XMNATIS

Vulnérabilités

Comprendre les mécanismes vulnérables

XWIKI NATIS

Compétence demandée :

Comprendre les mécanismes vulnérables

XWIKI NATIS

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

XWIKI SAS

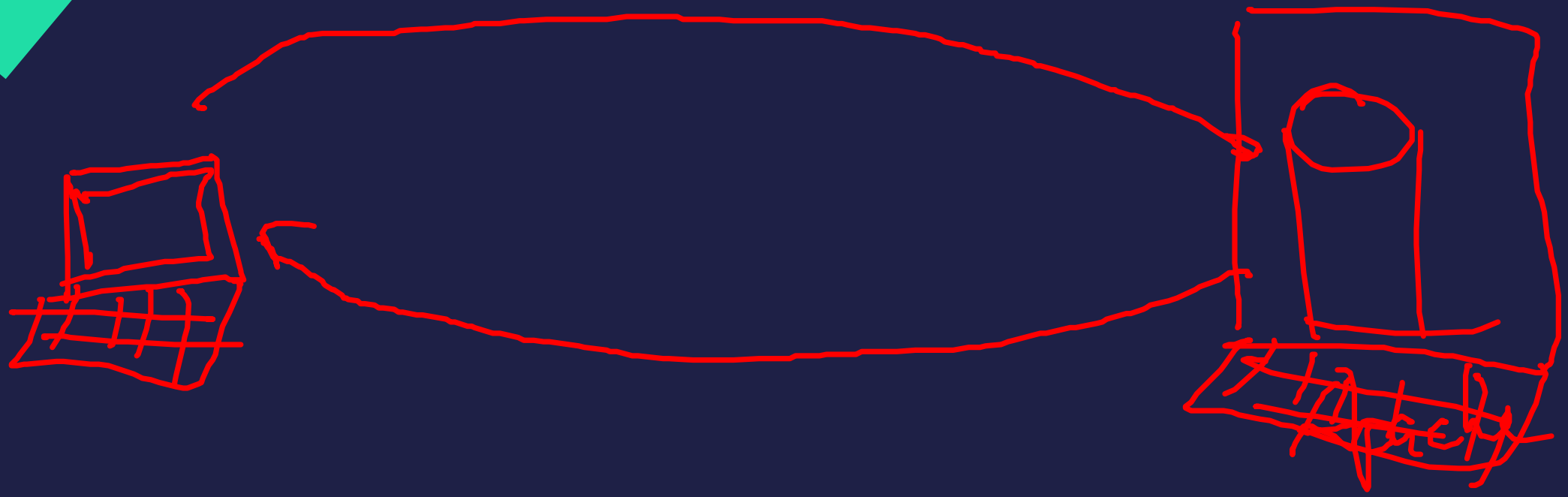
XMCO NATIS

LES ATTAQUES MITM

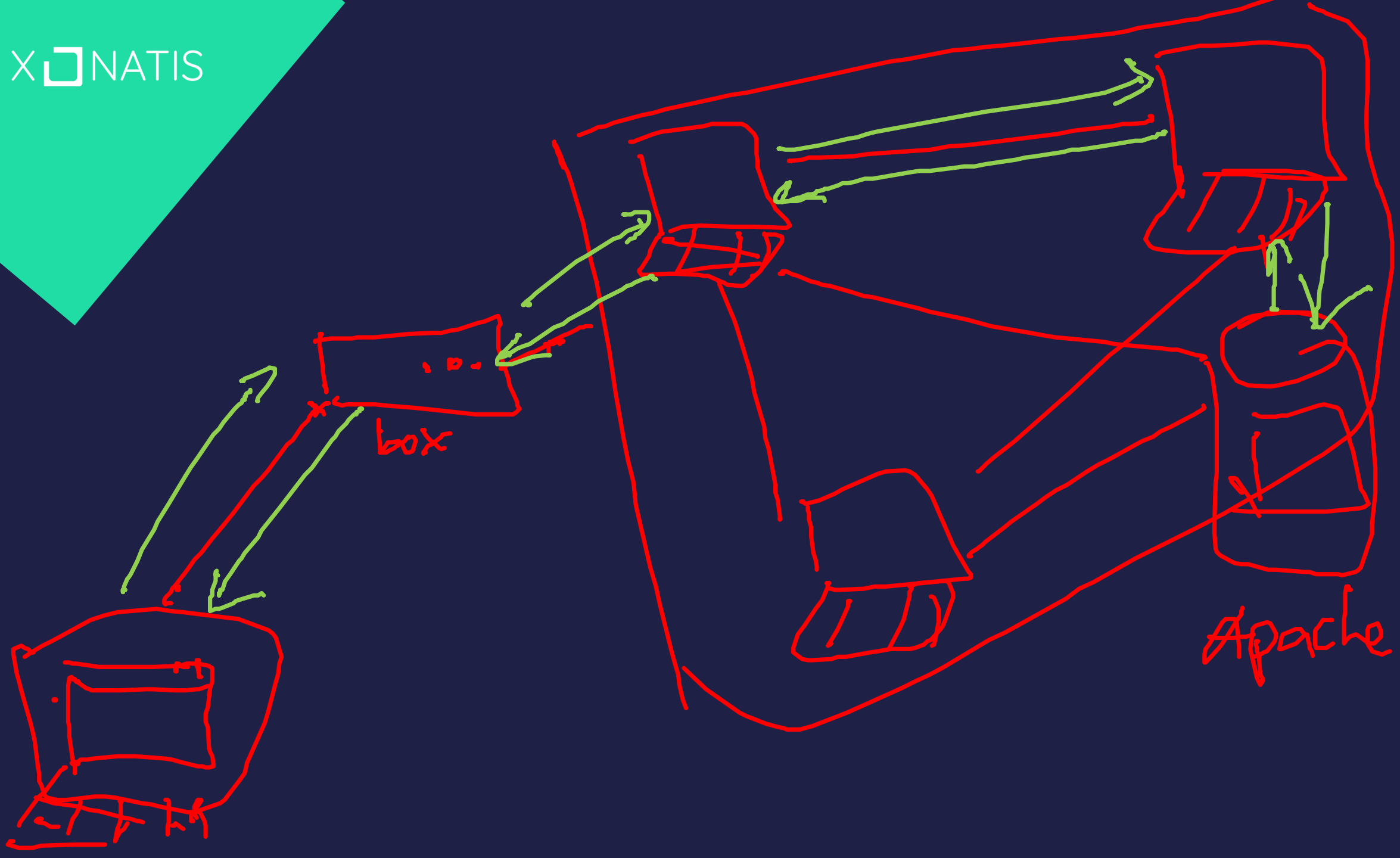
XMNATIS

Le Man In The Middle ?

