تمرین اول برنامه نویسی وب

امید جعفری‌نژاد

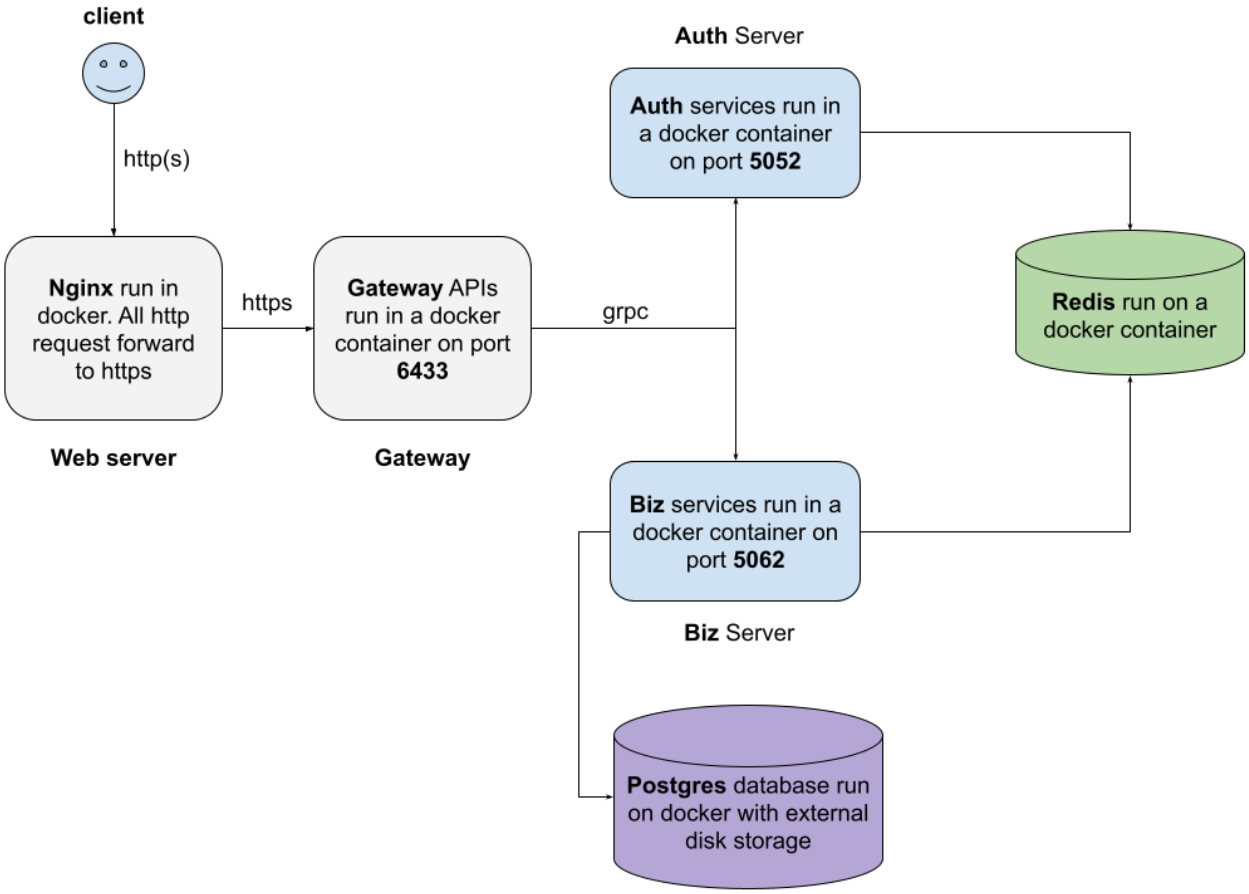
تاریخ تحویل: بیست و پنج اردیبهشت

مقدمه

در این تمرین مقدمات آماده سازی وب سرور ها، پیاده‌سازی یک وب سرویس توزیع شده با پروتکل grpc و همچنین روش‌های مختلف آزمون و مستندسازی کد را خواهیم آموخت.

