Security Models for ALICE Web-Based Applications

George RADUTA, Martin Boulais
on behalf of the ALICE O²/FLP Project

9th of May 2023
Servers are under constant attacks
Servers are under constant attacks

Regular heavy targeted attacks on ALICE

\textit{e.g.} 4th of Oct 2022
Servers are under constant attacks

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

Regular heavy targeted attacks on ALICE

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 Control Room
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

Online-Offline Computing System*

*CHEP 2023 talk, V Barroso, The new ALICE Data Acquisition System
How? What?
Logbook GUI*

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

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

![Logging GUI Screenshot](image-url)
QualityControl GUI

Provides an easy way for viewing ROOT objects from O$^2$ Quality Control$^1$ stored with CCDB$^2$.

$^1$CHEP 2023 talk, P Konopka, The ALICE Data Quality Control
$^2$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/
Software and data integrity*

@aliceo2/web-ui is an in-house developed and maintained library which means:
- as few 3rd party dependencies as possible
- from scratch implemented modules to use with CERN services

*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 3rd party dependencies as possible
- from scratch implemented modules to use with CERN services

*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 3rd 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/
Vulnerable and outdated components*

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

*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/
Vulnerable and outdated components*

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

*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/
Vulnerable and outdated components*

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

*https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Vulnerable and outdated components*

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

Weekly Triggered

Automatically packed

Dependencies checks

Automated Tested

*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/
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/
**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/
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/
Access Control*

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

*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/
Access Control*

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

*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/
Access Control*

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

Hi, I am user Alice
May I get Run 512345?

Roles for Alice, please
Alice is admin

*https://owasp.org/Top10/A01_2021-Broken_Access_Control/
Access Control*

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

Hi, I am user Alice
May I get Run 512345?

There you go,
Run 512345

Roles for Alice, please
Alice is admin

*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/
Access Control*

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

*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/
Access Control*

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

*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/
Access Control*

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

*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

*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/
Security misconfiguration*

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

*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/
Security misconfiguration*

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

*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/
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”

1. Receive user request
Scenario - ALICE Experiment Control System GUI

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

@aliceo2/web-ui server

1. Receive user request
2. Log system access request
Scenario - ALICE Experiment Control System GUI

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

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”

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”

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”

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”

@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

Open Control GUI
Scenario - ALICE Experiment Control System GUI

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

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”

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”

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

@aliceo2/web-ui server

1. Receive user request

Open Control GUI

Start Run with TST detector
Scenario - ALICE Experiment Control System GUI

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

@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

1. Receive user request
2. Log system access request

Open Control GUI

Start Run with TST detector
### Scenario - ALICE Experiment Control System GUI

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

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

**@aliceo2/web-ui server**

1. Receive user request
2. Log system access request
3. Validate token and user roles

---

**Open Control GUI**

**Start Run with TST detector**
Scenario - ALICE Experiment Control System GUI

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

@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

Open Control GUI

Start Run with TST detector

1. Receive user request
2. Log system access request
3. Validate token and user roles
4. Validate and Allocate detector LOCK to the user
Scenario - ALICE Experiment Control System GUI

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

@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

1. Receive user request
2. Log system access request
3. Validate token and user roles
4. Validate and Allocate detector LOCK to the user
5. Log lock transaction
Scenario - ALICE Experiment Control System GUI

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

@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

1. Receive user request
2. Log system access request
3. Validate token and user roles
4. Validate and Allocate detector LOCK to the user
5. Log lock transaction
6. Broadcast notifications to all clients that lock has been taken by user
Scenario - ALICE Experiment Control System GUI

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

@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

Open Control GUI

Start Run with TST detector

1. Receive user request
2. Log system access request
3. Validate token and user roles
4. Validate and Allocate detector LOCK to the user
5. Log lock transaction
6. Broadcast notifications to all clients that lock has been taken by user
7. Send request to ALICE Experiment Control System 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

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

Open Control GUI

Start Run with TST detector

1. Receive user request
2. Log system access request
3. Validate token and user roles
4. Validate and Allocate detector LOCK to the user
5. Log lock transaction
6. Broadcast notifications to all clients that lock has been taken by user
7. Send request to ALICE Experiment Control System to start a run
8. Log request transaction
Questions?