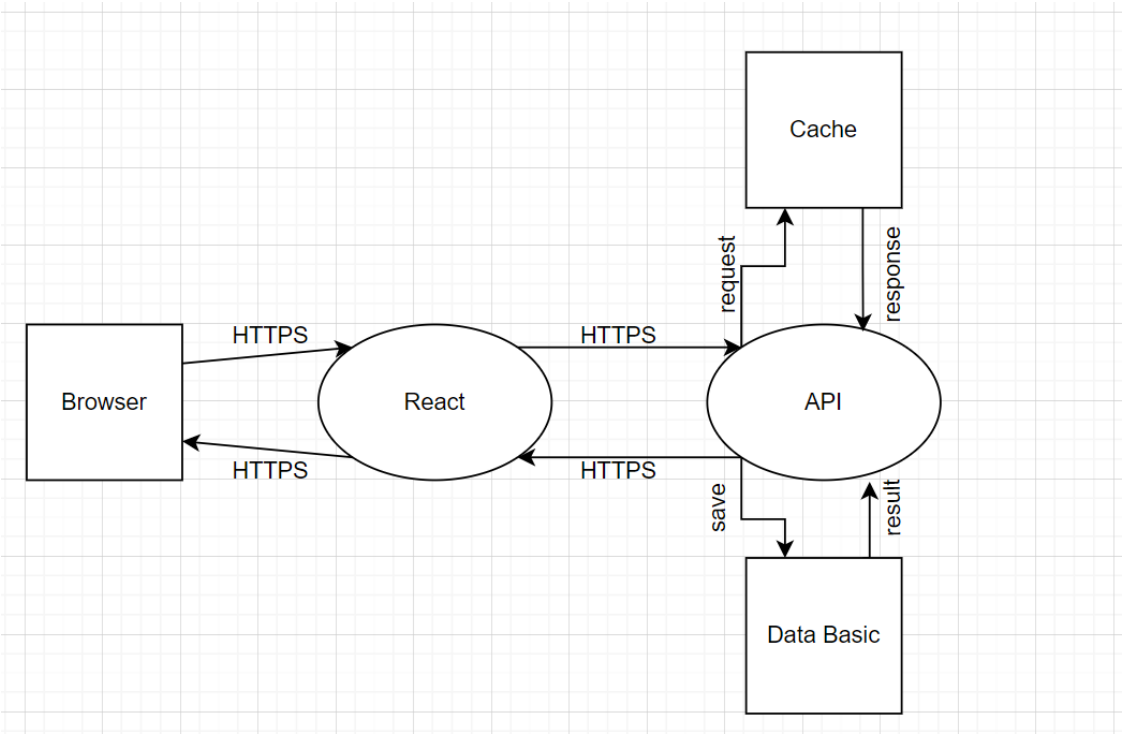
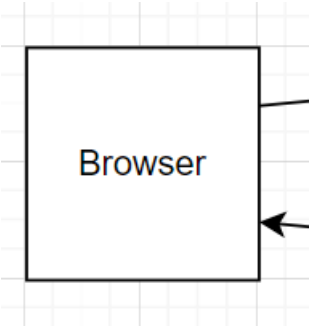
Security model

