HSTS

Inhaltsverzeichnis

HSTS weist Browser an, eine Website künftig ausschließlich per HTTPS aufzurufen. Dadurch werden Downgrade-Angriffe und versehentliche unsichere HTTP-Aufrufe reduziert.

HTTP Strict Transport Security, kurz HSTS, ist ein Sicherheitsmechanismus für HTTPS-Websites. Ein Server sendet einen Header, der Browser dazu verpflichtet, die Domain für einen bestimmten Zeitraum nur noch verschlüsselt aufzurufen.

1 Funktionsweise

Nach dem ersten erfolgreichen HTTPS-Aufruf speichert der Browser die HSTS-Regel lokal.

- **max-age:** Dauer der Regel in Sekunden.
- **includeSubDomains:** gilt auch für Subdomains.
- **preload:** Aufnahme in Browser-Vorladelisten möglich.

2 Vorteile

HSTS erhöht die Sicherheit, weil HTTP-Aufrufe automatisch auf HTTPS umgestellt werden.

- Schutz vor SSL-Stripping.
- Weniger Risiko durch alte HTTP-Links.
- Klare Durchsetzung verschlüsselter Verbindungen.

3 Risiken

Eine falsche HSTS-Konfiguration kann den Zugriff erschweren, wenn HTTPS nicht sauber funktioniert.

- Zertifikate müssen zuverlässig erneuert werden.
- Subdomains vor includeSubDomains prüfen.
- Preload nur mit stabiler HTTPS-Infrastruktur nutzen.

4 Fazit

HSTS ist eine starke Sicherheitsmaßnahme, sollte aber erst aktiviert werden, wenn HTTPS dauerhaft und vollständig korrekt eingerichtet ist.