SCENARIO

The application is vulnerable to server-side template injection due to the way it unsafely uses a template. We will try to figure out a way to know the template used in order to execute arbitrary code on the backend server.

**PROCEDURE**

1. Open the application and log in using the provided credentials to get access to the content editing functionality.
2. Navigate to any blog and click the edit template button, we see that the application uses **${}** syntax to something invalid.
3. We see that the application throws an exception revealing the name of the template engine the server is configured with.
4. So, we will try to inject the Payload into the template in order to do Remote Code Execution by going through the documentation of Freemaker template engine.

**PAYLOAD**

<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("rm /home/carlos/morale.txt") }

**REMEDIATION**