Sprint 7

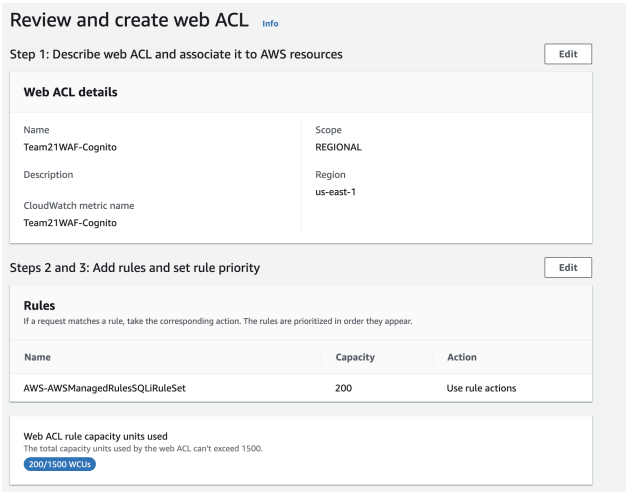
SQL Injection:

- AWS WAF

https://docs.aws.amazon.com/waf/latest/developerguide/classic-web-acl-sql-conditions.html
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-sqli-match.html

Attackers sometimes insert malicious SQL code into web requests in an effort to extract data from your database. To allow or block web requests that appear to contain malicious SQL code, create one or more SQL injection match conditions. A SQL injection match condition identifies the part of web requests, such as the URI path or the query string, that you want AWS WAF Classic to inspect. Later in the process, when you create a web ACL, you specify whether to allow or block requests that appear to contain malicious SQL code.

What I did:

1. Create a Web ACL
2. Choose the resource that we want to inspect web resources for
    a. Cognito User Pools
        i. Team21WAF-Cognito
3. Used the managed predefined rule for SQLi
4. 

Messaging:

Driver Alerts: RC2

Drivers receive automated alerts for the following operations:

- accepted/added by a sponsor/admin
    - this alert cannot be disabled
- dropped by a sponsor/admin
    - this alert cannot be disabled
- points are added/removed from their account
    - can enable/disable this alert
- an order is placed (summarizing the order)
    - can enable/disable this alert
- an issue/problem related to an order
    - can enable/disable this alert

Services & Setbacks:

- AWS Pinpoint

https://docs.aws.amazon.com/pinpoint/latest/userguide/gettingstarted.html

    - Import customer data and create a segment
    - Problem: Not event based
- RDS Event notification (SNS)
    - Problem: Must enter users to send an event to

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.overview.html#USER_Events.overview.process
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.overview.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_Events.Subscribing.html

- Lambda

- Set up a lambda to trigger an SNS when a new driver is accepted
- Setback: Must know how DB table is configured/set up a better configuration

---

Database Table Redesign

Current:

Table 1
Organizationid = _____
ApplicationStatus = 1/0

Redesign: Idea… max out 3 sponsors? (he doesn't specify max sponsor #, just that there have to be multiple)

Table 1
Userid: _____
Application1: application table
Application2: application table
Application3: application table

Table 2 (application table)
Organizationid: _____
Status: 1/0

Logging & Reporting

What we need:

1. Audit logging:
    a. driver applications
    b. point changes
    c. password changes
    d. login attempts

Password changes & Login Attempts:

- AWS CloudTrail – With CloudTrail you can capture API calls from the Amazon Cognito console and from code calls to the Amazon Cognito API operations. For example, when a user authenticates, CloudTrail can record details such as the IP address in the request, who made the request, and when it was made.

Driver applications & Point changes:

- AWS Cloudtrail
    - CloudTrail provides a record of actions taken by a user, role, or an AWS service in Amazon RDS
        - Create a trail
        - Create an S3 bucket
- RDS events (same as idea for messaging protocol)