

TP12 – Sécurisation des views

Introduction, Contexte et Objectifs

Nous allons commencer à différencier les fonctionnalités (dont les menus) en fonction du statut de l'utilisateur. Nous sécuriserons aussi les views pour éviter une action directe via l'url.

Différenciation des liens affichés

Pour le moment, tout le monde a les mêmes boutons d'actions dans la liste des pizzas ou dans les détails d'une pizza. Arrangez-vous, comme pour les menus, pour que :

- a. Dans la liste des pizzas, un utilisateur staff ait à sa disposition les liens détails, modification et suppression,
- b. Dans la liste des pizzas, un client ait un lien d'achat (type panier) et le lien détails,
- c. Dans la liste des pizzas, un utilisateur non connecté ait le lien détails,
- d. Dans les détails d'une pizza, les actions de suppression d'un ingrédient et d'ajout d'un ingrédient ne soient accessibles qu'au staff (et qu'un client ou un utilisateur non connecté n'aient accès qu'au tableau simplifié des ingrédients).

Vous pourrez utiliser les instructions :

- `{% if user.is_staff %}` (utilisateur staff)
- `{% if user.is_authenticated %}` (staff ou client)

les pizzas - Mozilla Firefox

les pizzas 127.0.0.1:8000/pizzas/

Appli Pizza 2023 les pizzas inscription connexion

voici nos 3 pizzas

pizza quatre fromages (prix : 15.50 €) pizza napolitaine (prix : 14.80 €) pizza végétarienne (prix : 14.50 €)

(i) *(i)* *(i)*

les pizzas pour un internaute non connecté

détails d'une pizza - Mozilla Firefox

détails d'une pizza 127.0.0.1:8000/pizzas/3/

Appli Pizza 2023 les pizzas inscription connexion

voici notre pizza

pizza végétarienne (prix : 14.50 €)

les 2 ingrédients de la pizza végétarienne

| ingrédient | quantité |
|-------------|-------------------|
| champignons | 20 grammes |
| roquette | quelques feuilles |

détails d'une pizza pour un internaute non connecté

les pizzas - Mozilla Firefox

les pizzas 127.0.0.1:8000/connexion/

Appli Pizza 2023 les pizzas panier commandes déconnexion

voici nos 3 pizzas

pizza quatre fromages (prix : 15.50 €) pizza napolitaine (prix : 14.80 €) pizza végétarienne (prix : 14.50 €)

i

i

i

les pizzas pour un client connecté

détails d'une pizza - Mozilla Firefox

détails d'une pizza 127.0.0.1:8000/pizzas/3/

Appli Pizza 2023 les pizzas panier commandes déconnexion

voici notre pizza

pizza végétarienne (prix : 14.50 €)

les 2 ingrédients de la pizza végétarienne

| ingrédient | quantité |
|-------------|-------------------|
| champignons | 20 grammes |
| roquette | quelques feuilles |

détails d'une pizza pour un client connecté

les pizzas - Mozilla Firefox

les pizzas 127.0.0.1:8000/connexion/

Appli Pizza 2023 les pizzas créer une pizza les ingrédients créer un ingrédient déconnexion

voici nos 3 pizzas

pizza quatre fromages (prix : 15.50 €)

pizza napolitaine (prix : 14.80 €)

pizza végétarienne (prix : 14.50 €)

les pizzas pour un utilisateur staff

The screenshot shows a Mozilla Firefox window with the title "détails d'une pizza - Mozilla Firefox". The address bar displays "127.0.0.1:8000/pizzas/3/". The page content is from the "Appli Pizza 2023" application. It shows a pizza titled "voici notre pizza" with a price of "pizza végétarienne (prix : 14.50 €)". Below this, it lists "les 2 ingrédients de la pizza végétarienne" with a table:

| ingrédient | quantité | action |
|-------------|-------------------|--------|
| champignons | 20 grammes | |
| roquette | quelques feuilles | |

Below the table, there is a section titled "ajouter un ingrédient" with a form:

ingredient
choisissez l'ingrédient à ajouter

quantité

Envoyer

© Appli Pizza 2023

détails d'une pizza pour un utilisateur staff

Mise en garde de sécurité !

Vous ferez attention à une chose : la sécurisation n'est pas faite sur les views (pour preuve, un utilisateur non connecté peut directement entrer une url de la forme

`http://127.0.0.1:8000/pizzas/1/update/`

et disposer des privilèges staff.

Il faut impérativement l'empêcher.

Sécurisation des views

1. Sécurisation de la liste des ingrédients

la view ingredients est un cas de base :

- si l'utilisateur est staff, on lui retourne la liste des ingrédients,
- sinon, si c'est un client, on lui retourne la liste des pizzas,
- sinon, (utilisateur non connecté), on lui retourne la page de connexion.

Cela se traduit par un aménagement de la view ingredients. Remarquez qu'à partir de maintenant, on retournera le user, ça peut toujours servir. En particulier, plus tard on affichera la photo de l'utilisateur connecté.

```
24     def ingredients(request) :
25         # création du user
26         user = None
27
28         # cas d'un utilisateur staff
29         if request.user.is_staff :
30             lesIngredients = Ingredient.objects.all()
31             user = User.objects.get(id = request.user.id)
32             return render(
33                 request,
34                 'applipizza/ingredients.html',
35                 {'ingredients' : lesIngredients, "user" : user})
36
37
38         # cas d'un client connecté
39         elif request.user.is_authenticated :
40             user = User.objects.get(id = request.user.id)
41             lesPizzas = Pizza.objects.all()
42             return render(
43                 request,
44                 'applipizza/pizzas.html',
45                 {'pizzas' : lesPizzas, "user" : user})
46
47
48         # cas d'un internaute non connecté
49         else :
50             return render(
51                 request,
52                 'applicompte/login.html',
53             )
```

2. Testez maintenant, dans les trois cas (utilisateur non connecté, client, staff), ce que donne l'injection dans la barre d'url de l'url

`http://127.0.0.1:8000/ingredients/`

3. Sécurisez maintenant TOUTES LES VIEWS. Les permissions d'accès aux pages du site ou aux actions de type contrôleur sont indiquées ci-dessous :

| Page du site | non connecté | client connecté | staff connecté |
|------------------------------------|--------------|-----------------|----------------|
| pizzas | autorisé | autorisé | autorisé |
| pizza | autorisé | autorisé | autorisé |
| ingrédients | interdit | interdit | autorisé |
| formulaire création pizza | interdit | interdit | autorisé |
| formulaire modification pizza | interdit | interdit | autorisé |
| formulaire création ingrédient | interdit | interdit | autorisé |
| formulaire modification ingrédient | interdit | interdit | autorisé |
| formulaire de connexion | autorisé | interdit | interdit |
| formulaire d'inscription | autorisé | interdit | interdit |

| Action | non connecté | client connecté | staff connecté |
|------------------------------|--------------|-----------------|----------------|
| creerIngredient | interdit | interdit | autorisé |
| supprimerIngredient | interdit | interdit | autorisé |
| modifierIngredient | interdit | interdit | autorisé |
| creerPizza | interdit | interdit | autorisé |
| supprimerPizza | interdit | interdit | autorisé |
| modifierPizza | interdit | interdit | autorisé |
| ajouterIngredientDansPizza | interdit | interdit | autorisé |
| supprimerIngredientDansPizza | interdit | interdit | autorisé |

4. Comme pour la page ingrédients, testez tous les accès.

Remarque : il y a des façons plus automatiques de gérer les permissions. Vous pouvez vous documenter sur ce sujet et voir de vous-même comment y arriver.