

Access Control Brief Sheet

Built on the OWASP Top 10:2025, A01 Broken Access Control. Read at owasp.org and checked 2 August 2026.

Fill this in before anyone draws a screen. Access control is the one thing that cannot be retrofitted cheaply, because it spreads through the whole codebase as it is written.

Why This One First

OWASP puts Broken Access Control at number one in its 2025 list, and reports that 100% of the applications tested were found to have some form of it. That figure covers applications that were examined, not every application in existence, and it is still the strongest reason to settle these questions before the build rather than after it. The category carries 40 distinct mapped weakness types, an average incidence rate of 3.74%, and more than 1.8 million occurrences in the contributed data.

1. List The Things

Not screens. The things the software holds.

- ☐ List every type of record the system will store.
- ☐ For each one, write who creates it.
- ☐ For each one, write whose data it actually is.

If two people disagree about whose data a record is, stop and settle that first. Every later question depends on the answer.

2. Who Can See Each One

- ☐ For each record type, list the roles that may view it.
- ☐ Write down whether a role sees all records of that type, or only their own.
- ☐ Name the one role that can see everything, and who holds it.

The second question is the one that gets skipped. "A customer can view an order" and "a customer can view their own orders" are different systems, and the difference is invisible on a screen design.

3. Who Can Change Each One

- ☐ For each record type, list the roles that may create, edit and delete.
- ☐ Note anything that must never be deleted, only marked inactive.
- ☐ Note anything where a change must be attributable to a person afterwards.

4. What Happens When It Is Wrong

- ☐ How would we find out that someone saw something they should not have?
- ☐ Could we answer, after the fact, who viewed a given record and when?
- ☐ Who is told, and how quickly?

The Two Words That Are Not The Same

Authentication is proving who you are. **Authorisation** is what you are then allowed to do. A brief that says "users must log in" has specified the first and said nothing about the second, and the second is where A01 lives.

How To Use This With A Supplier

Hand over parts 1 to 4 filled in, and ask for the answers to be reflected back as a table of role against record type before design starts. If a supplier cannot produce that table from your brief, the brief was not specific enough, or they have not read it.

A quote priced per screen will not include this work, because it is not a screen. It is the part that decides what the software costs to own.