

Soutenance du projet M1

MESSAGERIE INSTANTANÉE SÉCURISÉE (OU PAS...)



Sommaire

1. Gestion de projet

- Les besoins
- Répartition du projet
- Les Gantt

2. La messagerie

- Connexion et Inscription
- Le chat

3. Les failles

- Backdoor
- Injection SQL
- Injection XSS
- Gestion de cookies
- HTTP
- Hash MD5

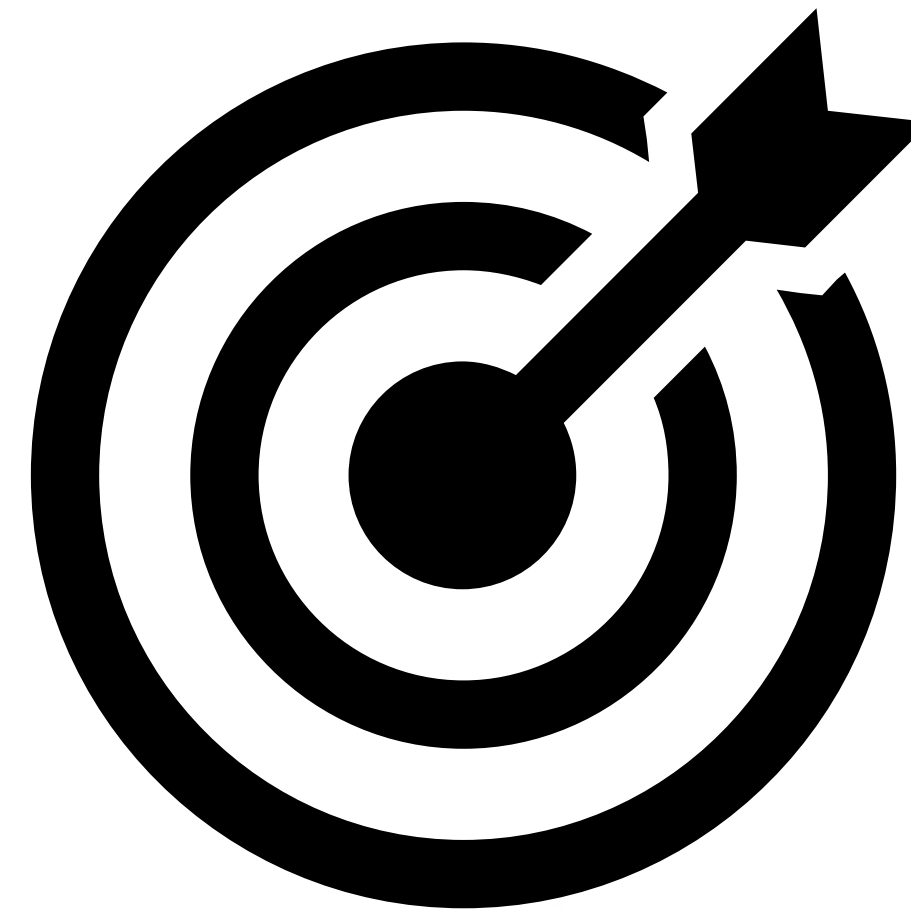
4. Les évolutions

5. Conclusion



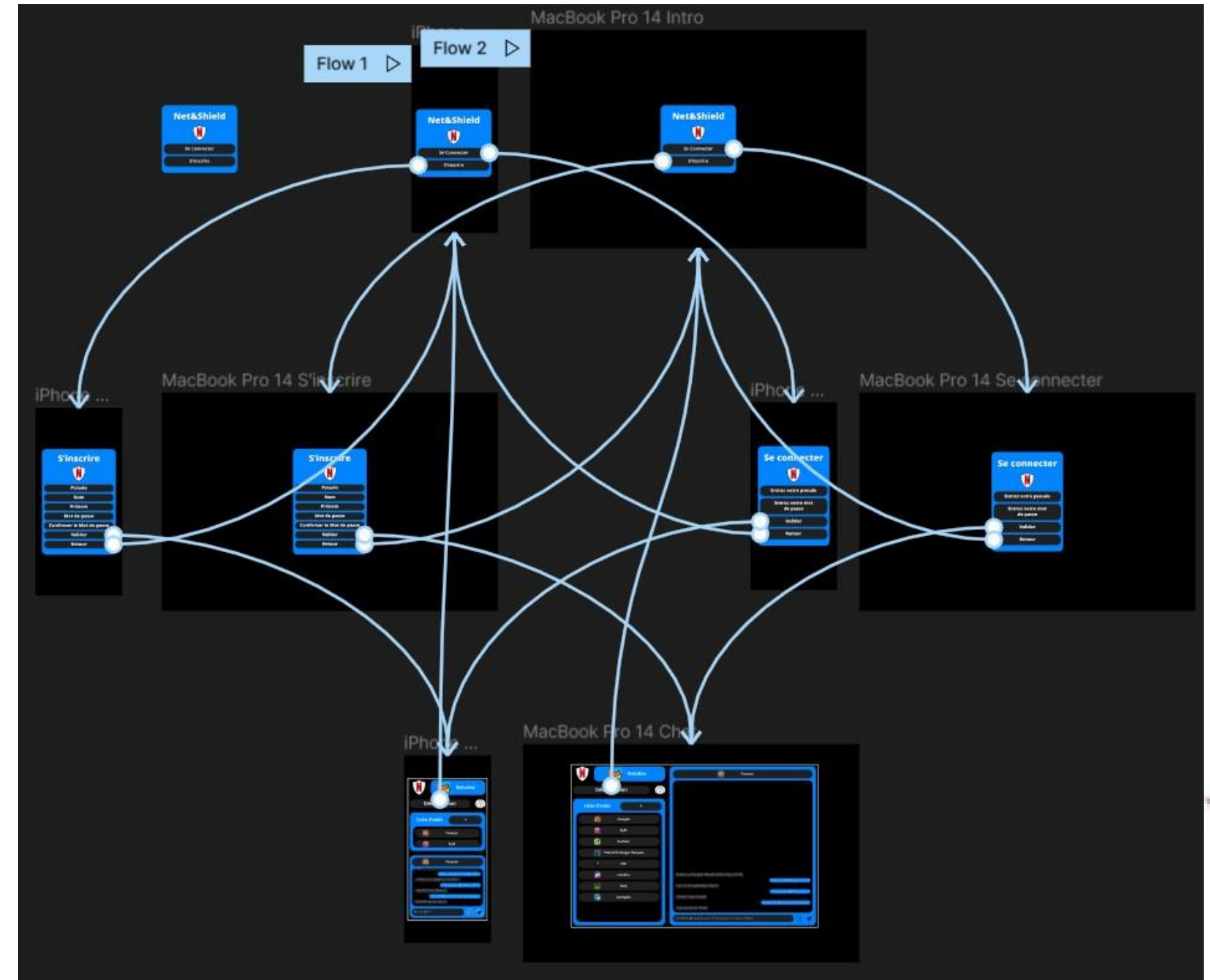
Gestion de projet – Les besoins

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



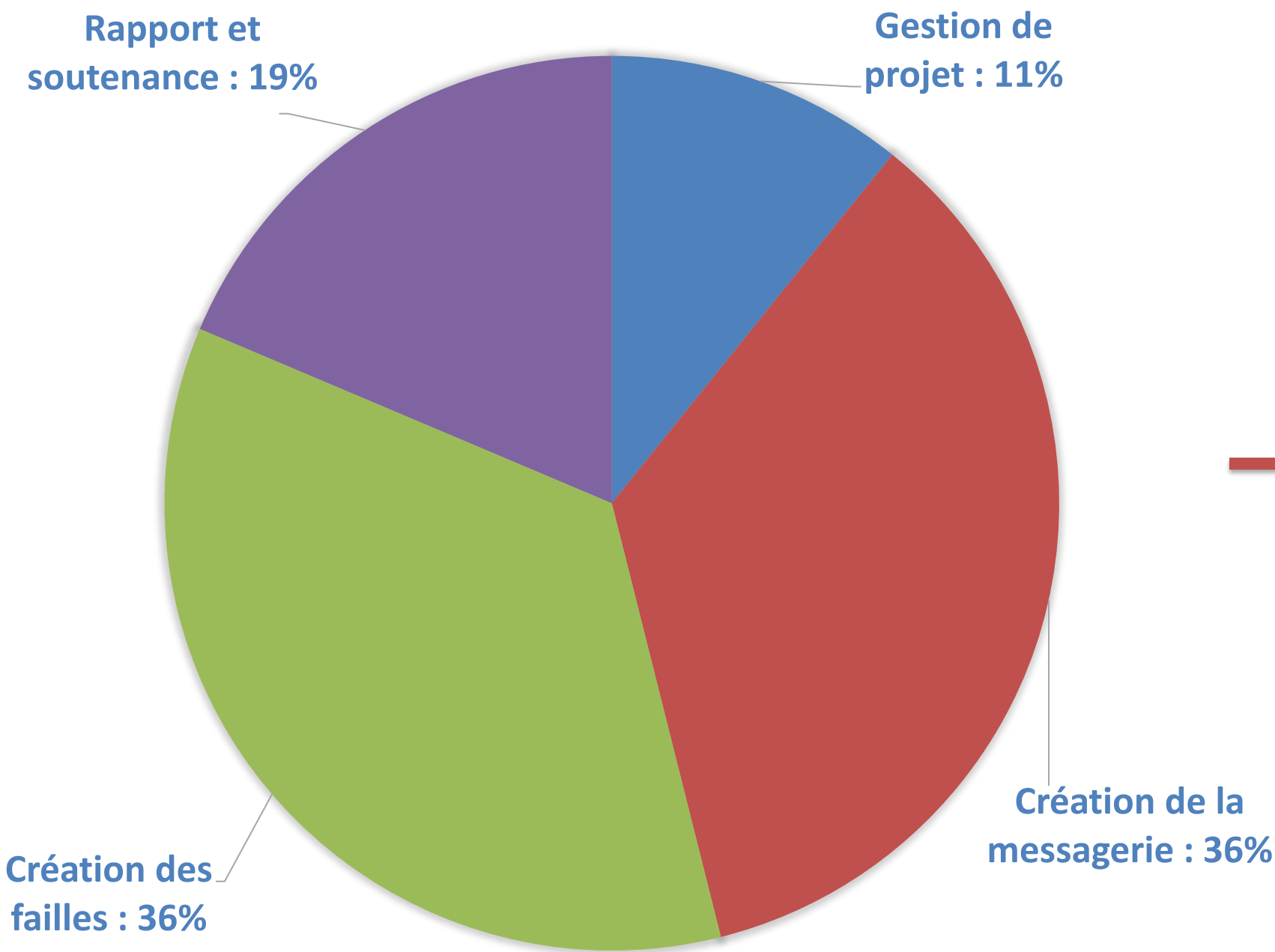
Gestion de projet – Répartition du projet

