ISEN ALL IS DIGITAL! | ynéréa

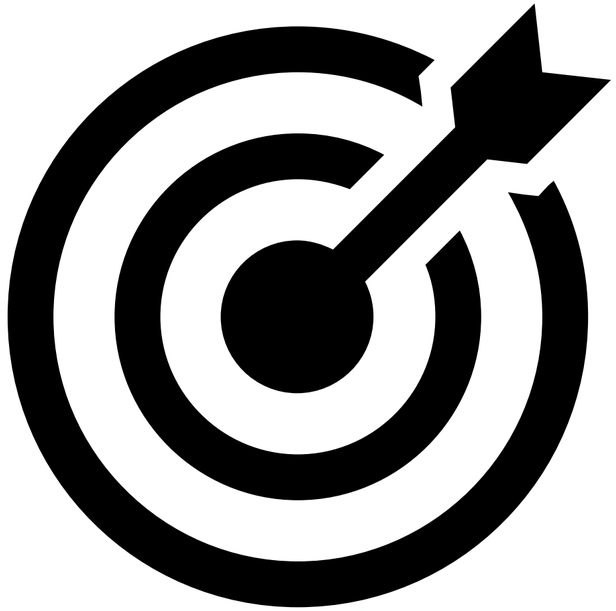
Soutenance du projet M1

MESSAGERIE INSTANTANÉE SÉCURISÉE (OU PAS…)

