Errori frequenti nel progetto d'esame
Applicazioni Web I, a.a. 2021/22

Consigli alla luce dell'esperienza degli esami degli anni passati
v. 2.1

(nota: le modifiche rispetto alla v.2.0 sono riportare in rosso per comodità)

Nota: l'elaborato può essere consegnato in qualsiasi condizione indipendentemente dal soddisfacimento dei punti descritti nel seguito, che non sono una condizione necessaria per arrivare alla sufficienza (ad eccezione della corretta modalità di consegna). In generale, però, soddisfare i punti dovrebbe garantire, in generale, una valutazione buona perché tipicamente si evitano i problemi di maggior gravità.

PROBLEMI DI LOGICA DELL'APPLICAZIONE che in generale portano a perdite di punti

- NON si devono creare ID sul client quando devono essere identificativi (chiavi uniche) nel DB: gli ID DEVONO essere creati dal server, e poi restituiti al client.
- Per gli ID da generare alla creazione di un nuovo elemento unico, usare di preferenza il meccanismo fornito dal DB (es. colonna auto-increment). Altre soluzioni sono in generale sbagliate e portano alla perdita di punti (creazione/calcolo sul client, calcolo del max sulla colonna del DB ecc.). Si ricordi che l'applicazione è utilizzabile da più utenti contemporaneamente, che possono anche non lavorare sugli stessi dati, ma l'unicità dell'ID deve essere garantita. Inoltre, l'ID generato dal DB è, in generale, non direttamente selezionabile o manipolabile dall'utente, quindi il suo valore non dovrebbe influenzare la logica dell'applicazione o essere visualizzato esplicitamente nell'interfaccia dell'applicazione.
- Usare sempre il metodo corretto nello scrivere e chiamare le API HTTP (es. mai POST al posto di GET, e viceversa)
- E' necessario verificare sempre, lato server, i ruoli/permessi di coloro che scrivono informazioni nel DB (aggiunte, modifiche, ecc...): non basta l'autenticazione iniziale, ma bisogna verificare che l'utente/utilizzatore abbia il permesso di fare la cosa (per es. con un'aggiunta di condizione su una query oppure una apposita query addizionale su db).
- Chi non pone attenzione all'autenticazione almeno di base sul server non potrà ottenere il massimo del punteggio, in particolare chi confonde la verifica lato client con quella lato server, che è errore grave. Chi afferma: "sul client ho controllato che non si possa fare l'azione X..." non ha compreso la problematica, e non potrà avere il massimo. La verifica della correttezza dei valori e della possibilità di svolgere determinate operazioni solo lato client è concettualmente sbagliata, come chiarito a lezione, ed è uno dei motivi per cui esistono così tanti problemi di sicurezza nelle applicazioni web che ci circondano. Sarà quindi fortemente penalizzata all'esame.
- EVITARE di scrivere regular expressions (regex) per informazioni/dati che sono facilmente gestibili da una libreria: si perde tempo, è molto probabile sbagliarsi, e all'esame spesso si testa un caso non considerato. Esempio: verifica correttezza email o data. Un programmatore non deve passare il suo tempo a scrivere regex per considerare anni bisestili e altre particolarità, deve usare una libreria (ragionevolmente affidabile), far convertire e trasferire le date in qualche formato standard se serve (es. formato stringa ISO).
- NON scrivere un unico componente enorme con la logica di quasi tutta l'applicazione: illeggibile, ingestibile, e quasi sicuramente con errori (es. dipendenze useEffect difficili da

gestire ecc.)

