

MODULE 02

SÉANCE WEB 01

TP D'INFORMATIQUE

Durée 2h30

CONFIGURATION DMX ET ANALYSE WIRESHARK

BLOC DE COMPÉTENCES

U5 - EXPLOITATION ET MAINTENANCE DE RÉSEAUX INFORMATIQUES

COMPÉTENCE(S)

C09 - INSTALLER UN RÉSEAU INFORMATIQUE

OBJECTIF PÉDAGOGIQUE

Installation et configuration de matériel DMX : analyse Wireshark des données.

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- | | |
|-----------------------------------------------------------------------------------|----------|
| • Réseaux de terrain | Niveau 2 |
| • Réseaux informatiques (protocoles, équipements et outils usuels et industriels) | Niveau 3 |
| • Outils logiciels d'évaluation, de traçabilité de l'information | Niveau 3 |

CONNAISSANCES OPÉRATIONNALISÉES

- | | |
|--------------------------------------------------------------------|----------|
| • Installer et configurer un matériel à partir d'une documentation | Niveau 3 |
| • Analyser une communication réseau avec Wireshark | Niveau 2 |

TD

Étude de la norme et de la documentation du matériel

A partir de la norme DMX, donner la composition d'une trame DMX :

Quelles sont les durées maximum et minimum d'une trame DMX ?

D'après la documentation du SPOTEX15 (version 5 canaux), donner la composition de la trame permettant les effets suivants :

PAN à mis parcours, TILT au maximum, clignotement rapide d'une fleur rose :

PAN au minimum, TILT à mis parcours, motif "éclairs" Arc-en-ciel avec 50% de lumière :

En étudiant la documentation de 4 appareils DMX disponibles dans la salle, compléter le tableau :

Appareil DMX	Nombre de canaux utilisés
- SPOT EX-15	- 5 ou 13 canaux
-	-
-	-
-	-
-	-

En étudiant la documentation du matériel DMX qui vous est confié, remplir la fiche suivante en se limitant à 8 effets possibles :

Référence de l'appareil DMX :

Canal	Valeur	Effet
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-

TP

Installation du module Artnet-DMX Enttec, configuration du matériel DMX et analyse réseau des données transmises

Installation du module Enttec

Installer NMU (Node Management Utility).

Dans le logiciel NMU, lancer la recherche des modules Enttec présents sur le réseau, et compléter les informations suivantes (accessibles dans la fenêtre de configuration d'un module) :

- IP :	Univers :
- IP :	Univers :

Configuration de votre appareil DMX

En suivant attentivement la documentation constructeur de votre appareil :

- Configurez l'appareil en mode DMX.
- Affectez lui l'adresse DMX $10 \times \text{numéroDeVotrePC}$ (canal de départ)

Test de pilotage via NMU (module Enttec)

Choisir Arnet-test et valider le mode Arnet : vous pouvez maintenant actionner les curseurs et vérifier la bonne configuration de votre matériel en vérifiant les effets lumineux : attention chaque binôme/trinôme devra faire ses tests lorsque les autres n'en feront pas.

Analyse Wirshark des données

Quel filtre permet d'isoler les trames issues de votre PC et utilisant le protocole UDP ?

Lancer Wireshark et isoler les trames UDP issues de votre PC : indiquer l'entête de cette trame :

Indiquer, d'après la documentation constructeur du module Enttec, la signification des 14 premiers octets de donnée.

Vérifier l'évolution de la valeur des données correspondant à votre matériel lors du pilotage.

MODULE 02

SÉANCE WEB 02

TP D'INFORMATIQUE

Durée 2h30

FORMULAIRE D'ENVOI UNE TRAME DMX

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Codage d'une page Web permettant l'envoi d'une trame DMX au serveur web (HTML et CSS). On donne le code AJAX permettant la requête HTTP et le PHP permettant l'envoi de la trame DMX au serveur UDP Enttec. Analyse Wireshark du cheminement de la donnée.