Sommaire

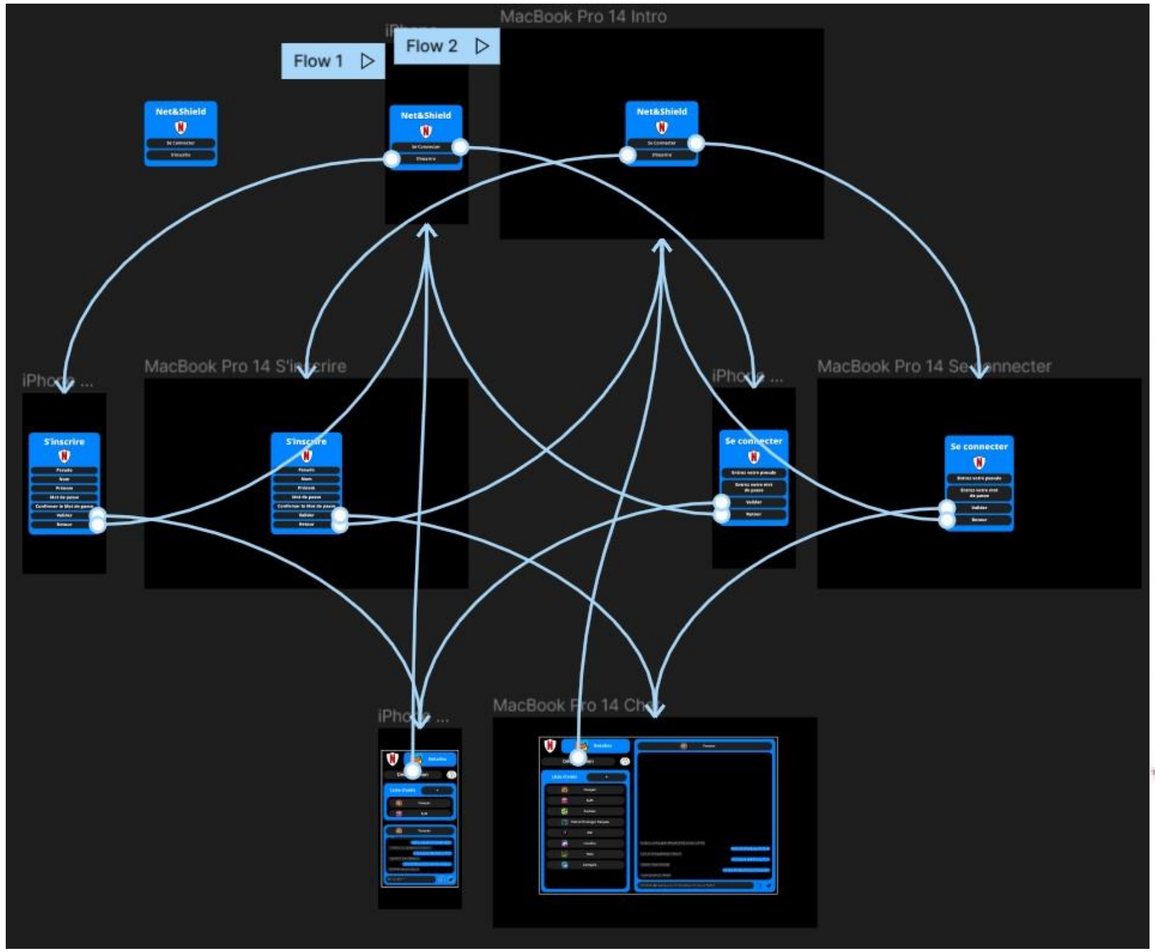
Gestion de projet – Les besoins

- Messagerie instantanée
- Mode sécurisé/vulnérable
- Responsive/multiplateforme
