https://labs.hackxpert.com/BUSINESS_LOGIC/

What are Business Logic Exploits?

Business logic exploits are vulnerabilities in a web application that allow an attacker to abuse the intended functionality of the application for their own gain.
They are typically caused by flaws in the business logic of the application, which can be difficult to detect and exploit.

How to look for Business Logic Exploits?

Here are some techniques to look for business logic exploits:

- **Review application logic:** Review the business logic of the application to identify areas where the application may be vulnerable to abuse.
  Look for areas where the application makes assumptions about user behavior or where the application provides functionality that can be abused.

- **Test edge cases:** Test the application with edge cases to identify vulnerabilities that may not be apparent in normal usage.
  For example, test the application with large inputs, negative inputs, or unexpected input sequences.

- **Use automation:** Use automated tools to test the application for common business logic vulnerabilities.
  For example, tools like OWASP ZAP can be used to test for common business logic vulnerabilities like authorization bypass or data manipulation.

- **Perform manual testing:** Perform manual testing to identify vulnerabilities that may not be detected by automated tools.
  For example, try to abuse the intended functionality of the application by submitting unexpected input or by manipulating data.

- **Conduct security reviews:** Conduct security reviews of the application code and design to identify areas where the application may
  be vulnerable to business logic exploits. This can be done through code reviews, threat modeling, or other security assessments.