



Business Logic Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



BUSINESS LOGIC

Business logic vulnerabilities refer to flaws or weaknesses in the decision-making processes and rules of a software application, which can be exploited by attackers to bypass security measures and gain unauthorized access to sensitive data or system resources.



BUSINESS LOGIC

- Understand the application in full
- Understand all flows
- How shall it work?
- What have the developers intended / anticipated?
- Check how old features interact with new features



BUSINESS LOGIC

- Can a user manually change price values? Client-side controlled?
- Can I claim a price I haven't won?
- Can I skip steps in checkout process?
- Can I deviate away from the intended checkout path?



BUSINESS LOGIC

- Can a user manually change price values? Client-side controlled?
- Can I claim a price I haven't won?
- Can I skip steps in checkout process?
- Can I replay steps?
- Can I deviate away from the intended checkout path?



BUSINESS LOGIC

- Can I sign up with martin@target.com?
- Is the email address verified?
- Can I access Beta content?
- Can I access Premium content without paying?



BUSINESS LOGIC

- Can I sign up with martin@target.com?
- Is the email address verified?
- Can I access Beta content?
- Can I access Premium content without paying?



BUSINESS LOGIC

- Client-side only controls
- Negative quantities (shopping cart)
- Introduce extremely long input / high numbers etc.
- Can I change other people's password by removing "current password" parameter and simply change the ID to theirs?



BUSINESS LOGIC

- Can I re-use gift codes / vouchers?
- Are they leaked elsewhere?
- Can I like an article more than once?
- Is the old password not checked when changing to a new password?
- Can I access paid / premium content?
- Can I get articles for free?



BUSINESS LOGIC

- Can I override other user's profile pictures by selecting the same filename?
- Can I sign up with null bytes i.e. %00, %09 etc. in my email and take their account over?
- Can I re-use the password reset token?



Thank You!

Become a Successful
Bug Bounty Hunter