Analyzing JS files

BY UNCLE RAT

Agenda

- What is a JS files
- Show me your secrets!
- Attack strategy
- Defense mechanisms

What is a JS files

What is a JS files

- Client side object oriented scripting language
- Makes static websites dynamic
- Can change a website without reloading it

Show me your secrets!

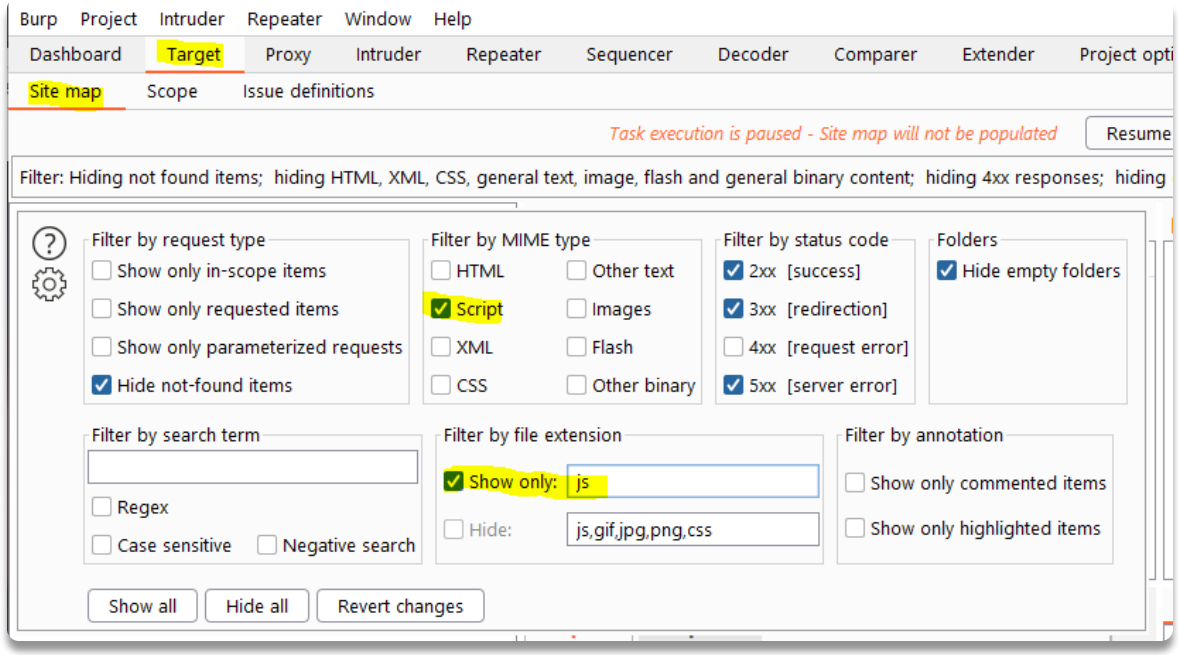
Show me your secrets!

- New endpoints
- Hidden parameters
- API keys
- Business logic
- HTML/Javascript sinks
- Secrets/passwords
- Potentially dangerous areas in code(eval, dangerouslySetInnerHTML etc)

