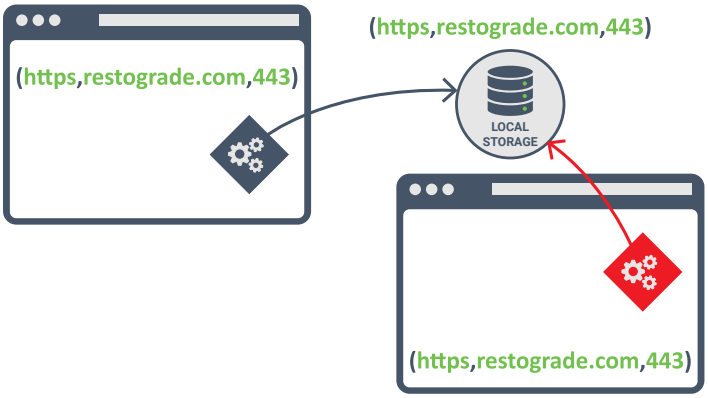
SECURE DATA STORAGE IN THE BROWSER

Secure data storage in a browser is quite a challenge. This cheat sheet explores the security properties of data storage mechanisms in the browser. It offers origin-based isolation as an alternative over the use of *localStorage* or *sessionStorage*. The cheat sheet also covers how to encrypt data for online or offline use. Also check out the code examples and live demo.

STORING DATA IN LOCALSTORAGE

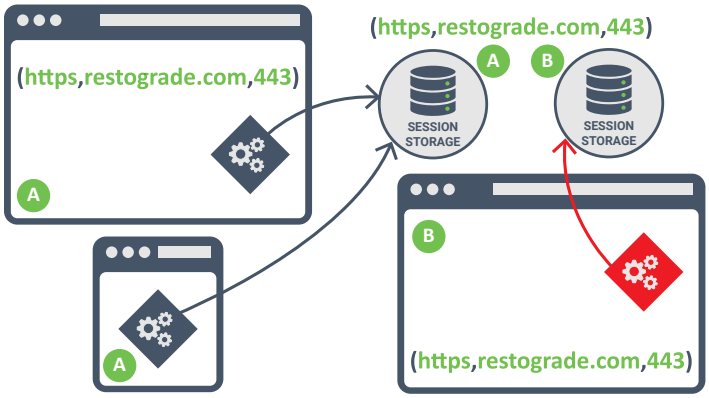
LocalStorage is the most widely used browser storage mechanism. It offers key/value-based storage. By design, *localStorage* is accessible to the entire origin.



- ✓ *localStorage* offers easily accessible long-term storage
- ✗ All script code running within the origin can access the data
- ✗ Legitimate code has no exclusive control over the data
- ✗ Data is stored in plaintext on the file system

STORING DATA IN SESSIONSTORAGE

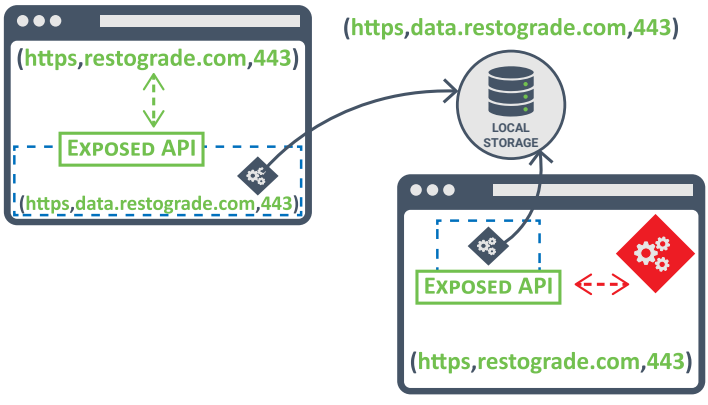
SessionStorage is part of the same API as *localStorage* and also offers key/value-based storage. *SessionStorage* is associated with an origin **and** a set of browsing contexts.



- ✓ *sessionStorage* offers easily accessible short-term storage
- ✓ Data access is limited to code running in related contexts
- ✗ Legitimate code has no exclusive control over the data
- ✗ Data is stored in plaintext on the file system

ORIGIN-ISOLATED DATA STORAGE

The origin-isolated storage pattern offers a way to keep data out of reach of malicious code. The attack surface is reduced from raw data access to abuse of an exposed API.

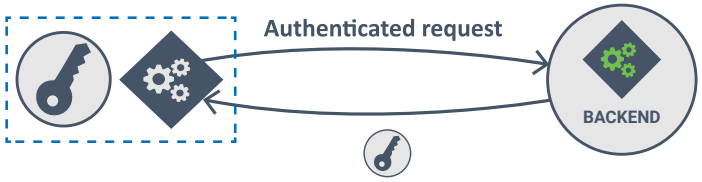


- ✓ Origin-based isolation is suited for storing sensitive data
- ✓ The API can enforce origin-based access control
- ✓ The absence of third-party code ensures full control
- ✗ Data is stored in plaintext on the file system

ENCRYPTED DATA STORAGE

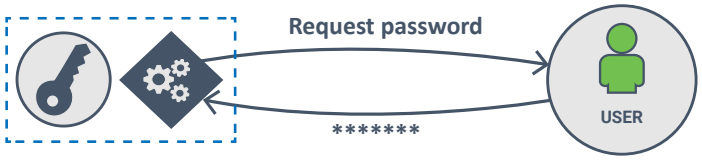
The *WebCrypto API* allows clients to encrypt and decrypt data before storing it. Doing so is the only way to prevent data theft through the device's file system.

ENCRYPTED DATA WITH ONLINE ACCES



- ✓ Data is stored encrypted on the file system
- The key is retrieved from a server-provided endpoint

ENCRYPTED DATA WITH OFFLINE ACCES



- ✓ Data is stored encrypted on the file system
- The key is derived from a user-provided password

Code and live demo available at https://browsersecrets.restograde.com/