specialization** 



#### THANK YOU & QA

Meet our team at

## Security Summit

#### Rome

Auditorium Della Tecnica







