The bug hunter’s methodology

1. Theory

* The web application hacker’s handbook
* Web Hacking 101
* OWASP Top 10
* Breaking into information security
* Mastering modern web penetration testing

1. Discovering IP-space

* <https://bgp.he.net/> (search IP and IP-ranges for companies and other stuff)
* <https://whois.arin.net/ui/query.do>
* <https://apps.db.ripe.net/db-web-ui/#fulltextsearch>
* <http://reverseip.domaintools.com/search/>
* <https://shodan.io/search?query?=org%3a%22Mail.Ru%22>

1. Discovering new targets

Acquisitions

Brand Discovery

Linked Discovery

Weighted links and reverse tracker analysis

* Asquisitions

Example: <https://www.crunchbase.com/organization/mail-ru>

* Linked Discovery (Burp Suite Spidering)

1. Turn off passive scanning
2. Set forms auto to submit
3. Set scope to advanced control and use strings of target name (not a normal FQDN)
4. Walk + browse, then spider all hosts recursively
5. Profit (more targets)

* DomLink



Resource: <https://github.com/vysecurity/DomLink>

* Builtwith

Example: <https://builtwith.com/mail.ru>

* Google Dorks

1. Discovering new targets (subdomains)

* Amass

Resource: <https://github.com/OWASP/Amass>

* SubFinder

Resource: <https://github.com/subfinder/subfinder>

1. Subdomain bruteforcing

* massdns
* gobuster
* SubFinder

1. Sub Bruting (wordlist)

* <https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056>
* <https://scans.io/>
* <https://github.com/pentester-io/commonspeak>

1. Auxiliary

* Dnssec/ nsec/ nsec3 walking
* Github recon
* Dorking

Resource: <https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration/blob/master/esoteric_subdomain_enumeration_techniques.pdf>

1. Enumerating targets

* Port scanning (masscan, nmap)

1. Credential bruteforcing

Brutespray

Cred’s Bruteforce

Nmap service scan - Og

masscan

Resource: <https://github.com/x90skysn3k/brutespray>

1. Visual identification

Resource: <https://github.com/FortyNorthSecurity/EyeWitness>

1. Wayback enumeration (401/403 HTTP Reauests)

Resource: <http://archive.org/web/>, <https://github.com/tomnomnom/waybackurls>

1. Organization process

Xmind, cherrytree a.s.o.

1. Platform identification and CVE searching (burp vulners scanner, wappalyzer, built with)
2. Parsing JavaScript (Zap Ajax Spider, Jsparker, linkfinderm JSParser)
3. Content discovery
4. Parameter bruting

Resource: <https://github.com/maK-/parameth>

1. Blind XSS Framework Continues

Resource: <https://github.com/LewisArdern/bXSS> (SMS support), <https://github.com/ssl/ezXSS>

1. SSRF
2. IDOR (id, hashes, emails)
3. Subdomain takeover

Resource: <https://github.com/EdOverflow/can-i-take-over-xyz>, <https://github.com/sa7mon/S3Scanner>