Threat model

Diagram

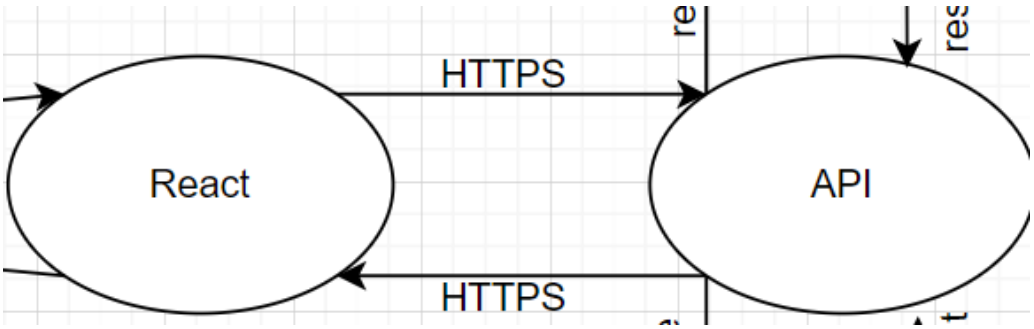


Interaction: in-browser manipulation



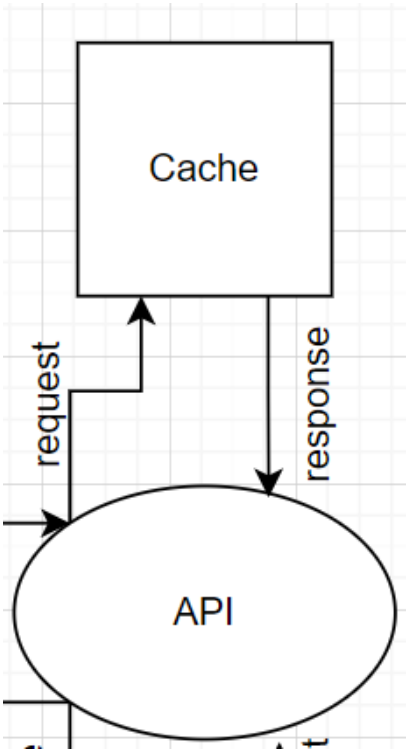
Category	Description	Control category	Effort
Spoofing	An adversary can steal application and service code on the client side.	Technology	High
DDOS	An adversary can spam system with account creation	Technology	Medium

Interaction: HTTPS



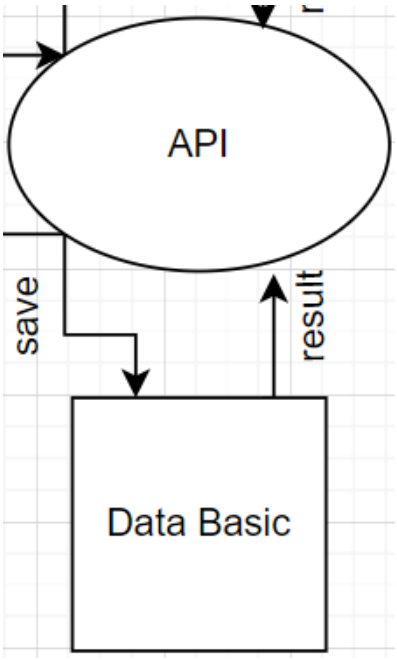
Category	Description	Control category	Effort
Spoofing	An adversary can steal data using man-in-the-middle-attack.	Data	High
Denial of service	An adversary may block access to the application or API hosted on React through a denial of service attack.	Technology	Medium

Interaction: Request/Response



Category	Description	Control category	Effort
Denial of service	An adversary may block access to the application or API hosted on API through a denial of service attack.	Technology	High
Denial of service	An adversary may assessing functionality of Cache API and change books information	Data	High

Interaction: Save



Category	Description	Control category	Effort
Elevation Of Privilege	An adversary may directly connect to DB from anywhere	Data	Medium
Elevation Of Privilege	If there is no restriction at network or host firewall level, to access the database then anyone can attempt to connect to the database from an unauthorized location	Data	Medium

Elevation Of Privilege	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.	Data	High
Elevation Of Privilege	An adversary may read unauthorized content stored in DB	Data	Low

Migitation plan of potential risks

Risk	Solution
user data stealing (password, login, email)	provide access to db only for privileged accounts with admin rights
user account stealing(weak password)	ensure that user create strong password or generate it instead
account spamming	allow to create account only using gmail or phone number, or create strong verification during long time to avoid temporary mails accounts creating
sql injection and cross site scripting	not to use outdated components and 3rd sides libraries; provide additional penetration testing
DDOS	block ip addresses or add request timer with available amount of requests
code stealing	prevent using open source platform and use private repositories/ obfuscate client code
data spoofing	using https protocol instead of http