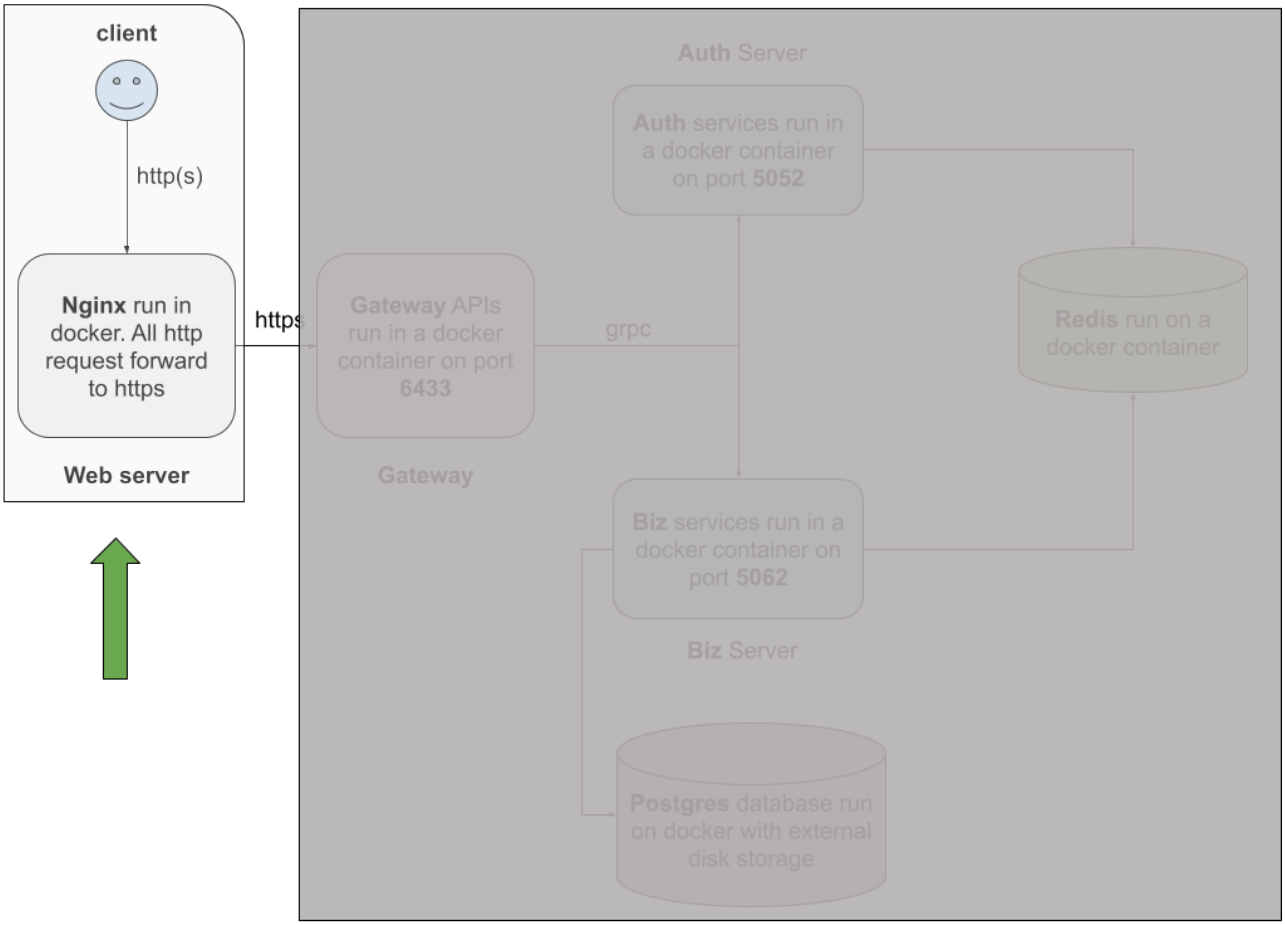
شرح تمرین

در این تمرین از شما خواسته شده است که یک سناریو ارتباطی بین client و سرور را شبیه‌سازی کنید. توجه داشته باشید این طرح آموزشی است و برای استفاده در محیط عملیاتی و یا production لازم است بر اساس نیازمندی‌های خاص پروژه تصمیم‌گیری شود . شمای کلی طرح تمرین در شکل زیر آورده شده است.