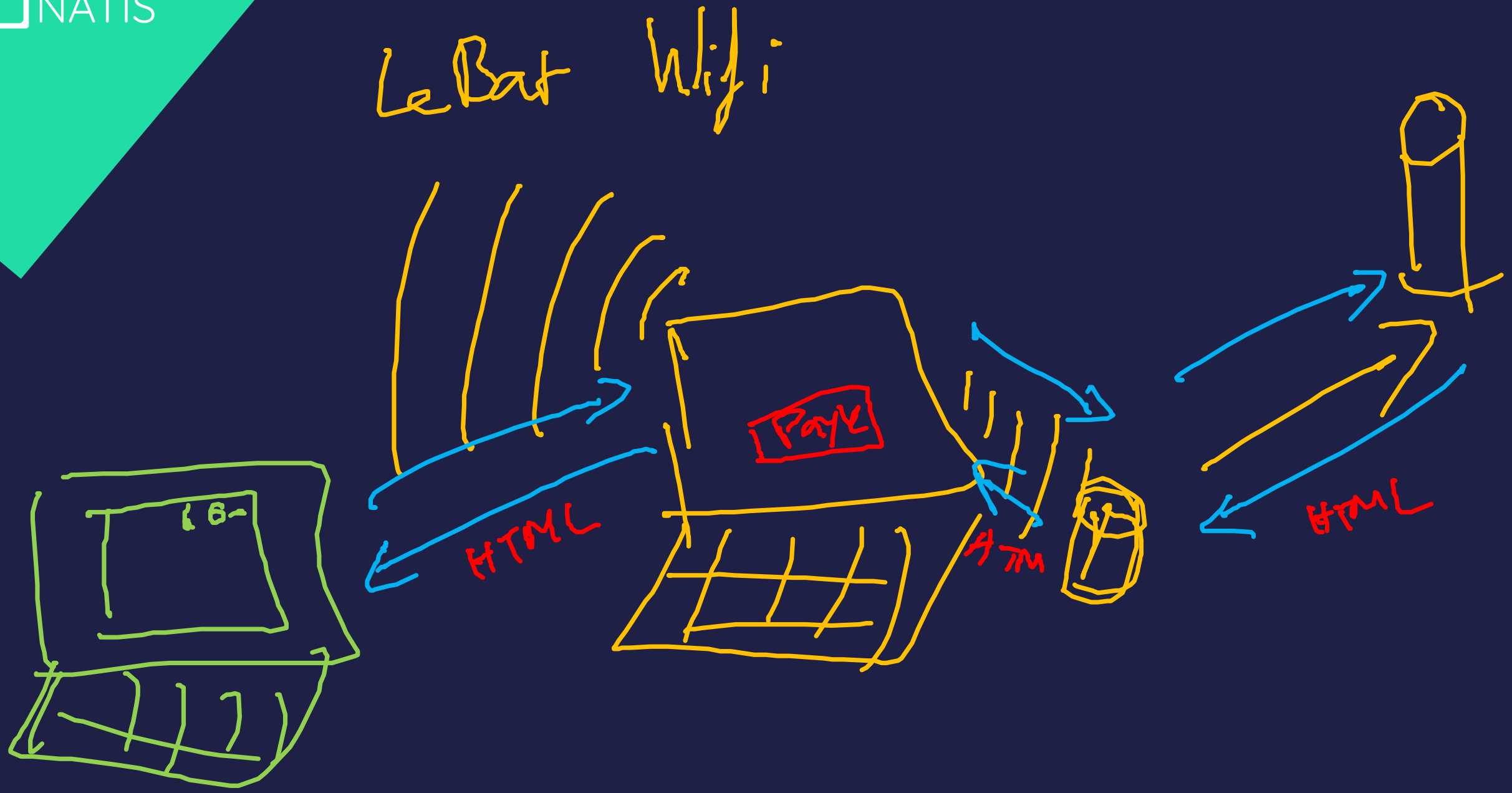
XWIKI NATIS



XWIKI NATIS



XWIKI



XWIKI SAS

XWIKI SAS

XWIKI SAS

XWIKI SAS

XMNATIS

Une attaque MITM (Man In The Middle) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

XWIKI NATIS

Une attaque MITM est facilement réalisable sur une connexion HTTP, mais plus difficilement avec connexion est chiffrée (mais pas impossible !)

XWIKI NATIS

Objectifs :

1. modifier les requêtes HTTP vers le serveur (en se faisant passer pour le client)

2. modifier les réponses HTTP vers le client (en se faisant passer pour le serveur)

