Broken Access Control (Initial Post)

Broken Access Control is now in first place and rightly so in my opinion (Fig. 1).

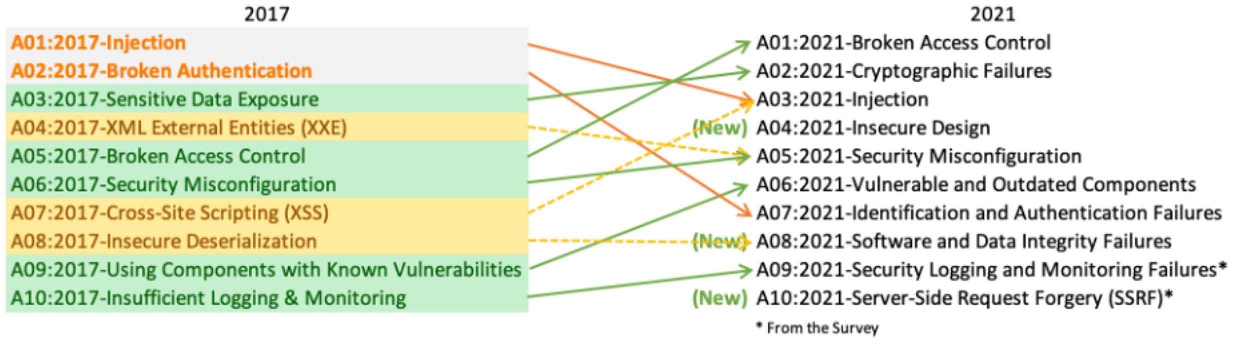
2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

Figure 1: What's changed in the Top 10 for 2021 (OWASP, 2021a)

Patchy access control is often a problem with applications that have grown in size over their version history. Instead of consciously designing access control schemes from the beginning, access control has been added and extended in an unstructured way over time. In cases where access control is not centralised but distributed in various places in the code, this often leads to poor manageability and complexity that is difficult to understand.

A particularly dangerous form of Broken Access Control are interfaces through which administrators can manage a site via the internet. Because of their power, these interfaces are often targets for attacks. All known servers and web application environments are vulnerable to this type of problem. Even if a site is completely static, it is vulnerable to attack unless properly configured (Köhntopp, 2021; OWASP, 2021b)

The following activity diagram demonstrate a simple example what for risks can be occured if an unauthorized person have either the administrator access or user access.

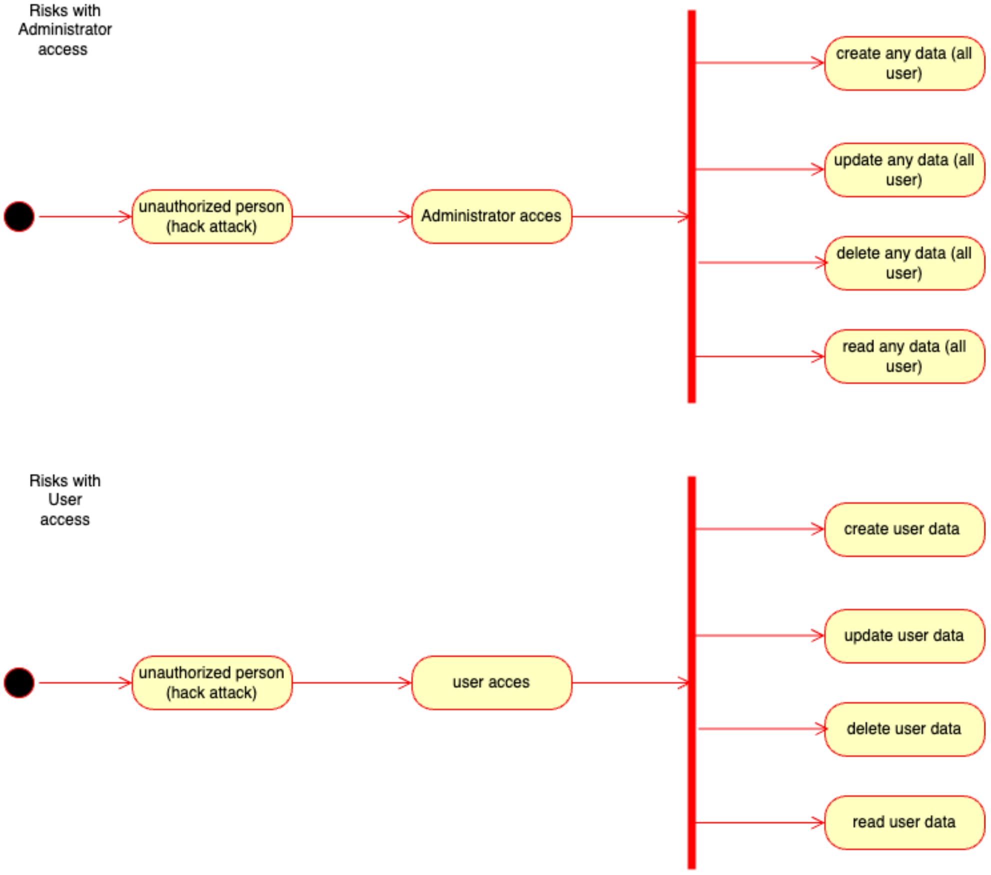
Risks with Administrator access
unauthorized person (hack attack)
Administrator acces
create any data (all user)
update any data (all user)
delete any data (all user)
read any data (all user)
Risks with User access
unauthorized person (hack attack)
user acces
create user data
update user data
delete user data
read user data

Figure 2: Activity diagram User vs Administrator Power

The worst case is if the unauthorised person steals and deletes the users' data. For example, with the help of administrator access, the hacker can manipulate all user data. On the contrary, the hacker can only manipulate one user's data with user access. Therefore developer must secure the administrator access at the very highest level.

Avoidance

Almost all sites have access control requirements. Therefore, an access control policy should be documented and policies enforced for implementation. Access control code should be well structured, modular and centralised. Penetration testing can help determine if broken access control issues exist. Specialists should check any remote administrative access interface particularly carefully to ensure that only authorised persons have access according to their different roles (Onlinesolutionsgroup, 2022).

References:

Köhntopp, K. (2021) A01:2021 - Broken Access Control. Available from: https://blog.koehntopp.info/2021/11/16/a01-2021-broken-access-control.html [Accessed 27 September 2022].

Onlinesolutionsgroup (2022) Broken Access Control. Available from: https://www.onlinesolutionsgroup.de/blog/glossar/b/broken-access-control/ [Accessed 27 September 2022].

OWASP (2021a) OWASP Top 10 - 2021. Available from: https://owasp.org/Top10/ [Accessed 27 September 2022].

OWASP (2021b) OWASP Top 10 - 2021. Available from: https://owasp.org/Top10/A01_2021-Broken_Access_Control/ [Accessed 27 September 2022].