- NON inventarsi cose in più non richieste, in particolare se divergono dal testo trascurandone anche solo una parte. Se per esempio si chiede di aggiungere un nuovo corso specificando (nome, codice, crediti), prendere un corso da una lista predefinita è sbagliato: se lo scelgo da una lista predefinita NON posso aggiungere il nome che voglio, e in più non implemento (cioè mi semplifico indebitamente il progetto) una parte di controlli sul form che definisce il corso, per es. che il numero di crediti sia un numero, e maggiore di 0.
- NON inventarsi formati di dati strani per il trasferimento compatto delle informazioni da client a server e viceversa (es. separando i campi manualmente con virgole o altri simboli speciali, e tra l'altro dovendo poi gestire con pezzi di codice aggiuntivo questi casi). In generale, i campi di testo di un form (titoli, testi, ecc.) devono poter supportare spazi, punti e virgola, virgole e simboli vari. Dove abiti? Ad Ascoli Piceno (nome con spazio). A Mondovi' (con l'accento), e così via. Usare il JSON per serializzare/deserializzare informazioni contenute nelle stringhe Javascript, come viene spiegato nel corso.
- Evitare di usare useEffect se non serve effettivamente. Per esempio: evitare di usarla per reagire al cambiamento di un valore di un campo di un form. Se il form è di tipo controlled, l'handler può gestire la cosa. Molte useEffect nel codice, in particolare per casi facilmente gestibili diversamente, rendono i componenti difficili da capire, gestire, modificare. Invece, usare useEffect in tutti i casi in cui è effettivamente necessaria (caricamento asincrono di dati ecc.). Evitare di usare useEffect con dipendenza su location o history per gestire il cambiamento di pagina quando la paginazione è stata implementata tramite un Router.
- Se non è esplicitamente richiesto qualcosa di diverso, le operazioni che lavorano sul DB a seguito della chiamata di una API possono include più query eseguite separatamente (ossia non in una transazione, che è complicata e difficile da implementare in sqlite3, quindi non è richiesta per il corso di Applicazioni Web I). Si assume per semplicità che tra una query e l'altra durante l'esecuzione del codice che corrisponde ad una API del server non avvengano modifiche al DB.
- Analogamente a prima, una operazione atomica a livello logico deve essere realizzata all'interno di un'unica API. Il classico caso è la creazione/modifica/cancellazione di una informazione complessa che richiede più operazioni lato server (es. query). Per esempio, creazione/modifica/cancellazione di un questionario con tutte le sue domande, di un piano di studi con i relativi corsi, utente con tutte le risorse ad esso collegate, ecc. E' gravemente errato effettuare più chiamate dal client verso le API del server per realizzare un'operazione atomica a livello logico.
- Nel caso sia necessario effettuare delle modifiche ad una struttura complessa che devono rispettare dei vincoli dati, si deve PRIMA controllare che i vincoli siano soddisfatti per la situazione che si verrà a creare, e DOPO effettuare le modifiche (es. query) che vanno ad implementarle, così da evitare situazioni di errore che diventano difficili da annullare (soprattutto in assenza delle transazioni, che si preferisce non usare).

PROBLEMI DI INTERFACCIA, se gravi portano a perdite di punti, di sicuro infastidiscono

- Se l'utente non ha ancora fatto nulla, non deve apparire un form che mostra già errori (es. campi bordati di rosso): per es. login con username e password rossi perché vuoti, appena arrivati sulla pagina. Solo dopo la pressione del bottone login (o Invio) devono comparire gli eventuali errori (es. è richiesta un'email, manca @, ecc.).
- Il login è come si presenta l'applicazione. Se dopo aver inviato le credenziali non ci si può autenticare (per es. perché il server le rifiuta) questo deve essere indicato all'utente, altrimenti l'utente neanche si accorge dell'invio e che c'è stato un problema. Se ci sono più posti in cui fare il login (per es. pagina apposita ma anche campi sempre visibili in alto), TUTTI devono

mostrare un messaggio in caso di problemi, non solo quello dell'apposita pagina. Non inserire modi di autenticazione se non richiesti nel testo (es. "login as guest"). Usare o dare l'impressione di doversi autenticare, seppur senza credenziali, quando non richiesto, è un errore.

