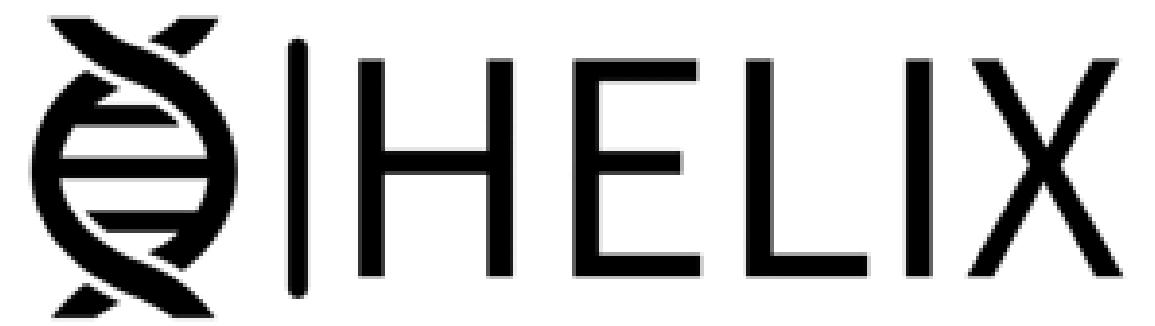


Smart Inventory System

Automated Inventory Management





Smart Inventory System

Automated Inventory Management



Github

Key Features



- Inventory Management and Automated Stock Ordering
- Generate Orders based on predefined rules and current stock levels



- Supplier management
- Centralised supplier info for easy communication and order management



- Role-based access control



- Secure authentication
- AWS Cognito



- Event driven Processes
- Responsive system. Adapts to inventory changes, supplier information, user actions etc.



- Interactive and Customisable Dashboard



- WOW Factor - Predictive Analytics
- EOQ model, ROP calculation, ABC analysis, FB Prophet Model

WOW Factor - Predictive Analytics

EOQ Model

- Economic Order Quantity
- Determines optimal quantity to reorder
- Minimises total inventory costs

ROP Calculation

- Reorder Point Calculation
- Determines the stock threshold to place a new order
- Based on lead time and demand variability
- Optimises inventory levels
- Calculates Safety Stock - prevent stockouts

ABC Analysis

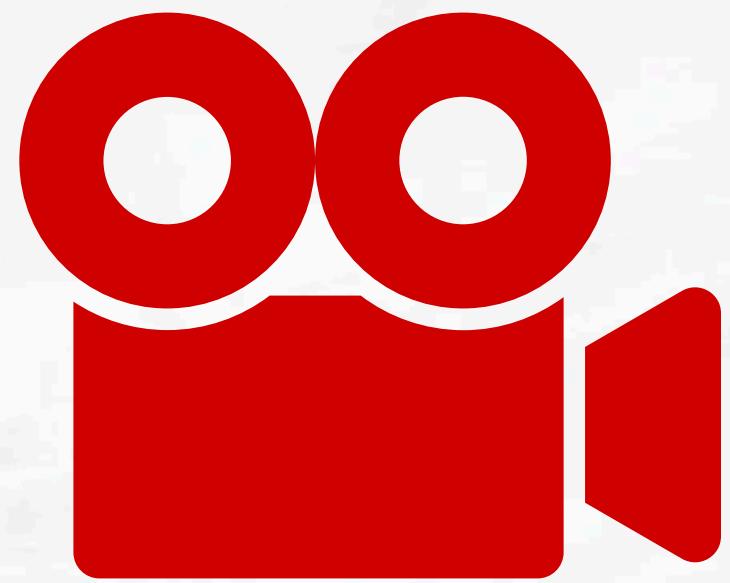
- Inventory Prioritisation
- Categorises inventory based on importance
- Importance measured by annual consumption value
- Allows differentiated management strategies for each category

FB Prophet Model

- Facebook Prophet Model
- Time Series Forecasting for future inventory prediction
- Is able to factor in trends, seasonality and holidays
- Very little data needed