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- | | |
|------------------------------------------------------------------------------------|----------|
| • Langages de développement, de description, de création d'API et les IDE associés | Niveau 4 |
| • Chaînes de développements (ordinateur, embarqué, cross compilation) | Niveau 3 |
| • Programmation réseau | Niveau 2 |
| • Outils logiciels d'évaluation, de traçabilité de l'information | Niveau 3 |

CONNAISSANCES OPÉRATIONNALISÉES

- | | |
|--------------------------------------------------------------|----------|
| • Installation d'un module PHP sur un mini PC sous Linux | Niveau 2 |
| • Codage d'une page HTML adaptée aux codes AJAX et PHP donné | Niveau 2 |
| • Analyse d'un code AJAX utilisant les XMLHttpRequest | Niveau 2 |
| • Analyser une communication réseau avec Wireshark | Niveau 2 |
| • Versionner un code | Niveau 2 |

TP

Installation des modules PHP et JS sur le mini-PC

Codage d'une page WEB de test

Créer un répertoire M02W

Placer le fichier client_udp.php dans le répertoire M02SW

Créer un fichier main.js contenant : (modifier éventuellement l'adresse et l'univers)

```
function Ecrire()  
{  var valeur=document.getElementById("edit").value;  
  var client = new XMLHttpRequest();  
  client.open("POST","client_udp.php", false);  
  donneesJson='{"univers":"0","adresse":"0","valeur":"' +valeur+'"}';  
  client.send(donneesJson);  
}
```

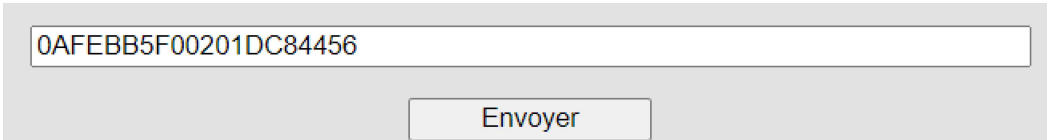
Coder une page HTML contenant : (rechercher sur Internet)

- Un Edit (input) avec l'identifiant « edit »
- Un Bouton (button) dont le paramètre onclick est :onclick="Ecrire()", cette fonction appelée lors du click est la fonction JavaScript codée dans le fichier main.js.

Inclure le script Javascript en fin de fichier HTML : (dans le body)

```
<script type="text/javascript" src="main.js"></script>
```

Tester l'application Web en entrant dans la zone Edit les caractères hexadécimaux correspondant à la trame désirée : exemple : 0AFEBB5F00201DC84456



0AFEBB5F00201DC84456

Envoyer

Vérifier les effets lumineux.

Versionner le code.

TD

Analyse du script JavaScript AJAX

En utilisant Internet, répondre aux questions suivantes au sujet du script JavaScript donné :

```
function Ecrire()  
{  var valeur=document.getElementById("edit").value;  
  var client = new XMLHttpRequest();  
  client.open("POST","client_udp.php", false);  
  donneesJson='{"univers":"0","adresse":"0","valeur":"' +valeur+'"}';  
  client.send(donneesJson);  
}
```

Que permet la fonction getElementById ?

Que permet le constructeur XMLHttpRequest ?

A quoi correspond la méthode HTTP « POST » ?

Qu'est-ce qu'un fichier PHP ?

Qu'est-ce qu'une donnée JSON ?

Quel est, dans ce script, l'effet de la fonction open ?

Quel est, dans ce script, l'effet de la fonction send ?

Qu'est-ce-que l'AJAX ?

TP**Analyse Wireshark de la communication TCP et HTTP**

Lancer l'analyse et expliquer les trames HTTP (entre le navigateur et le serveur WEB) en détail (filtre `ip.src==... && http`), puis les trames au niveau du TCP (filtre `ip.src==... && tcp`), préciser les adresses mac et les ports

BONUS : en se basant sur les relevés WireShark, proposer un diagramme UML de séquence visant à décrire (lors de l'envoi d'un effet) les échanges entre le client HTTP et le serveur HTTP. Ajouter les échanges entre le client UDP (serveur PHP) et le serveur UDP (Enttec).