- Testare TUTTI i modi di usare i campi dei form, in particolare i campi HTML5: se scrivo direttamente il numero anziché usare le freccette del campo numerico (es. campo numerico "crediti di un corso"), deve funzionare, altrimenti l'applicazione perderà punti perché certe funzionalità non si riescono a testare. Attenzione anche che, se non specificato, non è detto che i numeri siano interi.
- NON fare assunzioni non specificate sui dati: un codice identificativo, per esempio, NON è necessariamente numerico. L'ID interno può essere numerico, ma all'utilizzatore dell'applicazione NON interessa e non deve essere utilizzato nell'interfaccia. Se il codice è visibile (per es. "codice corso"), non assumere che sia solo numerico, se non è esplicitamente indicato nel testo. Il codice di un oggetto/elemento/prodotto generico NON è per forza numerico. Può essere comodo implementarlo come numero, ma comunque anche in questo caso è concettualmente sbagliato acquisirlo/gestirlo con campi type=number, se tale operazione fosse necessaria.
- NON fare assunzioni inutili, non richieste o sbagliate sui dati: es. almeno 6 caratteri per il nome del corso (esempi di 4 caratteri: "math", o "greco", "arabo"). In generale NON è compito dello sviluppatore ragionare su questo aspetto, se non è richiesto nella traccia. Testare se è vuoto o no ha senso (eventualmente rimuovendo gli spazi a inizio/fine), ma il numero di caratteri in generale no. Altro esempio: specificare luogo (min 6 caratteri): es. di 4 caratteri: Roma.
- Evitare di restringere le possibilità di scelta se non indicato dalla traccia. Esempio: se prenoto un appuntamento di cui devo specificare la durata, la durata (es. in minuti) NON deve essere un multiplo di 10, se non esplicitamente richiesto o derivante dalla logica del problema. Se è un problema di interfaccia (perché risulterebbe es. in una combo box troppo lunga), cambiare interfaccia (es. campo numerico o di testo verificato successivamente). Esempio: Il numero di crediti di un corso non deve essere predeterminato (es. 6 8 10 12), ma libero, eventualmente anche con la virgola, a meno di vincoli differenti nel testo. Nel dubbio, chiedere chiarimenti. In generale vincolare questo genere di valori comporta più lavoro, non richiesto e non valutato, e spesso non consente di testare agevolmente l'applicazione.
- Se la scelta possibile di un campo è ristretta (es. solo un prodotto, persona, codice corso, o altro già esistente nell'applicazione) è consigliabile usare un elemento adeguato nell'interfaccia, per es. combo box (menù a tendina) e NON un campo libero, tantomeno richiedendo all'utilizzatore l'ID interno oppure mostrando solo l'ID come identificativo di scelta (come fa l'utilizzatore a sapere a cosa corrisponde l'ID?)
- Se il numero è, semanticamente, una stringa, il campo NON deve essere numerico (NO type=number). Esempi: numero di carta di credito, numero di telefono, codice prodotto.
- Precisare sempre l'unità di misura di quello che si chiede, per es. Durata: scrivendo "1" cosa vuol dire? 1h , 1min? In questo caso può andare bene anche usare il campo numerico HTML5, ma si deve anche poter scriverci direttamente dentro senza usare le freccette per selezionare il numero. Se devo scrivere 300 non devo fare 300 click o attendere che si girino tutti i numeri.
- Campi data/ora: evitare di farli di solo testo senza esempi: come scrivo se non c'è un esempio? (Uso /, - o che simbolo tra anno, mese e giorno? e in che ordine, italiano o inglese? Il mese è in numero o lettere?) In generale preferire il type=date o usare librerie per avere un box che si apre che consente la selezione della data. Il minimo è avere un esempio su come scrivere, dentro o di fianco al campo, es. YYYY/MM/DD.
- NON si deve fare il controllo del contenuto della password in fase di login ma solo (se

richiesto) in fase di creazione di una nuova password. Controllare in fase di login è generalmente scorretto, si danno informazioni su come sono fatte le password ad un eventuale attaccante (es. minimo 6 caratteri, almeno una maiuscola, ecc.), oltre ad essere scomodo in fase di valutazione dell'applicazione perché non consente di usare password qualsiasi per testare login falliti.

- E' comodo che i form facciano partire la sottomissione anche con l'INVIO, non solo con il click sul bottone (si risparmia tempo nel test ed è anche buona norma, es. login)
- NON usare le funzioni di creazione di finestre del browser, MAI (per es. alert(), prompt(), confirm()). Problemi: non sono integrati con la gestione dell'applicazione di React, la visualizzazione è potenzialmente differente per ogni browser, possono essere disabilitate nel browser, se sono troppe il browser le ferma, ecc.
- NON usare funzioni per ricaricare la pagina del browser da Javascript (es. window.location.reload()). L'applicazione, dopo essere stata caricata la prima volta, non deve richiedere ricaricamento, altrimenti non è una Single Page Application (SPA).
- Campi di un form: evitare di renderli non editabili per costringere ad usare i bottoni, es. + e - in un campo numerico. Se devo scrivere 1000 devo fare 1000 click?
- Il testo nei campi di testo è libero e in generale deve poter supportare spazi, e soprattutto non fallire senza chiarire l'errore se c'è uno spazio (che spesso è invisibile e/o inserito per errore).
- Quando un'operazione si è svolta, si dovrebbe dare un feedback all'utilizzatore: o cambia qualcosa nell'interfaccia (aggiunta/rimozione di un elemento nell'interfaccia), o si mostra un messaggio di conferma/esito. In particolare, in caso di errore, si dovrebbe capire cosa non va. (La gestione errori non è semplice, ma si può raggiungere un buon compromesso, soprattutto seguendo le regole sopra si minimizzano i potenziali problemi)
- Usare il log degli errori tramite console.log(), sulla console del browser, solamente per lo sviluppo. Il progetto consegnato non dovrebbe usarne per gestire condizioni che si possono verificare durante l'esecuzione dell'applicazione. Eventuali errori dovrebbero sempre essere mostrati all'utente (per es. definendo uno stato e una funzione handleError che lo imposti).
- Provare l'applicazione anche quando il server delle API non è attivo. Spesso durante i test il server non funziona per vari motivi (es. manca un pacchetto npm, il nome del file del DB è scritto in maniera non corretta a causa di maiuscole/minuscole).
    - Nel caso della configurazione "due server con CORS" non si può fare molto
    - Se si usa la configurazione con il proxy React, considerare che un server HTTP risponde sempre (quello di sviluppo di React), ma non quello che l'applicazione si aspetta. Evitare che l'applicazione si apra mostrando una schermata senza dati, che induce a pensare che non funzioni. Questo si verifica spesso con i progetti che mostrano qualcosa in homepage, anche prima dell'autenticazione. Cercare di gestire questo caso, per esempio gestendo la Promise rejected del metodo .json() che fa il parsing.

