



App Core Features Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



CORE FEATURES

- Understand the app in depth
- Depends on app (mail, health, shop...)
- Consistency of APIs or a mix?
- Are all features on the web also available on mobile and vice versa?
- Different versions have a different code base?



CORE FEATURES

- Test different TLDs if in scope
- Different countries
- Different features
- Different teams
- Different payment options
- Different security (.com vs. com.mx)



CORE FEATURES

- What features are available to me?
- What do they do?
- What type of data is handled?
- Do they all use the data source?
- Example: Address selection in different places of the app



CORE FEATURES

- Are the requests the same to retrieve API info or are different endpoints used?
- Can I pay for upgraded features?
- Test paid vs. free
- Can you access paid features without paying?



CORE FEATURES

- What's the oldest feature? (Research)
- Did they announce new features but didn't release?
- Dork around. Old code = bugs
- What next feature they announced?
- Subscribe to newsletters, follow their social media



CORE FEATURES

- Do any features offer privacy options (public, private etc.)
- Do they actually work?
- How many levels of access (unauthenticated, guest, user, moderator, admin etc.)
- Broken access control?



Thank You!

Become a Successful
Bug Bounty Hunter