

CS 4293

Tutorial 11 Solution

Q1

This is because cookies for one web server usually contain user-specific information to be used by that web server for user authentication, service personalization, as well as user tracking etc.

If such cookies are accessed by other web servers, it would violate user side privacy and also introduce new vulnerabilities where attackers from malicious web servers can easily access/change the victim users' cookies.

Q2

Reflected XSS, Stored XSS, DOM-based XSS.

Q3

1 and 2 only.

In 3, everything after the # is not sent to the server; these are fragment URLs, and the browser does not send them in the server. (Won't be tested in final exam);

In 4, the web application firewall sits at <http://www.example.com>, not at <http://blog.example.com>