MICHIGAN STATE UNIVERSITY

Beta Presentation

Remediating AWS Security Gaps Using Generative AI

The Capstone Experience

Team Amazon

Ilyas Abdulrahman
Jaden Cabansag
Ndiaga Diouf
Nate Mikkola
Sardar Murtaza
Valdine Pegy Tchinda Pegou

Department of Computer Science and Engineering
Michigan State University

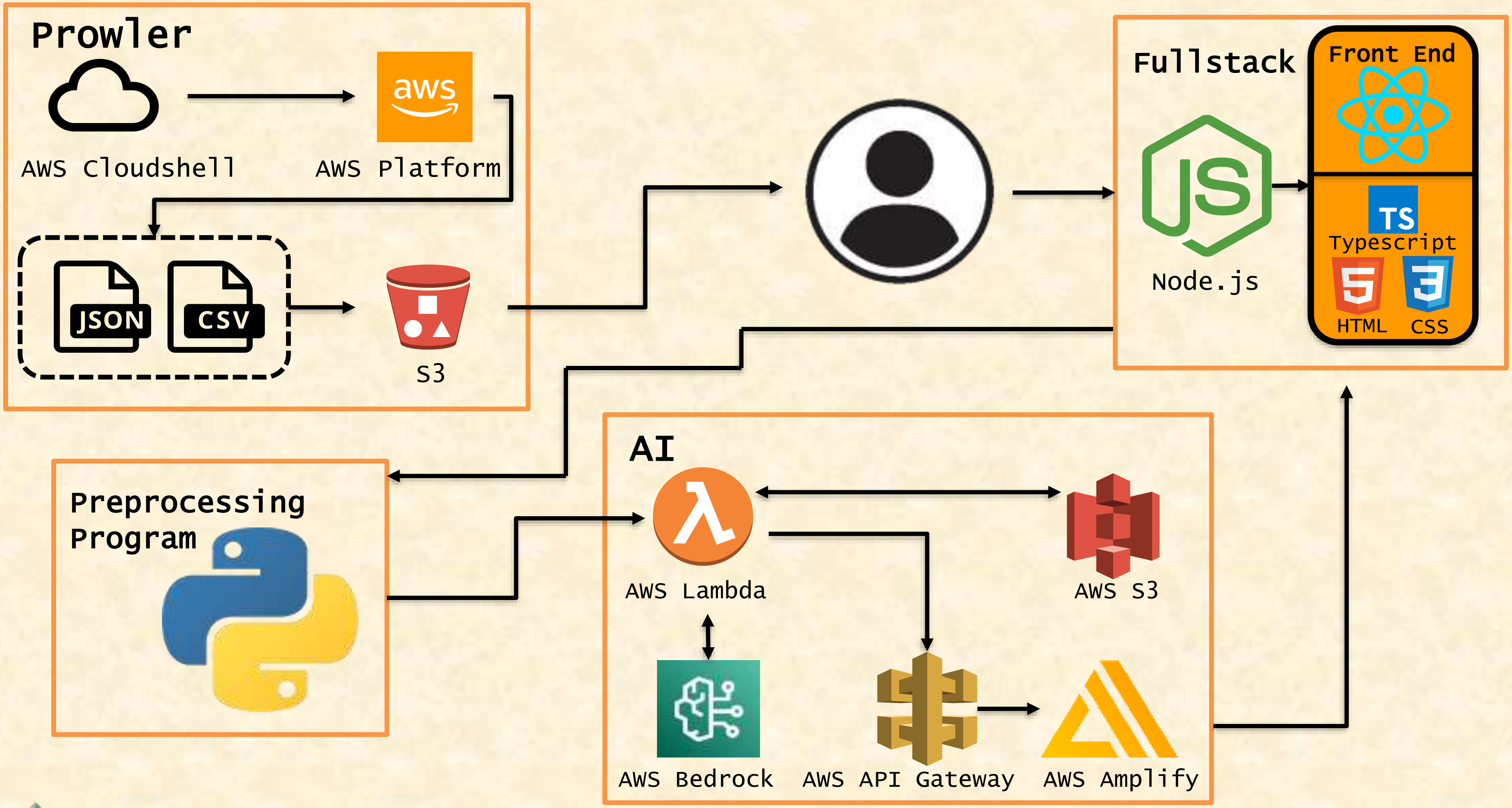
Fall 2024

From Students…
…to Professionals

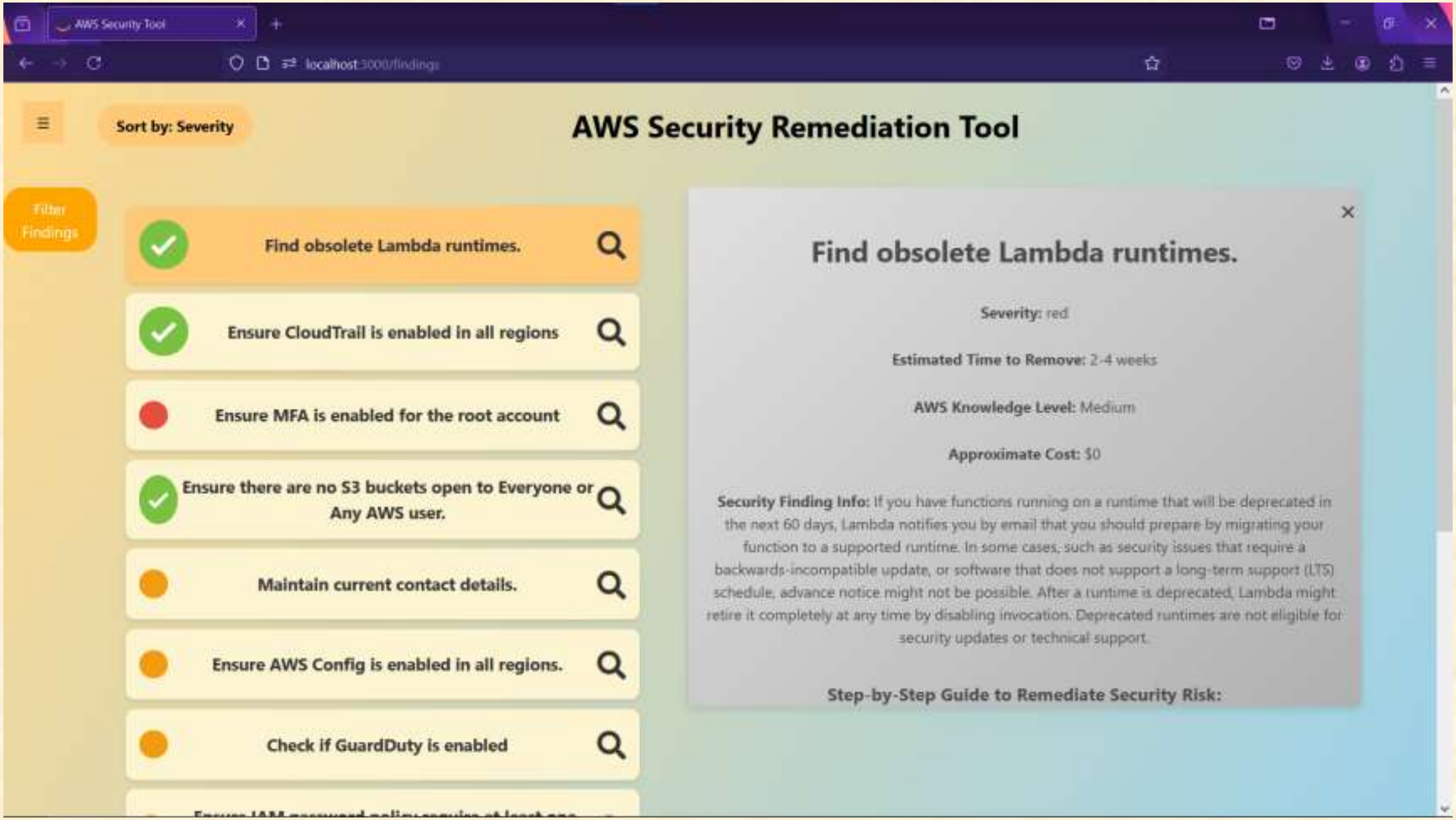
Project Overview

- AWS security analyses are currently difficult to understand for users
- Our AI and webpage classifies AWS security risks and provides a step-by-step guide to rectifying these issues
- Intended users are non-tech-savvy AWS clients
- Users can submit analyses and gain a better understanding of what are the risks, their priorities, and steps to remediation

System Architecture



Main Page



AWS Security Remediation Tool

- ✓ Find obsolete Lambda runtimes.
- ✓ Ensure CloudTrail is enabled in all regions
- ● Ensure MFA is enabled for the root account
- ✓ Ensure there are no S3 buckets open to Everyone or Any AWS user.
- ● Maintain current contact details.
- ● Ensure AWS Config is enabled in all regions.
- ● Check if GuardDuty is enabled
- Ensure IAM password policy require at least one

Find obsolete Lambda runtimes.

