- Filename: eccouncil-ceh31250-v11-13-1-1-web-server-hacking-concepts.md
- Show Name: CEHv11 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Servers
- Episode Name: Web Server Hacking Concepts
  ==

Web Server Hacking Concepts

Objectives:

- Define what a web server is and its function
- List the components of a web server
- List and define common security vulnerabilities found in web servers
- List and explain common security controls, tools, and strategies used to combat attacks against web servers

---

- Web Server basics
  - HTTP Server software
    - Apache
    - NGNX
    - IIS
  - HTTP Server Components
    - Document Root
      - Where is your `index.html`?
    - Server Root
      - Where is your server configs, logs, cgi-bin,
    - Virtual Document Tree
      - Remote/Other Disk storage of web content
    - Virtual Host
      - Using multiple names for the same site
    - Web Proxy
      - Proxy that should be used
- What makes web servers vulnerable?
  - Lacking OS updates/patches
  - Using defaults
  - Poor/No Authentication
  - OS/HTTP_Server/Website/Permissions misconfiguration
  - Software vulns
    - They are running web apps
      - Those apps could also have security issues
- Countermeasures?
  - DMZs / Network segmentation and firewalling
  - WAFs
  - Patches and updates
  - Change defaults

- File permissions
- Secure coding
- Filtering of user input and acceptable file types
- Disable directory listing
- Use encryption
- Honeypot the site
- Disable errors
- Be vague with responses