- Filename: eccouncil-ceh31250-v10-11-1-2-session_hijacking_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Session Hijacking Pt.2
- Description: In this episode, Daniel and Zach continue to explore session hijacking. Here they will discuss token prediction, Cross-Site Request Forgery (CSRF/XSRF), Session Fixation, and Man-in-the-Browser attacks.

==========

Session Hijacking Pt.2

- Session token prediction
    - Tokens with low randomization is susceptible to prediction
- Cross Site Request Forgery attack
    - Attacker tricks target into performing an action on a website that the target has an active session with
        - Change password
        - Transfer funds
    - Done through Social Engineering
        - Malicious links are common tactics (**csrf.html**)
            - Find CSRF vulnerability in bWAPP
            - Capture request with Burp
            - Forge malicious link using captured request
            - Send phishing email to target
            - When target clicks on link, malicious action is performed
- Session Fixation
    - **DIAGRAM**
    - https://www.lanmaster53.com/2014/10/29/session-fixation-demystified/
- Man-in-the-Browser (**DIAGRAM**)
    - Target is infected with malware/trojan
    - Malware intercepts banking traffic
        - Since this is done in the browser, security controls are ineffective
    - Malware returns false information back to the user
        - All while making slight modifications to transactions
            - aka stealing money