wib

OWASP API5:

Broken Function - Level Authorization

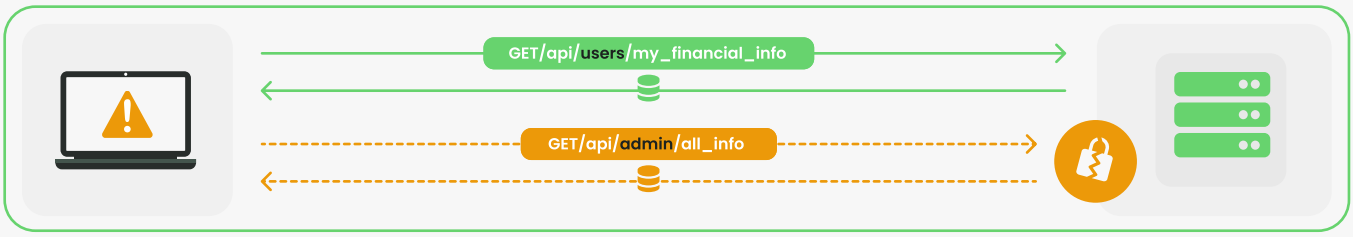
OWASP top 10

Authorization issues are frequently the consequence of misconfigured or incorrectly implemented authorization. Broken function-level authorization occurs when applications fail to limit sensitive functions to the authorized users. As a result, unauthorized users can inappropriately access sensitive or restricted capabilities. If an ordinary user can access admin capabilities on a site or if one user can alter another user's account, access controls that are absent or incorrect are often the culprit.

How Hackers Exploit It

Suppose a mobile application makes an API request to GET /api/invites/{invite_guid} during the registration process for an application that only permits invited users to join. The response includes information about the invitation, such as the user's job and email address.

An attacker can replicate the request and change the HTTP method and destination to POST /api/invites/new. Although only administrators should access this endpoint using the admin console, it does not implement function-level authorization checks.
The attacker takes advantage of the flaw and sends themself an invite to create an admin account:
POST /api/invites/new {"email":"jack@yahoo.com","role":"admin"}



Why You Should Care

Attackers can access sensitive resources, take over another user's account, create/delete accounts, or escalate privileges to achieve administrator access by exploiting broken function-level authorization flaws. Additionally, they may collect personally identifiable information (PII) and use it to compromise the organization or blackmail employees.

Traditional Tools Will Not Protect You

Traditional security controls like WAFs and API Gateways lack the context of API activity. They hence are unaware that the attacker in the above example should not be able to submit a POST request. They would treat this API call as valid and would bypass security measures. As threats become more complicated and sophisticated, these tools miss attacks that target the logic of APIs. WAFs and API Gateways occasionally support the exact matching of statically configured message filters. Still, these techniques can restrict or eliminate required business functionality, and most companies find it difficult to scale them.

How to Level Authorization Threats

All of your business operations should call on a uniform and easy-to-understand authorization module in your application. Protection is frequently supplied by one or more components outside of the application code.

1. Deny all access by default, with explicit permissions for particular roles required for access to every function
2. Examine your API endpoints for function-level authorization problems while keeping the application's business logic and group structure in mind
3. Ensure that all administrative controllers utilize an abstract administrative controller that performs authorization checks depending on the user's group/role.
4. Ensure that the administrative functions of a typical controller perform permission checks depending on the user's group and role

How Wib Can Help You

Wib is a full-lifecycle API security platform, defending against API security threats. The platform ensures comprehensive protection across the entire API software lifecycle from development to testing to production.

Wib utilizes state-of-the-art proprietary AI and ML to analyze millions of requests in real-time. It provides complete visibility of existing APIs, with actionable insights and comprehensive protection across the entire lifecycle. It learns your APIs inside and out and can provide complete visibility of your existing APIs, analyze their integrity, identify vulnerabilities, and detect attacks in real-time.

If you are building or using APIs in your applications (and you probably are), sign up for a demo to see Wib in action and learn more.