Broad scope methodology – The importance of manual testing

BY UNCLE RAT

Agenda

- Why it matters
- How we can test for it
- Script kiddie vs hacker
- General manual recon tips

Why it matters

Why it matters

- Automatic testing is often a black box
  - Even despite being open source
- Automation is good, automation + manual is even better
- Automation misses a lot
- We need to get to know the processes so we can improve our automation
- When we simply use tools, we don't improve tools
  - Standing still = moving backwards

How we can test for it

How we can test for it

- Google dorking
  - Site:*.target.com -www
  - Open subdomain + investigate
  - Site:*.target.com -www –login
  - Open next subdomain + investigate
  - Site:*.target.com -www –login –regsiter
- Waybackmachine(actual use it, not waybackurls)
- Don't just stick to google, also go to yahoo, duckduckgo, bing, ...

How we can test for it

- Github dorking
  - API keys
  - Secrets
  - Login data
  - Source code
    - This is a goldmine
    - A full map to the functionality
- Linkedin
  - New feature announcements

Script kiddie vs hacker

Script kiddie vs hacker

Script kiddie

- Only runs scripts other people write
- Never does original research
- Only ever goes for low hanging fruit
- Doesn't grow to their full potential

Hacker

- Does manual work and translates that into automation
- Takes pride in digging deep
- Doesn't rest until they reach their full potential

General manual recon tips

General manual recon tips

- Investigate all the subdomains
  - If it's a static page move on
  - If you find functionality, test it using your regular main app methdology
- Google Hacking - Free Google Dorks for Recon | Pentest-Tools.com (pentest-tools.com)
- First run your automation, then start manual testing
  - Check automation results after manual testing
- If the subdomain looks interesting, dig deep
- Trust your rat instincts
- If you come across a new technology, look up how to hack it

General manual recon tips

- If you see a custom login page, try directory brute forcing it
  - You might find unprotected pages
  - Make sure the program allows it
  - Keep the amount of requests/sec low
- Do write your own tools or try to add to existing ones