۱. راه‌اندازی وب سرور

در این بخش می‌خواهیم یک وب سرور درون یک docker container راه‌اندازی کنیم به عبارت دیگر میخواهیم بخش زیر از طرح کلی را پیاده‌سازی کنیم



پیاده‌سازی این بخش از تمرین دارای ۰.۲۵ نمره است که از کارهای زیر تشکیل شده است:

الف) وب سرور NGINX بر روی port استاندارد HTTP و HTTPS درون داکر راه‌اندازی کنید . (۰.۱۵ نمره)
ب) همه درخواست‌های بر روی HTTP به HTTPS ارجاع داده شوند . (۰.۰۵ نمره)
ج) فایل تنظیمات یا همان config مربوط به NGINX در یک پوشه بیرونی نگاشت شود و بتوان به سادگی تغییرات را درون آن انجام داد . (۰.۰۵ نمره)

از طریق کاوش در اینترنت این بخش به سادگی قابل پیاده‌سازی است به عنوان نمونه می‌توانید گام‌های زیر را دنبال کنید:

- port های استاندارد برای http و Https یا ssl چه هستند؟ لینک‌های What is an SSL port? و Port را مشاهده کنید
- چگونه یک وب سرور درون داکر راه اندازی کنیم؟ اگر هنوز داکر را نصب نکردید وای بر شما! به کمک Install Docker Engine آن را نصب کنید. لینک‌های How To Run Nginx in a Docker Container و یا Deploying NGINX ... on Docker را برای راه‌اندازی یک وب سرور ساده مطالعه کنید
- چگونه تنظیمات وب سرور را از بیرون از داکر انجام دهیم؟ در لینک Official NGINX Image on Docker Hub بخش Complex configuration را مطالعه کنید به عبارت دیگر به کمک Volumes Docker یا v- در داکر میتوانید این نگاشت را انجام دهید. برای مطالعه بیشتر لینک‌های Understanding Docker Volumes و Volumes را نیز مشاهده کنید.

- به منظور تنظیم SSL یا HTTPS یکی از لینک‌های NGINX SSL Configuration Step by Step Details و یا Configuring HTTPS servers را مطالعه کنید
- برای Redirect یا ارجاع دادن HTTP به HTTPS یکی از لینک‌های Nginx Redirect HTTP to HTTPS و یا How to Redirect HTTP to HTTPS in Nginx را مطالعه کنید

۱-۱. بخش امتیازی راه‌اندازی وب سرور

در این بخش شما می‌توانید با انجام کارهای زیر برای پیاده‌سازی وب سرور نمره امتیازی بدست آورید

الف) تنظیمات وب سرور برای بهبود کارایی را بهینه کنید. ۰.۱ نمره

- Tuning NGINX for Performance
- NGINX Tuning For Best Performance
- 7 Tips for NGINX Performance Tuning

