Broken Object Level Authorization (BOLA)

Ethical Hacking of RESTful & GraphQL API Training Course

Broken Object Level Authorization (BOLA)

API1:2023 - Broken Object Level Authorization (same as 2019)

APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface of Object Level Access Control issues. Object level authorization checks should be considered in every function that accesses a data source using an ID from the user.

https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/

Broken Object Level Authorization (BOLA)

API Broken Object Level Authorization is a security vulnerability where an API doesn't properly enforce access controls, enabling an attacker to manipulate or access unauthorized data objects;

For example, an e-commerce API allowing a user to change the product ID in a request and view or modify another user's orders.

Example: An online banking API that does not properly enforce authorization checks on individual account transactions, allowing any authenticated user to manipulate and view transactions of other users' accounts.

Broken Object Level Authorization (BOLA)

API Broken Object Level Authorization is a security vulnerability where an API doesn't properly enforce access controls, enabling an attacker to manipulate or access unauthorized data objects;

For example, an e-commerce API allowing a user to change the product ID in a request and view or modify another user's orders.

Example: An online banking API that does not properly enforce authorization checks on individual account transactions, allowing any authenticated user to manipulate and view transactions of other users' accounts.

Broken Object Level Authorization (BOLA)

Locating Resource IDs

GET /api/v1/user/account/1111

GET /api/v1/user/account/1112

Look for user ID names or numbers, resource ID names or numbers, organization ID names or numbers, emails, phone numbers, addresses, tokens, or encoded payloads.

Broken Object Level Authorization (BOLA)

Testing BOLA

- Create resources as Alice.
- Create resources as Bob.
- Swap out your Alice token for user Bob token.
- Using Bob's token, make the request for Alice's resources.

Create multiple accounts at each privilege level to which you have access.

Using your accounts, create a resource with account A and attempt to interact with it using account B

Broken Object Level Authorization (BOLA)

In a nutshell

Broken Object Level Authorization vulnerabilities are the same concept you are most likely already familiar with:

Broken Access Control
and
Insecure Direct Object References (IDOR)

Thank You!

Ethical Hacking of RESTful & GraphQL API Training Course