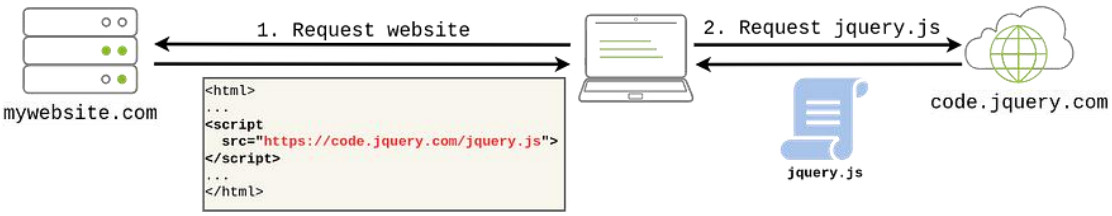
Task 19 : Software Integrity Failures

Software Integrity Failures

Suppose you have a website that uses third-party libraries that are stored in some external servers that are out of your control. While this may sound a bit strange, this is actually a somewhat common practice. Take as an example jQuery, a commonly used javascript library. If you want, you can include jQuery in your website directly from their servers without actually downloading it by including the following line in the HTML code of your website:

```
<script src="https://code.jquery.com/jquery-3.6.1.min.js"></script>
```

When a user navigates to your website, its browser will read its HTML code and download jQuery from the specified external source.



The problem is that if an attacker somehow hacks into the jQuery official repository, they could change the contents of https://code.jquery.com/jquery-3.6.1.min.js to inject malicious code. As a result, anyone visiting your website would now pull the malicious code and execute it into their browsers unknowingly. This is a software integrity failure as your website makes no checks against the third-party library to see if it has changed. Modern browsers allow you to specify a hash along the library's URL so that the library code is executed only if the hash of the downloaded file matches the expected value. This security mechanism is called Subresource Integrity (SRI), and you can read more about it here.

The correct way to insert the library in your HTML code would be to use SRI and include an integrity hash so that if somehow an attacker is able to modify

the library, any client navigating through your website won't execute the modified version. Here's how that should look in HTML:

```
<script src="https://code.jquery.com/jquery-3.6.1.min.js" integrity="sha256-o88AwQnZB+VDvE9tvIXrMQaPlFFSUTR+nldQm1LuPXQ="
crossorigin="anonymous"></script>
```

You can go to https://www.srihash.org/ to generate hashes for any library if needed.

Answer the questions below :

1. What is the SHA-256 hash of https://code.jquery.com/jquery-1.12.4.min.js?
A. sha256-ZosEbRLbNQzLpnKIkEdrPv7lOy9C27hHQ+Xp8a4MxAQ=