HSTS

The question

Browsers remember HSTS

An HTTPS response can tell browsers to keep using HTTPS for a specified lifetime. Reliable HTTPS must come first.

01 Understand

02 Observe

03 Verify

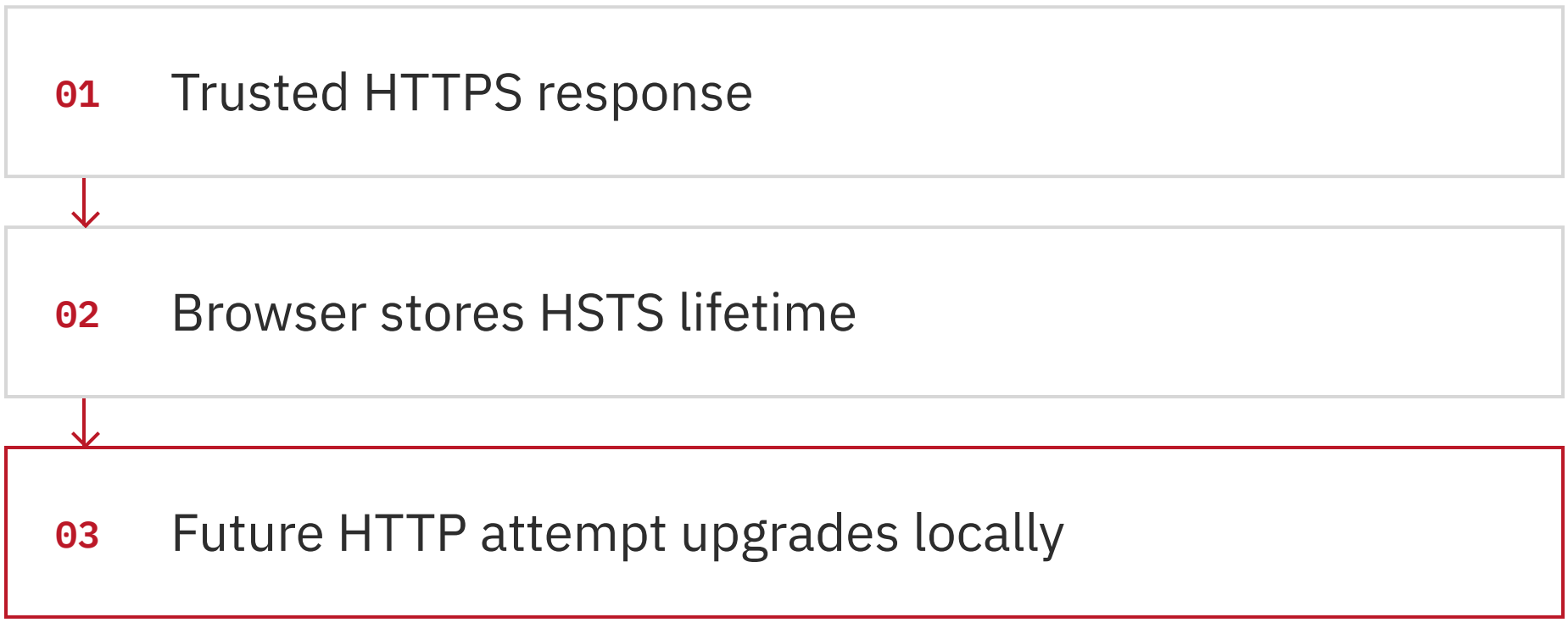
A practical briefing for the people who own your domain.

HSTS

The mechanism

The upgrade happens locally

Once learned, the policy upgrades future HTTP attempts before sending them. A first visit may still need to discover it.



The normal policy is learned over HTTPS. The scanner observes the header, not each browser's remembered state.

HSTS

The evidence

We check the observed lifetime

> Our baseline reads max-age on the final trusted HTTPS response. It does not verify preload lists or subdomain readiness.

PUT THE OBSERVATION IN CONTEXT

- **Public signal**
- **Service context**
- **Operational validation**

Use the finding to start an owned review.

HSTS

The handoff

Roll out with a recovery plan

Verify certificate renewal and critical journeys. Review every affected service before adding subdomain coverage or considering preload.

BRING THE RIGHT OWNERS TOGETHER

01 Web platform owner

02 Domain and application service owners

HSTS

Your checklist

Use the HSTS decision checklist

- ✓ Confirm HTTPS reliability
- ✓ Name the owner
- ✓ Review lifetime and scope
- ✓ Document recovery

> Read the full explainer before widening the commitment.
>
> **/learn/hsts**