Missing Function Level Access Control (A7)

Virtually all web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality.

Threat agent:

Anyone can send a request to web app. Question is, do they have access to private functions which are ment for registered users?

Attack Vector:

Simply URL changing. Access grant with URL - no check.

Security Weakness

Functions are not protected enough. Developers forget to include code check, if user is logged in, or do they have access. they assume that they have.

Detecting is easy. Hardest part is to get to know URLs and functions which there are available to attack.

Technical impacts

Unauthorized access to functions. Administrative functions are key targets.

Business impacts

Public reaction, reputation.

Am I Vulnerable to Forced Access?

Verify every application function. Try to use a proxy with a privileged role. Then revisit with less privileged role. Some proxies support this type of analysis.

Automated tools are unlikely to find these problems.

How do I Prevent Forced Access?

Audit should be done easily. Hardcoding is not an option!

Default should be access denial - if user has access -> then allow.

Example

SIS student schedule