XMNATIS

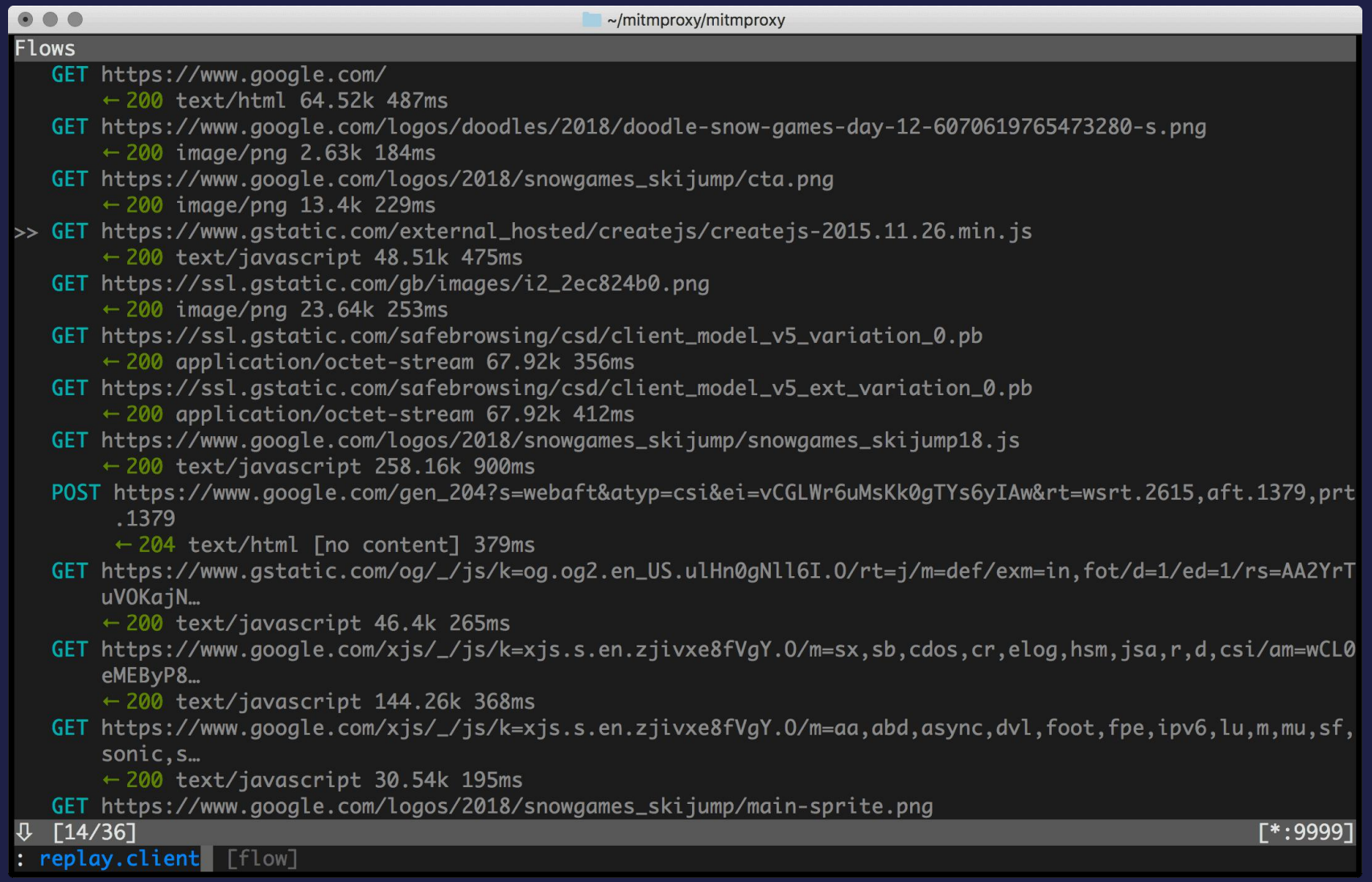
Mise en place :

1. Le client doit, pour se connecter à internet, se connecter à notre ordinateur (peut se faire par un réseau Wifi invité)

2. Tracer tout le trafic (entrant et sortant)

3. Ecrire un programme pour modifier ce trafic

XEBIA NATIS


~/mitmproxy/mitmproxy
Flows
GET https://www.google.com/
← 200 text/html 64.52k 487ms
GET https://www.google.com/logos/doodles/2018/doodle-snow-games-day-12-6070619765473280-s.png
← 200 image/png 2.63k 184ms
GET https://www.google.com/logos/2018/snowgames_skijump/cta.png
← 200 image/png 13.4k 229ms
>> GET https://www.gstatic.com/external_hosted/createjs/createjs-2015.11.26.min.js
← 200 text/javascript 48.51k 475ms
GET https://ssl.gstatic.com/gb/images/i2_2ec824b0.png
← 200 image/png 23.64k 253ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb
← 200 application/octet-stream 67.92k 356ms
GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
← 200 application/octet-stream 67.92k 412ms
GET https://www.google.com/logos/2018/snowgames_skijump/snowgames_skijump18.js
← 200 text/javascript 258.16k 900ms
POST https://www.google.com/gen_204?s=webaft&atyp=csi&ei=vCGLWr6uMsKk0gTYs6yIAw&rt=wsrt.2615,aft.1379,prt.1379
← 204 text/html [no content] 379ms
GET https://www.gstatic.com/og/_/js/k=og.og2.en_US.ulHn0gNll6I.O/rt=j/m=def/exm=in,fot/d=1/ed=1/rs=AA2YrTuVOKajN…
← 200 text/javascript 46.4k 265ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.O/m=sx,sb,cdos,cr,elog,hsm,jsa,r,d,csi/am=wCL0eMEByP8…
← 200 text/javascript 144.26k 368ms
GET https://www.google.com/xjs/_/js/k=xjs.s.en.zjivxe8fVgY.O/m=aa,abd,async,dvl,foot,fpe,ipv6,lu,m,mu,sf,sonic,s…
← 200 text/javascript 30.54k 195ms
GET https://www.google.com/logos/2018/snowgames_skijump/main-sprite.png
⇩ [14/36] [*:9999]
: replay.client [flow]

XWIKI SAS

XWIKI NATIS

LES VERIFICATIONS AU FRONT

XWIKI NATIS

En termes de sécurité, y a-t-il une différence entre :

1. écrire du code au front
2. écrire du code au back

?

