AYI NEDJIMI Consultants

# Web Cache Poisoning & Deception : Guide d'Ex

18 April 2026 • Mis à jour le 18 April 2026 • 48 min de lecture •

> Guide expert Web Cache Poisoning et Cache Deception : techniques d'exp
> WCVS), cas réels PayPal/GitHub, défense CDN.

Le web cache poisoning et le web cache deception constituent deux familles d'att
mécanismes de mise en cache déployés massivement sur Internet. Alors que les C
cache accélèrent la distribution de contenu pour des milliards d'utilisateurs, ces m
des vecteurs d'attaque lorsque leurs configurations présentent des failles. L'empo
attaquant d'injecter du contenu malveillant dans une réponse mise en cache, affec
utilisateurs qui accèdent ensuite à cette ressource. La tromperie de cache, quant a
cache des données sensibles d'un utilisateur authentifié, permettant à l'attaquant
Ces vulnérabilités, popularisées par les recherches de James Kettle chez PortSwig
PayPal, GitHub et de nombreuses plateformes protégées par Cloudflare ou Akama
aujourd'hui indispensable pour tout professionnel de la cybersécurité offensive ou

**Fonctionnement du cache web : fondations techniques**

Avant d'aborder les attaques, il est essentiel de comprendre en profondeur comm
cache HTTP est un mécanisme de stockage intermédiaire qui conserve des copie
directement aux requêtes ultérieures identiques, sans solliciter le serveur d'origine
latence, la bande passante consommée et la charge serveur. Les caches se déplo
navigateur (privé), cache de proxy direct, reverse proxy cache (Varnish, Nginx, HA
Network) comme Cloudflare, Akamai, Fastly ou AWS CloudFront.

## Cache keys et identification des requêtes

Le concept central du caching HTTP est la **cache key** (clé de cache). Elle détermi
considérées comme « identiques » et peuvent recevoir la même réponse mise en
composée de la méthode HTTP, de l'hôte (header `Host`), du chemin (path) et de
requête — headers additionnels, cookies, corps de la requête — est généralement
éléments exclus sont appelés **unkeyed inputs**, et c'est précisément là que réside l
poisoning.

Prenons un exemple concret. Les deux requêtes suivantes ont la même cache key
le host, le path et la query string :

```
GET /page?lang=fr HTTP/1.1
Host: example.com
X-Forwarded-Host: evil.com
Cookie: session=abc123

GET /page?lang=fr HTTP/1.1
Host: example.com
```