Security Engineer, For all Engineers - Homework

What is the take-home project for?

We have designed our take-home project around a real-life problem that we might need so solve, using the types of technology you can expect to work with on the Stitch Fix security team.

Firstly, there are a few things we are not expecting. We are not expecting you to find the right solution. There is no one right solution. We are not expecting you to spend days of your free time on the problem.

We don't expect candidates to be able to solve this homework off the top of their head. Instead, we tried to incorporate a handful of technologies for candidates to demonstrate their ability to learn new concepts in a practical way. It is totally acceptable to find relevant tutorials and use them as the basis for your solution. We don't expect you to understand every line of code that it takes to solve this - we're more interested in the journey you took to get there. We hope that you find it fun and rewarding!

Problem

The Stitch Fix security team is in the process of implementing Content Security Policy (CSP) to detect and mitigate Cross Site Scipting attacks. The organization has approximately 50 public facing hostnames where CSP must be implemented.

The security team needs a solution to monitor these hostnames for CSP headers - ensuring that they are always present at the root (/) of each hostname.

Requirements

Write a serverless function which tests for the presence or absense of CSP headers in an HTTP response. The function should be deployable to AWS Lambda with an AWS API Gateway for invoking, and it should be deployable with Hashicorp Terraform.

Additional Guidance

The take-home project evaluates your problem solving and coding skills. We want to see that you:

- Have the ability to write Infrastructure as Code (Terraform)
- Have the ability to write functional code (Lambda)
- Push the code to a **private** GitHub repo and share it with https://github.com/almostwhitehat

Please approach this project as you would a work assignment. If you wish to introduce a new feature or additional technology in the context of this assignment, please feel free. However, this is not intended as a general showcase for all the cool things you can pull off.

If you need to make an assumption about the vague requirements, please do so, and please document what it is somewhere in the repo (the bottom of this README is a good place to add documented assumptions).