# Cache poisoning attack

*Cache Server: is a dedicated network server or service acting as a server that saves web pages or other Content locally by placing previously requested information in temporary Storage or cache a cache server both speeds up access to data and reduces demand on an enter prise bandwidth.*

*بمعنى أن بيقلل فكرة اليوزر بطلب نفس الملف لأكثر من مرة فبعمله server load balancer و ده له أكتر من configuration لو مثلًا ملف js أو css أو أي ملف أكبر من 1 mega مثلًا و ممكن حتى أعمله caching لوقت معين خوف من انه يكون الملف اتغير .*

*Note : لو عندي يوزر طلب ملف حصل له كاش و طلبه تاني ايه اللي يعرف السيرفر ان ده نفس اليوزر ده بيتم من خلال ال key و ال key ممكن يكون :*

***1/ user agent .***

***2/ host headers.***

***3/ id.***

## *Cache poisoning :*

*Cache poisoning is a type of attack in which corrupt data is inserted into the cache database of the Domain Name System (DNS) name server. The Domain Name System is a system that associates domain names with IP addresses. Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses. In a DNS cache poisoning attack, a malicious party sends forged responses from an imposter DNS in order to reroute a domain name to a new IP address. This new IP address is almost always for a server that is controlled by the attacker. DNS cache poisoning attacks are often used to spread computer worms and other malware. More sophisticated uses for DNS cache poisoning include man-in-the-middle attacks and denial-of-service attacks.*

بمعنى هو مثلًا لو غيرت ال host مثلًا ل evil.com بس الموقع ده مش عليه حاجة فهو هيروح يجيبها و يعرض حاجة فاضية لكن لو كررت ارسال الموقع ده مثلًا مليون مرة فهو هيعمل حاجة اسمها cochinge معناها انه هيخزنه عنده و يبعته لأي يوزر جاي ال Cache poisoning بيحصل ايه بقا لو أنا مثلاً حطيت xss payload و بعته مليون مرة بالتالي هيخزنه عنده و يبعته لأي يوزر و بقت stored xss .

~~ مبدئيًا xss payload هو self يعني خاص بيا أنا بس لكن لو الموقع مصاب ب Cache poisoning أقدر أحول self xss إلى store or reflected .

https://github.com/search?q=cache+poisoning+writeups&type=Code