

課題1

クイズ作成と出題

クイズ作成と出題

次の内容でクイズを出題するWebアプリを制作する。

- クイズの出題とその答えをデータベースに保存する
- クイズ作成用の画面を表示し、入力欄に出題とその答えを入力して保存する
- 保存されている作成済みのクイズを修正・削除も可能とする
- データベースからクイズを読み込み、ランダムに画面に表示する
- クイズ出題用の画面を表示し、入力欄に答えを入力して送信し、正解か不正解を判定する
- 「正解」「不正解」を画面に表示する
- ボタンなどで別の問題を表示可能とする
- データベースはMySQLもしくはSQLiteを使用する

クイズ作成と出題

参考データとデータベースのテーブル例

【参考データ】

項目（列名）	データ1	データ2	データ3	データ4
問題(question)	サザエさんの弟は？ （カタカナ）	ドラえものの好物は？ （ひらがな）	「親人中？小」？に入る漢字は何？	「雨+二+ム=？」？に入る漢字は何？
答え(answer)	カツオ	どらやき	葉	雲

【テーブル例】

項目	列名	型	制約
番号	id	INTEGER	NOT NULL PRIMARY KEY AUTO_INCREMENT
問題	question	VARCHAR(256)	NOT NULL
答え	answer	VARCHAR(256)	NOT NULL

これは参考であり、詳細はこのテーブルと異なったものでもよい。

クイズ作成と出題(画面遷移)

トップ

クイズ作成と出題

クイズを作成保存し、保存したクイズを出題します。

[新規作成](#) [編集](#) [出題](#)

新規作成

クイズ新規作成

問題:

答え:

[トップ](#) [編集](#) [出題](#)

問題と答えを入力しDBへ保存する。

編集

クイズ編集

番号:

問題:

答え:

クイズ一覧

番号	問題	答え
1	サザエさんの弟は? (カタカナ)	カツオ
2	ドラえものの好物は? (ひらがな)	どらやき
3	「親人中?小」?に入る漢字は何?	葉
4	「雨+二+ム=」?に入る漢字は何?	雲

[トップ](#) [新規作成](#) [出題](#)

DBに保存している問題を修正・削除する。一覧には保存されている問題の一覧が表示される。

クイズ一覧

[トップ](#) [新規作成](#) [出題](#)

出題

クイズ出題

問題: ドラえものの好物は? (ひらがな)

答え:

結果表示

[トップ](#) [編集](#) [新規作成](#)

DBから読み込んだ問題リストからランダムに出題する。答えを入力し解答ボタンで判定する。

クイズ出題

問題がありません。

[トップ](#) [編集](#) [新規作成](#)

DBに問題がない場合は出題画面で「問題がありません。」を表示し編集画面では一覧が表示されない。

クイズ作成と出題(新規作成)

クイズ新規作成

問題：

答え：

[トップ](#) [編集](#) [出題](#)

保存できました。

クイズ新規作成

問題：

答え：

[トップ](#) [編集](#) [出題](#)


保存ボタンを押すと問題と答えをDBに保存し、保存したことを画面に表示する。

番号はAUTO_INCREMENTで自動的に付加されるため、ここでは入力せずにDBに保存する。

クイズ新規作成

問題：

答え：

 このフィールドを入力してください。

[トップ](#) [編集](#) [出題](#)

問題と答えのフィールドはどちらも入力必須とする。

保存されている問題と答えと同じものがあっても保存できる。

クイズ作成と出題(出題)

クイズ出題

問題：ドラえものの好物は？（ひらがな）

答え：

[解答](#)

結果表示

[次の問題](#)

[トップ](#) [編集](#) [新規作成](#)

答えを入力し解答ボタンを押して判定する

クイズ出題

問題：ドラえものの好物は？（ひらがな）

答え：

[解答](#)

結果表示

正解です

[次の問題](#)

[トップ](#) [編集](#) [新規作成](#)

クイズ出題

問題：ドラえものの好物は？（ひらがな）

答え：

[解答](#)

結果表示

不正解です(正解：どらやき)

[次の問題](#)

[トップ](#) [編集](#) [新規作成](#)

クイズ出題

問題：サザエさんの弟は？（カタカナ）

答え：

[解答](#)

結果表示

[次の問題](#)

[トップ](#) [編集](#) [新規作成](#)

「次の問題」ボタンを押すとランダムに問題が切り替わる。

クイズ作成と出題(編集)

クイズ編集

番号:

問題:

答え:

