- Filename: eccouncil-ceh31250-v12-14-3-1-web-app-hacking-methodology.md
- Show Name: CEHv12 (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/Enumeration
    - Discover networking information
      - IP address
      - DNS info
      - Sub-Domains
      - Virtual Hosts
      - Are there protections?
        - Firewalls, Proxy, WAF, Captcha, Rate-limiting
      - HTTP server version
      - Ports
      - Map out files and dirs and possible hidden content
      - CMS version
      - Discover inputs
      - Discover dynamic content (XSS)
- Once we've identified the moving parts, what's next?
  - Do a vulnerability assessment
    - Run vulnerability scanners
      - Nikto
      - Skipfish
      - Wapiti
      - ZAP
    - Test inputs for injections
      - Manually
      - Programmatically
        - Burp Intruder
        - SQLMap
        - Commix
        - wFuzz
    - Run CMS specific vulnerability scanners
      - WPScan
      - Joomscan
      - Drupwn
    - Manually check for PoC
      - Exploit-DB (searchsploit)
      - Vulners
      - VulnDB
      - Google
- 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
    - Basically the OWASP Top 10