MODULE 02

SÉANCE WEB 03

TP D'INFORMATIQUE

Durée 2h30

INTRODUCTION AU JAVASCRIPT

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Introduction au Javascript : gestion des événements

Cybersécurité : vérification des caractères saisis dans la zone Edit avant l'envoi de la trame DMX

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- Langages de développement, de description, de création d'API et les IDE associés Niveau 4
- Chaînes de développements (ordinateur, embarqué, cross compilation) Niveau 3

CONNAISSANCES OPÉRATIONNALISÉES

- Gestion des événements en Javascript Niveau 2
- Versionner un code Niveau 2

TP

Mon premier code JS

Le JS est un langage compilé ou interprété ? Et par qui ?

Les scripts peuvent être placés dans la section `<body>`, ou dans la section `<head>` d'une page HTML, ou dans les deux. Cependant, le fait de placer les scripts au bas de l'élément `<body>` améliore la vitesse d'affichage, car l'interprétation des scripts ralentit l'affichage.

(source : https://www.w3schools.com/js/js_where.asp)

Expliquer la différence entre placer le code dans le `<head>` ou le placer à la fin du `<body>` ?

Pour un développeur, il est essentiel de garder un code qui soit clair et réexploitable. Or mélanger dans un même fichier du HTML et du JS rend le code complexe. Il est de loin préférable de les séparer. Comment ? En créant des fichiers spécifiques pour le code écrit en JS. Ces fichiers auront pour extension `.js`.

Création d'un fichier test.js

Vous allez créer un nouveau fichier « test.js » qui vous servira simplement à faire des tests en JS pour découvrir ce langage et ses fonctionnalités. Dans votre répertoire de travail, créer un nouveau fichier nommé test.js. Mettre dans le fichier « test.js » le code JS :

```
alert("Test d'affichage d'un message");
```

Placer la balise script dans le fichier index.html :

```
<script src="test.js"></script>
```

Vérifier l'affichage du message d'alerte.

Les informations de débogage

Très souvent, le développeur veut afficher des informations, des données, des variables – juste pour en connaître l'état. Il ne souhaite pas que ces données soient vues par le visiteur. En JS, il est possible d'utiliser la console de débogage.

Remplacer le message d'alerte du fichier test.js par :

```
console.debug("Test d'affichage d'un message");
```

Rafraîchissez votre page. Le message apparaît-il ? Le message apparaît dans la console de débogage ! Appuyer sur la touche F12 (pour afficher l'inspecteur d'objet) puis sélectionner l'onglet Console (éventuellement sélectionner d'afficher les messages de debug). Vous devez constater que le message apparaît.

Les variables en JS

Remplacer maintenant le code du fichier test.js par le suivant puis tester-le. Afficher la console.

```
var message = "La somme fait : ";  
var val1 = 15;  
var val2 = 4;  
var resultat = val1 + val2;  
console.log("VAL1 vaut : " + val1);  
console.log("VAL2 vaut : " + val2);  
console.log("RESULTAT vaut : " + resultat);  
console.log(message + resultat);  
console.log(message + val1 + val2);
```

Combien de variables sont créées et quel est le type de chacune de ces variables ?

Expliquez la différence d'affichage des 2 dernières lignes.

Le mot clé var permet de créer des variables. Même si en JS les variables n'ont pas de type défini lors de leur création, la notion de type reste néanmoins primordiale et détermine la signification des opérations.

Évènements et fonctions en JS

L'objectif de cette partie est de comprendre la gestion des évènements en JS. Un évènement est déclenché généralement suite à une action de l'utilisateur : un clic sur un bouton, une saisie d'un texte, etc. Lorsqu'un évènement est déclenché, il est possible d'appeler une fonction.

En JS, la gestion d'un évènement se fait en 2 étapes :

1. On récupère l'objet sur lequel l'utilisateur interagit
2. On indique quel évènement de cet objet nous intéresse et la fonction qui sera exécutée.

Supposons que nous souhaitons afficher un message popup lorsque la souris de l'utilisateur survole le bouton envoyer de notre page.