XWIKI SAS

XWIKI NATIS

L’utilisateur a toujours accès en lecture et en modification à un code au front car ce code s’exécute sur la machine du client

XWIKI NATIS

L’utilisateur peut donc modifier
l’exécution des codes suivants :

- HTML
- CSS
- Javascript

XWIKI NATIS

Objectifs :

1. modifier le comportement d’un site internet (à condition que toutes les données nécessaires aient été téléchangées chez le client)

XDNATIS

Mise en place :

1. Ouvrir les outils de développement du navigateur
2. Modifier le DOM (HTML)
3. Modifier le code (Javascript ou CSS)
4. Créer une extension pour automiser les tâches

XWNATIS

Lighthouse Elements Console Memory Sources Network

top Filter Default levels No Issues

```
function supprimerElement(classCss) {
    let elements = document.getElementsByClassName(classCss);
    let element = elements[0];
    element.remove();
}

function supprimerClassCss(classCss) {
    let elements = document.getElementsByClassName(classCss);
    let element = elements[0];
    element.classList.remove(classCss);
}

supprimerElement('paywall');
supprimerElement('catcher--inline');
supprimerElement('article__status');
supprimerClassCss('article__content--restricted-media');
supprimerClassCss('article__wrapper--premium');
supprimerClassCss('zone--article-premium');
```

Le Monde

Se connecter S'abonner

La suite est réservée aux abonnés. Déjà abonné ? Se connecter

- Accédez à **tous les contenus du Monde** en illimité.
- Soutenez **le journalisme d'investigation et une rédaction indépendante**.
- Consultez le **journal numérique et ses suppléments, chaque jour avant 13h**.

S'abonner pour lire la suite

Contenus sponsorisés par **Outbrain**

PUBLICITÉ LA 1ERE

Maré : le grand chef Hippolyte Sinewami-Htamumu intronisé ce mardi

PUBLICITÉ FORGE OF EMPIRES

Si tu dois tuer du temps sur ton ordi, ce jeu de Civilization est incontournable. Pas d'installation

PUBLICITÉ SEDOMICILIER.FR/CONTACT

Découvrez comment domicilier votre entreprise à Paris avec un expert de SeDomicilier !

Dans la même rubrique

XWIKI SAS

XWIKI NATIS

LES INJECTIONS DE CODE

XWIKI NATIS

Que se passe-t-il lorsque l’utilsateur entre du code dans les inputs ou dans les liens ?

XWIKI SAS

XWIKI NATIS

Rien ne force l’utilisateur a joué le jeu !
N’importe quel visiteur peut entrer du code dans les inputs et dans les liens des pages internet

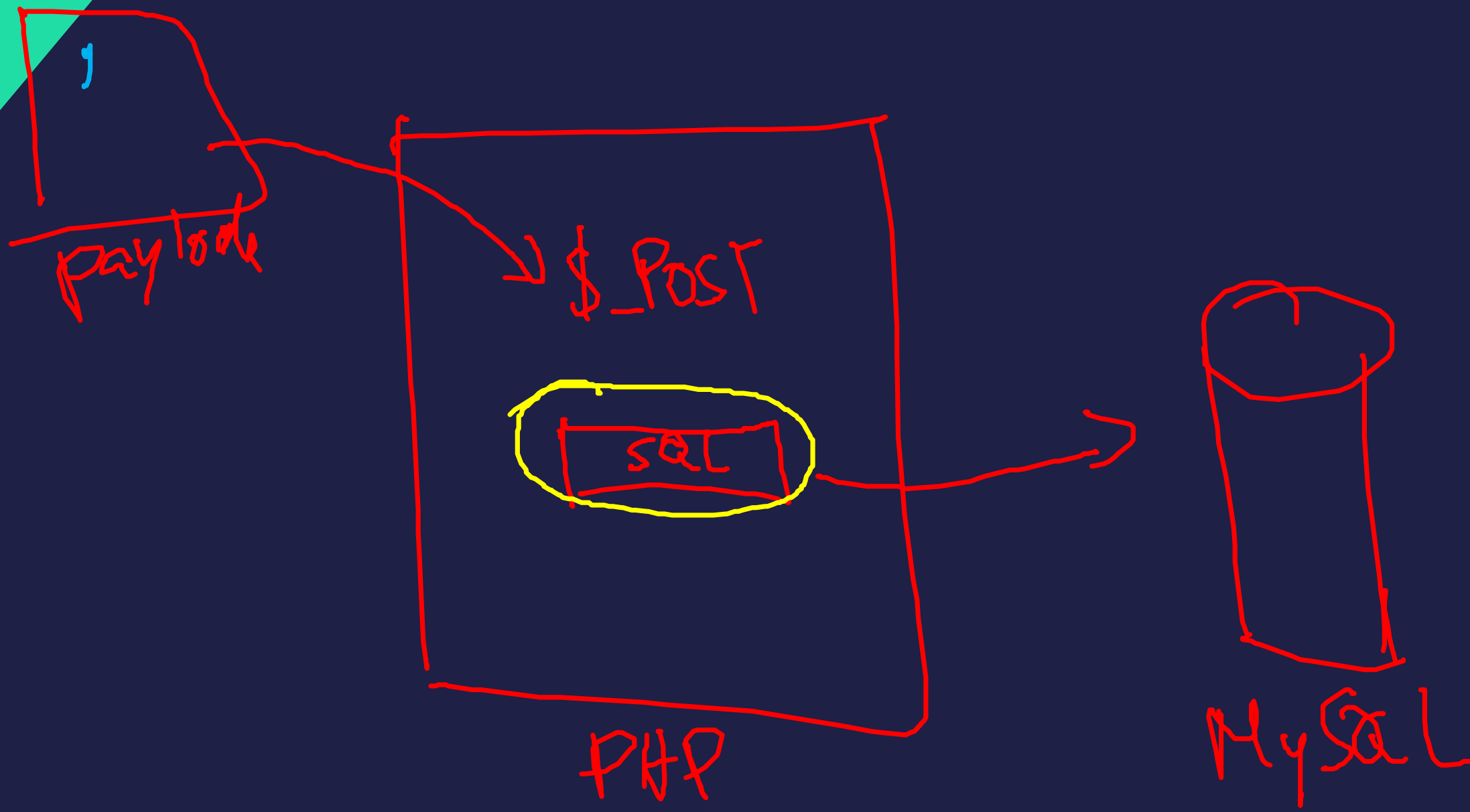
XMNATIS

Une injection SQL est une attaque faite lorsque l'utilisateur écrit du code SQL dans les éléments perméables d'un site internet (inputs ou URL)

XWIKI NATIS

Une injection SQL est une attaque faite lorsque l'utilisateur écrit du code SQL dans les éléments perméables d'un site internet (inputs ou URL)

XDNATIS



XWIKI SAS

XWIKI NATIS

Objectifs :

