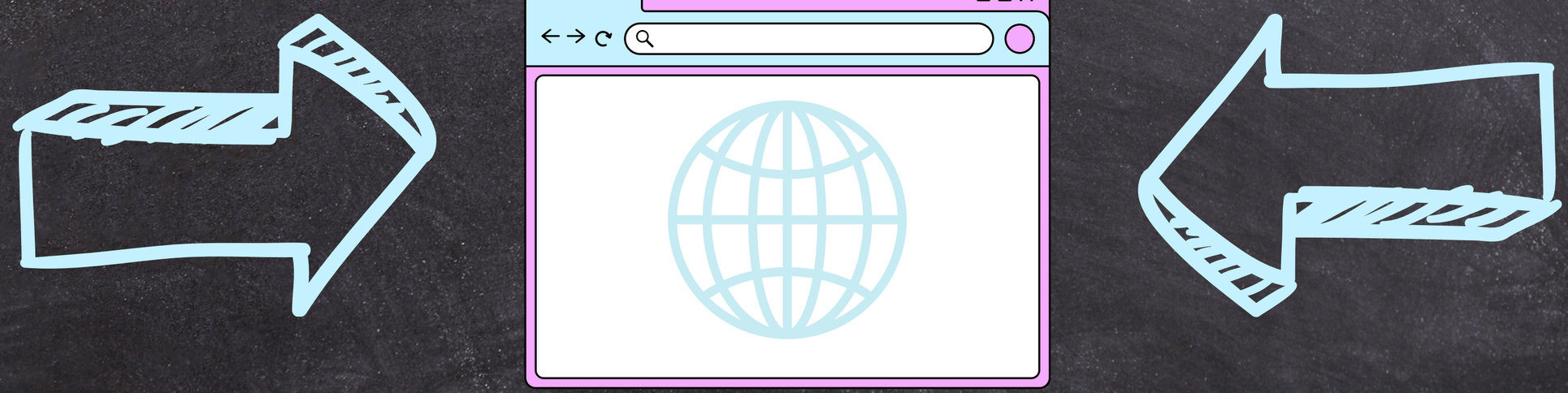
Web Cache Deception



WILLIAM HOLLAND

CSEC 302

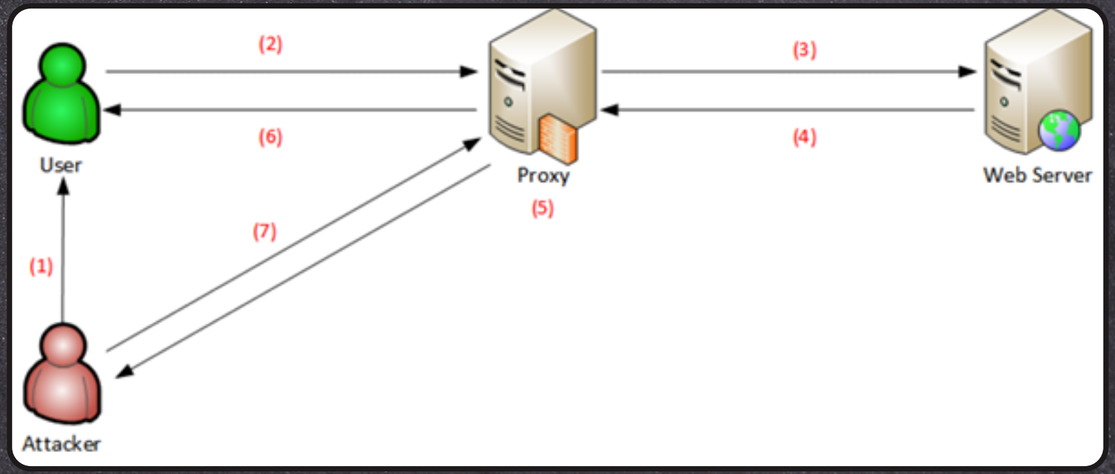
WHAT IS WCD?

Web Cache Deception (WCD) is a security vulnerability that arises when an attacker tricks a web cache into storing and serving sensitive information that is typically user-specific.

Oftentimes, an attacker manipulates the URL or parameters of a web request in such a way that the cache is deceived into storing the response for one user and serving it to another, which could result in a user gaining unauthorized access to sensitive information belonging to another user.

METHODOLOGY

- The attacker lures a logged-on user to access the victim's browser requests.
- The request arrives at the proxy, which is not familiar with this file, and asks the web server.
- The web server returns the content of the victim's account page with a 200 OK response, meaning the URL stays the same.
- The caching mechanism receives the file and identifies that the URL ends with a static extension.
- Since its configured to cache all static files and disregard catching headers, the imposter's file is cached.
- The user receives his account page.
- The attacker can access the file without any admin or raised priveliges, after the request arrives to the proxy and then returned the victim's cached account page to the attacker's browser.



SOLUTION

The solution to this vulnerability can vary, but often times the easiest solution is implementing a fixed route that can prevent an attacker being able to access exposed pages.