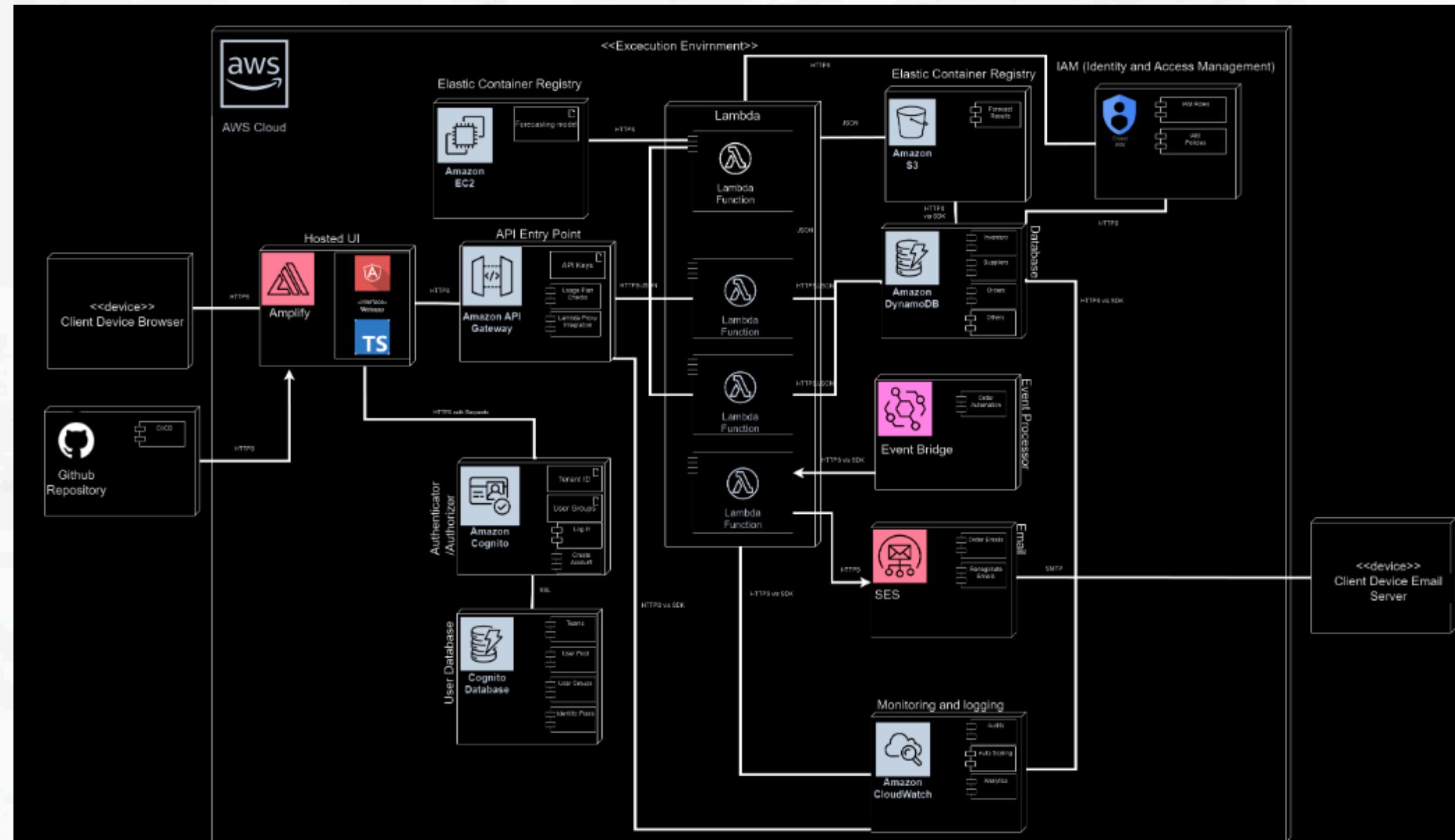
Fixes Added

- Input Validation:
 - Inventory Page
 - Suppliers Page
 - Orders Page
- Help Page
 - moved login assistance to the landing page to help users struggling to login
- Non Functional Requirements Testing
 - Usability Testing
 - Scalability and Reliability: Load Testing
 - Performance Testing (SEO, best practices, accessibility)
 - Performed Vulnerability Scanning