Dans la balise button :

```
onmouseover= "Mon_popup()"
```

Il reste maintenant à créer la fonction `mon_popup()` comme suit :

```
function Mon_popup() {  
    alert("Gestion de l'évènement 'mouse over' sur mon bouton");  
}
```

En JS, le mot-clé `function` permet de créer une nouvelle fonction avec un nom et si nécessaires des arguments. Ensuite, la définition de la fonction se fait entre les accolades ouvrante et fermante.

Gérer l'évènement `oninput` sur l'edit et exécuter la fonction `TrameValide()`. Écrire le code de cette fonction qui pour le moment affichera le message « vérification de la trame » dans la console.

Votre code html de la balise `input` :

Votre fonction JS `TrameValide()` :

TP

Cybersécurité : vérification des caractères de la trame avant l'envoi au serveur

Pour éviter le traitement par le serveur de trames erronées ou non conforme, il est indispensable de vérifier la trame côté client. Cela protégera le serveur d'éventuels bugs, tout en le soulageant puisqu'il n'aura pas à traiter des informations inexploitable.

Modification de la page html et ajout d'une feuille de style

Ajouter dans le fichier html une zone de texte visant à informer l'utilisateur d'une mauvaise saisie : le nombre de caractères hexadécimaux de la trame doit être pair, seuls des caractères hexadécimaux peuvent être présents dans la trame (0 à 9 puis A à F). Nous utiliserons 2 balises span :

- Pour vérifier la longueur : id="longueur" class="vert" avec le texte Longueur
- Pour vérifier les caractères : id="hexa" class="vert" avec le texte Hexa

Ajouter à la page une feuille de style et définir les classes :

- .vert fixant la couleur verte
- .rouge fixant la couleur rouge

Vos balises span :

Votre feuille de style :

Fonction JS permettant de vérifier la trame

Dans votre fonction TrameValide() :

Placer la valeur de la zone edit dans la variable trameHexa.

Si la longueur de la trame (trameHexa.length) est paire, modifier la classe du champ d'Id longueur de la page html pour qu'il passe en vert (document.getElementById("longueur").className). Sinon, il passera en rouge.

Une variable queDeLHexa initialisée à true permettra de vérifier la validité de chacun des caractères de la trame :

Pour tous les caractères de la trame (i allant de 0 à trameHexa.length par incrément de 1)

Si la condition : (trameHexa[i] est compris entre '0' et '9' ou entre 'A' et 'F') est fausse, placer queDeLHexa à l'état faux.

Positionner la couleur du texte d'Id hexa en rouge ou en vert en fonction de l'état de la variable queDeLHexa.

Votre fonction JS :

BONUS : n'autoriser l'envoi au serveur que d'une la trame valide.

[Versionner le code complet.](#)

MODULE 02

SÉANCE WEB 04

TP D'INFORMATIQUE

Durée 2h30

CONSOLE DMX VIRTUELLE

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Gestion d'un scrollbar : affichage de la valeur du scrollbar dans un edit (en décimal).
Modification de la trame DMX hexadécimale (Edit) lors de l'action sur un scrollbar : test de l'envoi et analyse Wireshark. Gestion de 6 scrollbars.

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- Langages de développement, de description, de création d'API et les IDE associés Niveau 4
- Chaînes de développements (ordinateur, embarqué, cross compilation) Niveau 3
- Outils logiciels d'évaluation, de traçabilité de l'information Niveau 3

CONNAISSANCES OPÉRATIONNALISÉES

- Gestion des événements scrollbar en Javascript Niveau 2
- Analyser une communication réseau avec Wireshark Niveau 2
- Versionner un code Niveau 2

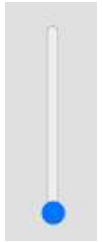
TP

Gestion d'un scrollbar

Ajouter à votre page html un scrollbar : un input de type "range" dont il faut définir le max, le min et la value. Il vous faut rechercher des exemples sur Internet.

Ajouter dans votre feuille de style le paramètre `webkit-appearance: slider-vertical;` pour l'objet scrollbar : il faut définir une classe dans la balise input correspondant au scrollbar du fichier html et définir ses paramètres dans la feuille de style.

