**Cookie Poisoning**

**Description 1**

On the Web, cookie poisoning is the modification of a cookie (personal information in a Web user's computer) by an attacker **to gain unauthorized information about the user** for purposes such as **identity theft.** The **attacker may use the information to open new accounts or to gain access to the user's existing accounts**. Cookies stored on your computer's hard drive maintain bits of information that allow Web sites you visit to **authenticate your identity, speed up your transactions, monitor your behavior, and personalize their presentations for you**. However, cookies can also be accessed by persons unauthorized to do so. Unless security measures are in place, an attacker can examine a cookie to determine its purpose and edit it so that it helps them get user information from the Web site that sent the cookie. [1]

**Description 2**

Cookies are supposed to be sent back to the server unchanged, but attackers can modify the value of a cookie before sending them back to the server. This is typically done to carry out some sort of attack against the server that relates to some sort of data contained in the cookie. **For example, if a cookie contains the price per item for something in the shopping basket, a change to this value in the cookie may cause the server to charge the user a lower price for that item.** This process of modifying a cookie before it is sent back to the server is called *cookie poisoning.* Sometimes, cookie poisoning is used after cookie theft.

**Description 3**

Cookie poisoning is an effort by an unauthorized person **to access and control aspects of the data** in a cookie, usually **in order to** **steal someone’s identity or financial information**. Many different kinds of hacking that focus on taking data from cookies can be called cookie poisoning, including **theft of passwords, credit card numbers or other identifiers that are stored on cookie files**.

**Description 4**

Cookie poisoning is the act of manipulating or forging a cookie (a small piece of data created and stored in a user's browser that keeps track of important information regarding his or her session information for a particular site) for the purpose of bypassing security measures or sending false information to a server. **An attacker using cookie poisoning can gain unauthorized access to a user's account on the particular site the cookie was created for, or potentially tricking a server into accepting a new version of the original intercepted cookie with modified values.**

If the developer of the web application that created the cookie chose to store important parameters within the application's created cookies, (especially if key parameters, such as privilege level, are labeled such that they can be easily identified) cookie poisoning can be carried out fairly easily and effectively. One such example of cookie poisoning might involve intercepting an online retailer's cookie before its information is sent from a user's computer to the server during a "cart checkout" process and modifying price values to trick the server into charging the user less money.

**Reference**

**[1]** [**http://searchsecurity.techtarget.com/definition/cookie-poisoning**](http://searchsecurity.techtarget.com/definition/cookie-poisoning)

**[2]** [**http://www.infosectoday.com/Articles/Cookie\_Tampering.htm**](http://www.infosectoday.com/Articles/Cookie_Tampering.htm)

**[3]** [**https://www.techopedia.com/definition/16076/cookie-poisoning**](https://www.techopedia.com/definition/16076/cookie-poisoning)

**[4]** [**https://security.radware.com/ddos-knowledge-center/ddospedia/cookie-poisoning/**](https://security.radware.com/ddos-knowledge-center/ddospedia/cookie-poisoning/)