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

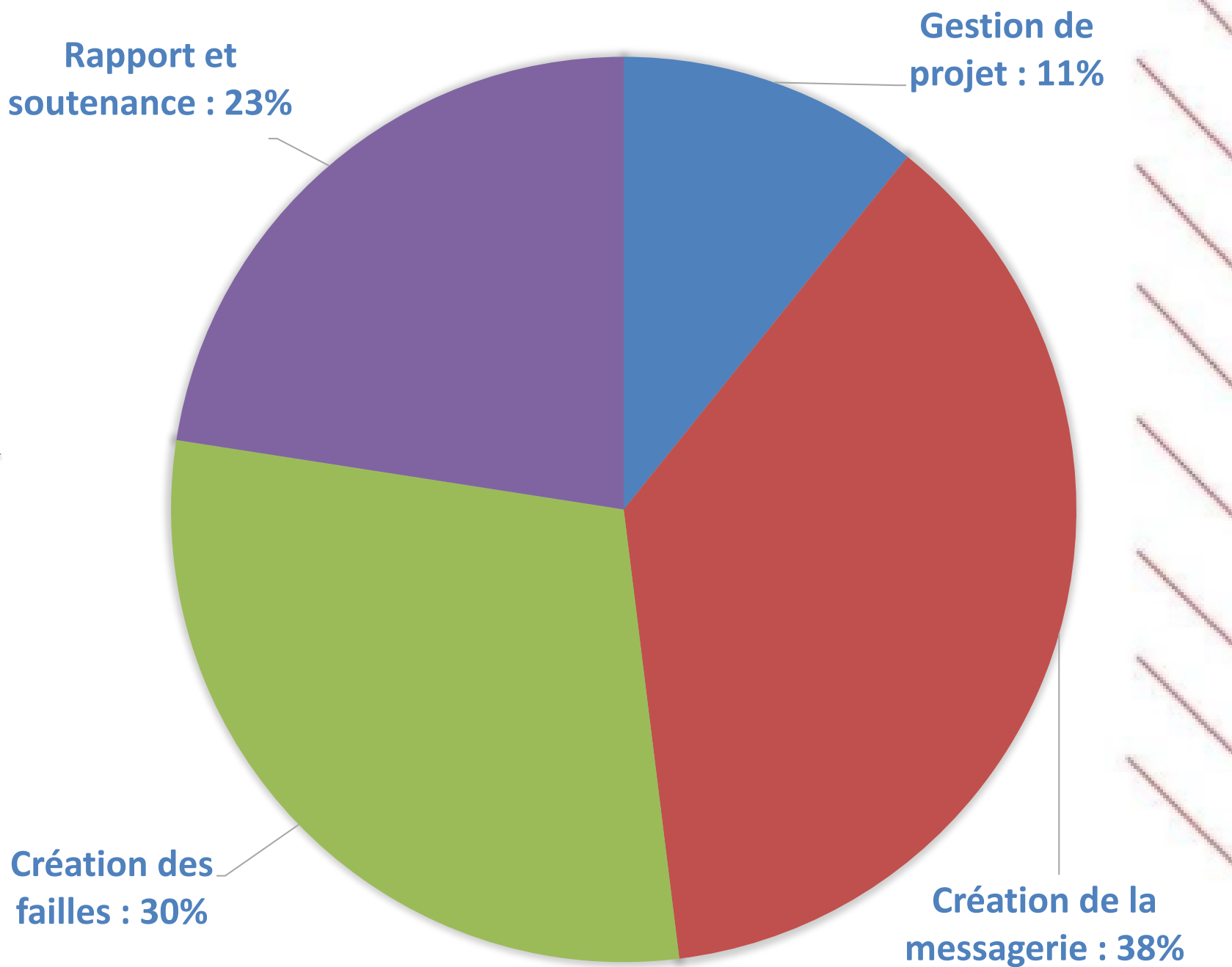


