CS392 – Quiz

Name: **Maheeth Reddy**

Roll No.: **1801CS31**

Date: **18-Apr-2021**

Ans 3:

Cross Site Scripting Attack (XSS) occurs when there is a malicious code in the user's input on a particular application. In other words, malicious code to the victim’s browser is injected by the attacker via the target website.

XSS attacks are of two types. The first one is Non-Persistent XSS Attack in which attacker puts JavaScript code in the input. So when the input is reflected back, the JavaScript code will be injected into the web page from the website.

The second type is Persistent XSS Attack in which the attacker stores malicious data (code) in target websites servers. And when other users access this data, they shall be affected.

Clearly, in XSS attack, the attacker is trying to inject malicious code via a possible attack surface. Therefore it is highly essential to sanitize the input for code.

Arunika can sanitize the code by identifing the <script> tags and removing them while parsing. But the attacker can use other tags to inject. Filtering is not the only method, as there are other encoding methods which convert HTML lines of code into non-malicious strings and various open source libraries like jsoup, to parse inputs from JavaScript codes.