ب) وب سرور را برای افزایش امنیت تنظیم کنید. ۰.۱ نمره

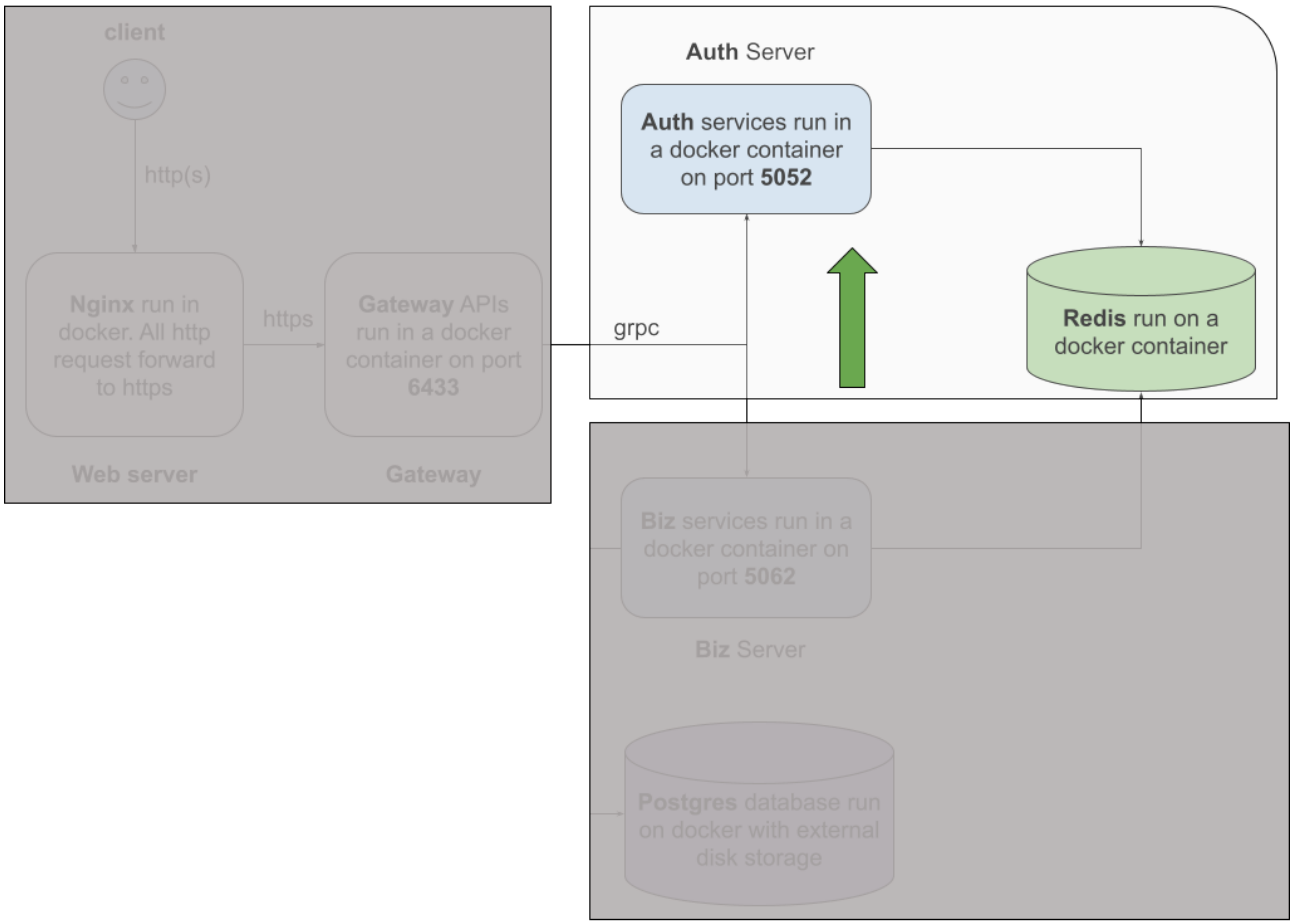
- Top 25 Nginx Web Server Best Security Practices
- nginx Security: How To Harden Your Server Configuration
- How to Secure Your Nginx Deployment: 10 Tips

۳. پیاده‌سازی **Auth server**

این سرور سرویس تبادل کلید دیفی‌ـهلمن را پیاده سازی می‌کند. به عبارت دیگر به کمک این الگوریتم کلاینت و سرور می‌توانند یک کلید رمز مشترک، از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل نمایند
در ادامه یک مثال عددی آورده شده است:

