Session 5

Configuration (HTTP-cookies, contents, scripting etc. attack to browsers, and users tracking/profiling

HTTP security vulnerabilities or attacks

Security Vulnerability or Attack	Description
Tracking cookies	Tracking cookies may be used to track Internet users' web-browsing habits. This can also be done in part by using the IP address of the computer requesting the page or the referer field of the HTTP header, but cookies allow for a greater precision. A tracking cookie may potentially infringe upon the user's privacy but they can be easily removed. Current versions of popular web browsers include options to delete "persistent" cookies when the application is closed.
Third-party cookies and web bugs	Cookies have some important implications on the privacy and anonymity of web users. While cookies are sent only to the server setting them or the server in the same Internet domain, a web page may contain images or other components stored on servers in other domains and cookies set during retrieval of these components are called third-party cookies, including cookies from unwanted pop-up ads. Third-party cookies can be used to create an anonymous profile of the use, namely by the advertising industry. The same technique can be used with web bugs. These are images embedded in the web page that are undetectable by the user (e.g., they are tiny and/or transparent). The possibility of building a profile of users is considered by some a potential confidentiality threat, and some countries have legislation about cookies.
Cookie hijacking	Normally cookies travel between a server, or a group of servers in the same domain (a server farm) and the computer of the web-browsing UA. Since cookies may contain sensitive information (user name, a password used for authentication, etc.), cookie contents should not be accessible to other actors. Cookie theft is the act of intercepting cookies by an unauthorized actor. Session hijacking is a technique used to steal cookies via packet sniffing where unencrypted traffic on a network can be intercepted and read (includes cookies) by computers on the network other than authorized sender and receiver (especially over IEEE 802.11a/b/g "Wi-Fi" and "Bluetooth" networks). This traffic sent on ordinary unencrypted http sessions. Attackers can intercept the cookies of other users and masquerade (impersonate) as a legitimate user on the websites to which the cookies apply.

Security Vulnerability or Attack	Description
Cookie poisoning	Cookie poisoning occurs when an attacker sends to a server an invalid cookie, possibly modifying a valid cookie it previously received from the server. While cookies are supposed to be stored and sent back to the server unchanged, an attacker may modify the value of cookies before sending them back to the server. The process of tampering with the value of cookies is called cookie poisoning. In cross-site cooking, the attacker exploits a browser bug to send an invalid cookie to a server. There are websites that are not stateless, storing persistent information about visitors, and only use cookies to store a session identifier in the cookie itself. All the other information remains on the server, thereby largely eliminating the problem of cookie poisoning.
Cookie theft	Cookies are required to be sent back only to the servers in the same domain as the server from which they originate. Scripting languages such as JavaScript and JScript are usually allowed access to cookie values and have the ability to send arbitrary values to arbitrary servers on the Internet.

support, via Unicode, for international character sets unlike the HyperText Markup Language (HTML), and is rapidly being used (as XHTML) instead of basic HTML for web pages. XML's design focuses on documents, yet it is widely used in web services for the representation of arbitrary data structures in different application situations. There are a variety of programming interfaces available to access XML data and several schema systems designed to aid in the definition of XML-based languages that include RSS,[10] SAML, SOAP, and XHTML; XML has also become the default file format for most office tools such as Microsoft Office and OpenOffice.org.

The XML specification defines an XML document as text that is well formed as it satisfies a list of required syntax rules, including:

- only properly encoded legal unicode characters are allowed;
- no special syntax characters, such as "<" and "&," appear except in markup delineation roles;
- begin, end, and empty element tags, which delimit elements, are correctly nested, not missing and none overlapping;
- element tags are case-sensitive, requiring that beginning and end tags match exactly; and
- there is a single "root" element that contains all the other elements.