1. accéder à des données de la base de données

2. exécuter des requêtes SQL à l'intérieur de la base de données (pour supprimer des données par exemple)

XWIKI NATIS

Mise en place :

1. Prédire comment le backend envoie les requêtes SQL (sous forme de requêtes préparées ou non)

2. Ecrire une moitié de requête SQL pour que, une fois combiner avec le code du backend, elle devienne une requête SQL complète en utilisant les caractères suivants : ‘ ; et --

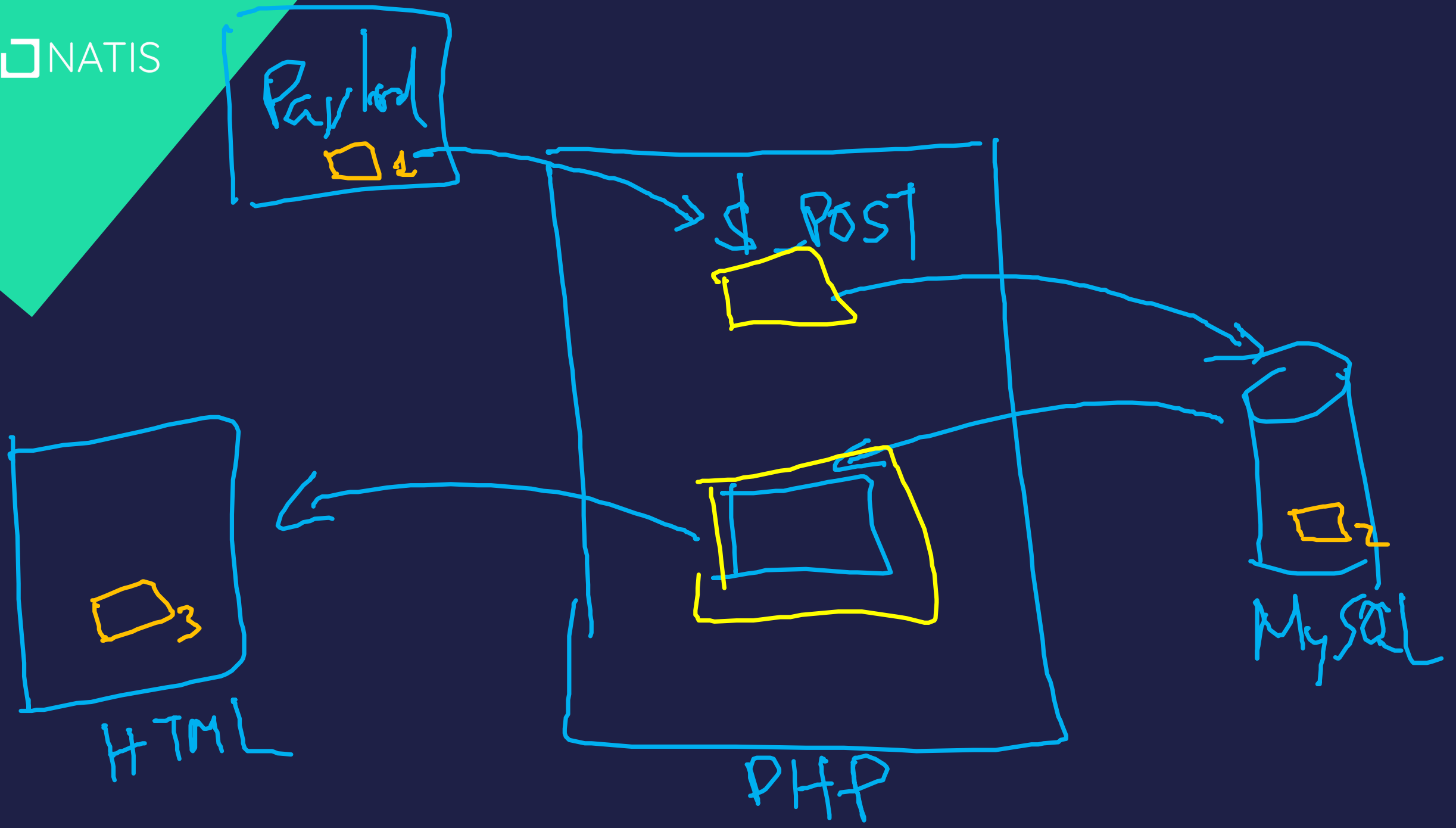
XDNATIS


NATIONAL SECURITY BRANCH
FEDERAL BUREAU OF INVESTIGATION
F.B.I.
' OR 2=2; --
Valider

XWIKI NATIS

Une injection XSS est une attaque faite lorsque l'utilisateur écrit du code HTML/Javascript dans les éléments perméables d'un site internet (inputs ou URL)

XWIKI NATIS



XWIKI SAS

XWIKI NATIS

Une injection XSS est une attaque faite lorsque l'utilisateur écrit du code HTML/Javascript dans les éléments perméables d'un site internet (inputs ou URL)

XWIKI NATIS

Objectifs :

1. exécuter du code Javascript du navigateur des visiteurs du site

2. modifier la structure du site pour tromper les visiteurs du site

XWIKI NATIS

Mise en place :

1. Cibler les pages qui affichent ce que l'utilisateur a entré (commentaires, recherches etc.)

2. Entrer du code Javascript pour modifier la structure de la page

XWIKI

magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

```
<script>
let element = document.getElementById("formulaire");
element.innerHTML = "<a href=\\"https://www.paypal.com/donate/?
hosted_button_id=EDR23XH22FMHN\\" class=\\"btn btn-primary\\">Payez ici pour payer
moins cher</a>";
</script>
```

Poster

XWNATIS

SUSHI

Plat de sushi délicieux

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Payez ici pour payer moins cher

XMNATIS

Les injections de base sont les injections SQL et les injections XSS.

Il faut absolument les connaître !