- دو طرف روی مقدار عدد اول $p = 23$ و مقدار اولیهٔ $g = 5$ توافق می‌کنند.
- طرف اول مقدار پنهانی یا همان کلید خصوصی $a = 6$ را انتخاب (در شبکه ارتباطی رد و بدل نمی‌شود) و مقدار $A = g^a \bmod p = 8$ که در واقع کلید عمومی است را برای طرف دوم ارسال می‌کند (از طریق شبکه ارتباطی).
- طرف دوم مقدار پنهانی $b = 15$ را انتخاب (در شبکه ارتباطی رد و بدل نمی‌شود) و $B = g^b \bmod p = 19$ را برای طرف اول ارسال می‌کند (از طریق شبکه ارتباطی).
- طرف اول مقدار $p \bmod B^a = 2$ را محاسبه کرده و به عنوان کلید رمز مشترک در نظر می‌گیرد.
- طرف دوم مقدار $p \bmod A^b = 2$ را محاسبه کرده و به عنوان کلید رمز مشترک در نظر می‌گیرد.

به عبارت دیگر مقدار کلید مشترک ۲ بین دو طرف ارتباط توافق شد بدون آنکه این عبارت در شبکه ارتباطی جابه‌جا شود و یا بخواهیم درون کد هاردکد کنیم. این الگوریتم در پیاده‌سازی SSL کاربرد دارد. در ادامه سرویس‌های سرور Auth آورده شده است. توجه کنید برای بخش‌های مختلف نمونه کد پیشنهاد شده است که به راحتی بتوانید بر اساس آن سرویس خواسته شده را پیاده سازی کنید.



الف) یک سرویس GRPC با مشخصات زیر پیاده‌سازی کنید. ۰.۲۵ نمره

- نام سرویس: req_pq
- ورودی‌های این سرویس عبارتند از:
  - پارامتر ورودی به نام nonce اجباری و از نوع رشته‌ایی، به طول ۲۰ است که به صورت تصادفی توسط کلاینت تولید و ارسال می‌شود.
  - message_id یک عدد صحیح و بزرگتر از صفر و زوج است
- خروجی این سرویس شامل فیلدهای زیر است:
  - nonce از نوع رشته‌ایی و دقیقا همان رشته‌ایی است که کلاینت ارسال کرده است
  - server_nonce یک رشته تصادفی به طول ۲۰ که سرور برای کلاینت ارسال می‌کند
  - message_id یک عدد صحیح و بزرگتر از صفر و فرد است
  - p از نوع عدد و عدد اول به طور مثال عدد ۲۳
  - g از نوع عدد و مولد یک ترتیب به طور مثال عدد ۵
- این سرویس پارامترهای الگوریتم دیفی‌ـ هلمن را برای کلاینت ارسال می‌کند. توجه داشته باشید در ارتباط بین کلاینت و سرور این اولین متدی است که فراخوانی می‌شود. کلاینت ابتدا یک عدد تصادفی و عدد صفر به عنوان message_id برای سرور ارسال می‌کند، در پاسخ، سرور، با تولید یک عدد تصادفی و message_id فرد بزرگتر از صفر به درخواست

کاربر پاسخ می‌دهد. توجه کنید لازم است این داده‌ها درون Redis به کمک حداکثر به مدت ۲۰ دقیقه کش شوند. برای کلید دخیره داده‌ها در Redis ابتدا nonce و server_nonce را به هم بچسبانید و SHA۱ را به عنوان کلید قرار دهید.

- برای ارتباط با Redis لینک‌های زیر پیشنهاد می‌شوند
  - guide Go - Redis
  - go-redis