- Service client/serveur
- HTTP/HTTPS
- Système d'inscription



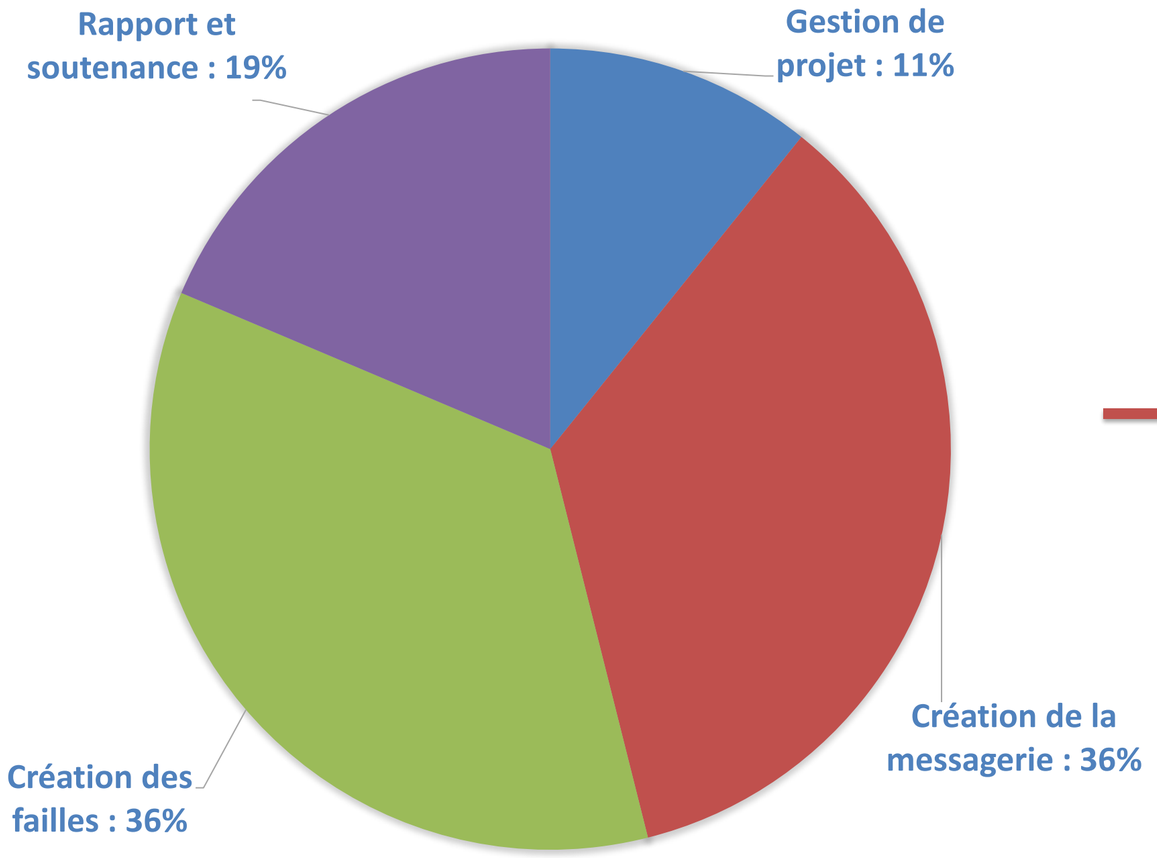
Gestion de projet – Répartition du projet