Votre code html de la balise input :



Votre code css correspondant à la classe utilisée :

Dans votre code JS, créer une variable `s1` permettant de récupérer l'objet scrollbar par Id. Écouter l'événement 'change' et modifier la valeur de la zone Edit en fonction de la position du scrollbar (compléter et tester le code suivant :

```
var s1= ... ;

s1.addEventListener('change', function ()
{   document.getElementById("edit").value= ... ;
}, false);
```

TP

Modification de la trame DMX hexadécimale lors de l'action sur le scrollbar

Lors de l'écoute du changement de la position du scrollbar, il ne faut maintenant que modifier la valeur du premier octet de la trame hexadécimale dans l'Edit. Stocker dans une variable trameHexa la valeur de l'Edit. Puis ajouter dans la fonction d'écoute du changement de la position :

```
var numeroCanal=1 ;
```

```
var entier=Math.abs(S1.value).toString(16).toUpperCase();  
if(S1.value<16) entier="0"+entier;  
var indice=(numeroCanal-1)*2;  
trame=trame.substring(0,indice)+entier+trame.substring(indice+2, trame.length);  
document.getElementById("edit").value=trame;  
Ecrire();
```

Avant de tester, nous allons analyser ce code, en faisant des recherches sur Internet :

Quel est l'effet de `Math.abs(s1.value)` ?

Si la valeur du scrollbar est 20, quelle est la valeur renvoyée par `Math.abs(s1.value).toString(16)` ?

Quel est le rôle de la fonction `toUpperCase()` ?

A quoi sert le code : `if(s1.value<16) entier="0"+entier;` ?

Que vaut l'indice lorsque numeroCanal=

1 :
2 :
3 :

A quoi correspondent les 2 arguments de la méthode substring ?

Expliquer en détail l'instruction :

```
trame=trame.substring(0,indice)+entier+trame.substring(indice+2,trame.length);
```

Tester l'envoi de la trame : analyser les échanges avec Wireshark.

Gestion de 6 scrollbars pour piloter 6 effets lumineux



Modifier le code afin de gérer 6 scrollbars.

Versionner le code complet.

MODULE 02

SÉANCE WEB 05

TP D'INFORMATIQUE

Durée 2h30

BOUTONS DE PILOTAGE RAPIDES

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Codage des boutons d'accès rapides : FullON, FullOff, aléatoire.
Ajouter le numéro du canal de départ dans un Edit

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- Langages de développement, de description, de création d'API et les IDE associés Niveau 4
- Chaînes de développements (ordinateur, embarqué, cross compilation) Niveau 3

CONNAISSANCES OPÉRATIONNALISÉES

- Codage d'une page HTML et d'un script Javascript permettant de lancer automatiquement des effets lumineux Niveau 2
- Versionner un code Niveau 2

TP

BOUTONS D'ACCÈS RAPIDE AUX EFFETS LUMINEUX

Modifier la page html afin de pouvoir saisir le numéro du canal de départ (zone input). Adapter le code JS en affectant cette valeur à la variable numeroCanal.

Tester votre code en vérifiant la trame à l'aide de Wireshark.

Ajouter dans la page html les boutons FullON et FullOff : ces boutons auront pour effet, respectivement, de mettre les curseurs au maximum ou au minimum. Coder les fonctions JS correspondantes : la trame présente dans la zone Edit doit être également modifiée.

Tester votre code en vérifiant la trame à l'aide de Wireshark.

Votre fonction FullON() :

BONUS : ajouter un bouton Aléatoire permettant, toutes les 2 secondes, de modifier la position des scrollbars (et la trame hexadécimale) de manière aléatoire.

Donner en JS le code permettant de générer un nombre aléatoire de 0 à 255 :

Donner la description des arguments de la fonction JS setInterval(... , ...)

Tester votre code en vérifiant la trame à l'aide de Wireshark.

Versionner le code complet.

