SCENARIO

The application is vulnerable to server-side template injection due to the unsafe construction of an ERB template. We will try to figure out the way to execute arbitrary code on the backend server.

**PROCEDURE**

1. Open the application and click on the first product itself to get more information about it.
2. We see that the application renders a message saying that the product is out of stock.
3. Notice the URL and we see that the message parameter is appended into it.
4. Now, to identify the template we will try to execute the Payload 1 into the URL within the message parameter.
5. We see that instead of getting the supplied input reflected on the screen we get 49 as response which confirms that the server is using ERB template engine.
6. So, we will try to inject Payload 2 into the URL in the message parameter in order to do Remote Code Execution by going through the documentation of ERB template engine.

**PAYLOAD**

1. <%= 7\*7 %>
2. <%= system("rm /home/carlos/morale.txt") %>

**REMEDIATION**