1. Création du Figma
2. Définition des fonctions
3. Rédaction du cahier des charges
4. Création du Gantt

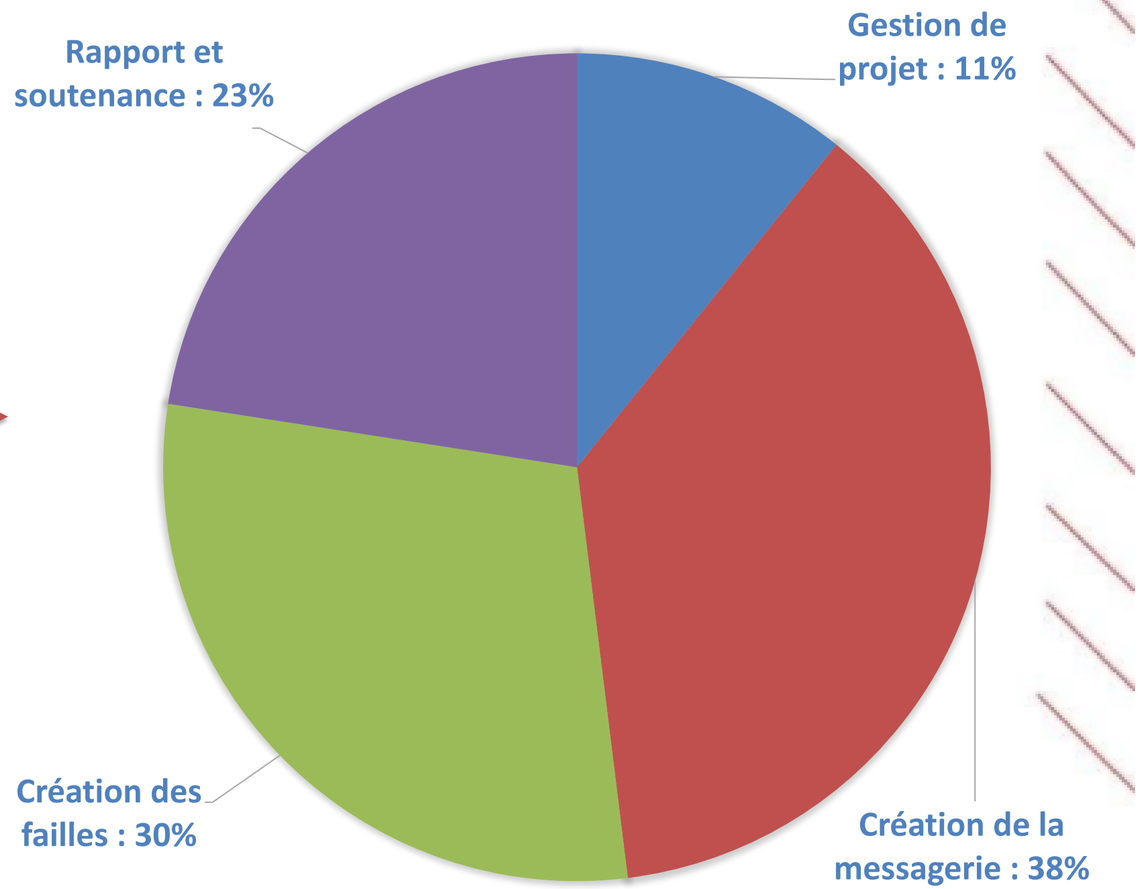


Gestion de projet – Les Gantt

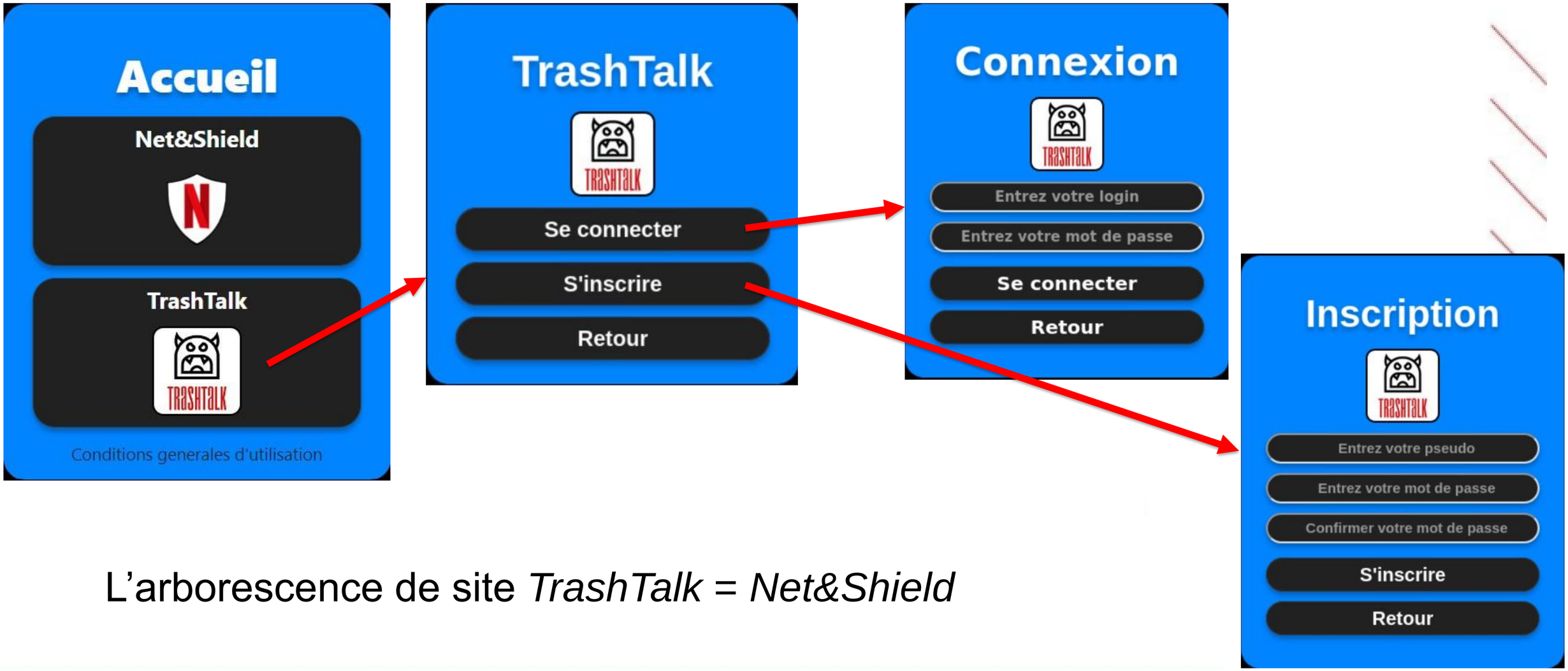
TEMPS PRÉVISIONNEL PAR ÉTAPES DU PROJET EN %