Gestion de projet – Les Gantt

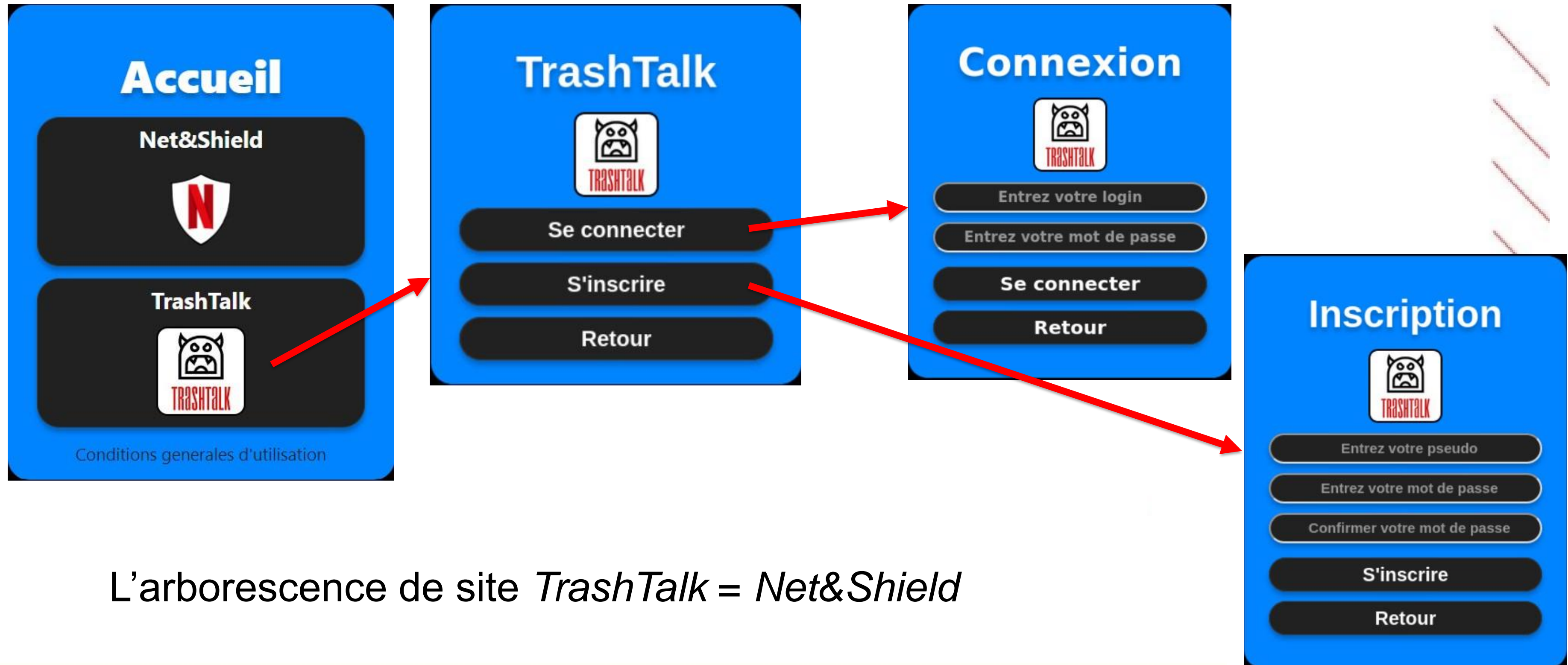
TEMPS **PRÉVISIONNEL** PAR ÉTAPES DU PROJET EN %



