Security Scanning

What is scanned, what it looks for, and what to do about a finding

What this service does

Every PHP file in your hosting account is read on a schedule and checked against a set of malware and webshell signatures. Anything matching is reported so you can look at it.

Targets are re-scanned when the last scan is more than seven days old.

What it looks for

These are the patterns that show up in real compromises, not theoretical ones:

- eval() wrapping a decoder such as base64_decode or gzinflate, which is how injected code hides itself.
- assert() executing request input directly.
- preg_replace() using the old /e modifier, which executes what it matches.
- The names of well-known webshells.
- system() or passthru() running request input, which is a remote command shell in one line.

False positives are expected

The signatures are deliberately broad. A scanner tuned to never flag legitimate code will also miss real compromises, and missing one is far more expensive than checking a file that turns out to be fine.

So a finding means look at this file, not this file is malicious. Minified libraries and some caching code legitimately trip these patterns.

If something is found

- Do not simply delete the file. Look at when it changed and what else changed at the same time.
- Update everything: the application, its plugins, its themes. Most compromises arrive through an out-of-date plugin rather than through the server.
- Change the control panel, database and application admin passwords. Assume anything the account could reach was readable.
- Restore from a backup taken before the change, then patch before putting it back online.

Open a ticket if you would rather we walked through it with you.

What it does not do

It reads and reports. It does not quarantine, modify or delete anything on your account, because a scanner that edits files unattended can take a working site down over a false positive.

It scans PHP files in the hosting account. It is not a network intrusion detector and it does not scan a server you administer yourself.

HostCommerceAI - questions about anything in this guide are worth a support ticket. This document describes the service as it works today; if something here does not match what you are seeing, tell us, because one of the two is wrong.