TEMPS RÉALISÉ PAR ÉTAPES DU PROJET EN %



La messagerie – Connexion et Inscription



L’arborescence de site *TrashTalk = Net&Shield*

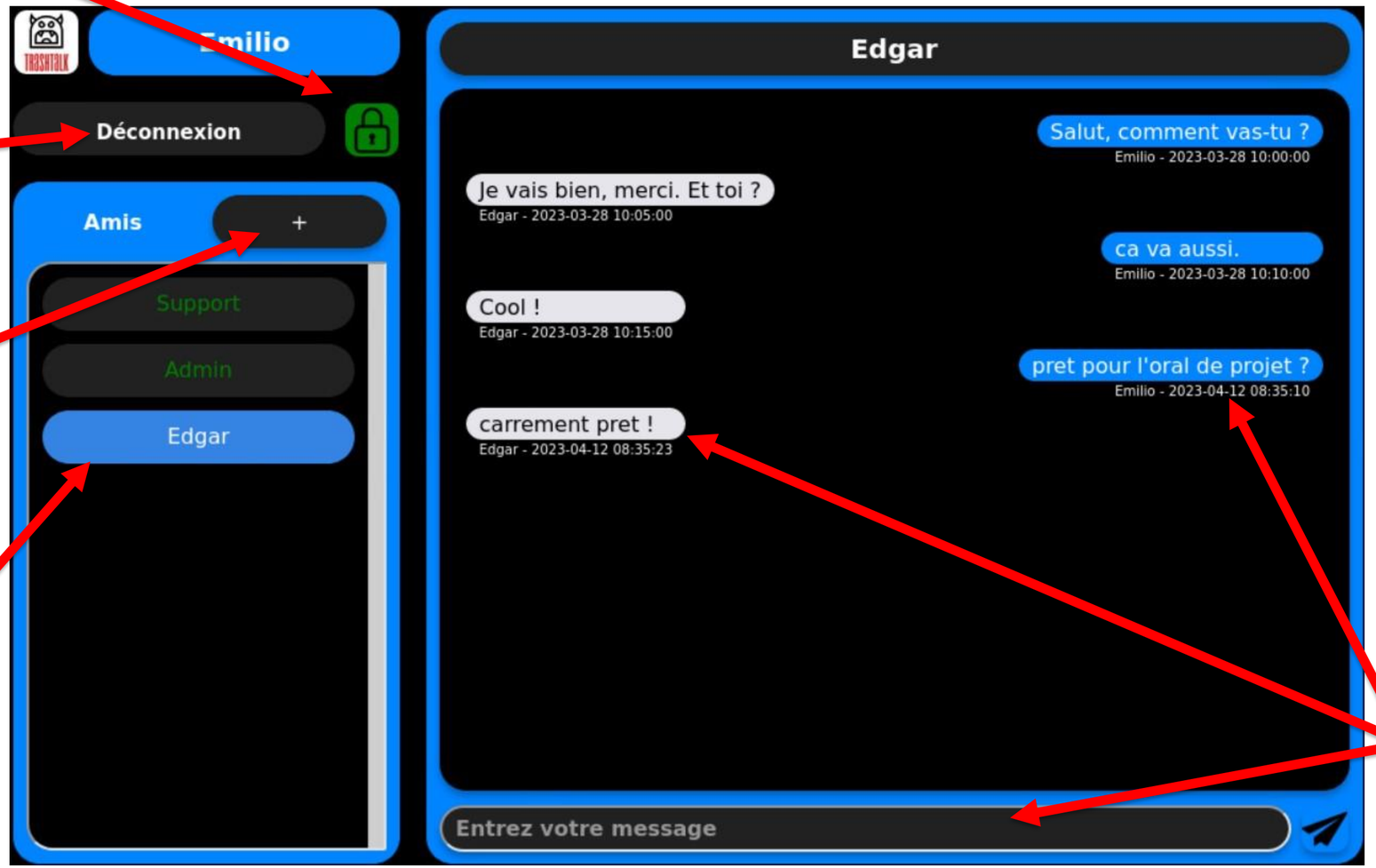
La messagerie – Le chat

HTTP / HTTPS

Déconnexion

Ajout d’amis

Sélection de l’ami avec qui échanger



Envoi et réception des messages

Les failles – Backdoors

- Fonction permettant d'accéder à du contenu/des droits non autorisés.
- Vecteur d'attaque
- Relecture de code, audit sécurité

