We have found that cross-site scripting is one of the major attacks to the magneto system from the previous assignment use case and misuse cases. In most of the use case and misuse case scenarios for the Magento system, cross-site scripting is a major thing that attackers prone to attack the Magento system. We found that the CWE are related to this attack and we got to know the CWE-79 and CWE-1004 that are related to this attack. When I try to search for the code related to these CWE in the code. As the code base is too large we found that there are few files related to this common weakness enumeration.

CWE-79: Improper Neutralization of Input During Web Page Generation.  
CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag.

The CWE-79 is related to the inject the malicious code into the user session cookies and gain control over the username and password of the users of the Magento and with the help of username and password the attackers try to run the commands which make changes in the Magento system. This type of attack also has an impact on the Availability Access control mechanism. The SSL certificate will avoid all such kinds of attacks related to Magento. Magento documentation provides the instructions to setup SSL for Magento systems.  
The CWE-1004 is related to the that whenever we include the ‘HttpOnly’ flag value in the session cookie which avoids all the attacks of CSS. But in our code, there is no flag value is used as magneto proposes the solution to set the flag value with environment variables or with the help of GUI from admin console can be used to make changes by the super admin.

<https://github.com/magento/magento2/blob/2.4-develop/lib/internal/Magento/Framework/Session/Config.php>

public function setCookieSecure($cookieSecure)

{  
$this>setOption('session.cookie\_secure',(bool)$cookieSecure);  
return $this;  
}