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

```
..  
..  
auth.php  
chat.php  
constants.php  
database.php  
trashtalktest.sql
```

Exemple backdoor cmd

passage dans sendMessage

```
(3) [...]  
▶ 0: Object { 0: "amis", Tables_in_trashtalk: "amis" }  
▶ 1: Object { 0: "messages", Tables_in_trashtalk: "messages" }  
▶ 2: Object { 0: "user", Tables_in_trashtalk: "user" }  
length: 3  
▶ <prototype>: Array []
```

passage dans sendMessage

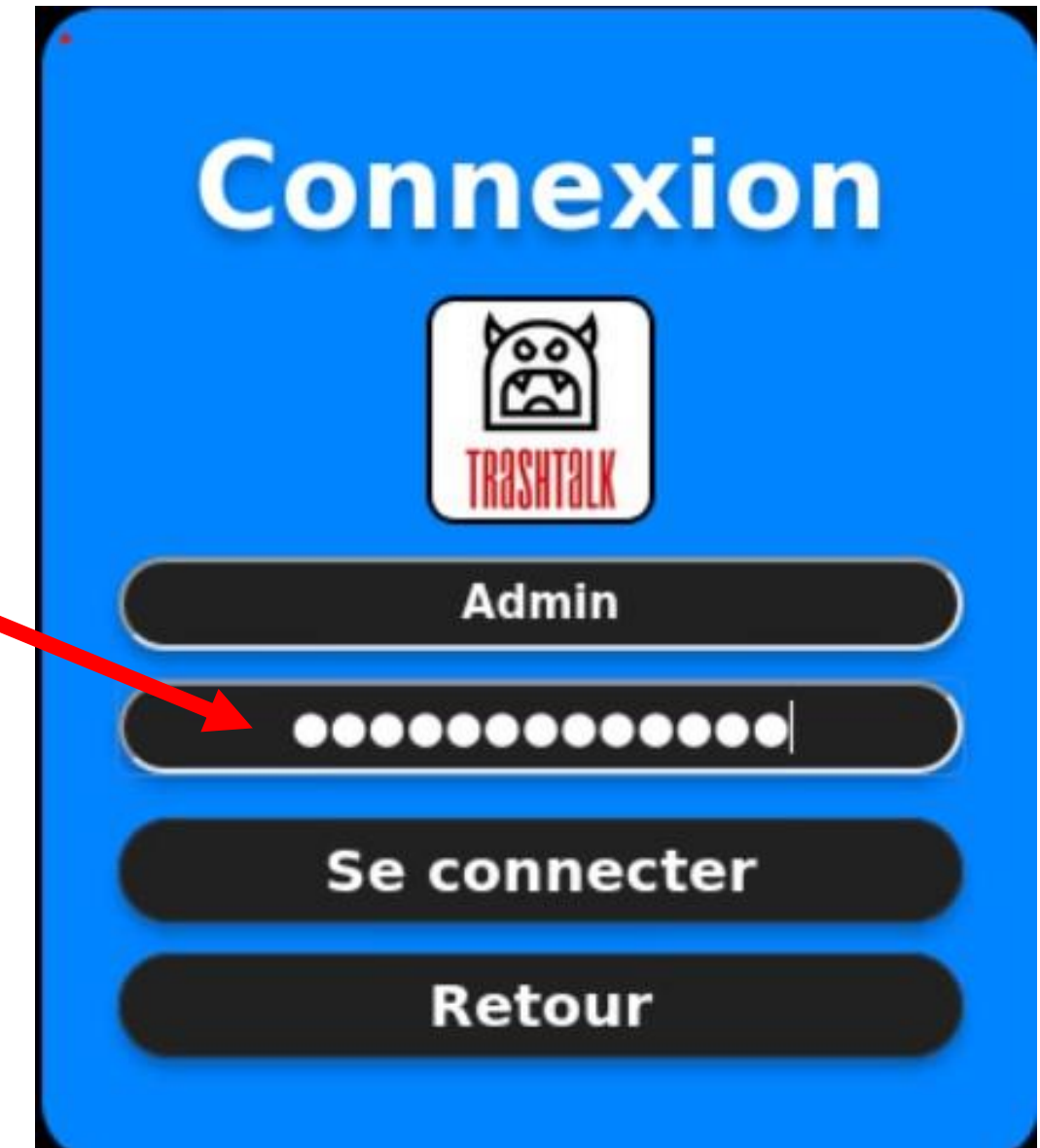
```
(9) [...]  
▶ 0: Object { 0: "1", 1: "Support", 3: "7c6a180b36896a0a8c02787eeafb0e4c", ... }  
▶ 1: Object { 0: "2", 1: "Admin", 3: "e3afed0047b08059d0fada10f400cle5", ... }  
▶ 2: Object { 0: "3", 1: "Emilio", 3: "819b0643d6b89dc9b579fd9c9094f28e", ... }  
▶ 3: Object { 0: "4", 1: "Edgar", 3: "34cc93ece0ba9e3f6f235d4af979b16c", ... }  
▶ 4: Object { 0: "5", 1: "NicoCharbo", 3: "db0edd04aaac4506f7edab03ac855d56", ... }  
▶ 5: Object { 0: "6", 1: "Quentin", 3: "218dd27aebeccecae69ad8408d9a36bf", ... }  
▶ 6: Object { 0: "7", 1: "Mathieu", 3: "00cdb7bb942cf6b290ceb97d6aca64a3", ... }  
▶ 7: Object { 0: "8", 1: "Hugo", 3: "b25ef06be3b6948c0bc431da46c2c738", ... }  
▶ 8: Object { 0: "9", 1: "Pierre", 3: "5d69dd95ac183c9643780ed7027d128a", ... }  
length: 9  
▶ <prototype>: Array []
```