Les failles – Injection SQL

- Insertion de code SQL dans un champ de texte pour modifier les requêtes server

- Vulnérabilité courante
- Top 3 OWASP

- Usurpation d’identité

- Pour corriger : filtrer les requêtes
- PDO Mysql

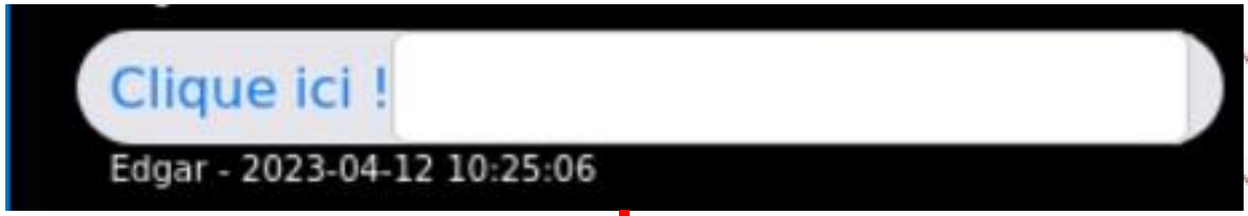
') OR ('1'='1

Les failles – Injection XSS

- L'injection XSS (Cross-Site Scripting) faille informatique qui permet d'injecter du code dans une page web.
- 3e de l'OWASP
- Vol de sessions
- Tester entrées/échapper

Insertion de la requête

Affichage côté victime



Récupération des cookies de la victime

```
GET /?cookies=login=Edgar;%20token=%0Az1Wel+vPR+qNbGvs;%20id=4
```

Les failles – Gestion de cookies

- Petit fichier texte hébergé sur l'ordinateur d'un client d'un site web pour stocker des infos sur cet utilisateur

- Modification possible
- Vol de session
- 5e de l'OWASP

- 1 seul cookie sur *Net&Shield*
- 3 sur *TrashTalk*

Nom du cookie

Valeur modifiable

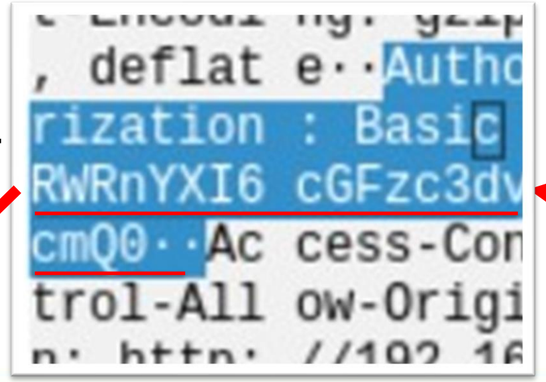
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
id	3	messagerie.c...	/	Session	3	false	false	None
login	Emilio	messagerie.c...	/	Session	11	false	false	None
token	%0AjODmbYw+s9nBridX	messagerie.c...	/	Session	24	false	false	None