入力必須

空白入力可
*削除動作のため
バックエンドで編集
時にエラーを出す

クイズ一覧

番号	問題	答え
1	サザエさんの弟は？ (カタカナ)	カツオ
2	ドラえものの好物は？ (ひらがな)	どらやき
3	「親人中？小」？に入る漢字は何？	葉
4	「雨+ニ+ム＝？」？に入る漢字は何？	雲
5	サザエさんの弟は？ (カタカナ)	カツオ

[トップ](#) [新規作成](#) [出題](#)

クイズ編集

番号:

問題:

答え:

クイズ編集

番号:

問題:

答え:

編集画面の問題と答えの入力欄は空白でもPOST送信でき、番号だけが入力必須となる。これは、読込ボタンが番号だけを利用するためである。

クイズ編集

番号:

問題:

答え:

修正ボタンで指定した番号の内容を書き換える

クイズ編集

番号:

問題:

答え:

削除ボタンで指定した番号の内容を削除する

クイズ編集

番号:

問題:

答え:

番号5の問題を削除しました。

DBにあるクイズを一覧表示

クイズ作成と出題(脆弱性対策)

クイズ新規作成

問題：

答え：

保存

[トップ](#) [編集](#) [出題](#)

クイズ新規作成

問題：

答え：

保存

[トップ](#) [編集](#) [出題](#)

クイズ編集

番号：

問題：

答え：

クイズ一覧

番号	問題	答え
1	サザエさんの弟は？（カタカナ）	カツオ
2	ドラえものの好物は？（ひらがな）	どらやき
3	「親人中？小」？に入る漢字は何？	業
4	「雨+ニ+ム＝？」？に入る漢字は何？	雲
5	<script>alert('XSS');</script>	<script>alert('XSS');</script>
6	0;DELETE FROM questions;	0;DELETE FROM questions;

[トップ](#) [新規作成](#) [出題](#)

クイズ出題

問題： 0;DELETE FROM questions;

答え：

解答

結果表示

不正解です(正解：0;DELETE FROM questions;)

[トップ](#) [編集](#) [新規作成](#)

クイズ出題

問題： <script>alert('XSS');</script>

答え：

解答

結果表示

不正解です(正解：<script>alert('XSS');</script>)

[トップ](#) [編集](#) [新規作成](#)

クロスサイト・スクリプティング対策として、入力したデータを表示する際はHTMLエスケープすること。またSQLインジェクション対策として、SQL文の実行は、プリペアドステートメントを使用すること。

課題1：動作確認用チェックシート(正常系)

1	クイズ新規作成画面を表示し、問題と答えを入力し「保存」ボタンを押すとDBに保存する。(正常に保存したことを表示)	5	クイズ編集画面を表示し、DBに保存しているクイズ情報一覧を表示する。
2	クイズをランダムに出題する画面を表示し、答えを入力し「解答」ボタンを押すと「正解・不正解」の結果を画面に表示する。	6	クイズ編集画面でDB保存時に割り当てる番号を入力し、「読込」ボタンを押すと問題と答えの入力フィールドにその番号の内容が表示される。
3	不正解の場合は正解を表示する。	7	クイズ編集画面で問題と答えの入力フィールドに入力し、「修正」ボタンを押すと、DBにある情報が更新される。(正常に修正したことを表示)
4	クイズを出題する画面で、「次の問題」ボタンを押すと別の問題をランダムに表示する。	8	クイズ編集画面で番号の入力フィールドに番号を入力し、「削除」ボタンを押すと、その番号のクイズ情報がDBから削除される。(正常に削除したことを表示)

課題1：動作確認用チェックシート(異常系)

1	新規作成画面で問題と答えを入力するフィールドは空白で保存しようとするときエラーを表示する。(入力必須)	4	編集画面で番号を入力するフィールドは空白で読込、修正、削除しようとするときエラーを表示する。(入力必須)
2	新規作成画面で問題と答えを入力するフィールドにHTMLタグやSQL文を入力しても文字として扱う。(例 ：<script>alert('XSS');</script>、 0;DELETE FROM table名)	5	編集画面で番号、問題、答えを入力するフィールドにHTMLタグやSQL文を入力しても文字列として扱う。(例 ：<script>alert('XSS');</script>、 0;DELETE FROM table名)
3	出題画面で答えを入力するフィールドにHTMLタグやSQL文を入力しても文字として扱う。 (例：<script>alert('XSS');</script>、 0;DELETE FROM table名) 正解の時と、不正解の時の両方の動作を確認	6	DBに問題がない場合は出題画面で、「問題がありません。」を表示し、編集画面では一覧になにも表示しない。

※SQLインジェクション対策がされているかをチェックする際に入力するSQL文のテーブル名を講師に伝える。