Severity: red

Estimated Time to Remove: 2-4 weeks

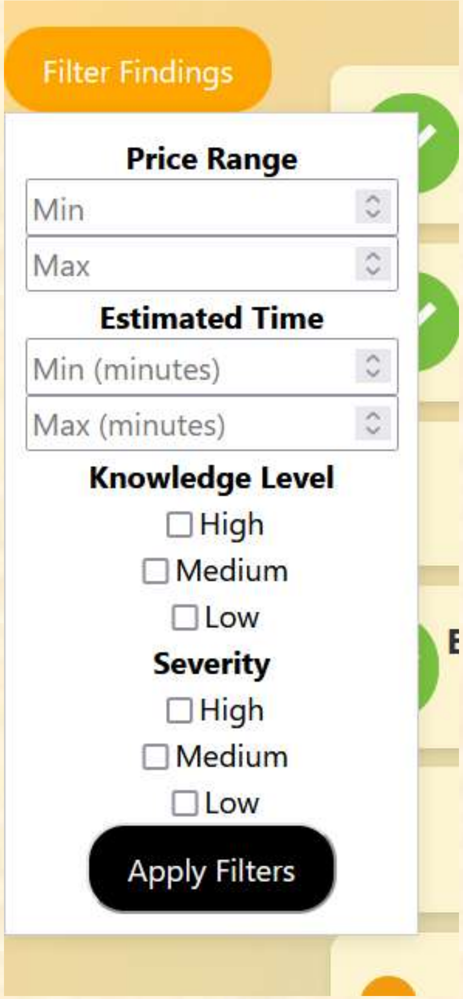
AWS Knowledge Level: Medium

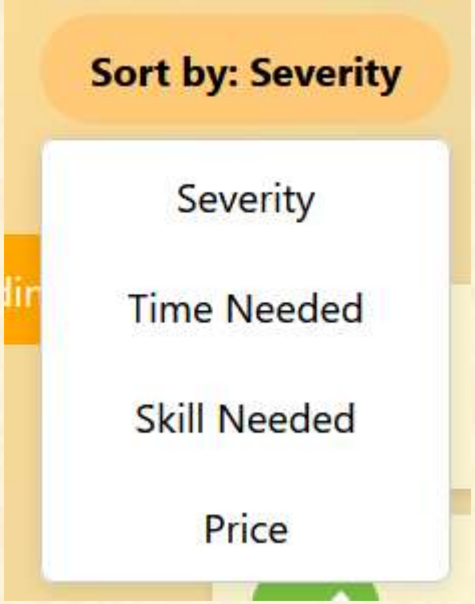
Approximate Cost: $0

Security Finding Info: If you have functions running on a runtime that will be deprecated in the next 60 days, Lambda notifies you by email that you should prepare by migrating your function to a supported runtime. In some cases, such as security issues that require a backwards-incompatible update, or software that does not support a long-term support (LTS) schedule, advance notice might not be possible. After a runtime is deprecated, Lambda might retire it completely at any time by disabling invocation. Deprecated runtimes are not eligible for security updates or technical support.

