DVWA
- SQL Injection (Blind) (low and medium)

Program #1: Blind SQL injection (WFP2: MongoDB Example #2)
- Consider
  http://<wfp2_site>/mongodb/example2/?search=admin
- Searches for usernames, but we want to steal passwords
- But, if injectable, then we can use conjunctions and try regular expressions against password
- Consider
  http://<wfp2_site>/mongodb/example2/?search=admin%27%26%26this.password.match(\^a/)///+%00
  - Assuming password alphabetic
  - If entry remains, first character of password is ‘a’
    - Add ‘a’ to test condition and move on to second character of password
  - If entry disappears, move on to next candidate letter (e.g. ‘b’)
- Now, consider
  http://<wfp2_site>/mongodb/example2/?search=admin%27%26%26this.password.match(\^[a-zA-Z]////+%00
  - Checks for passwords with alphanumeric first character
  - If entry remains, first character is a letter
    - Split search space in half and try again
  - If entry disappears, first character is not a letter
    - Search half of non-alphabetic characters
  - Continue to narrow regexp until next character of password found
- Write a Python program that performs a blind SQL injection to obtain the password of the user admin
  - For efficiency, your program must implement a binary search algorithm that uses conjunctions and regular expressions against password