NAVIGAZIONE DELL'APPLICAZIONE

- Mettere gli eventuali bottoni di navigazione BEN IN VISTA, non nascosti in qualche menu a scomparsa (es. icona utente): diventa una perdita di tempo per chi testa/usa l'applicazione, rischiando che sia considerata una funzionalità mancante nel progetto.
- Se c'è una legenda dei simboli (che in certe applicazioni non sono intuitivi) deve essere sempre visibile o almeno accessibile senza cambiare vista da tutte le viste dell'applicazione dove i simboli compaiono.

- Deve sempre esserci un bottone per navigare indietro o in una vista/condizione nota, per es. "Annulla/Indietro" (preferibile), o almeno "Home", ben chiaro, non in chissà quale punto o sotto chissà quale scritta cliccabile (es. "MyApp" o loghi vari). Se non si identifica il bottone, non c'è alternativa a usare il Back del browser, che è sconsigliabile come spiegato nel corso.
- Evitare di inserire ritardi artificiali lato server per mostrare la condizione di loading, perché ciò rallenta il test dell'applicazione. La presenza della gestione del loading sarà comunque rilevata dall'analisi del codice.

BUONE NORME

- Mostrare da qualche parte nell'interfaccia l'informazione se l'utente è autenticato o meno. Se ha un ruolo (studente/amministratore/altro) mostrare anche quello correntemente selezionato.
- Scrivere sempre l'intestazione delle tabelle e liste: cosa c'è nella prima, nella seconda colonna ecc...? Ogni tanto è intuitivo, ma spesso non lo è, in particolare nei tests con dati di prova.
- A livello grafico: evitare effetti particolari (ombre di riquadri ecc...) che rischiano di non essere ben testati e andare in crisi quando le liste si allungano o ci sono tanti elementi. La bella grafica non è richiesta né valutata. I template di default (di bootstrap o altre librerie simili) sono già sufficientemente belli.
- Non esagerare nell'uso della disabilitazione dei warning sulla useEffect (per es. con il commento `//eslint-disable-line`). In alcuni casi può essere necessario e/o comodo, ma non dev'essere la norma. In generale, si dovrebbe evitare che si verifichi il warning evitando la dipendenza, come visto a lezione. Per le funzioni pure, per evitare il warning, spesso è sufficiente definirle all'interno della callback passata alla useEffect e non fuori. Nel caso di altre funzioni ciò può essere inevitabile.

CONSEGNA (alcuni problemi portano a perdite di punti o all'impossibilità di valutazione)