Exemple
Backdoor
bdd

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



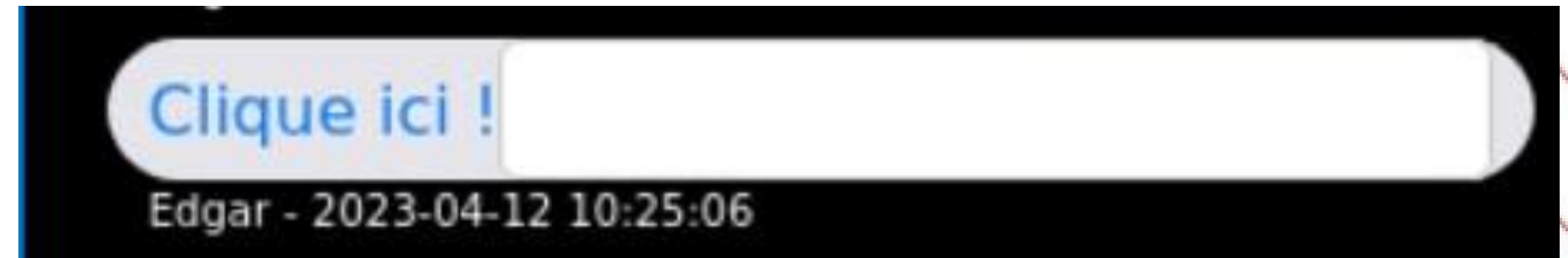
Les failles – Injection XSS

- L'injection XSS (Cross-Site Scripting) faille informatique qui permet d'injecter du code dans une page web.
- 3^e 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=%0Az1We1+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
- 5^e 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	messengerie.c...	/	Session	3	false	false	None
login	Emilio	messengerie.c...	/	Session	11	false	false	None
token	%0AjODmbYw+s9nBridX	messengerie.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

