Identifying poor security practices

1. Security practice not followed:

**Best Practice**: You must have WAF for defending your externally facing application to protect against hacking.

Why: Web application firewalls or WAFs are missing in the design between a client and an application. WAF helps to inspect application HTTP traffic and determine if any exploitation attempts. It’s a good practice to a have WAF set up to block or log suspicious traffic from certain IPs or regions or DDoS attacks.

1. **Best Practice**: Using VPC end Points: with VPC endpoints, the data between the VPC and S3 is transferred within the amazon network, and protects from internet traffic. VPC endpoints for S3 adds additional security control to help limit access to S3 buckets. You can control what buckets, requests, users, or groups are allowed through a specific VPC endpoint.

Why: Instead of using Internet Gateway to communicate with S3, if should have added VPC endpoint the access to S3 as a best practice. This architecture has 3 Internet Gateways which would be more risk and easy access to attackers.

1. **Best Practice**: Protecting API Keys. We don’t need to know the raw API key, but just need to validate that the key is correct. So instead of storing the key in plain text or encrypting it, we should store it as a hashed value within our database.

Why: In this architecture the API Keys are exposed and hacker was able to get them and stole the date.

1. **Best practice**: Improve Windows Security by Closing Ports that are not needed. Open ports can cause security risk and attacks. This architecture is not clear on what ports are open to the application.
2. **Best practice**: Security Group access on webservice Instance should only access from Application Load Balancer.
3. **Best practice**: Access to Secret Recipe Bucket- privileged BU should have IAM role assigned. And S3 bucket should be encrypted with Aws- KMS CMK.

