**Task 1 answer**

Password are often the weakest link in the security chain. A weak password is often a re-used password, and it is easily exploitable with a brute-force attack reading from a list of common weak passwords. These weak password lists have been catalogued over the years from case studies in hacked sites and are widely available.

**Task 2: Command injection**

1. flag{command\_injection\_is\_a\_serious\_vulnerability}
2. 1;cd ../../../../www/blob/hackable/uploads/;cat flag.txt
3. Because the web’s input of the IP address is not being sanitized, you are able to add a semicolon to the input and then add subsequent shell commands. Here are examples of some of the shell commands I used to find my way around the directory structure

**1;ls -- To get the list of files**

**1;cd ../../../../;ls; -- Get list of directory at this level**

**1;cd ../../../../www/blob/hackable/uploads/;ls -- Found the hackable directory**

**Task 3: Local file inclusion**

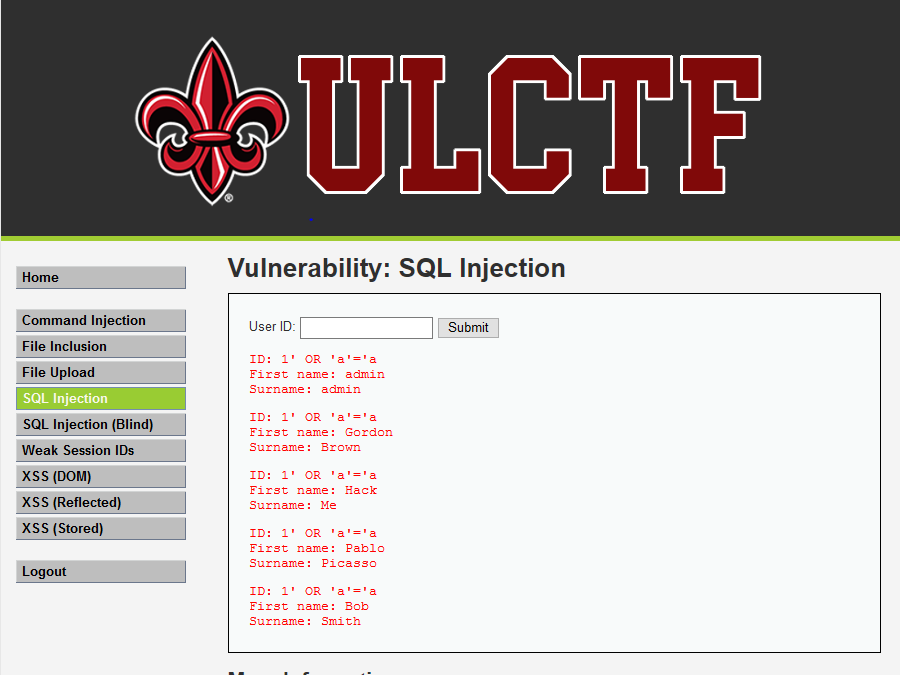
**Task 4: File upload**

**Task 5: SQL injection**

**Payload:** 1' OR 'a'='a

**Note about vulnerability –** The vulnerability exists because the query is concatenating strings on the where clause to build the query that is executed. No sanitation of input is present. Because of this you can add OR 'a'='a to the input which causes the where clause to always evaluate to true, so the query becomes logically equivalent to the much simpler query: select … from users

**Screenshot**



**Task 6: Blind SQLI**

**Why your payload from Task 5 does not work in this page?**

Task 5 payload doesn’t work because the page’s php code is checking for the count of rows retrieved by the query. The Task 5 exploit returns more than 1 row, and it branches to the *“User ID exists in the database.”* message.

**Command line arguments passed to the sqlmap.py**

**Task 6: Weak Session ID**