The provided code has a major security issue:

Use of `eval()`:

- The line:

  ```javascript
  const uppercaseName = eval('"' + name + '"' + '.toUpperCase()');
  ```

  uses the `eval()` function, which is notoriously dangerous. `eval()` takes a string as an argument and executes it as JavaScript code. By directly injecting user input (the `name` query parameter) into the `eval()` function, the code is susceptible to **Arbitrary Code Execution**. An attacker can provide malicious input that gets executed, leading to potential remote code execution on the server.

For example, an attacker might send a request like:

```
/customerOnboarding?name="); malicious_code_here; //
```

This would interrupt the string and run `malicious_code_here` on the server.

Recommendations:

1. **Avoid `eval()`**:

   - You should almost never use `eval()` in a JavaScript application, especially not with user input. If you need to convert a string to uppercase, you can do so directly without `eval()`:

     ```javascript
     const uppercaseName = name.toUpperCase();
     ```

2. **Input Validation and Sanitization**:

   - Always validate and sanitize user input. Even if you remove the `eval()`, you should still ensure that the input adheres to expected patterns and is free from potential malicious content.

By following these recommendations, you can enhance the security of the provided code snippet.