SCENARIO

The application contains a simple reflected cross site scripting vulnerability in the search functionality so we will try to exploit it by injecting some malicious script.

**PROCEDURE**

1. Go to the vulnerable web application.
2. Try to search for something in the provided search bar and we can see that in the URL the searched keyword is directly appended to it.
3. So, we will modify the parameter in order to inject the payload to generate a basic alert on the page.
4. Now we get an alert, it is clear that we can exploit the application more by injecting reflected XSS.

**PAYOAD**

<script>alert("Hey!")</script>

**PROOF OF CONCEPT**

**REMEDIATION**

1. **Input Validation:** Implement strict input validation. Use allow-lists to ensure only expected input is processed, and reject any input that contains unexpected data or characters.
2. **Escape Output:** Ensure all user-derived data is escaped before it's displayed on the webpage. Convert characters like <, >, &, " and ' to their respective HTML escape codes to prevent them from being executed as code.
3. **Content Security Policy (CSP):** Implement a strong Content Security Policy to specify which sources of scripts and other resources are valid. This will help prevent the browser from executing malicious, injected scripts.