

Beware of Traps!

Honey token

A Honey token can take a variety of forms: file, URL, API key, environment variable, or any login information.

A Honey token is a piece of information that will not be used by legitimate users but is likely to be used by hackers. When an attacker interacts with this token, an alert is triggered to inform security administrators that suspicious activity has taken place.

For instance:

Security administrators of a web service place fake credentials in their database. When an attacker tries those credentials in the web service, the authentication page detects the usage of a honeypot which raises an alarm. Security administrators are now aware that the database has probably leaked.

How to detect a honey token

Detecting a honeypot is not an easy task. Therefore, in the context of CTF, Honeypot has been made less stealthy to help players to find the traps.

Some honeypots have clear identification to help security administrators distinguish honeypots and real pieces of information. Honeypot may be obvious.

`{id: root, password: hon3yPassword!}` is an obvious honeypot

Some honeypots may not work at all. In this context, the attacker won't have any impact on the service because the honeypot exists but has no interaction with the real system.

ID and password may not work but raise an alarm when tried to authenticate in a service

Some honeypot may lead to services that strangely behave. These are advanced honeypot as attackers may not notice they have been detected. The main goal of these tokens is to help security administrators to capture more activity linked to the honeypot and so, to the attacker.

New processes or scripts are executed when a resource is accessed. The attacker will still be able to read the resource or a part of it while they think they remain undetected.

Honeypot may bring the attacker in a copy of the service.

Some honeypot may provide security to bring attackers in a honeypot.

No multifactor-authentication or simple password on a specific account or service.