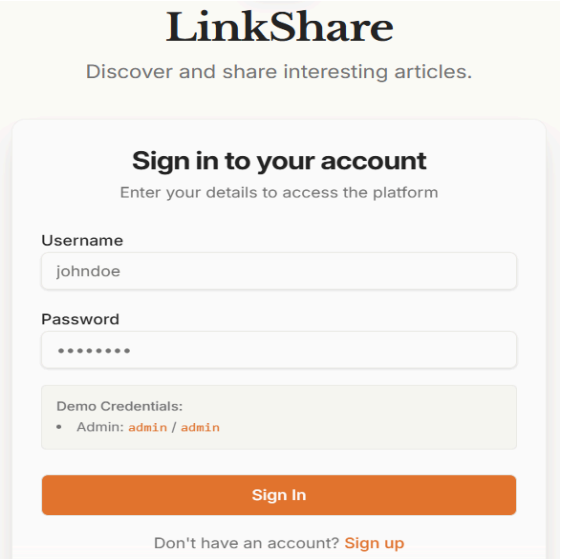
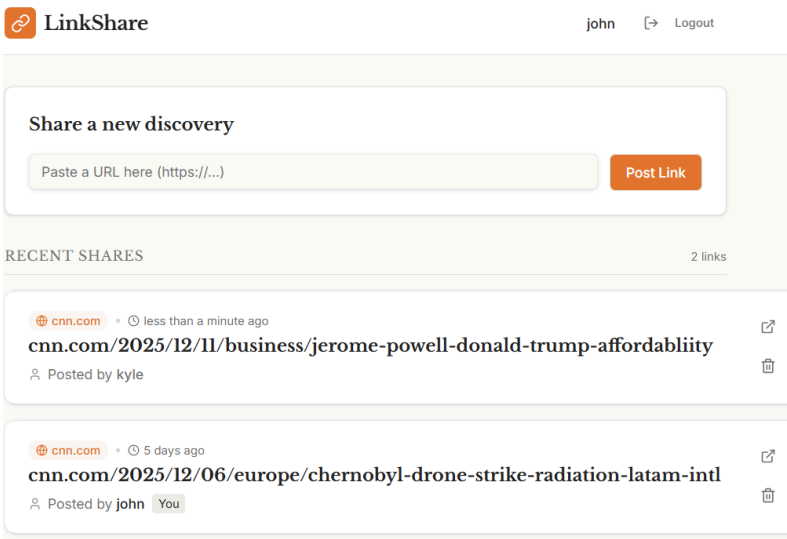
Implemented

Login page: Replit implemented a login page that allows a user to log in. If a user does not have an account, they can sign up for one. They also have admin credentials, which are saved as username: admin, password: admin.



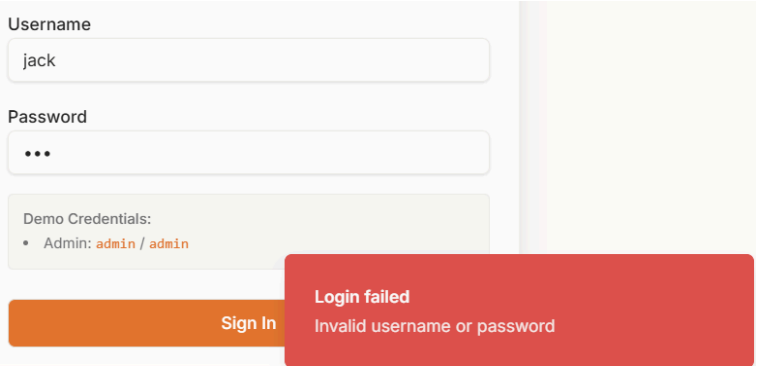
Home page: This is another main page that Replit created. On the home page, you can paste a URL and view other articles that users have posted. You can see here that even though I'm logged in as john, the button to delete kyle's post is still there. So, Replit did not properly implement correct access. This is an instance of Broken Access Control, because a user can act outside of their intended permissions. The admin is able to delete every post on the board.



They do actually hash the password before inserting into the Postgresql Database, which was a nice surprise. This also prevents injections because of Drizzle's built-in safety checks for insert(), delete(), etc.

```
async createUser(insertUser: InsertUser): Promise<User> {
  const hashedPassword = await bcrypt.hash(insertUser.password, 10);
  const result = await this.db.insert(users).values({
    username: insertUser.username,
    password: hashedPassword,
  }).returning();
  return result[0];
}
```

Error Logging: The app also notifies when there are errors. If a user fails to log in, it notifies the user. But, it doesn't seem to tell the server that there was a failed login attempt. This could be an instance of "Logging & Alert Failures" from the OWASP Top Ten.



Error Page: If a page that doesn't exist is trying to load, then the NotFound() function is called. This displays an error message to the user.

```
import { Card, CardContent } from "@/components/ui/card";
import { AlertCircle } from "lucide-react";

export default function NotFound() {
  return (
    <div className="min-h-screen w-full flex items-center justify-center bg-gray-50">
      <Card className="w-full max-w-md mx-4">
        <CardContent className="pt-6">
          <div className="flex mb-4 gap-2">
            <AlertCircle className="h-8 w-8 text-red-500" />
            <h1 className="text-2xl font-bold text-gray-900">404 Page Not Found</h1>
          </div>

          <p className="mt-4 text-sm text-gray-600">
            Did you forget to add the page to the router?
          </p>
        </CardContent>
      </Card>
    </div>
  );
}
```

Not Implemented

It looks like Replit did not put anything in place to use Web Tokens. This is probably due to the fact that I didn't specify that I wanted it in my queries.

Another feature that could be built upon is having a more robust, secure admin account. For the purposes of this project it's fine, but in reality the admin should be named something else and the password should be super long and random. That way not just any user can log in to the admin account.

There is currently nothing in place to prevent brute force attacks on the password as well. The user can try to log in as many times as they want.