XWIKI SAS

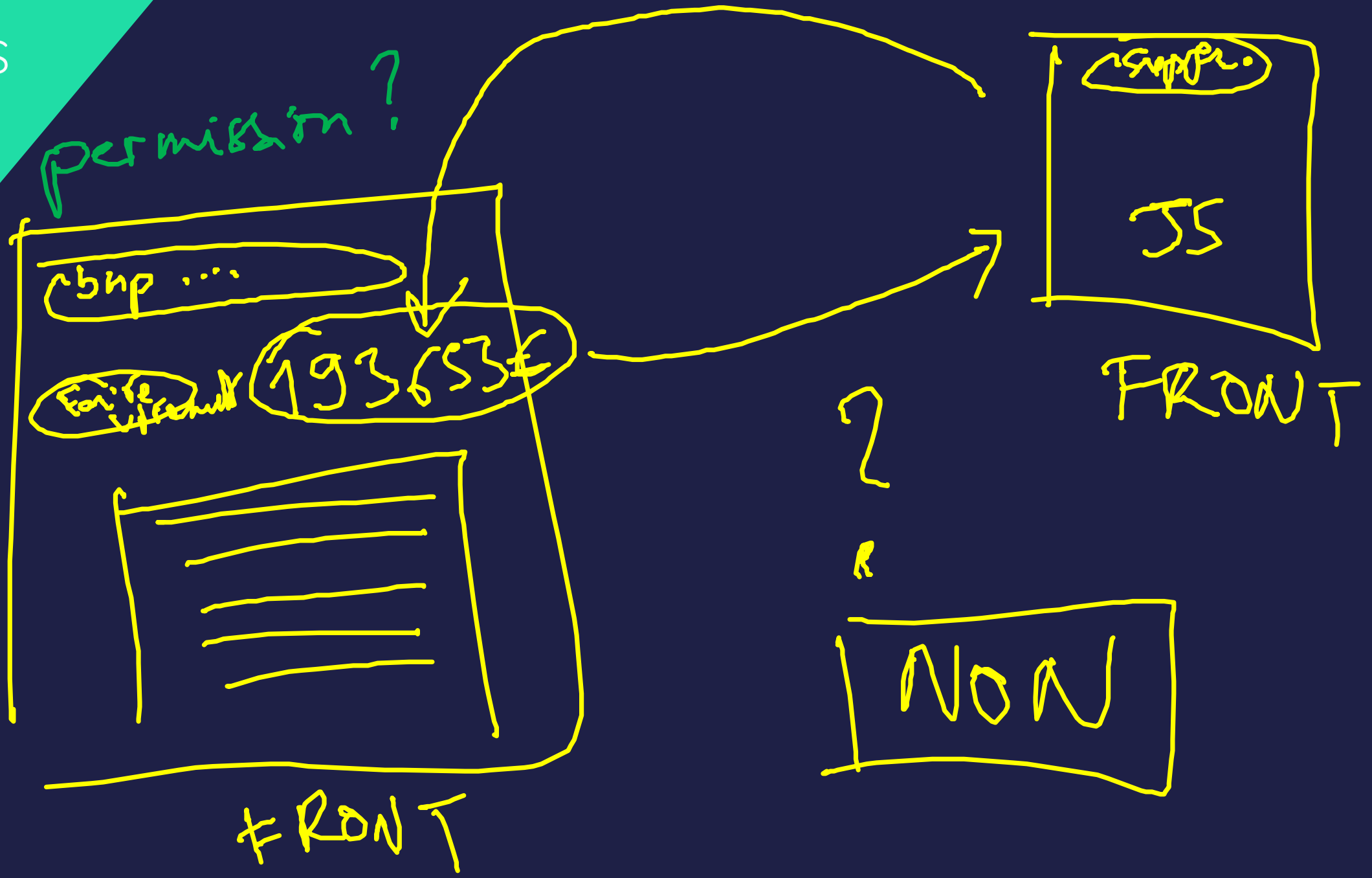
XWIKI NATIS

LES ATTAQUES CSRF

XWIKI NATIS

Doit-on empecher des sites différents (origine différente) de commnuniquer entre eux ?

XWIKI SAS



XWIKI NATIS

Traversée d'origine

CROSS-ORIGIN

XWIKI SAS

XWIKI SAS

XWIKI SAS

XEBIA NATIS

https://w3school.com:443

L'origine d'un site internet est déterminée par les éléments suivants :