Live Demo

Deployment Diagram

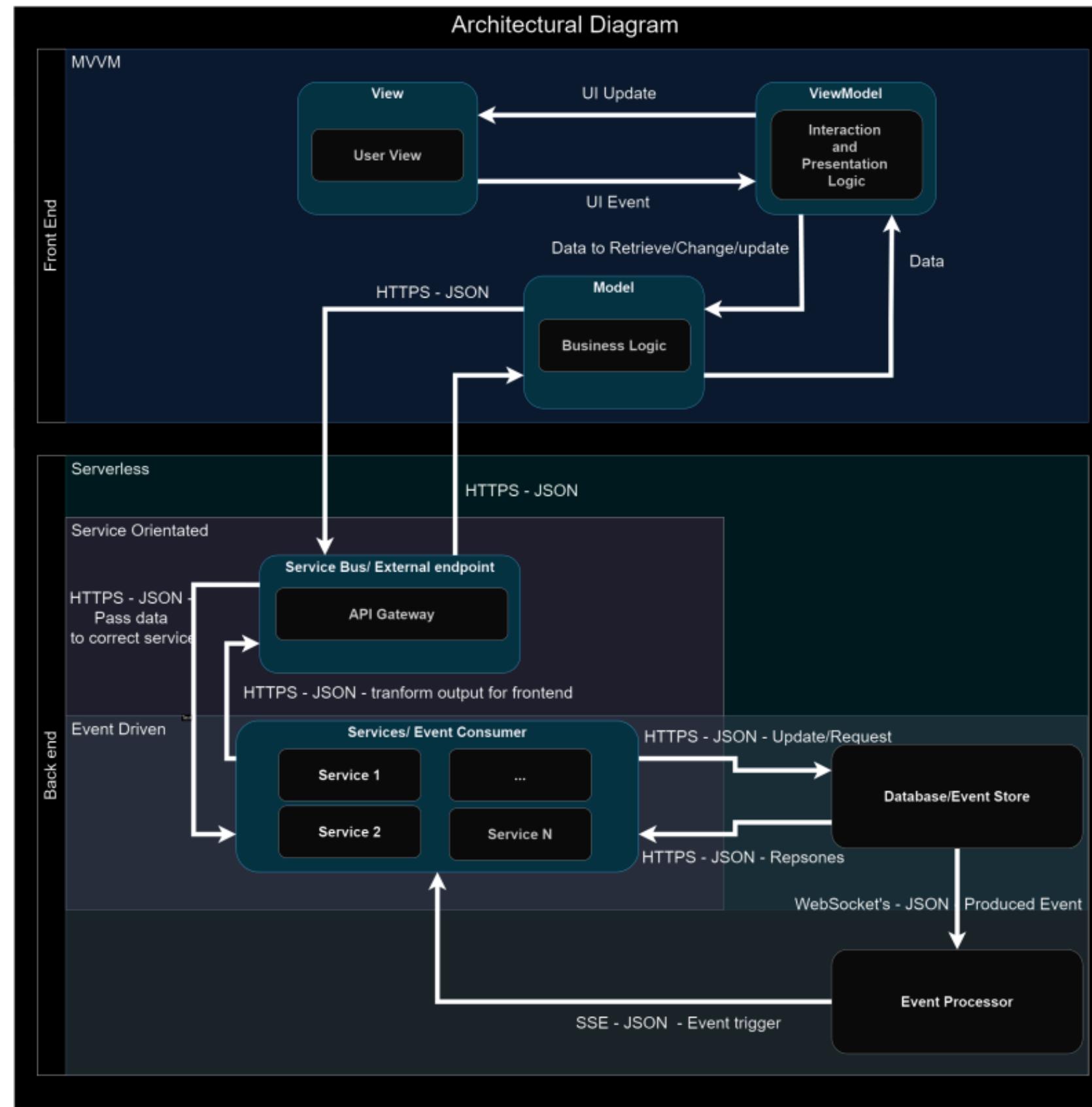


Quality Requirements

- Security
- Reliability
- Usability
- Maintainability
- Scalability

Architectural Styles

- MVVM
- Event Driven
- Serverless
- Service Oriented



Technologies



Lambda



Event Bridge



DynamoDB



IAM



Amplify



CloudWatch



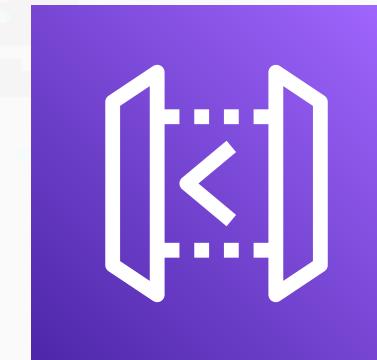
Cognito



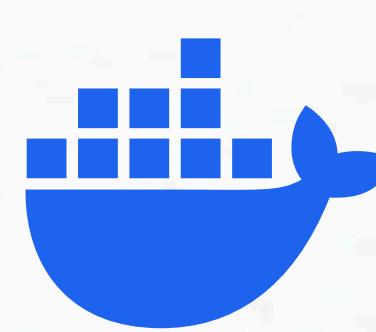
Simple Email
Service



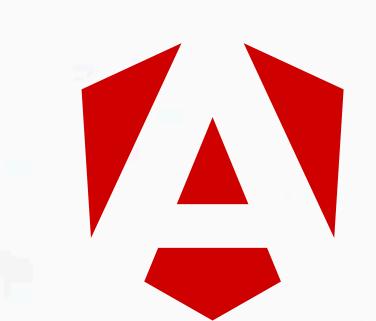
Simple Notification
Service



API Gateway

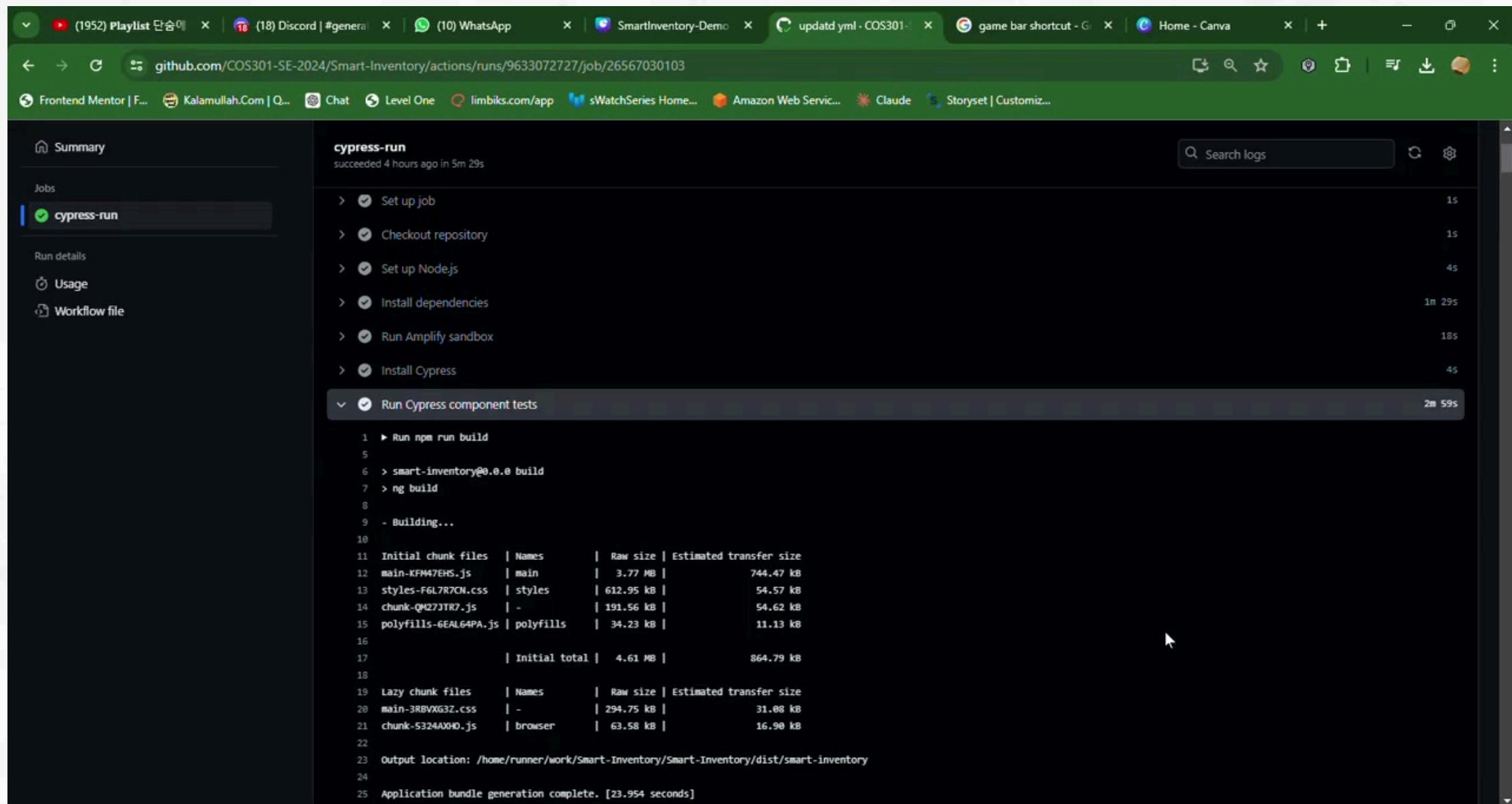


Docker