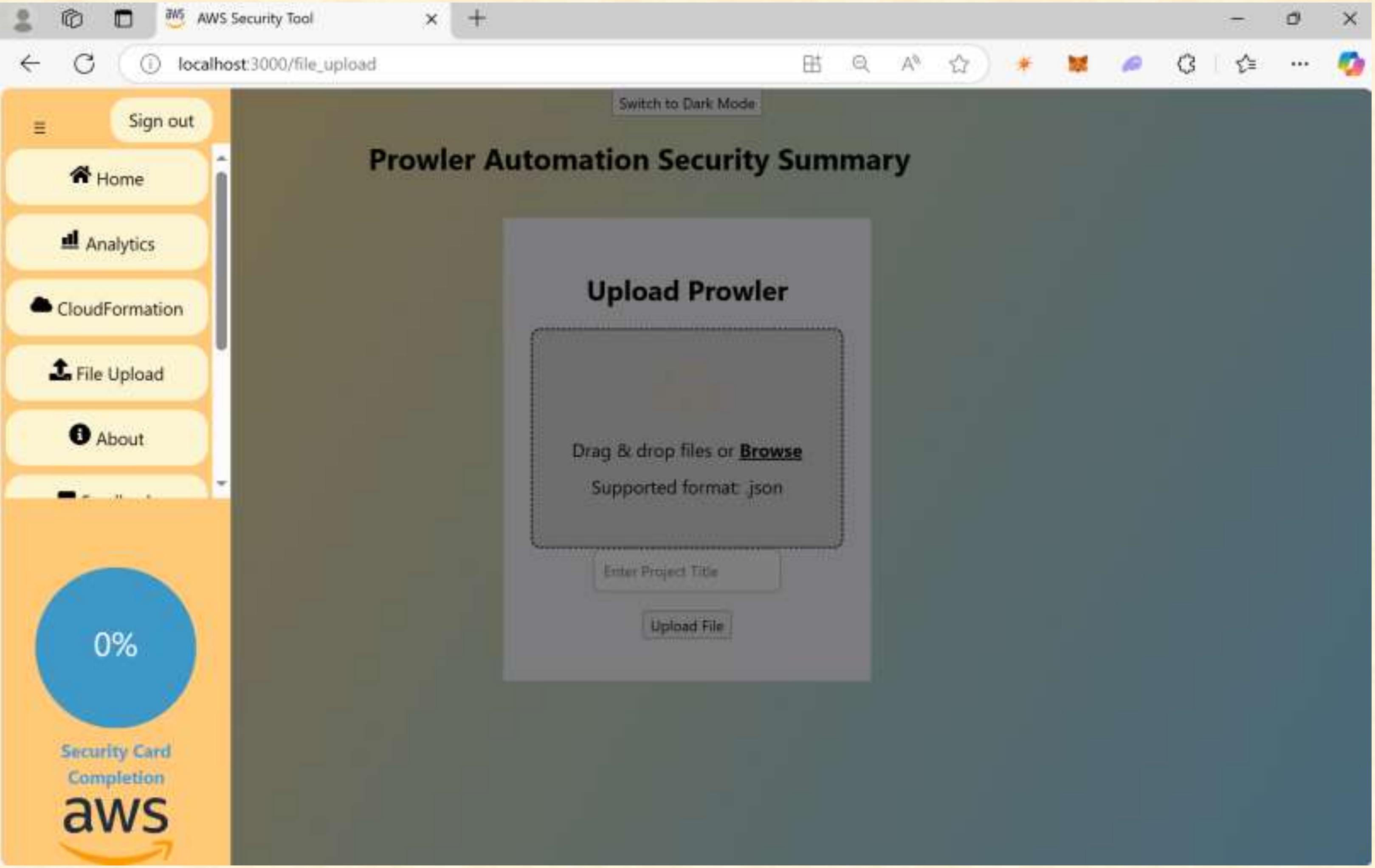
Step-by-Step Guide to Remediate Security Risk:

