

IK2206 – Internet Security and Privacy

Chapter 25 – Web Issues

25.1 Introduction (READ)

25.2 URLs/URIs (READ)

- What is the complete, general syntax of a URL?
- How can user names be specified in URLs? What are they used for, and how does a browser typically process such a URL?

25.3 HTTP (READ)

- What does it mean that HTTP is stateless?
- What consequences does this have for applications such as web shopping sites?

25.4 HTTP Digest Authentication (READ)

- Why is there a need for a separate user authentication mechanisms, given that we already have TLS/SSL for secure web communication?
- How does digest access authentication avoid sending passwords in the clear?
- How does the protocol work, which information is exchanged between client and server?

25.5 Cookies (READ)

- What is a cookie?
- Where is it stored, and who creates it?

25.5.1 Alternatives to Cookies (READ BRIEFLY)

- Make sure that you understand the need for maintaining user session information in web applications
- Consider the alternatives to using cookies. In particular, consider how URLs could be used to carry session information

25.5.5.2 Cookie Rules (READ)

- How can cookies be used for a shopping basket?
- What web server(s) can access a cookie? What are the cookie access rules?
- What are temporary and persistent cookies? (Note that those terms are not used in the textbook)

25.5.5.3 Tracking Users (READ)

- What is tracking, in this context?
- Consider why cookies are being blamed for privacy violation.

25.6 Other Web Security Problems (READ)

25.6.1 Spoofing a Site to a User (READ)

- Consider different methods of tricking a user to a different web site

25.6.2 Merchants Unclear on the Concept (READ)

25.6.3 Getting Impersonated by a Subsequent User (READ)

- What mechanisms and methods are there that could make it possible for a user to "take over" (deliberately or unintentionally) the authentication of a previous user?

25.6.4 Cross-Site Scripting (READ)

- What is a script in this context?
- Why is this a security vulnerability?

Read more on for instance Wikipedia about different kinds of cross-site scripting threats.

25.6.5 Poisoning Cookies (READ)

- What are the security threats here, and how can they be avoided?
- Why is it called "Poisoning", do you think?

25.6.6 Other Misuse of Cookies (READ BRIEFLY)

Make sure that you understand the nature of the threats and the vulnerabilities that were exploited here.