Broken Authentication

Ethical Hacking of RESTful & GraphQL API Training Course

Broken Authentication

API2:2023 - Broken Authentication (same as 2019)

Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising a system's ability to identify the client/user, compromises API security overall.

https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/

Broken Authentication

API Broken User Authentication is a security vulnerability where an API fails to adequately authenticate and verify the identity of users, potentially allowing unauthorized access to sensitive data or actions;

For example, an API not properly validating user tokens, permitting an attacker to forge a token and gain unauthorized access to a user's account.

Another example: An API that uses weak or easily guessable passords, enabling attackers to perform brute-force attacks and gain unauthorized access to user accounts and sensitive data.

Broken Authentication

In a nutshell

Broken Authentication include any flaws related to the Authentication process.

- Stealing Oauth Tokens, flawed Oauth implementations
- Modifying JWT Tokens to gain access
- Rate Limiting issues -> Brute Forcing
- User enumeration / weak passwords
- Unauthenticated API endpoints

Thank You!

Ethical Hacking of RESTful & GraphQL API Training Course