Angular

Testing



The screenshot shows a GitHub Actions workflow log for a job named "cypress-run". The job succeeded 4 hours ago in 5m 29s. The log details the steps taken:

- Set up job (1s)
- Checkout repository (1s)
- Set up Node.js (4s)
- Install dependencies (1m 29s)
- Run Amplify sandbox (18s)
- Install Cypress (4s)
- Run Cypress component tests (2m 59s)

The "Run Cypress component tests" step shows the command output:

```
1 ► Run npm run build
5
6 > smart-inventory@0.0.0 build
7 > ng build
8
9 - Building...
10
11 Initial chunk files | Names | Raw size | Estimated transfer size
12 main-KFM47EHS.js | main | 3.77 MB | 744.47 kB
13 styles-F6L7R7CN.css | styles | 612.95 kB | 54.57 kB
14 chunk-QM27JTR7.js | - | 191.56 kB | 54.62 kB
15 polyfills-6EAL64PA.js | polyfills | 34.23 kB | 11.13 kB
16
17 | Initial total | 4.61 MB | 864.79 kB
18
19 Lazy chunk files | Names | Raw size | Estimated transfer size
20 main-3RBVXKG3Z.css | - | 294.75 kB | 31.08 kB
21 chunk-5324AXHO.js | browser | 63.58 kB | 16.98 kB
22
23 Output location: /home/runner/work/Smart-Inventory/Smart-Inventory/dist/smart-inventory
24
25 Application bundle generation complete. [23.954 seconds]
```

