Securing API Access for `api.vinylvibe.live`

Below outlines the steps to:

1. Redirect users accessing `api.vinylvibe.live` directly in a browser to the frontend (`vinylvibe.live`).
2. Ensure API responses are accessible only from the frontend (`vinylvibe.live`).
3. Block or redirect requests from unauthorized origins.

Frontend Code (No Changes Needed)

- The frontend will continue to send requests to the API at `https://api.vinylvibe.live` .
- No modifications are required in your frontend.

Backend Code (Node.js/Express)

1. **Redirect Root Endpoint**
   - Redirect any request to `https://api.vinylvibe.live/` (without an API path) to your frontend.
   - Add this code to your `index.js` or main backend file:

```
app.get("/", (req, res) => {
    res.redirect("https://vinylvibe.live");
});
```

---

2. **CORS Configuration**

   - Only allow requests from your frontend (`https://vinylvibe.live`) or API subdomain (`https://api.vinylvibe.live`).

   - Add this code to configure CORS:

```
const cors = require("cors");

const allowedOrigins = [
    "https://vinylvibe.live",
    "https://api.vinylvibe.live",
];

app.use(
    cors({
        origin: function (origin, callback) {
            if (!origin || allowedOrigins.includes(origin)) {
                callback(null, true);
            } else {
                callback(new Error("Not allowed by CORS"));
            }
        },
    })
);
```

---

3. **Middleware to Check Origin**

- Add middleware to validate the `Origin` or `Referer` headers for requests that bypass CORS (e.g., via tools like Postman).
- If the request does not come from an allowed origin, redirect it to your frontend or block it.

```
app.use((req, res, next) => {
    const allowedOrigins = [
        "https://vinylvibe.live",
        "https://api.vinylvibe.live",
    ];
    const origin = req.get("origin");

    if (!origin || allowedOrigins.includes(origin)) {
        return next();
    }

    // Redirect to frontend if the origin is invalid
    res.redirect("https://vinylvibe.live");
});
```

---

4. **Block Unauthorized Requests**

- For additional security, return a `403 Forbidden` status for requests that don't meet the origin criteria:

```
app.use((req, res, next) => {
    const allowedOrigins = [
        "https://vinylvibe.live",
        "https://api.vinylvibe.live",
    ];
    const origin = req.get("origin");

    if (!origin || allowedOrigins.includes(origin)) {
        next();
    } else {
        res.status(403).json({ error: "Forbidden" });
    }
});
```

Testing

1. Visit `https://api.vinylvibe.live` in a browser:
    - You should be redirected to `https://vinylvibe.live`.
2. Make requests to the API from the frontend (`vinylvibe.live`):
    - Requests should work without errors.
3. Test requests from unauthorized origins (e.g., Postman):
    - Requests should fail with `403 Forbidden` or be redirected.

By following these steps, your API will only respond to requests made by your frontend, and direct or unauthorised access will be blocked.