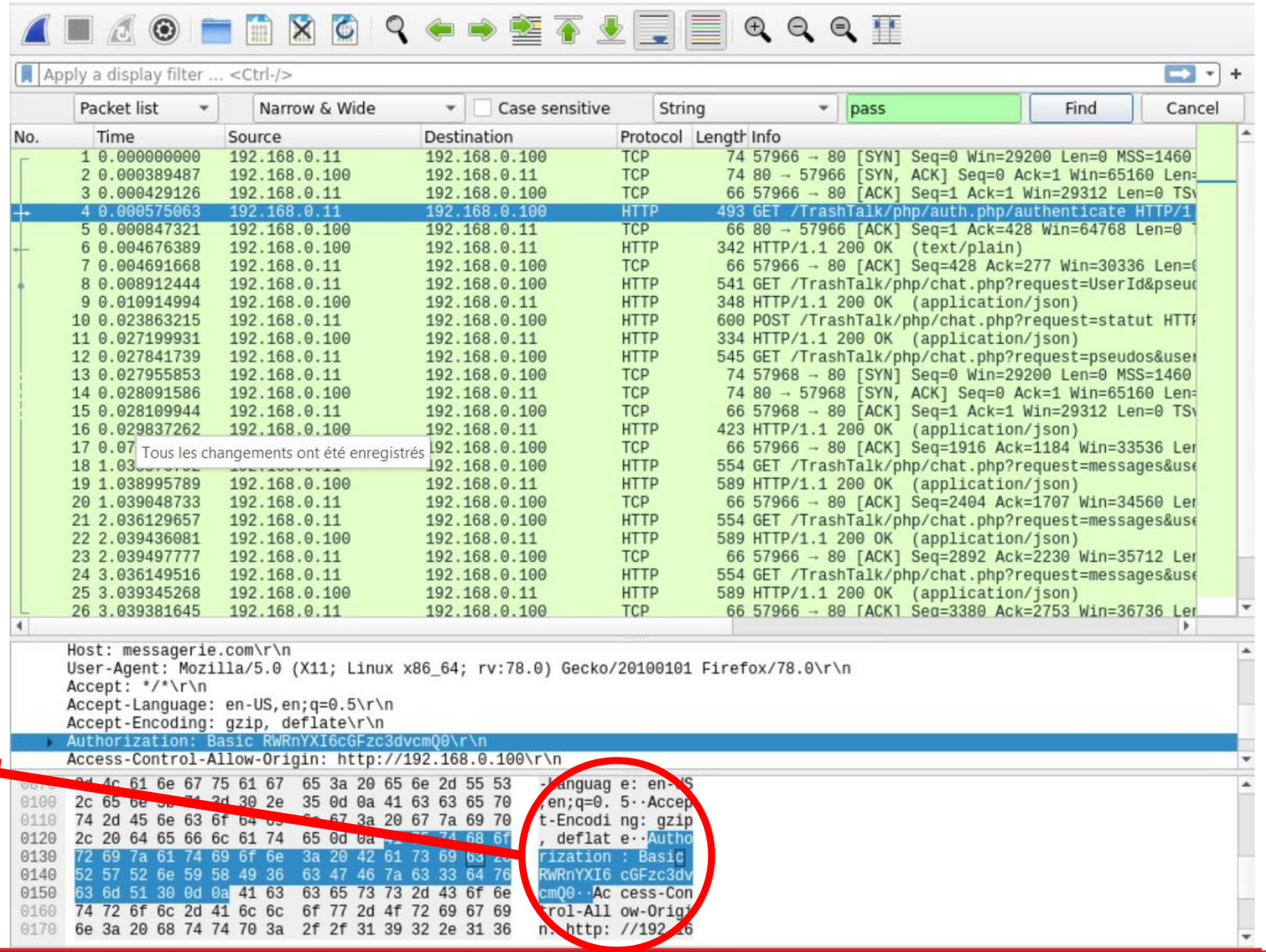
Les failles – HTTP

- Protocole de communication client server non chiffré
- Démonstration pédagogique
- Attaque « Man in the middle »
- Utilisation HTTPS
- Clé SSL : OpenSSL

Encodé en Base 64

Edgar : password4





Les failles – Hash MD5

- Technique pour convertir un mot de passe en une chaîne de caractères incompréhensibles.