Apply a display filter ... <Ctrl-/>

Packet list

Narrow & Wide

Case sensitive

String

pass

Find

Cancel

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.11	192.168.0.100	TCP	74	57966 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
2	0.000389487	192.168.0.100	192.168.0.11	TCP	74	80 → 57966 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
3	0.000429126	192.168.0.11	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSv
4	0.000575063	192.168.0.11	192.168.0.100	HTTP	493	GET /TrashTalk/php/auth.php/authenticate HTTP/1.1
5	0.000847321	192.168.0.100	192.168.0.11	TCP	66	80 → 57966 [ACK] Seq=1 Ack=428 Win=64768 Len=0
6	0.004676389	192.168.0.100	192.168.0.11	HTTP	342	HTTP/1.1 200 OK (text/plain)
7	0.004691668	192.168.0.11	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=428 Ack=277 Win=30336 Len=0
8	0.008912444	192.168.0.11	192.168.0.100	HTTP	541	GET /TrashTalk/php/chat.php?request=UserId&pseud
9	0.010914994	192.168.0.100	192.168.0.11	HTTP	348	HTTP/1.1 200 OK (application/json)
10	0.023863215	192.168.0.11	192.168.0.100	HTTP	600	POST /TrashTalk/php/chat.php?request=statut HTTP
11	0.027199931	192.168.0.100	192.168.0.11	HTTP	334	HTTP/1.1 200 OK (application/json)
12	0.027841739	192.168.0.11	192.168.0.100	HTTP	545	GET /TrashTalk/php/chat.php?request=pseudos&user
13	0.027955853	192.168.0.11	192.168.0.100	TCP	74	57968 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
14	0.028091586	192.168.0.100	192.168.0.11	TCP	74	80 → 57968 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
15	0.028109944	192.168.0.11	192.168.0.100	TCP	66	57968 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSv
16	0.029837262	192.168.0.100	192.168.0.11	HTTP	423	HTTP/1.1 200 OK (application/json)
17	0.07	Tous les changements ont été enregistrés	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=1916 Ack=1184 Win=33536 Len=0
18	1.03	192.168.0.11	192.168.0.100	HTTP	554	GET /TrashTalk/php/chat.php?request=messages&use
19	1.038995789	192.168.0.100	192.168.0.11	HTTP	589	HTTP/1.1 200 OK (application/json)
20	1.039048733	192.168.0.11	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=2404 Ack=1707 Win=34560 Len=0
21	2.036129657	192.168.0.11	192.168.0.100	HTTP	554	GET /TrashTalk/php/chat.php?request=messages&use
22	2.039436081	192.168.0.100	192.168.0.11	HTTP	589	HTTP/1.1 200 OK (application/json)
23	2.039497777	192.168.0.11	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=2892 Ack=2230 Win=35712 Len=0
24	3.036149516	192.168.0.11	192.168.0.100	HTTP	554	GET /TrashTalk/php/chat.php?request=messages&use
25	3.039345268	192.168.0.100	192.168.0.11	HTTP	589	HTTP/1.1 200 OK (application/json)
26	3.039381645	192.168.0.11	192.168.0.100	TCP	66	57966 → 80 [ACK] Seq=3380 Ack=2753 Win=36736 Len=0

Host: messagerie.com\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n

Accept: */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Authorization: Basic RWRnYXI6cGFzc3dvcmQ0\r\n

Access-Control-Allow-Origin: http://192.168.0.100\r\n

0100 2c 65 6e 3d 51 2d 30 2e 35 0d 0a 41 63 63 65 70

0110 74 2d 45 6e 63 6f 64 63 67 3a 20 67 7a 69 70

0120 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70

0130 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20

0140 52 57 52 6e 59 58 49 36 63 47 46 7a 63 33 64 76

0150 63 6d 51 30 0d 0a 41 63 63 65 73 73 2d 43 6f 6e

0160 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f 72 69 67 69

0170 6e 3a 20 68 74 74 70 3a 2f 2f 31 39 32 2e 31 36

Encodé en Base 64

Edgar : password4

Projet M1 | 2023 | ISEN Brest

12

E. CHATEL, E. LEFEVRE | S. LANGLAIS

Les failles – Hash MD5

- Technique pour convertir un mot de passe en une chaîne de caractères incompréhensibles.
- 2e OWASP
- Algorithme plus fort