ب) یک سرویس GRPC با مشخصات زیر پیاده‌سازی کنید. ۰.۲۵ نمره

- نام سرویس: req_DH_params
- ورودی‌های این سرویس عبارتند از:
  - پارامترهای nonce و server_nonce دقیقا مطابق با پاسخ درخواست req_pq
  - message_id یک عدد صحیح و بزرگتر از صفر، زوج و برزگتر از عدد درخواست شده در req_pq
  - پارامتر a که مقدار محاسبه شده کلید عمومی در الگوریتم دیفی_هلمن توسط کلاینت است
- خروجی این سرویس شامل فیلدهای زیر است:
  - nonce از نوع رشته‌ایی و دقیقا همان رشته‌ایی است که کلاینت ارسال کرده است
  - server_nonce همان رشته تصادفی که در مرحله قبل ایجاد شده است
  - message_id یک عدد صحیح و بزرگتر از صفر و فرد است
  - b مقدار محاسبه شده کلید عمومی در الگوریتم دیفی_هلمن توسط سرور است
- در پاسخ به این سرویس کلید مشترک تولید شده برای این کلایت در Redis ذخیره میشود و اطلاعات قبلی برای این کلاینت از Redis پاک می‌شوند

۴. پیاده‌سازی Biz Server

در این سرور لازم است دو سرویس GRPC برای ارتباط با پایگاه داده Postgres پیاده‌سازی کنید. در یک سرویس از شما خواسته شده است که مخاطره امنیتی Injection SQL وجود داشته باشد. برای این منظور لازم است در پایگاه داده یک جدول به نام USERS با فیلدهای نام (name) ، نام خانوادگی (family) ، شناسه (id) ، سن (age) ، جنسیت (sex) ، زمان ایجاد رکورد (createdAt) را ایجاد کنید.
الف) یک سرویس GRPC با مشخصات زیر پیاده‌سازی کنید. ۰.۲۵ نمره

- نام سرویس: get_users
- ورودی‌های این سرویس عبارتند از:
  - پارامتر ورودی به نام user_id به منظر فیلتر کردن کاربر. اگر این فیلد مقدار داشته باشد کاربر با این شناسه را برمی‌گرداند. در صورتی که این فیلد خالی باشد ۱۰۰ رکورد اول از جدول USERS را به عنوان خروجی برگردانده می‌شود

- auth_key کلید احراز هویت کاربر در مرحله ورود به سیستم است و مقدار آن باید معتبر باشد
- message_id یک عدد صحیح و بزرگتر از صفر، زوج و معتبر است

- خروجی این سرویس شامل فیلدهای زیر است:
  - users آرایه ایی از کاربران در پاسخ به query اجرا شده است.
  - message_id یک عدد صحیح و بزرگتر از صفر و فرد است

ب) یک سرویس GRPC با مشخصات زیر پیاده‌سازی کنید. ۰.۲۵ نمره

- نام سرویس: get_users_with_sql_inject
- پارامترهای ورودی و خروجی این سرویس مانند سرویس get_users است فقط در ارسال درخواست به این سرویس امکان inject کردن درون query وجود دارد.

راهنمایی: نوع پارامتر user_id در سرویس get_users از نوع عددی و در سرویس get_users_with_sql_inject از نوع رشته‌ایی در نظر بگیرید.

۲. پیاده‌سازی **Gateway server**

به کمک Gin Web Framework یک وب Gateway برای دسترسی به سرویس‌های GRPC فوق پیاده‌سازی کنید. ۰.۵ نمره

- سرویس‌های سرور Biz باید حتما باید دارای یک کلید Auth معتبر باشند. به عبارت دیگر کاربر باید پیش از فراخوانی هر یک از دو سرویس درون این سرور یک بار فرایند ایجاد کلید Auth را انجام داده باشد.
- در صورت فراخوانی سرویس‌های سرور Auth بیش از ۱۰۰ بار در یک ثانیه کاربر به مدت ۲۴ ساعت در Block list قرار گیرد و هر گونه سرویسی به کاربر با آن Ip جلوگیری شود.

۵. آزمون بار

برای سرویس‌های Biz, Auth و Gateway پارامتر تعداد درخواست در ثانیه RPS را به کمک ابزار Locust اندازه گیری کنید. ۰.۵ نمره

۶. مستند فراخوانی سرویس‌ها

برای سرویس‌های Biz, Auth و Gateway به کمک Swagger یک واسط کاربری برای آزمون و مستندات سرویس‌ها برپا کنید. ۰.۲۵ نمره