Web13: Session Hijacking Hacking Techniques

In this article, TipsMake.com invites you to learn the Session Hijacking hacking technique.

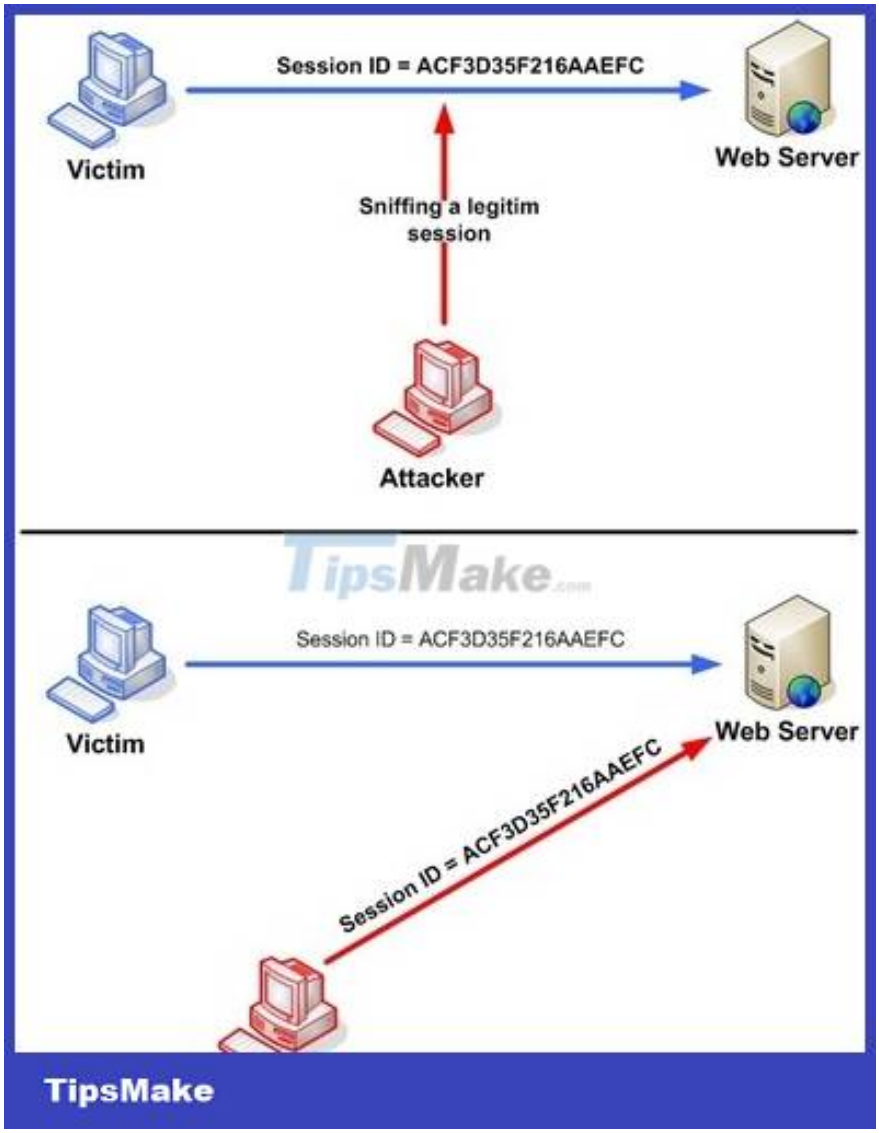
1. Cause

After each successful user login, the session will be redefined and have a new session ID. If the attacker knows this new Session ID, then the attacker can access the application as a normal user. There are many ways for the attacker to get the session ID and take over the user's session such as: Man-in-the-middle attack: eavesdropping and stealing the user's session ID. Or take advantage of XSS errors in programming to get the user's Session ID.

2. Mining ways

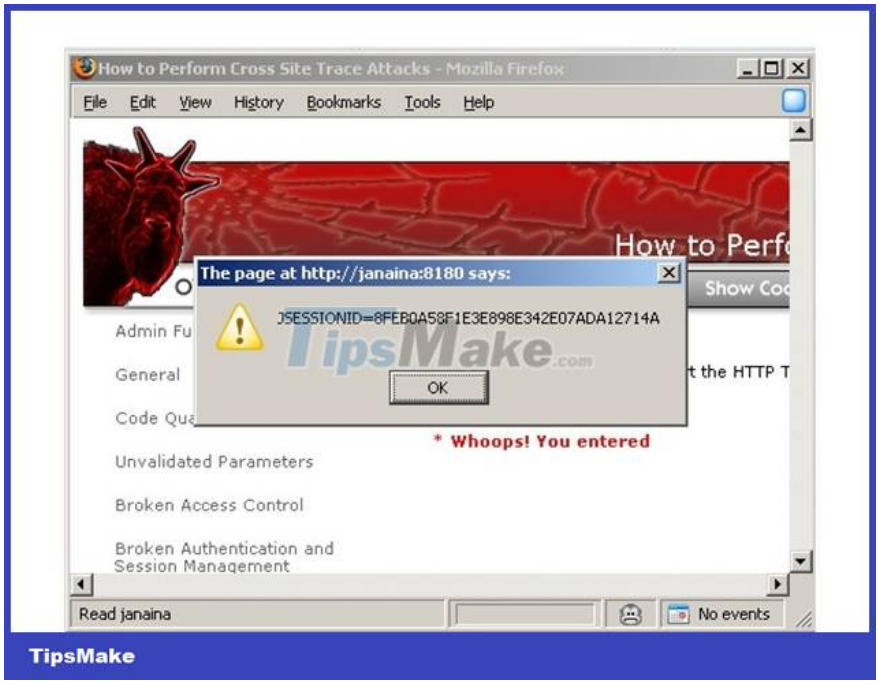
Session Sniffing

As we can see in the figure, first, the attacker will use a sniffer tool to capture the valid session ID of the victim, then he uses this session ID to work with the Web Server under the victim's authority.



Cross-site script attack

An attacker can obtain the victim's session ID by means of malicious code that runs on the client side, such as JavaScript. If a website has an XSS vulnerability, an attacker can create a link containing malicious JavaScript code, and send it to the victim. If the victim clicks on this link, his cookie will be sent to the attacker.



3. Prevention

The following methods can be used to prevent Session Hijacking:

1. Use HTTPS in data transmission to avoid eavesdropping.
2. Use a large random string or number to limit the success of a bruteforce attack.
3. Regenerate session ID after each user successfully login, to avoid Session Fixation attack.

Wish you get more knowledge after each lesson with TipsMake.com!