- Filename: eccouncil-ceh31250-v11-14-7-1-web-app-hacking-methodology.md
- Show Name: CEHv11 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: Web App Hacking Methodology
  ==========

Web App Hacking Methodology

Objectives:

- What are the first steps towards successfully hacking a Web App?
    - Recon | Footprinting
- Once we've identified the moving parts, what's next?
    - Do a vulnerability assessment
        - Find inputs
        - Enumerate software and server-side technologies
        - Find where the app is generating dynamic content
        - Map out the web app's files and directories
        - Find areas that could have commonly vulnerable coding errors
        - Create a plan of attack / map the attack surface
- So now we're ready to attack the web app?
    - Yes.
        - You're going to follow your attack map
            - But, attacks could be...
                - Login/Authentication bypass
                    - Injections
                    - Brute force
                - Authorization attacks
                    - HTTP Parameter Tampering
                    - POST data tampering
                - Logic Flaws
                    - Can I just bypass the 'payment' page?
                - Injections
                - Client-based
                    - XSS
                    - CSRF
                    - Redirects and Forwards