Cypress Testing

Security

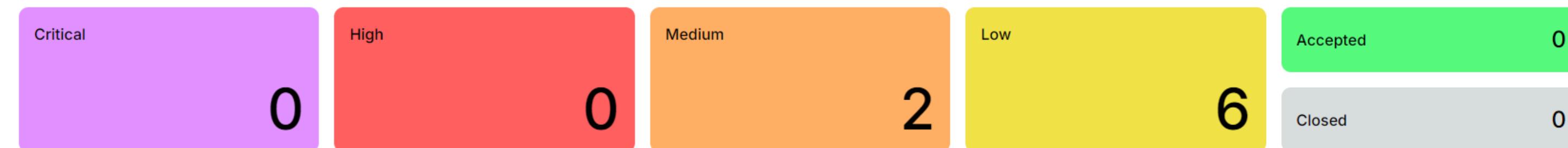


Hosted Scan - identified vulnerabilities

Dashboard

0 scans in progress | 3 scheduled scans

Risks detected Total: 8



Security



Hosted Scan - identified vulnerabilities

[Risks](#) Filters

Threat	Vulnerability	Target	Detected	Status
>	OpenVAS TCP Timestamps Information Disclosure CVSS: 2.6 QoD: 80%	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 3 days ago Last: 3 days ago	<input type="radio"/> Accept Risk
>	OWASP ZAP Server Leaks Version Information Via "Server" HTTP Response Header Field OWASP Top 10	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	OWASP ZAP X-Content-Type-Options Header Missing OWASP Top 10	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	OWASP ZAP Content Security Policy (CSP) Header Not Set OWASP Top 10	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	OWASP ZAP Missing Anti-Clickjacking Header OWASP Top 10	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	OWASP ZAP Strict-Transport-Security Header Not Set OWASP Top 10	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	Nmap Open TCP Port: 80	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
>	Nmap Open TCP Port: 443	https://main.dxgjrxhqoh4ot.amplifyapp.com/	First: 4 days ago Last: 4 days ago	<input type="radio"/> Accept Risk
Rows per page: 30 ▾ 1-8 of 8 < >				

Security

Security Headers
Powered by  Probely

POST Scan

Security Report Summary

	Site: https://main.dxgjrxhqoh4ot.amplifyapp.com/
	IP Address: 3.165.232.11
	Report Time: 17 Oct 2024 13:16:11 UTC
	Headers: ✓ X-Frame-Options ✓ X-Content-Type-Options ✓ Strict-Transport-Security ✓ Content-Security-Policy ✓ Referrer-Policy ✓ Permissions-Policy
	Warning: Grade capped at A, please see warnings below.
	Advanced: Great grade! Perform a deeper security analysis of your website and APIs: Try Now

Usability

Conducted usability tests with 50 users

Results:



[Link to usability
google form](#)

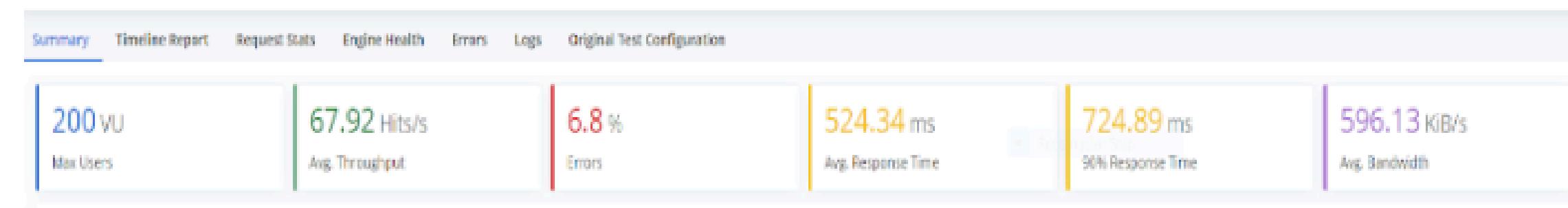


[Link to usability google
form spreadsheet](#)



[Link to usability test
report](#)

Reliability and Scalability



Response Time