http://localhost:4200

- (http) : le protocol
- (localhost) : le hostname
- (4200) : le port

XDNATIS

https://w3schoool.com

↓

→ https://w3school.com:443

---

https://lemonde.fr

↓

→ https://lemonde.fr:443

---

http://localhost

↓

→ http://localhost:80

XWIKI SAS

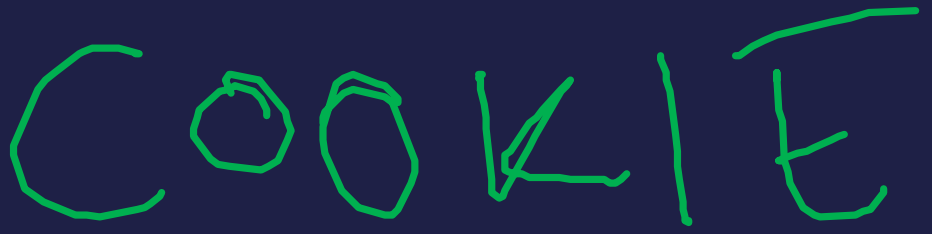
XWIKI SAS

XWIKI NATIS

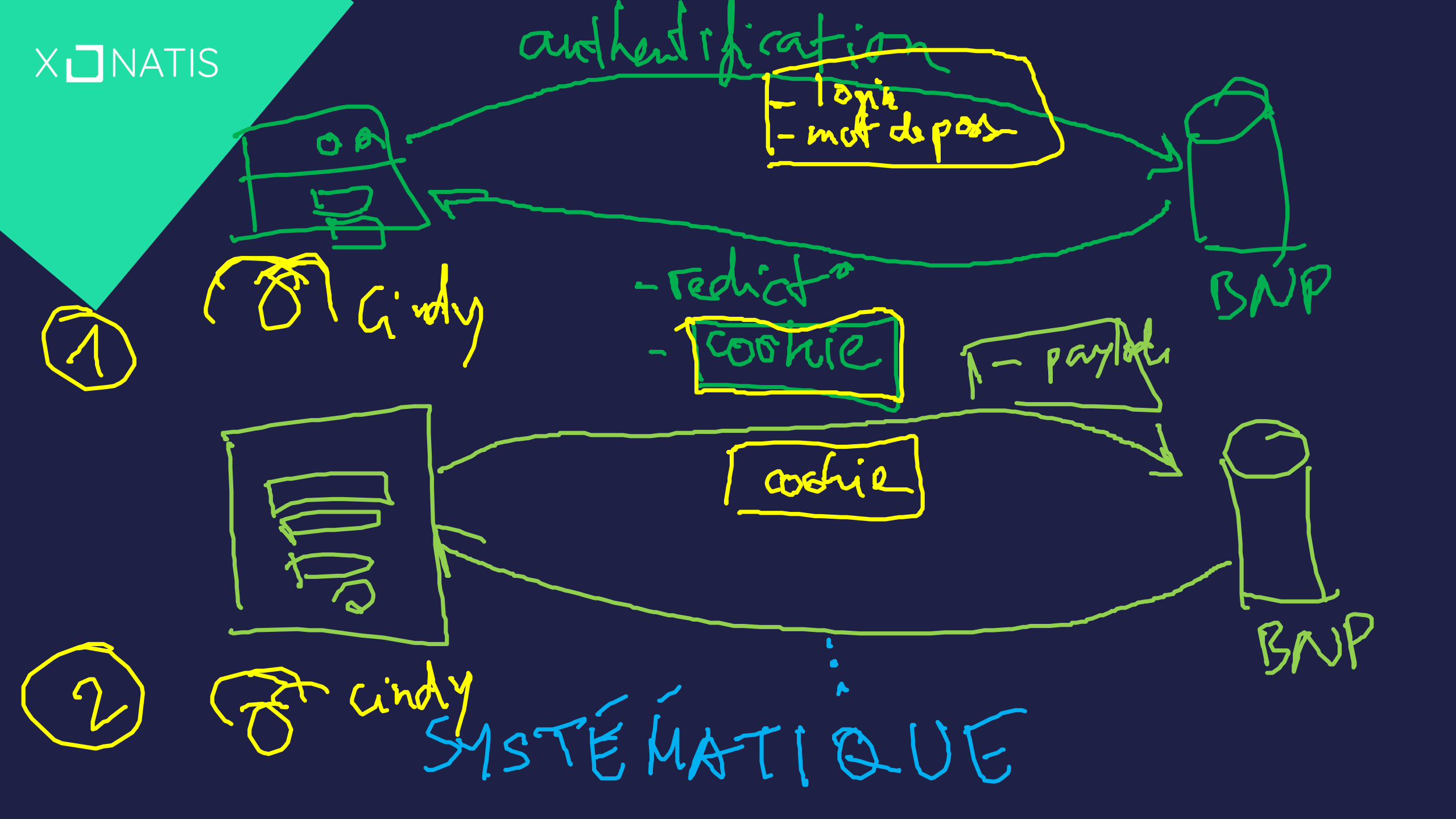
Same-Origin Policy (SOP) est implémenté dans les navigateurs pour empêcher 2 sites internet d'orgine différente de communiquer

XWIKI NATIS

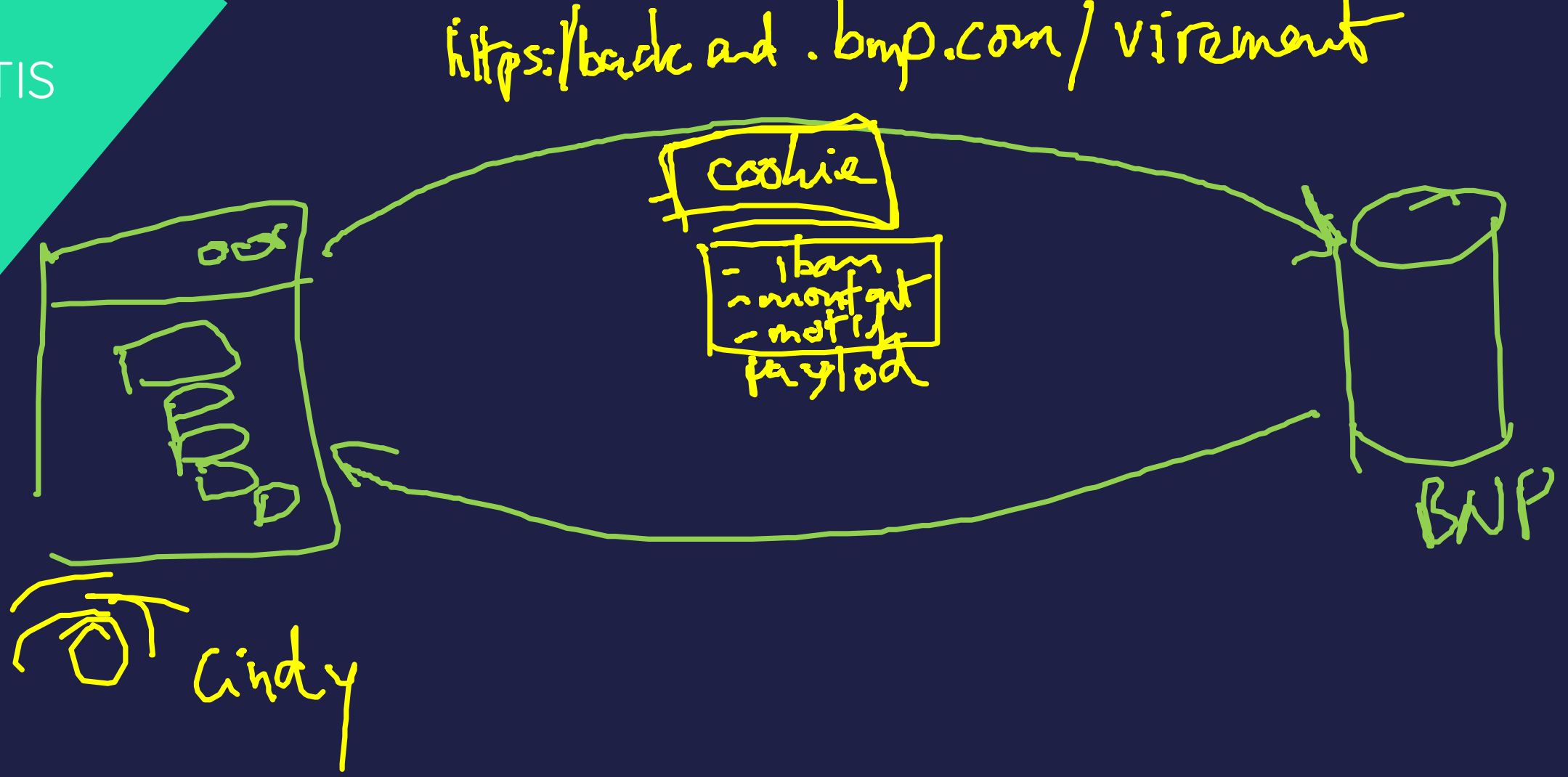
Comment un site se souvient de nous ?



