CS 410: Web Security
A4/A7: Labs and Homework

WFP1: File include

- **Example #1**
  - **Perform both a Local File Include (LFI) and a Remote File Include (RFI) attack on the site using /etc/passwd and http://www.google.com.**
- **Example #2**
  - **Site now appends "`.php`" to page parameter**
  - **Learn to use URL encoding of special characters**
  - **Recall the character that is often used to terminate strings**
  - **Use it to perform both an LFI and RFI attack**

WFP1: XML

- **Example #1**
  - **Use XML Entity tag to do an LFI attack on the site**
  - **You will need to URL encode the XML included**

WFP1: Directory traversal

- **Example #1**
  - **Use directory traversal on image icon to perform an LFI**
- **Example #2**
  - **Filter ensures that files begin with a specified directory prefix (/var/www..)**
  - **Bypass filter to perform an LFI**
- **Example #3**
  - **Filter ensures filename parameter ends with ".png"**
  - **Bypass filter to perform an LFI**

WFP1: File upload

- **Example #1**
  - **Upload a PHP file to obtain a directory listing**

- **Example #2**
    - **Filter now ensures no files ending with ".php" are allowed**
    - **Bypass the filter using alternate PHP filename extensions**

<u>WFP2: Authorization</u>

- **Example #1**
    - **Access subpages from the site while logged out**
- **Example #2**
    - **Granularity of user access is too coarse**
    - **Valid logins allow one to access profiles of other users**
    - **Access the profile of another account**
- **Example #3**
    - **Original page fixed**
    - **Find an alternate way to access profile of another account**

<u>Homework</u>

- **Lessons: Failure to Restrict URL Access**
- **Lessons: Insecure Direct Object References**
- **Challenges: Failure to Restrict URL Access #1-3**
    - **#3: Go to cheat directly since Injection not covered yet. Must inject UserList to get all accounts. Default URL will list a subset only**
- **Challenges: Insecure Direct Object References #1-2, Bank**
    - **Bank: Note mis-spelling of recieverAccountNumber**