

Ffuf

<code>ffuf -h</code>	ffuf help
<code>ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ</code>	Directory Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/indexFUZZ</code>	Extension Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/blog/FUZZ.php</code>	Page Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ -recursion -recursion-depth 1 -e .php -v</code>	Recursive Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u https://FUZZ.hackthebox.eu/</code>	Sub-domain Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u http://academy.htb:PORT/ -H 'Host: FUZZ.academy.htb' -fs xxx</code>	VHost Fuzzing
<code>ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php?FUZZ=key -fs xxx</code>	Parameter Fuzzing - GET
<code>ffuf -w wordlist.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx</code>	Parameter Fuzzing - POST
<code>ffuf -w ids.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs xxx</code>	Value Fuzzing

Wordlist

<code>/opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt</code>	Directory/Page Wordlist
<code>/opt/useful/seclists/Discovery/Web-Content/web-extensions.txt</code>	Extensions Wordlist
<code>/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt</code>	Domain Wordlist
<code>/opt/useful/seclists/Discovery/Web-Content/burp-parameter-names.txt</code>	Parameters Wordlist

Misc

<code>sudo sh -c 'echo "SERVER_IP academy.htb" >> /etc/hosts'</code>	Add DNS entry
<code>for i in \$(seq 1 1000); do echo \$i >> ids.txt; done</code>	Create Sequence Wordlist
<code>curl http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=key' -H 'Content-Type: application/x-www-form-urlencoded'</code>	curl w/ POST



By **Gossip1185**

Published 30th May, 2025.
Last updated 5th May, 2025.
Page 1 of 1.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>