XSS Hunting Methodology

- MPA Apps
  - Full-Auto Testing
    - Endpoint Enumeration + Verify
      - Passive
        - Wayback
          - 2XX
            - gau -> (gf) -> qsreplace -> httpx
            - gau -> qsreplace -> httpx
            - gau -> httpx -> Gxss
          - 3XX
            - gau -> login -> httpx (-H) -> Gxss/qsreplace (-H)
      - Active
        - Application Endpoints
          - Content Discovery + Authentication Header
            - Analyze Target
              - qsreplace + Gxss
                - Dynamic URLs?
                  - qsreplace -> httpx/Gxss (-H)
                - Static URLs (Path Values)
                  - cat urls.txt | deduplicate.exe --hide-useless
                  - uddup
      - Exploit
        - Dalfox
        - WAF
          - Known WAFs
            - Pre-Defined Payloads + Generate Similar Payloads
            - Find a Payload
          - Unknown WAFs
        - CSP
          - cspvalidator
          - CSP Bypass
  - Semi-Auto Testing
    - Query String/Path Values
    - Forms
    - self-xss
      - Forms
        - CSRF
        - IDOR
        - Web Cache Deception
      - Headers
        - Web Cache poisoning
        - Request Smuggling
    - Blind XSS
      - contact us
      - Forms
        - contact us
        - report
        - subscription
        - feedback
      - Headers
- SPA Apps