1620815 muhammad yusuf bin zainul ariffin

What is XSS?

A weakness that permits an assailant to add his own content code to a weak web application's page. It utilizes HTML structure rather than URL encryption layer of SSL/TLS to ensure the traffic (HTTPS) diverse with XSS.

How did XSS occur?

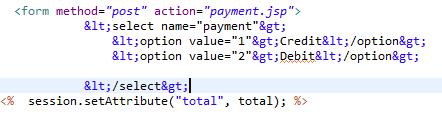
Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

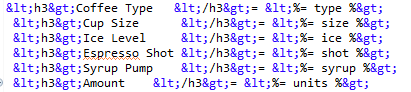
[Injection](https://owasp.org/www-community/Injection_Flaws) is an attacker’s attempt to send data to an application in a way that will change the change the command and follow the new line. For example, the most common example is SQL injection.

How to prevent?

Our defence mechanism to prevent XSS attack is first to encode specific important part of our page which is the payment page



And also we tried to encode several other part also



We also filtered our code with avoiding any <script> tag to sanitize the website and make it safe HTML. We also planned to use HttpOnly attribute to flag cookies but got a few problem with the nginx.

CSRF prevention.

We are implementing reauthenticate measure for another session that the user want to use, like maybank apps.Preventing XSS attack is also a good measure to prevent CSRF attack.