What are unsecured credentials?

Unsecured credentials are passwords, API keys, and tokens stored in plain, readable places rather than a secure vault: config files, scripts, environment variables, command history, CI/CD variables, cloud metadata, and infrastructure-as-code. After landing on a host, attackers simply search the filesystem for them, no dumping or cracking required. It is one of the most common and reliable ways to escalate or move laterally, which is why secrets management and scanning matter so much. It maps to MITRE T1552.

HOW IT WORKS

01 Where attackers look and payload

On any foothold, the attacker greps for secrets:

- Config and code: `grep -rinE "password|secret|api[_-]?key|token" /var/www /opt /home`
- History and env: `cat ~/.bash_history`, `env`, `cat ~/.aws/credentials`, `~/.ssh/`
- Cloud metadata (from a server): query the instance metadata endpoint for temporary cloud keys.
- CI/CD and IaC: pipeline variables, `.env-`, Terraform state, Kubernetes manifests.

Whatever turns up is used directly, no cracking. Documented for defensive context.

> NO CRYPTOGRAPHY TO BEAT
>
> *Unsecured credentials need no dumping or cracking, just `grep`. That makes them one of the highest-return, lowest-effort wins for an attacker, and one of the most preventable.*

HOW TO DEFEND

- Use a secrets manager / vault and inject secrets at runtime, never hardcode them in code, configs, or images.
- Scan repositories, images, and pipelines for secrets in CI and pre-commit.
- Use short-lived, scoped credentials (cloud roles, workload identity) so any leaked secret expires fast.
- Protect cloud metadata (enforce IMDSv2, restrict access) so server-side requests cannot harvest keys.
- Rotate exposed secrets immediately and audit history/env for leftovers.

SOURCES

[1] MITRE ATT&CK: Unsecured Credentials (T1552)

[2] MITRE ATT&CK: Credential Access (TA0006)

[3] NIST SP 800-63B Digital Identity Guidelines

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-are-unsecured-credentials

Open online