**Cache Poisoning**

**other names: Http cache poisoning, Web cache poisoning, DNS cache poisoning and even DNS spoofing**

**Description 1**

Cache Poisoning is an attack that seeks to introduce false or malicious data into a web cache, normally via HTTP Response Splitting. The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a response is cached in a shared web cache, such as those commonly found in proxy servers, then all users of that cache will continue to receive the malicious content until the cache entry is purged. Similarly, **if the response is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is purged,** although only the user of the local browser instance will be affected. [1] (for an example you can watch [2]) To successfully carry out such an attack, an attacker:

* Finds the vulnerable service code, which allows them to fill the HTTP header field with many headers.
* Forces the cache server to flush its actual cache content, which we want to be cached by the servers.
* Sends a specially crafted request, which will be stored in cache.
* Sends the next request. The previously injected content stored in cache will be the response to this request.

**Description 2**

**other names: Http Cache Poisoning , Web Cache Poisoning**

A Web cache (or more precisely, an HTTP cache) typically caches the content of URLs, keyed by the URLs. It can be implemented as an intermediate HTTP proxy server (or as part of the Web client (most modern browsers have a built in Web cache component). Note that the browser caches can also cache HTTPS URLs and content, since they can be implemented such that they access the HTTP requests before SSL encryption and HTTP responses after SSL decryption.

Web Cache Poisoning (Http Cache Poisoning) is an attack against the integrity of an intermediate Web cache repository, in which genuine content cached for an arbitrary URL is replaced with spoofed content. **Users of the Web cache repository will thus consume spoofed content instead of a genuine one when requesting this URL through the Web cache. [2]**

**Description 3**

**other names: DNS cache poisoning, DNS spoofing**

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 i**n 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. [3] [4]**

**Reference**

**[1]** [**https://www.owasp.org/index.php/Category:Attack**](https://www.owasp.org/index.php/Category:Attack)

**[2]** Klein, Amit. "Web cache poisoning attacks." *Encyclopedia of Cryptography and Security*. Springer US, 2011. 1373-1373.

**[3]** <https://www.veracode.com/security/cache-poisoning>

**[4]** https://en.wikipedia.org/wiki/DNS\_spoofing