SCENARIO

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

**PROCEDURE**

1. Open the application and log in using the provided credentials to act as a target.
2. Make a request to the server in order to change what the site displays in place of your name and study the request in BurpSuite’s Repeater.
3. We see that in the parameter **blog-post-author-display,** a parameter is sent.
4. Now, to identify the template we will try to execute the Payload 1 into the request within the **blog-post-author-display** 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 Tornado template engine.
6. We know that we can execute arbitrary python in Tornado template.
7. So, we will try to inject Payload 2 into the URL in that parameter in order to do Remote Code Execution by going through the documentation of Tornado template engine.

**PAYLOAD**

1. user.name}}{{7\*7}}
2. user.name}}{%25+import+os+%25}{{os.system('rm%20/home/carlos/morale.txt')

**REMEDIATION**