Attack strategy

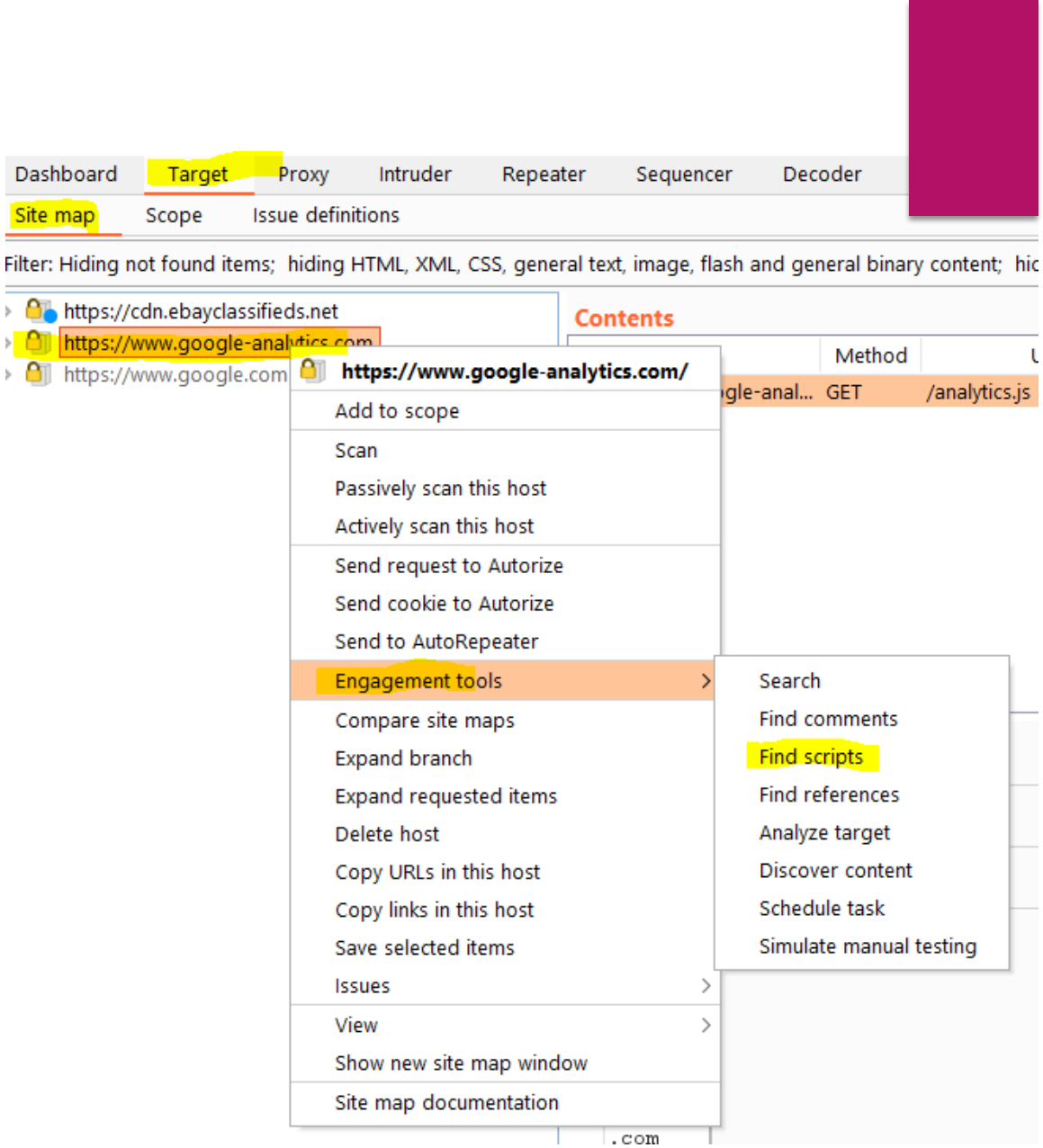
Attack strategy – Gathering JS files

- Use burp filters
  - Explore the website with burp in the background
  - Open site map
  - Set filter



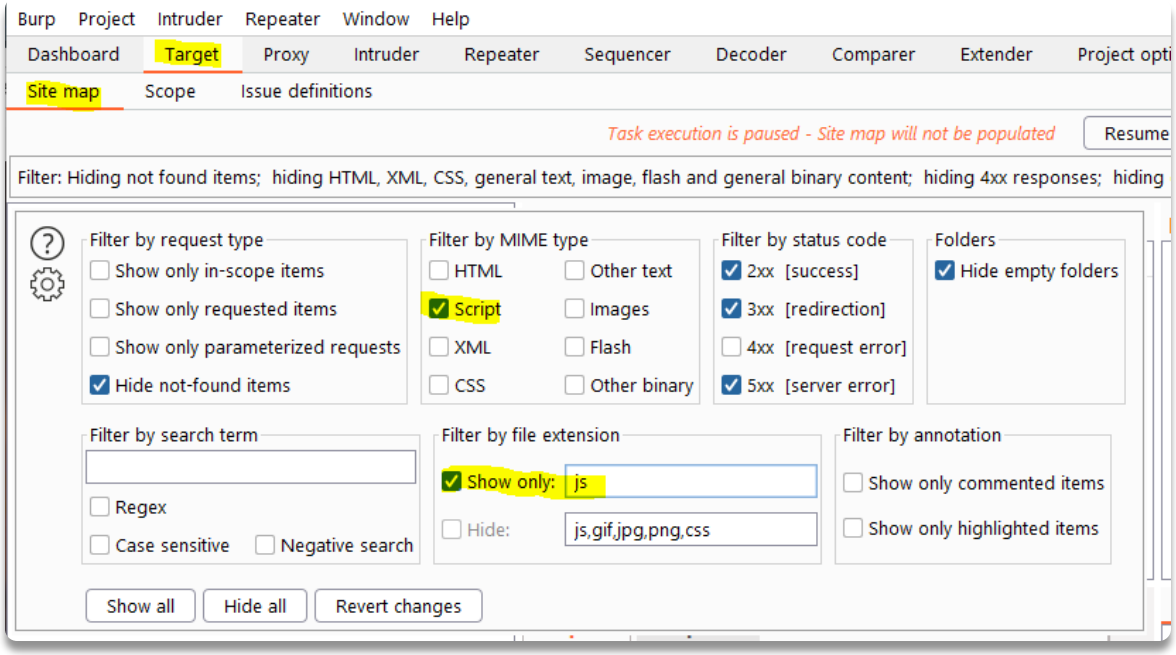
Attack strategy – Gathering JS files

- Use burp suite PRO
  - Explore the application with burp open
  - Right click the target in site map
  - Engagement tools > Find scripts



Attack strategy – Gathering JS files

- Use waybackmachine
  - Install waybackurls
    - go get github.com/tomnomnom/waybackurls
  - Grep for JS files
    - `waybackurls google.com | grep "\.js" | uniq | sort`



Defense mechanisms

Defense mechanisms

- JS minification
  - Decompress using UglifyJS
- JS obfuscation
  - There is no one-size fits all solution
- JS chunking
  - Manual de-chunking