Sorting Methods




Sort by: Severity

Upload Page with Nav Bar



Prowler Automation Security Summary

Upload Prowler

Drag & drop files or **Browse**

Supported format: .json

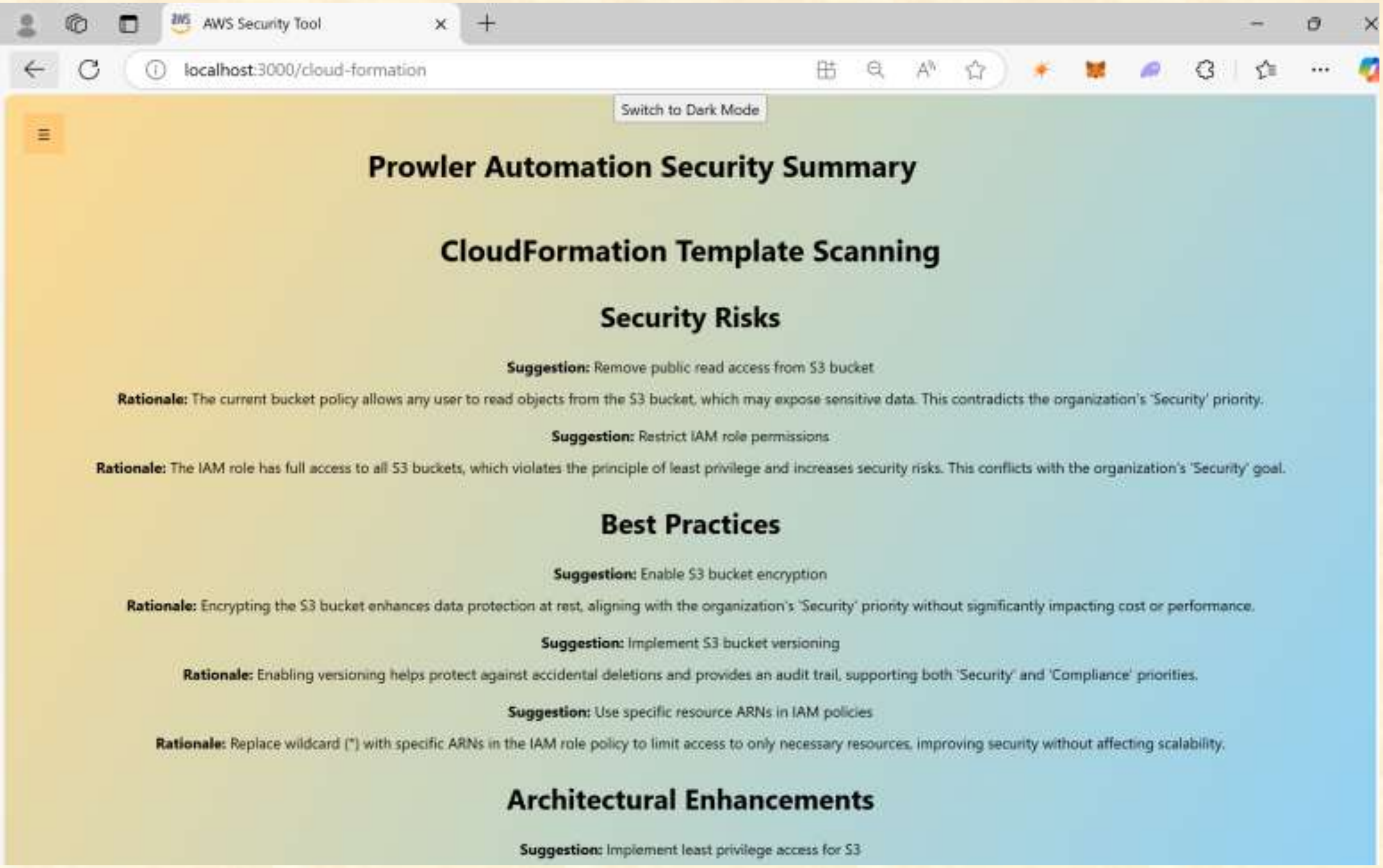
Enter Project Title

Upload File

0%

Security Card Completion

CloudFormation Scan



Prowler Automation Security Summary

CloudFormation Template Scanning

Security Risks

Suggestion: Remove public read access from S3 bucket

Rationale: The current bucket policy allows any user to read objects from the S3 bucket, which may expose sensitive data. This contradicts the organization's 'Security' priority.

Suggestion: Restrict IAM role permissions

Rationale: The IAM role has full access to all S3 buckets, which violates the principle of least privilege and increases security risks. This conflicts with the organization's 'Security' goal.

Best Practices

Suggestion: Enable S3 bucket encryption

Rationale: Encrypting the S3 bucket enhances data protection at rest, aligning with the organization's 'Security' priority without significantly impacting cost or performance.

Suggestion: Implement S3 bucket versioning

Rationale: Enabling versioning helps protect against accidental deletions and provides an audit trail, supporting both 'Security' and 'Compliance' priorities.

Suggestion: Use specific resource ARNs in IAM policies

Rationale: Replace wildcard (*) with specific ARNs in the IAM role policy to limit access to only necessary resources, improving security without affecting scalability.

Architectural Enhancements

Suggestion: Implement least privilege access for S3

What’s left to do?

- Stretch Goals
  - Select multiple options in CloudFormation
- Other Tasks
  - Frontend styling
  - Identifying and fixing bugs
  - Adding ARN location specification to findings

Questions?

? ? ? ?

? ?

? ? ?