MODULE 02

SÉANCE WEB 06

TP D'INFORMATIQUE

Durée 2h30

PAGE DE PRÉSENTATION DU MATÉRIEL DMX

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Création d'une page WEB de présentation du matériel DMX : documentation constructeur et vidéos

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- Langages de développement, de description, de création d'API et les IDE associés Niveau 4
- Chaînes de développements (ordinateur, embarqué, cross compilation) Niveau 3

CONNAISSANCES OPÉRATIONNALISÉES

- Codage d'une page Web intégrant des vidéos Niveau 2
- Versionner un code Niveau 2

TP

Conception d'une page Web de présentation du matériel DMX utilisé : intégration d'une vidéo

Créer une nouvelle page html visant à présenter l'appareil DMX que vous avez configuré. Intégrer la documentation du constructeur en pdf. Votre page doit être attractive et esthétique : une feuille de style est impérative.

Balise vidéo


Quelle balise permet d'intégrer une vidéo à une page Web ?

Faites une vidéo de démonstration du pilotage de votre matériel DMX, puis intégrez cette vidéo à votre page html.


Versionner le code complet.


Présentation


Lyre Beam à lampe 5R, contrôlable en musical, automatique, maître-esclave et DMX-512
Evolite Moving Beam 5R, une prouesse technique et tarifaire signée Evolite !



Manuel







Description

- Evolite Moving Beam 5R
- Lyre à lampe Philips Platinum 5R (fournie)
- 5 modes de fonctionnement : DMX, Maître / Esclave, Automatique, Musicale et Manuel
- 8 ou 16 canaux DMX
- Faisceau de 3°
- Prism 8 facettes
- Mode de défilement des Gobos
- Effet Gobo Shake
- Gobos Indépendants des couleurs
- Effet stroboscopique
- Filtre Frost
- Pan : 540°, Tilt : 280°
- Obturateur : Effet Pulse, stroboscope aléatoire rapide, effet arc-en-ciel
- Contrôle de la luminosité : 0 - 100 %
- Repositionnement auto X-Y
- Moteur pas à pas (micro déplacements)
- Connecteur XLR 3 broches In / Out
- LUX : 99250 à 10 m, 70030 à 15 M
- Lampe : Philips Platinum 5R à décharge, 8,000 ° K - 2,000 heures Longue durée de vie
- Ecran LCD pour contrôle des menus et options (Français et Anglais)
- Alimentation : 110/230Vac 60/50Hz
- Dimensions (L x l x h) : 320 x 390 x 470 mm
- Poids : 18 kgs

MODULE 02

SÉANCE WEB 07

TP D'INFORMATIQUE

Durée 2h30

DESIGN DU SITE COMPLET

BLOC DE COMPÉTENCES

U6 – VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

COMPÉTENCE(S)

C08 – CODER

OBJECTIF PÉDAGOGIQUE

Design du site complet : header - nav - section - footer (CSS)
Gestion du clic dans la barre de navigation

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- Langages de développement, de description, de création d'API et les IDE associés Niveau 4
- Chaînes de développements (ordinateur, embarqué, cross compilation) Niveau 3

CONNAISSANCES OPÉRATIONNALISÉES

- Mettre en forme un site Web sur plusieurs pages en utilisant les feuilles de style. Niveau 2
- Gestion des événements en Javascript
- Versionner un code Niveau 2

