

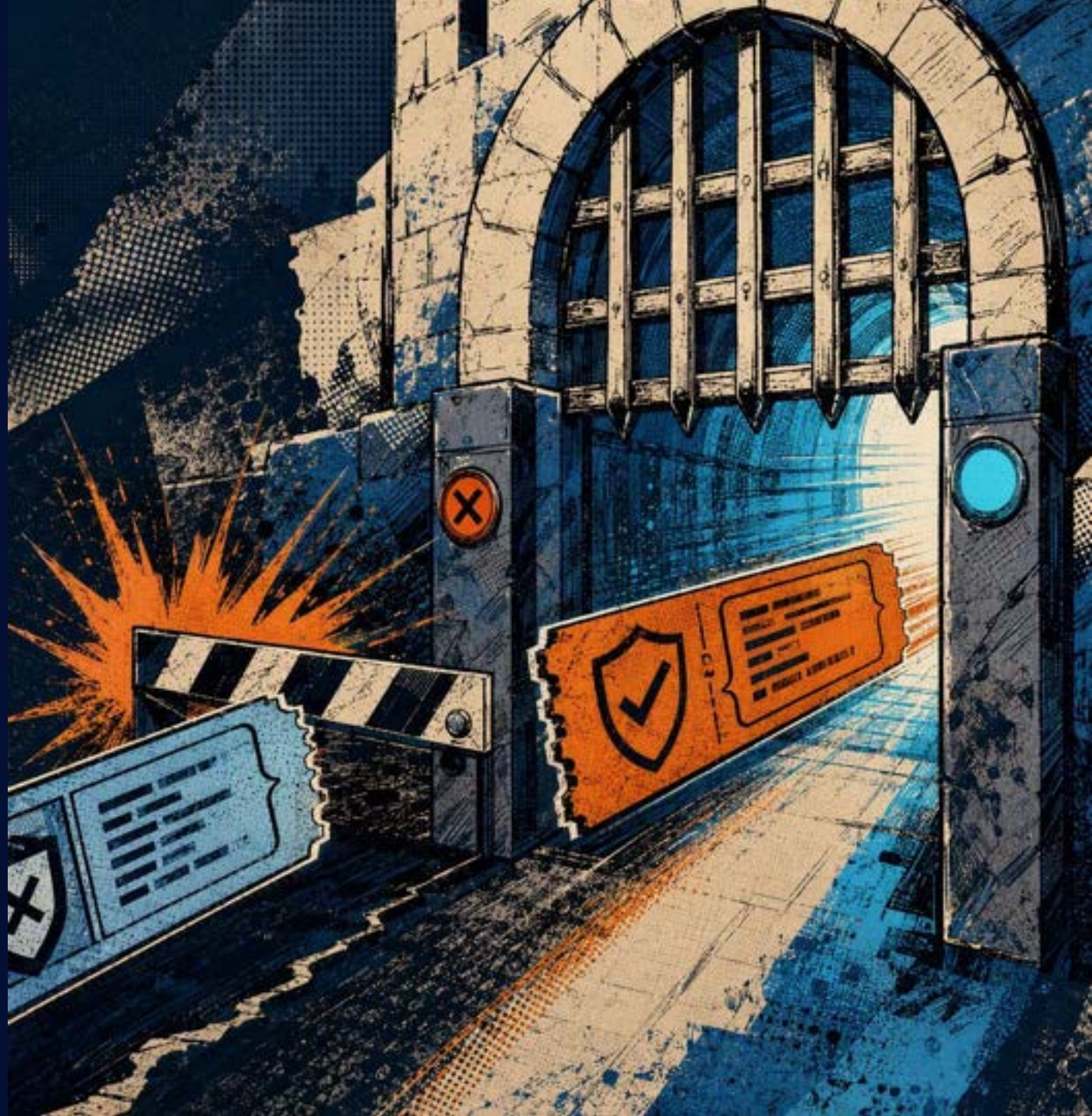
PREDICTABLE USERNAME + PASSWORD

Two credentials. One underlying value.

A code-review finding in a temporary-account workflow.

CLIENT CONFIDENTIALITY

Details are always altered to protect client confidentiality while technical substance is preserved.



THE SETUP

A temporary account was still a real account.

The platform created active temporary accounts for people who had not fully enrolled yet. Those accounts were usable for authentication, even though the workflow treated them as temporary scaffolding.

Temporary did not mean harmless.



THE OBVIOUS HALF

The “random” value was predictable.

The utility combined `microtime()`, MD5, `str_shuffle()`, and truncation to ten hexadecimal characters. The result looked random, but its inputs and generator were not cryptographically secure.

The first problem was weak randomness.



THE DISCOVERY

The same value played both roles.

One ten-character value was inserted into the temporary username. A known prefix plus that same value became the password. Learning or predicting one exposed the other.

The username and password were not independent.



THE DEEPER PROBLEM

A stronger RNG would not fully fix it.

Even if the generated value were unpredictable, the password would still be derivable from the username. A username exposed through logs, support, cache, or normal product behavior could reveal the credential. A stronger **RNG** would not remove the dependency.

The structural dependency survived an RNG fix.



THE PATTERN

One value supported two security roles.

A username identifies an account. A password authenticates it. When both come from the same source, the authentication layer only appears to have two independent factors.

Count independent values, not just fields.



MYTH: “Fix the randomness and we’re done.”

BUSTED. Use a cryptographically secure source, but also generate identifiers and authenticators independently. Treat temporary accounts and credentials as real security boundaries.

Independent controls require independent secrets.

WANT TO KNOW MORE?

[Read the full Field Note on the Anvil Secure blog →](#)

FIELD NOTES

FROM THE FORGE AT ANVIL SECURE

**Security findings, carefully examined.
Lessons built to travel beyond one
system.**