February 4, 2020

Bug Searching

- [ ] Run Amass
- [ ] Run Findomain
- [ ] Run Turbolist3r and can use assetfinder
- [ ] run dnsgen and filter live subdomain
- [ ] masscan for port scanning or Nmap
- [ ] Passive scanning
  - [ ] shodan
  - [ ] Censys
  - [ ] Virustotal
  - [ ] securitytrails
  - [ ] Google dorks and github dorking
  - [ ] other website as told by prateek
- [ ] Test All Port it may have something found in masscan, censys , shodan etc.
- [ ] Test for any bucket
- [ ] Run aquatone
- [ ] check for broken Link using tool for all subdomains
- [ ] run Diresearch or ffuf for subdomain
- [ ] Wayback machine
- [ ] LinkFinder and JSparser for javascript finding
- [ ] Manually explore the site
- [ ] Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store
- [ ] Check for differences in content based on User Agent (eg, Mobile sites, access as a Search engine Crawler)
- [ ] Parameter Pollution can used in other vulnerability
- [ ] Oauth misconfig
- [ ] XSS every param and test and change payloads
- [ ] Read all history in burp and understand both request and response
- [ ] SSTI --> if Tech is AngularJs
- [ ] Value which is not understandable try to decode it
- [ ] Try different methods Like DELETE,PUT GET in place of POST and viceversa
- [ ] Identify technologies used

- [ ] Check for sensitive data in client-side code (e.g. API keys, credentials)
- [ ] Try Registering in website and check for confirmation mail
- [ ] Open Redirect try bypass as much you can and try to chain it
- [ ] Authentication Bypass
- [ ] password reset functionality
- [ ] Host Header Injection
- [ ] Cache Poising + CPDos
- [ ] Race Condition --> Try in redeem or same functionality
- [ ] Rate Limiting in good field
- [ ] IDOR in functionality like adding something removing something or even unsubscribing
- [ ] SQL injection in param when trying for xss
- [ ] privilege Escalation
- [ ] 2FA Bypass
- [ ] LFI for this you can check for burp all analys where could be file is asked from server
- [ ] CORS misconfig in different subdomain try with bypassed too
- [ ] XXE
- [ ] CSRF check for all subdomain
    - [ ] IF token is present try different bypass for them try all not one
- [ ] SSRF --> test for extension too and try different bypasses too
- [ ] File upload try bypasses and try in multiple subdomain don' t trust automation everytime test by yourself
- [ ] CRLF injection test in all place subdomain subdirectory