- 2e OWASP

- Algorithme plus fort

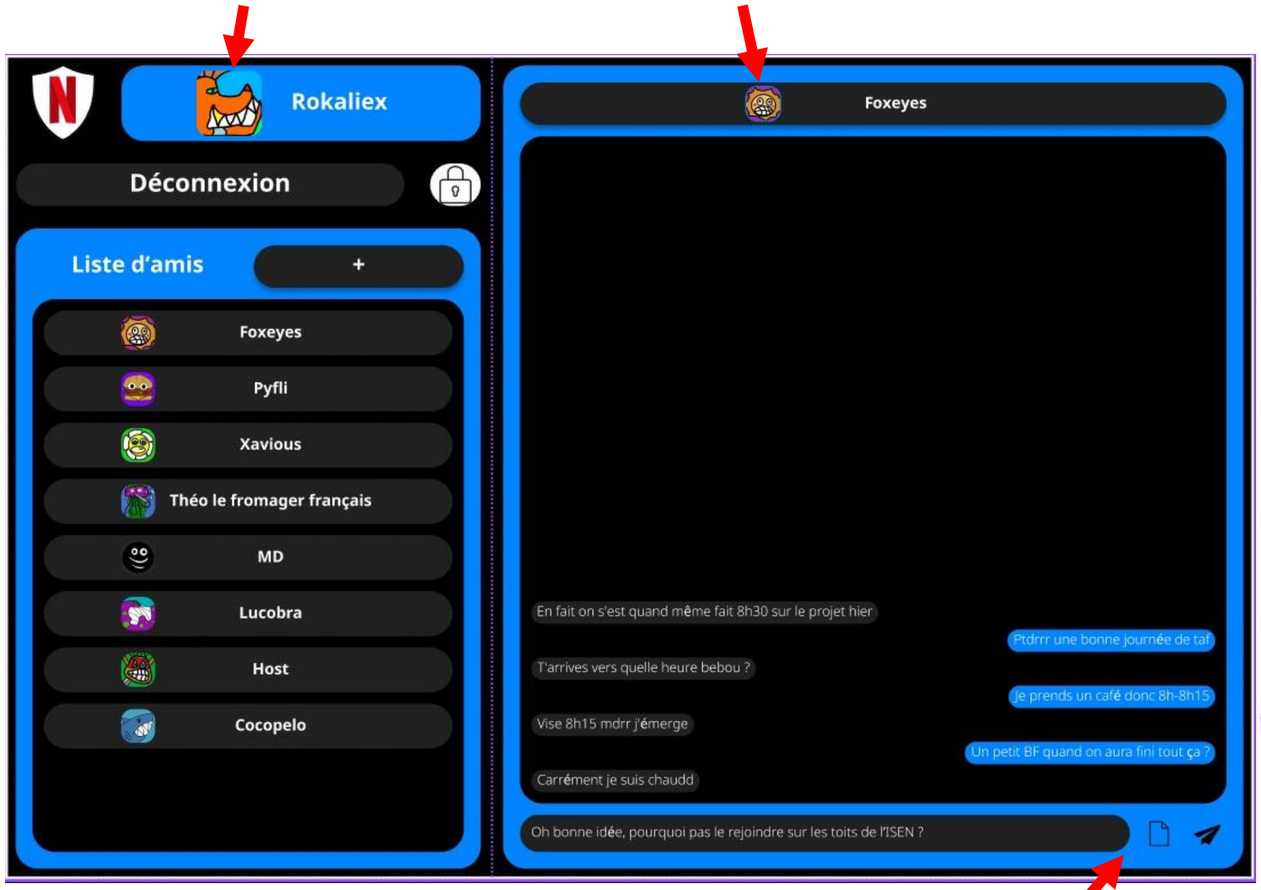
Mots de passe hachés en MD5

user_id	pseudo	image	hash	token	etat
1	Support	NULL	7c6a180b36896a0a8c02787eeafb0e4c	NULL	1
2	Admin	NULL	e3afed0047b08059d0fada10f400c1e5	JObUGmpEmkB+NOBk	0
3	Emilio	NULL	819b0643d6b89dc9b579fdfc9094f28e	jODmbYw+s9nBridX	1
4	Edgar	NULL	34cc93ece0ba9e3f6f235d4af979b16c	6i3NVmnV15FIc05J	0
5	NicoCharbo	NULL	db0edd04aaac4506f7edab03ac855d56	NULL	0
6	Quentin	NULL	218dd27aebeccecae69ad8408d9a36bf	NULL	0
7	Mathieu	NULL	00cdb7bb942cf6b290ceb97d6aca64a3	NULL	0
8	Hugo	NULL	b25ef06be3b6948c0bc431da46c2c738	NULL	0
9	Pierre	NULL	5d69dd95ac183c9643780ed7027d128a	NULL	0

Les évolutions

- Une gestion des messages différente
- Profil personnalisé et envoi d'images
- Man in the middle
- Injections XSRF

Ajout des photos de profil



Possibilité d'ajouter des images

Conclusion

Avez-vous des questions ?