A5 - Broken Access Control

Exploitation of access control is a core skill of attackers. Source Code Analysis Tool (SAST) and Dynamic Application Security Testing (DAST) can detect the absence of access control but these tools cannot verify if it is functional when it is present. Due to lack of automated detection and the lack of effective functional testing made by developers, access control weaknesses are very common.

Attackers impersonate users using privileged functions by accessing, updating or deleting every record.

Medication

To prevent broken access control to happen, the developer should implement access control mechanisms once and use it again to implement the application. The web server directory listing should be disabled and to ensure that the file metadata has a backup. The admins should be inform every log access control failures. Developers and QA staff should include functional access control unit and integration tests.

Example

An attacker simply modifies the 'acct' parameter in the browser to send whatever account number they want. If not properly verified, the attacker can access any user's account.

Another example is when an attacker simply force browses to target URLs. Admin rights are required for access to the admin page. If an unauthenticated user can access either page, it’s a flaw. If a non-admin can access the admin page, this is a flaw.