Name: **Date:** **Class:**

Section 5: Independent Practice Worksheet

Part 1
Instructions: Check out the screenshot of the DVWA login page. What is the URL for this page?

Part 2
Instructions: Log in to the DVWA web server and in the Security menu section change the security level to “Low”.

Part 3
Instructions: Remember how to build a Massprocessor username list and password list? Let’s assume you know the first three lower alpha letters of the user password. Build the list *username_wordlist2.txt* and display the first and last 10-character strings.

Part 4
Instructions: Now assume you know the first six letters of the lower alpha password. Use Massprocessor to build the list *password_wordlist2.txt* and show the first and last 10-character strings:

Part 5
Instructions: Use the two wordlists (*username_wordlist2.txt*, *password_wordlist2.txt*) you recently generated with Maskprocessor (mp64).

1. Do some AI searching with Grok and Gemini on how to use Hydra to brute force the DVWA login page. Make sure you preface your searches with “ethical hacking” and “authorized” to avoid being flagged!
2. Use what you’ve learned from the AI language learning models and build a successful command string to brute force the DVWA login page with Hydra and your two wordlists. Submit a screenshot of your command string and successful attempt.
3. Break down the parts of the command string and explain the purpose of each part!
4. Analyze and compare the differences between Grok’s and Gemini’s command string.