Web Application Security

IMPORTANT NOTES:
Study lecture materials at least 1 hour and prepare Q1 prior to the tutorial session. Prepared questions will be discussed in the tutorial session.

1. Cookies can be used to identify a particular session between client and server. In combination with a TLS tunnel, cookies can provide a good solution for session identification, if the browser does not provide the cookie to another server, which it usually should not do. Why could an XSS attack still enable an attacker to take over the session?

   Read `https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)` to learn about other possible XSS Attack Consequences and go through the examples.

   - The main effect of an XSS attack is that code coming from the attacker is executed on the victims machine as if it was coming from the correct server. Thus, this code gets access to the session cookie and can just forward cookie content to the attacker.
   - Examples on the OWASP side are really useful to get an understanding how and why XSS actually works.

2. A hacker discovered the following fact about an online music sales website Ktunes.com: when a client finalizes his music purchase, Javascript running on the client's web browser adds up the client's total order payment amount and sends the total to the Ktunes.com sales server. The server then charges this amount to the client's credit card.

   (a) Explain why this fact reveals a vulnerability in the Ktunes.com website, and explain how the hacker can exploit this vulnerability to breach the website's security.

   (b) Explain how Ktunes.com should change its web application design to remove this vulnerability.

   (a) The attacker can read the content of the Javascript and know how the payment amount is sent to the server. He can then change the amount and send whatever payment amount he wants to the server e.g. purchasing music without paying any money.

   (b) Compute the payment amount on the server side.