20 min

FUZZING 🤖

DAY 04

TYPES OF FUZZING

- DIRECTORY FUZZING
- CONTENT FUZZING
- PARAMETER FUZZING
- HEADER FUZZING
- …
- ANY PART OF REQUEST CAN BE FUZZED

TOOLS ⚒🔪

- HTTPS://GITHUB.COM/OJ/GOBUSTER
- BURP PRO CONTENT DISCOVERY
- HTTPS://GITHUB.COM/FFUF/FFUF
- HTTPS://GITHUB.COM/MAUROSORIA/DIRSEARCH

TIPS

- SOMETIMES YOU WILL GET STATUS CODES YOU DO NOT WANT
  - EITHER FILTER THEM OUT
  - OR FOLLOW THE REDIRECTS
- POST DATA CAN ALSO BE FUZZED
- YOU CAN FUZZ SUBDOMAINS
  - https://fuzz.hackxpert.com
- DON'T BLINDLY RUN T00LS, MIND RATE LIMITS

ASSIGNMENT (15M)

- FUZZ DIRECTORIES HTTP://HACKXPERT.COM WITH FFUF
- DO NOT FUZZ HTTPS, BUT MAKE SURE IT'S HTTP
- YOU WILL GET AN ERROR CODE
- WORK AROUND IT