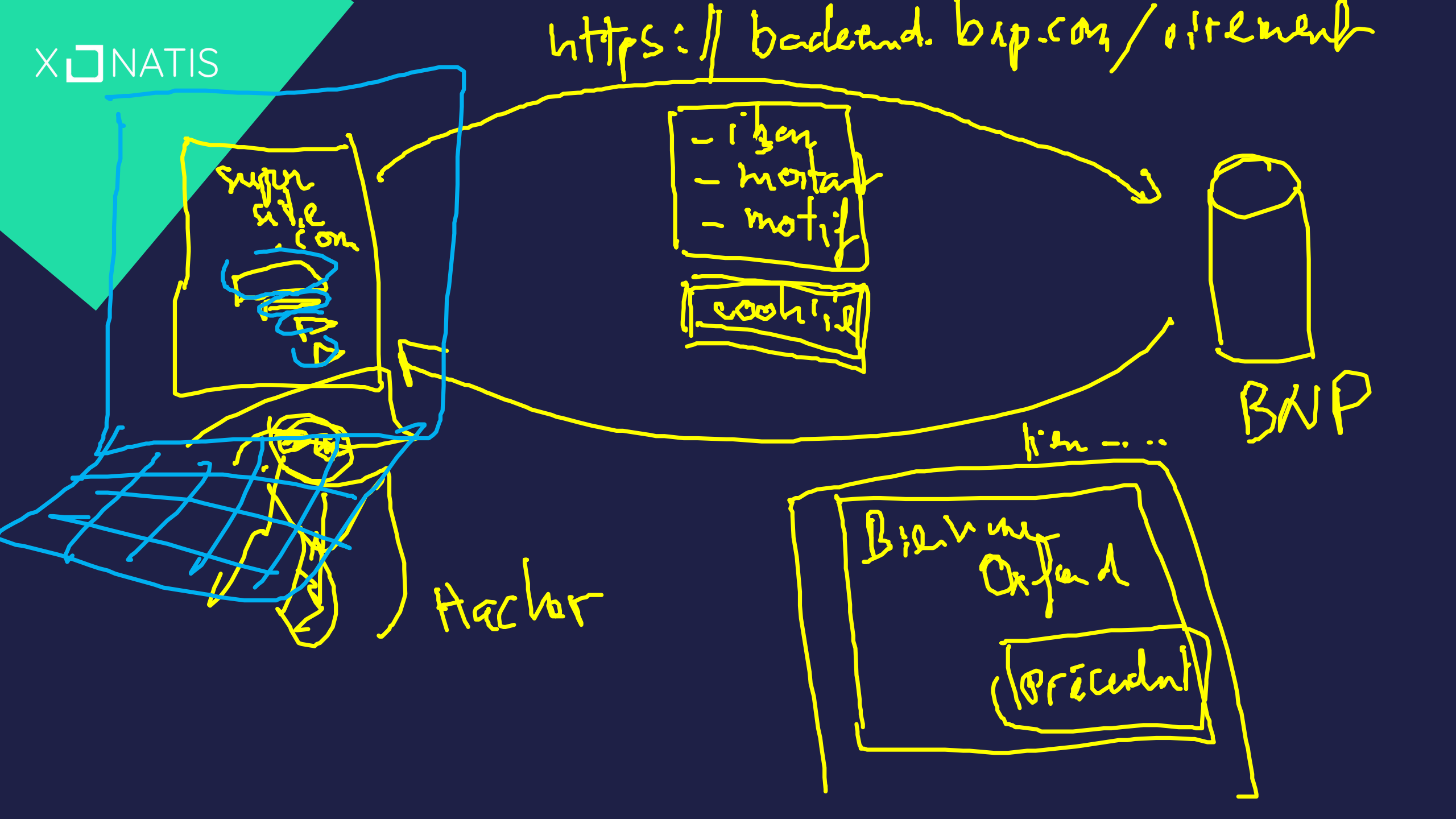
XEBIA NATIS


authentification
- login
- mot de pass
BNP
Cindy
1
- redirect
- cookie
- payload
cookie
BNP
2
cindy
SYSTÉMATIQUE

XKNATIS


https://backend.bnp.com/virement
cookie
- iban
- montant
- motif
payload
BNP
Cindy

XEBIA NATIS


https://backend.bnp.com/virement
- iban
- montant
- motif
cookie
BNP
Hacker
Virement
Ordre
précédent

XWIKI SAS

XWIKI SAS

XWIKI SAS

XWIKI NATIS

Le Cross Site Request Forgery (CSRF)

XWIKI NATIS

Une attaque CSRF consiste à tromper les visiteurs en les redirigeant vers une page d'action (/delete par exemple) pour qu'ils effectuent des actions (avec leur login) en leur nom

XWIKI SAS

Objectifs :

1. forcer les visiteurs à effectuer des actions en leur nom

XMNATIS

Mise en place :

1. Mettre un lien ou une redirection vers une page d’action et profiter que le site cible authentifie automatique le visiteur (par ses cookies)

XWIKI NATIS

```php
<?php

header('LOCATION: bnpparibas.fr/virements/399405/9483/effectuer');
```

XWIKI SAS