

# Rapport de Sécurité – Formulaire

## Sécurisé

Nom : Projet Formulaire Sécurisé

Auteur : Badreddine khalil

Date : 12/05/2025

### Mesures de sécurité mises en place

- **HTTPS :**

Utilisation d'un certificat SSL auto-signé pour chiffrer les communications via https.createServer.

- **Helmet :**

Ajoute des en-têtes HTTP pour prévenir XSS, Clickjacking, sniffing, etc.

- **reCAPTCHA :**

Empêche les bots d'envoyer le formulaire sans validation humaine (Google reCAPTCHA v2).

- **Sessions sécurisées :**

Cookies configurés avec les flags HttpOnly, Secure, SameSite=strict.

- **Hachage des données :**

bcrypt est utilisé pour hacher les mots de passe et les messages avant sauvegarde.

- **Rate limiting :**

Limitation à 100 requêtes/heure pour éviter les attaques par force brute.

### Risques couverts

- Bot/Spam automatisé → reCAPTCHA
- Vol de session → cookies HttpOnly + Secure + SameSite
- Interception de données → HTTPS
- Injection XSS → Helmet + validation de saisie
- Attaque par force brute → express-rate-limit

## Tests réalisés et résultats

Test	Résultat
Accès sans session à /Dashboard	Refusé (Redirection) <input checked="" type="checkbox"/>
Formulaire sans reCAPTCHA	Rejeté <input checked="" type="checkbox"/>
Message sauvegardé	Haché dans messages.json <input checked="" type="checkbox"/>
Login avec mauvais mot de passe	Rejeté <input checked="" type="checkbox"/>
Limite de requêtes	Testé avec curl → bloqué <input checked="" type="checkbox"/>
HTTPS activé	Oui, sur https://localhost:3000 <input checked="" type="checkbox"/>

## Déroulé de l'utilisation du système (avec captures d'écran)

### 1. Authentification de l'utilisateur

L'accès à l'application commence par une page d'authentification sécurisée. L'utilisateur doit entrer un **nom d'utilisateur** et un **mot de passe** valides.

Avant de pouvoir valider les identifiants, l'utilisateur doit également prouver qu'il **n'est pas un robot**, grâce à un **reCAPTCHA v2** visible ci-dessous.



# Formulaire de Connexion

Nom d'utilisateur :

Mot de passe :

En cas de succès, l'utilisateur est redirigé automatiquement vers le tableau de bord  
(/Dashboard).

## For

Nom d'u

Mot de p

Se con

Sélectionnez toutes les images montrant des **escaliers**

VALIDER

## 2. Accès au formulaire sécurisé

Une fois connecté, l'utilisateur accède à un **formulaire de contact** sécurisé. Celui-ci contient plusieurs champs :

- **Nom** (obligatoire)
- **Email** (obligatoire, validé par un format conforme)
- **Message** (obligatoire, taille minimale imposée)

# Formulaire sécurisé

Nom: khalil badreddinr

Email: badre



Veuillez inclure "@" dans l'adresse e-mail. Il manque un symbole "@" dans "badre".



Je ne suis pas un robot



reCAPTCHA  
Confidentialité - Conditions

Envoyer

Une vérification est effectuée côté client (HTML5) et côté serveur pour éviter les injections ou l'envoi de données invalides.

# Formulaire sécurisé

Nom:

Email:

Message:



Je ne suis pas un robot



reCAPTCHA  
Confidentialité - Conditions

Envoyer

Se déconnecter

**For**

Sélectionnez toutes les images montrant des voitures

Nom:

Email:

Message:

Envoyer

VALIDER

### 3. Protection anti-robots avant soumission

Avant de pouvoir envoyer le formulaire, l'utilisateur doit **cocher un reCAPTCHA**, attestant qu'il n'est pas un robot.

Si toutes les conditions sont réunies, les données sont :

- Validées
- Le message est **haché avec bcrypt**
- Stocké de manière sécurisée dans un fichier `messages.json`

```
index.html messages.json server.js key_no_passphrase.pem key.pem cert.pem
data > {} messages.json > {} 3
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
```

The screenshot shows a code editor with several tabs at the top: index.html, messages.json, server.js, key\_no\_passphrase.pem, key.pem, and cert.pem. The messages.json file is open and displays an array of three objects, each representing a message. Each object has properties: timestamp, nom, email, and message. The timestamps are in ISO 8601 format. The names and emails correspond to the users listed in the database dump below.

```
[{"username": "admin", "password": "$2b$10$hgTdxdc0Jypjkl.FQoEQF.FgEm7KBae4D0FlwOvGDrxq6tByLLKC", "date": "2025-05-12T18:38:35.537Z"}, {"username": "admin", "password": "$2b$10$0kqILtzA4Q9ct4K1SK8Bz.un47a23yt8JGZ5WV1b9Ie1dCUwc9w3K", "date": "2025-05-12T19:08:28.539Z"}]
```

```
[{"username": "admin", "password": "$2b$10$hgTdxdc0Jypjkl.FQoEQF.FgEm7KBae4D0FlwOvGDrxq6tByLLKC", "date": "2025-05-12T18:38:35.537Z"}, {"username": "admin", "password": "$2b$10$0kqILtzA4Q9ct4K1SK8Bz.un47a23yt8JGZ5WV1b9Ie1dCUwc9w3K", "date": "2025-05-12T19:08:28.539Z"}]
```

Une pop-up de succès est affichée à l'utilisateur.



Cookies											
Name	Value	Domain	Path	Expires...	Size	HttpOnly	Secure	SameSite	Partition	Cross Site	Priority
connect.sid	s%3Agn7FW5eYPlOTVzHtnvXLIb0uhaeRUUV.gpl	localhost	/	2025-01-01T00:00:00Z	99	✓	✓	Strict			Medium