

- Filename: eccouncil-ceh31250-v12-13-2-1-web-server-attacks.md
- Show Name: CEHv12 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Servers
- Episode Name: Web Server Attacks

=====

## Web Server Attacks

### Objectives:

---

- What kinds of attacks to web servers face?
  - DoS
  - Directory Traversal
    - Use dir traversal to access source code to current page.
      - See that code makes a call to `admin/settings.php`
        - Use traversal to read `admin/settings.php`
          - See MySQL DB creds
            - Use creds to access DB remotely
              - `mysql -u root -p -h 192.168.202.133`
  - Phishing
  - Defacement
    - Deface a page
  - Brute force remote administration
    - RDP
    - SSH
    - Web-based Administration portals
  - SSRF (Server Side Request Forgery)
    - Abuse of requests by the web app to web server to access internal resources
      - Detection
        - Look for parameters like
          - `/file=`
          - `/path=`
          - `/src=`
    - Port scan
      - `payload = src=http://127.0.0.1:PORT`
    - File Read
      - `payload = src=file:///etc/passwd`
  - XSS
  - CSRF
  - IDOR
  - Injection
    - Code/Command Execution
  - File inclusions