Bug Bounty (BB)

Programme de Bug Bounty

Principe et objectif:

Une entreprise met à disposition de chercheurs en sécurité (hunters) leur système d'information (Web, API, apk ,. . .) dans le but de trouver des failles de sécurité en échange d'une rémunération

Difference Pentest vs Bug Bounty

- Dépend du besoin du client
- Pentest apporte plus de conformité et répond aux risques metiers
- Profondeur du test plus importante pour le BB et complétude pour le pentest

Vision "pentester"

Exemples:

- Outdated software
- weak/insecure method (TRACE)
- Cleartext (Telnet, http, etc)
- Ciphers and protocols
- Expired/invalid certificates
- basic authentication
- Brute forcing / no CAPTCHA
- user account enumeration
- No lockout policy
- Cookies not expiring
- weak password policy
- cookie flags

Vision (vulnérabilités qualifiantes) "hunter"

- Remote code execution (RCE)
- Local files access and manipulation (LFI, RFI, XXE, SSRF, XSPA)
- Code injections (HTML, JS, SQL, PHP, . . .)
- Cross-Site Scripting (XSS)
- Cross-Site Requests Forgery (CSRF) with real security impact
- Open redirect
- Broken authentication & session management
- Insecure direct object references
- CORS with real security impact
- Horizontal and vertical privilege escalation