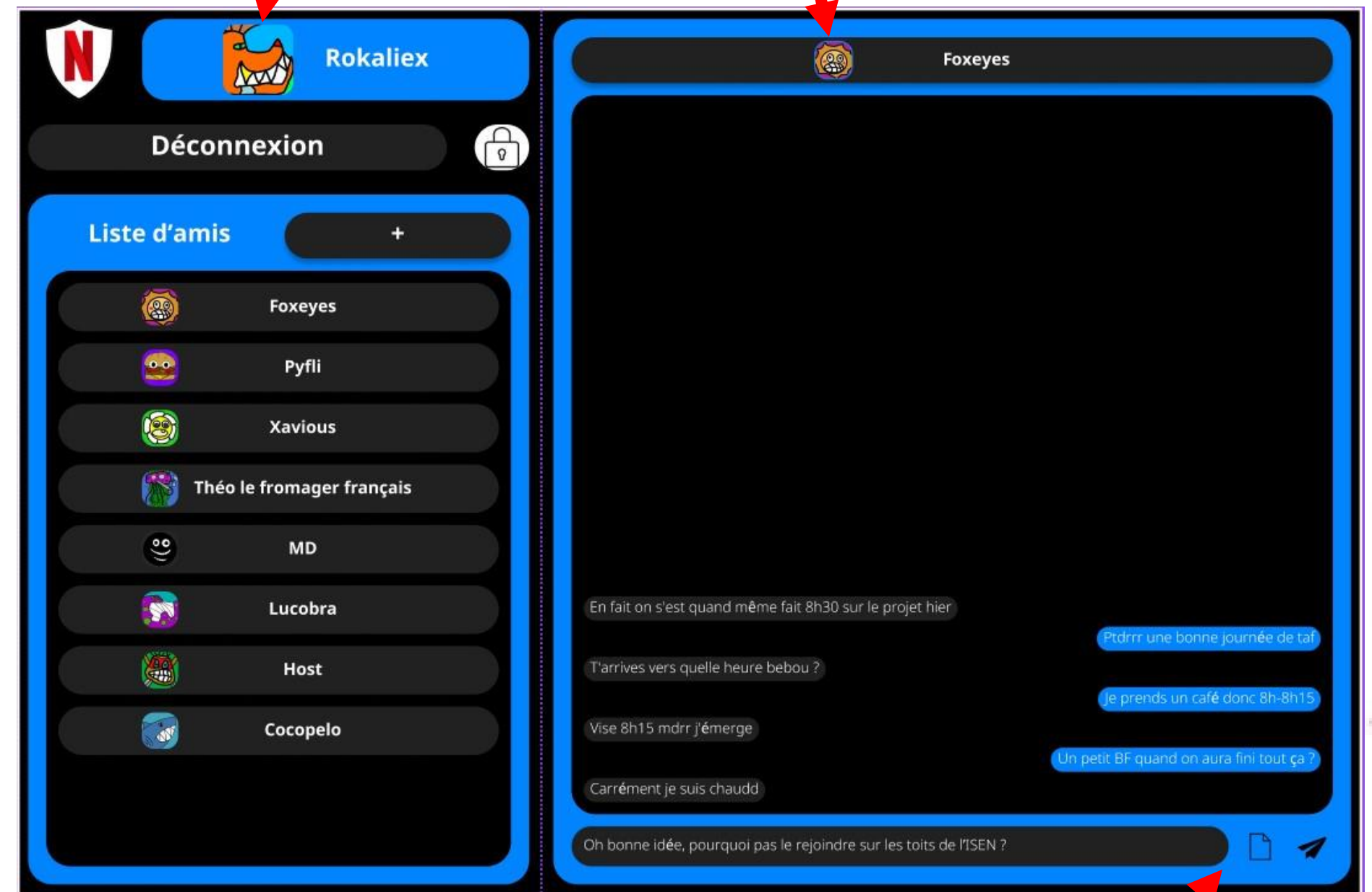
Mots de passe hachés en MD5

user_id	pseudo	image	hash	token	etat
1	Support	NULL	7c6a180b36896a0a8c02787eeafb0e4c	NULL	1
2	Admin	NULL	e3afed0047b08059d0fada10f400c1e5	JObUGmpEmkB+N0Bk	0
3	Emilio	NULL	819b0643d6b89dc9b579fd9c9094f28e	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

Ajout des photos de profil

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



Possibilité d'ajouter des images

Conclusion



Avez-vous des questions ?

