BEFORE:

AFTER:



**CHANGES (SYSTEM OWNER AND MERCHANT)**

Modify web.xml:

1. Add

***<error-page>***

***<error-code>400</error-code>***

***<location>/cc\_iam/WEB-INF/vm/400.vm</location>***

***</error-page>***

***<error-page>***

***<error-code>404</error-code>***

***<location>/cc\_iam/WEB-INF/vm/404.vm</location>***

***</error-page>***

***<error-page>***

***<error-code>500</error-code>***

***<location>/cc\_iam/WEB-INF/vm/500.vm</location>***

***</error-page>***

1. Enable httpHeaderSecurity
2. Add hstsEnabled

***<init-param>***

***<param-name>hstsEnabled</param-name>***

***<param-value>true</param-value>***

 ***</init-param>***

1. Enable filter-mapping httpHeaderSecurity
2. Add in session-config section

***<cookie-config>***

***<http-only>true</http-only>***

***<secure>true</secure>***

***</cookie-config>***

Reference:

1. <https://docs.bmc.com/docs/security/basic-tomcat-security-configuration-recommendations-924057229.html>
2. <https://eliarms.medium.com/how-to-implement-httponly-and-secure-cookie-in-web-servers-ebad20427b94>