CSP Demo

Security questions

1. what is the meaning of data in `<script src="data:;base64,YWxlcnQoZG9jdW1lbnQuZG9tYWluKQ=="></script>`

With data: it's possible to set the data inline, instead as a location like https://.../script.js. Because of the base64 encoding, its possible to decode the content is `alert(document.domain)`

2. what is the difference between hash and nonce

- `<script nonce="ABC">alert(document.cookie)</script>`
- `<img onerror=alert("HASH") src=x>`

Nonce: This is applied to a script tag and don't guarantee that the content between the tags is manipulated. it's only purpose is to allow the execution of a script tag.

Hash: By hashing the executed part it's guarantee that there is no manipulation in the code. For the execution of the `<img onerror=alert("HASH") src=x>` it's necessary to add unsafe-hashes in the CSP.

1. explain the following csp script-src 'unsafe-hashes' 'self' 'sha256-bnQkgwAfjTxnZSlFxZe1ogJadBHLnRuuL54WC+v+tMY='

Only script from the same domain and port are allowed, the script has to match the sha256 hash and are allows inline ex. `<button onclick=open() >`