XWIKI NATIS

Prévention

Avoir les réflexes préventifs

XANATIS

Compétence demandée :
Avoir les réflexes préventifs

XWIKI NATIS

1. Les attaques MITM
2. Vérifications au Frontend
3. Injections
4. CSRF

XMNATIS

1. SSL/TLS Handshake protocol
2. Développement backend
3. Echappements
4. Tokens anti-CSRF

XWIKI SAS

XENATIS

SSL/TLS Handshake protocol

XMNATIS

Comment brouiller les pistes aux attaques MITM ?

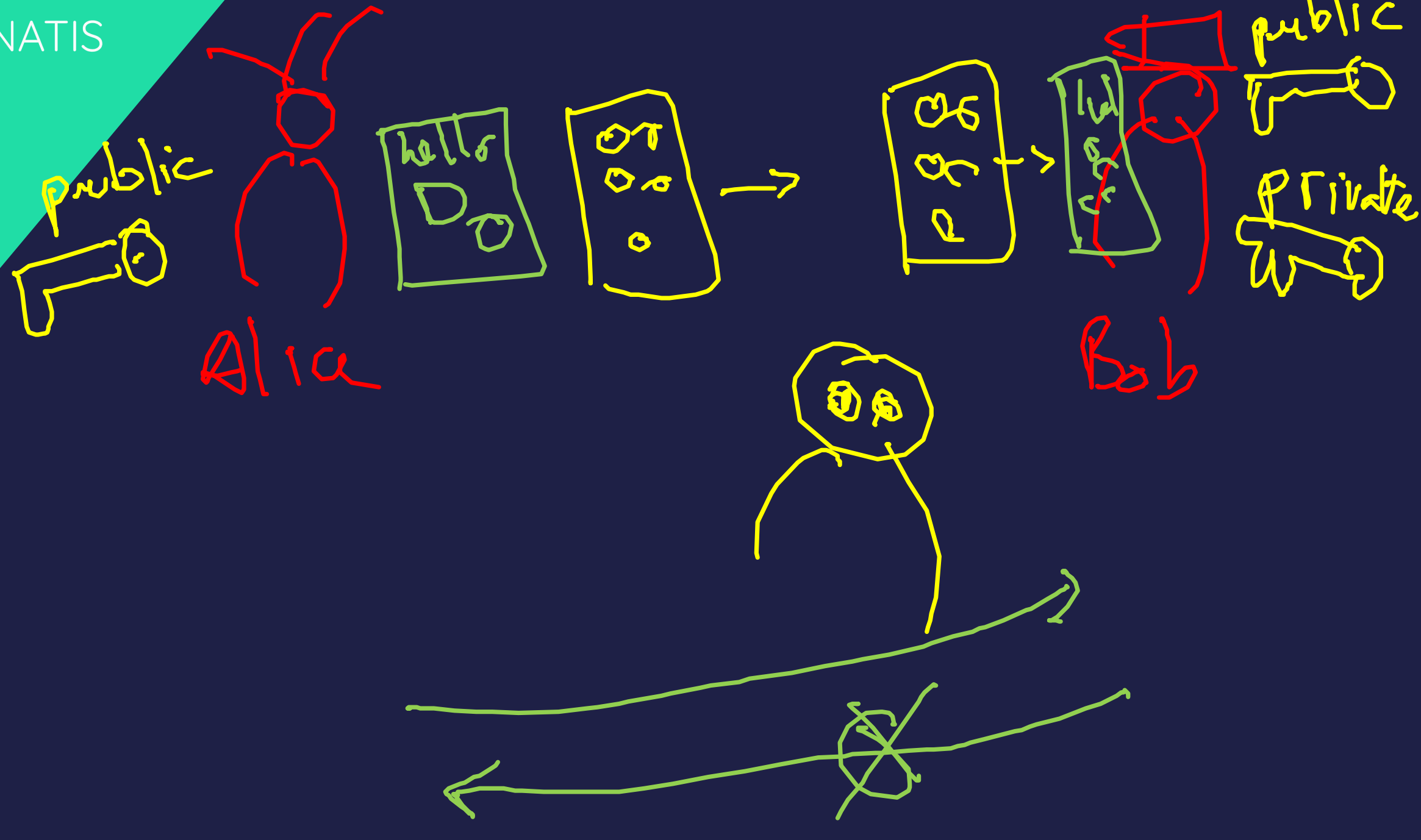
XWIKI SAS

XWIKI NATIS

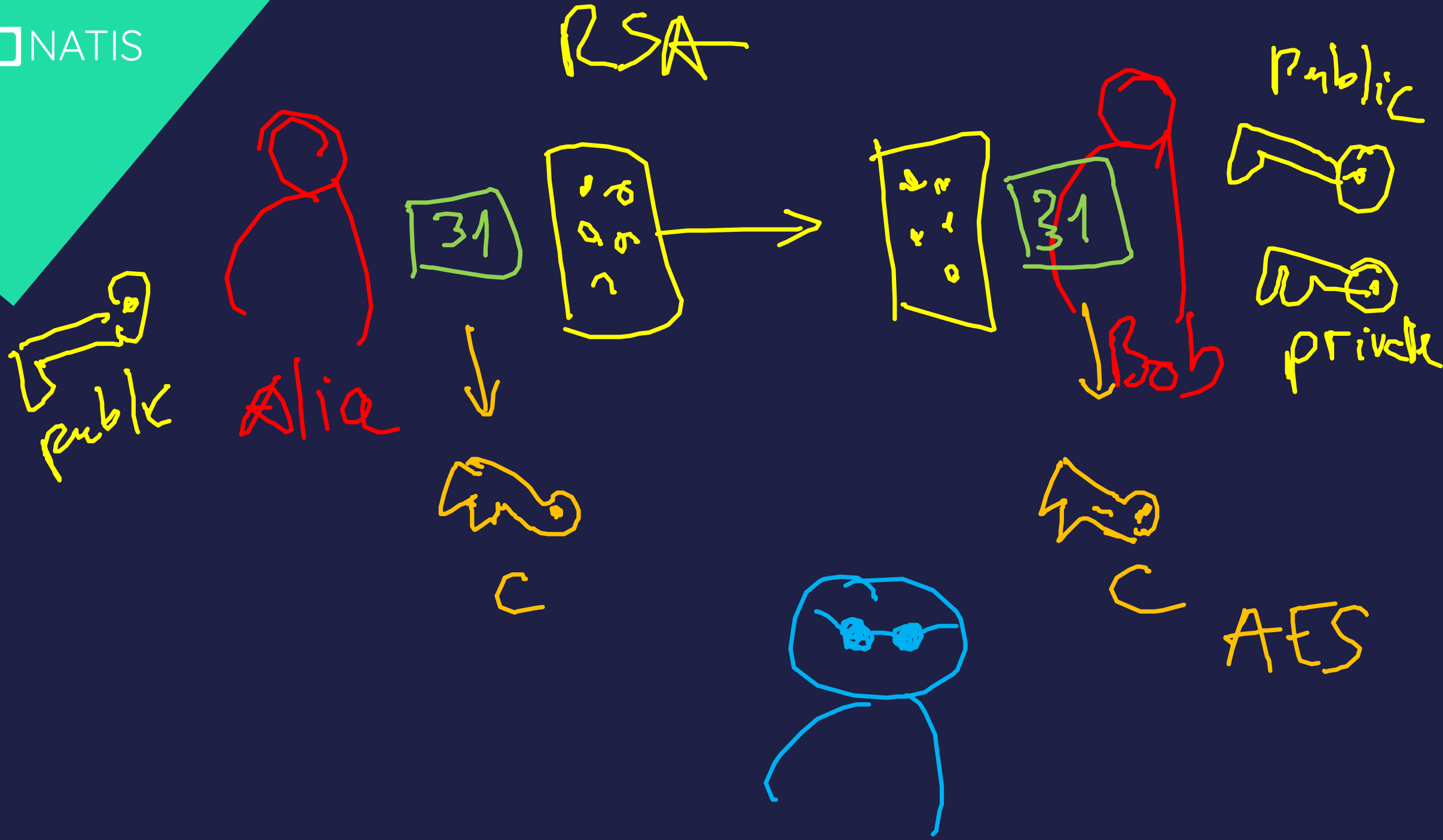
Le SSL (Secure Sockets Layer) et son successeur TLS (Transport Layer Security) sont des protocols cryptographiques utilisés pour crypter les communications entre logiciels