- Il tag da usare è "`final`" (scritto minuscolo, senza le virgolette, senza spazi), applicato al commit da valutare, che deve trovarsi nel branch main o master. Si consiglia di controllare che tutto sia a posto verificandone la presenza dall'interfaccia web di GitHub. Se il tag non è presente in forma corretta la consegna non sarà considerata, essendo indistinguibile dal caso in cui non si voglia consegnare. Si ricorda che la data/ora dei commit, per come funziona git, è generata localmente sul PC prima del "push", quindi tale informazione non dimostra nulla riguardo all'avvenuta consegna nei tempi.
- Testare su sistema **CASE SENSITIVE**. MacOS e Windows NON LO SONO. MacOS sembra case sensitive ma NON lo è, il file system ricorda il case dei nomi ma i files si aprono con qualunque case. Attenzione in particolare al file del db che non si legge a causa di maiuscole/minuscole, e che spesso non produce un errore sul lato client dell'applicazione se non ben gestito. Attenzione a import/require. Se il nome del file del DB è errato, l'applicazione in genere non funziona ed è difficile capire il perché (spesso il messaggio è "internal server error", che non aiuta).
- Ricordare di includere tutti i pacchetti nel `package.json`, sia per il server, sia per il client, altrimenti l'applicazione non è testabile. In altre parole, non installare mai alcun pacchetto a livello globale (tranne nodemon, che comunque non sarà usato in fase di test)
- Essere disordinati nel codice non è "una propria scelta". L'ordine è parte della valutazione. Non consegnare un file unico (o quasi) con tutti i componenti dentro, ma neanche esagerare all'opposto: raggruppare nello stesso file componenti per funzionalità logiche va più che bene (es. amministratore/utente, o ruolo nell'interfaccia - es. barre di navigazione/menu). Come regola approssimativa, files da 500+ linee di codice sono indice di cattiva organizzazione.

- CLONARE il repository per l'esame e NON modificare la struttura delle cartelle, non rinominare, non spostare, in particolare "client", "server", e README.md
- Al fine dell'esame, usare password degli utenti tutte uguali e la stessa password (ma con sale differente) per molti/tutti semplificano di molto la verifica manuale dell'applicazione (es. usare valori semplici come "password", o "pwd"). NON vengono tolti punti all'esame per questo, anzi è apprezzato, così come lasciare un utente e password di default già pre-compilati nel form di login (cosa facilmente realizzabile inizializzando lo stato del componente del form, come suggerito a lezione).
- Al fine dell'esame, usare username semplici e corti da scrivere, e regolari, soprattutto email (es. u1@p.it, u2@p.it, u3@p.it), è molto apprezzato. In generale, ogni due/tre minuti in più spesi per testare ognuna delle 100+ consegne al primo appello comporta potenzialmente lo slittamento di un giorno degli esami orali.

README.md: come scriverlo

- Riportare il proprio vero nome cognome e matricola al posto della dicitura generica Student: s123456 LASTNAME FIRSTNAME! Lasciare `Student:` (in inglese) che può essere comodo per processare automaticamente i files README.md
- Per il corso in italiano (Applicazioni Web I), ad eccezione delle prime 2 righe (Exam e Student) il resto può essere scritto sia in italiano sia in inglese, ciò non comporta penalizzazioni né aggiunta di punti.
- Verificare ATTENTAMENTE username/password indicate nel file README. Se per esempio si dimentica il dominio dell'email, o la password, l'applicazione non è testabile e non sarà valutata. E' inutile e indice di scarsa comprensione della problematica riportare l'hash della password nel README.md
- Controllare che gli screenshot inclusi nel README.md siano collegati correttamente (percorso e nome file con il case giusto). Si verifica facilmente con la funzionalità PREVIEW di VSCode sui file .md
- ".md" è un formato ben definito, sebbene semplice. Non è solo un modo carino di scrivere file di testo. Se non si rispetta la sintassi, non funziona. Non è sufficiente includere immagini/screenshots in una cartella qualsiasi. Verificare se è tutto ok tramite il PREVIEW di VSCode. Esistono anche degli editor per scrivere più facilmente il file: cercare "markdown editor" sui motori di ricerca. Alcuni sono anche online, è sufficiente fare copia/incolla della parte testuale risultante.
- Per le tabelle del DB, NON riportare l'SQL di creazione: è di difficile leggibilità. Mettere i nomi delle colonne (possibilmente usare nomi significativi), e tra parentesi le informazioni importanti, es. chiave primaria (se non evidente) o campi unique.
- Le API: se si includono esempi di richiesta/risposta, mettere esempi CORTI, evitando liste di N oggetti con M campi l'uno. Valutare se ridurre il numero di "a capo" nel JSON per migliorare la leggibilità del README.
- Ricordarsi di specificare il ruolo degli utenti inseriti, amministratore, gestore, utente, creatore, ecc., oppure utente di tipo A, B, C, ecc. (se applicabile, secondo la traccia d'esame).
- Per il corso in italiano, è consentito, se desiderato, scrivere le descrizioni e tutto il resto in italiano. Per comodità, evitare di modificare i titoletti già inseriti nel README.md di esempio (`Application Routes`, `API Server`, ecc.)