- Filename: eccouncil-ceh31250-v12-13-3-1-web-server-hacking-methodology.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Servers
- Episode Name: Web Server Hacking Methodology
  ==

Web Server Hacking Methodology

Objectives:

- What is the common method used to attack web servers?

  - Recon

    - Ports (HTTP/HTTPS)
    - Service Enumeration

      - Apache, Nginx, IIS
      - Database
      - CMS

    - Banners
    - Sub-Domain Enum
    - DNS

  - Vulnerability Scan

    - Nikto
    - Skipfish
    - Burpsuite Pro Scanner
    - ZAP

  - Directory Fuzzing

    - Feroxbuster
    - Gobuster
    - Dirb
    - Dirbuster
    - robots.txt

  - Abuse Defaults

    - Login creds
    - Config files

      - phpinfo
      - apache

  - Web App Attack

    - Vulnerability Scan Results
    - Manual testing for vulns/exploits

      - Burp Suite
      - ZAP