XWIKI

XWIKI NATIS



XKNATIS



XWIKI SAS

XWIKI SAS

XWIKI NATIS

La négotiation inclut le client hello message, le cipher suite, le server hello message et le certificat SSL/TLS, le hello done message et conclut sur l'échange de la pre-master et la cipher spec qui vont permettre de générer la clé symétrique utilisée dans la bulk encryption

XWIKI SAS

XWIKI SAS

XWIKI SAS

XWIKI SAS

XMNATIS

Parer les attaques MITM :

1. utiliser le protocol HTTPS basé sur le TLS Handshake protocol

XWIKI SAS

XWIKI NATIS

Développement backend

XWIKI NATIS

Comment éviter que les utilisateurs puissent modifier le code ?

XWIKI SAS

XWIKI NATIS

Développer le code au backend permet de ne pas rendre le code accessible aux visiteurs, ainsi il n’est pas modifiable

XWIKI SAS

XWIKI NATIS

Parer les modifications de code :

1. développez le code métier au backend

XWIKI SAS

XWIKI NATIS

Echappements

XWIKI NATIS

Quel caractère permet de passer du “texte” au “code” ?

XWIKI SAS

XWIKI NATIS

Échapper une chaîne de caratères signifie réduire l'ambiguité (de certains caratères) utilisés dans cette chaîne.

Echappant une chaine de caractères désactive une des fonctionnalités de certains caractères qui peuvent être ambigues

XWIKI NATIS

```
mysqli_real_escape_string ( mysqli $mysql , string $string ) : string
```

XEBNATIS

Le mieux reste d'utiliser les requêtes préparées

```php
$connexion = new PDO('mysql:host=localhost;dbname=c1377631c_training_security', 'c1377631c_public_user', 'Uek9dvTwWrMdVGka');
$requete = "SELECT COUNT(id) FROM fbi_user WHERE username = '$username' AND password = '$hashedPassword'";
$resultat = $connexion->query($requete);
$row = $resultat->fetch();
```

```php
$connexion = new PDO('mysql:host=localhost;dbname=c1377631c_training_security', 'c1377631c_public_user', 'Uek9dvTwWrMdVGka');
$requete = $connexion->prepare("SELECT COUNT(id) FROM fbi_user WHERE username = ? AND password = ?");
$requete->execute([$username, $password]);
$row = $requete->fetch();
```

XILINATIS

```
htmlentities ( string $string , int $flags = ENT_COMPAT , string|null $encoding = null , bool
$double_encode = true ) : string
```

XDNATIS

```php
foreach ($comments as $comment)
{
    echo '<div class="p-3 border m-3">' . $comment['content'] . '</div>';
}
```

```php
foreach ($comments as $comment)
{
    echo '<div class="p-3 border m-3">' . htmlentities($comment['content']) . '</div>';
}
```

XWIKI NATIS

Parer les modifications de code :

1. échapper les chaines de caractères pour ne pas laisser place à l’ambiguite

XWIKI SAS

XWIKI NATIS

Token Anti-CSRF

XWIKI SAS

XWIKI SAS

XWIKI SAS

XWIKI NATIS

Parer les attaques CSRF :

1. Générer un nombre à stocker dans le cookie
2. Inclure ce nombre dans l'URL

Le hacker ne saura pas quelle URL utiliser car il ne connait pas ce nombre (il n'a pas accès au cookie de la victime)

XWIKI SAS