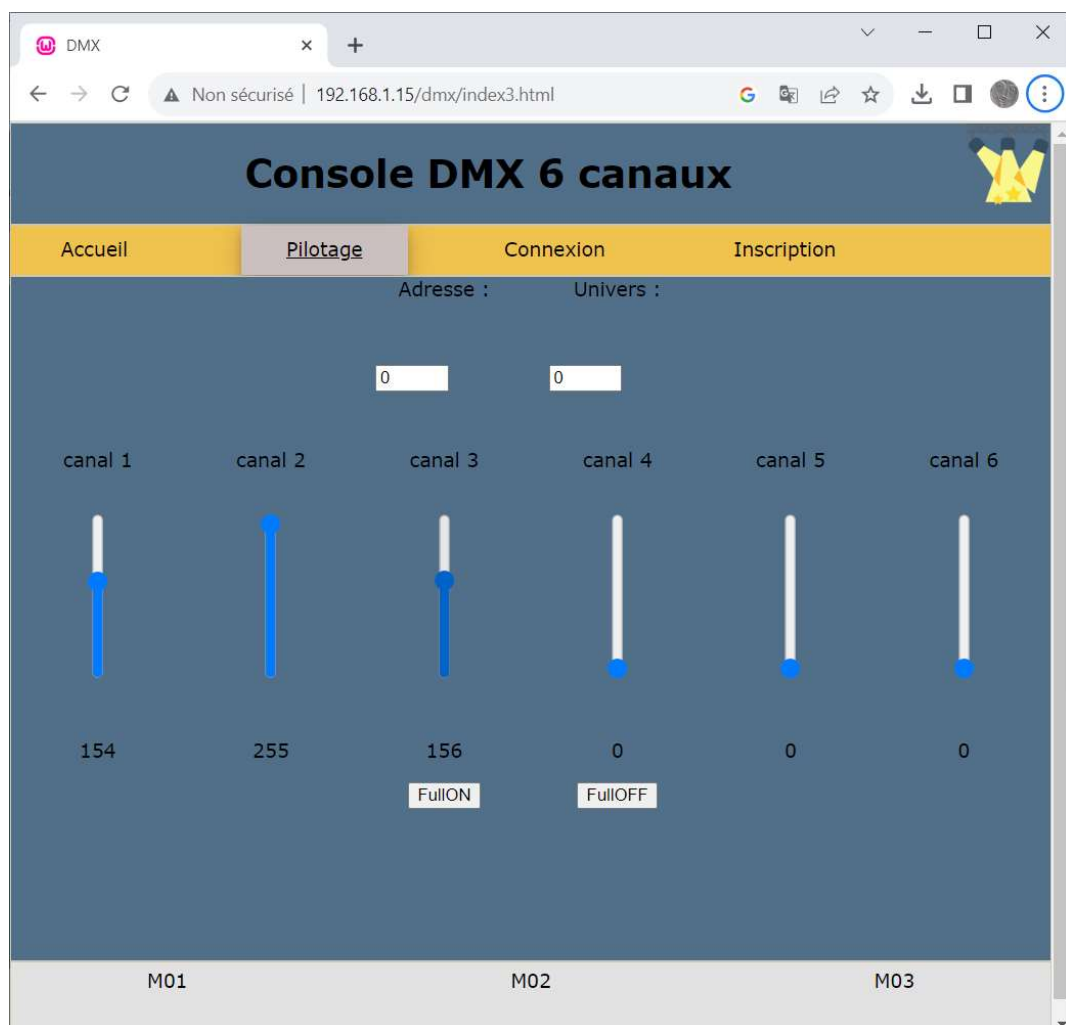
TP

Design du site complet

En se basant sur les GRID CSS décrites dans la module 01, effectuer le design du site complet en intégrant : header - nav - section - footer.

Gérer le clic dans la barre de navigation (la fonction AJAX permettant de charger une page dans une section est donnée)

Versionner le code complet.



MODULE 02

SÉANCE WEB 08

TP D'INFORMATIQUE

Durée 2h30

SÉCURITÉ : CRYPTAGE DE LA TRAME

BLOC DE COMPÉTENCES

U5 – EXPLOITATION ET MAINTENANCE DE RÉSEAUX INFORMATIQUES

COMPÉTENCE(S)

C06 – VALIDER UN SYSTÈME INFORMATIQUE

OBJECTIF PÉDAGOGIQUE

Sécurité : Cryptage de la trame AES (CryptoJS.AES.encrypt)

CONNAISSANCES ISSUES DU RÉFÉRENTIEL

- | | |
|---------------------------------------------------------------------------------------------------------------------------------------|----------|
| • Protocoles usuels IPv4, HTTP, HTTPS, TCP/IP, Ethernet, IPv6, DNS, DHCP, SSH | Niveau 4 |
| • Sécurisation des réseaux (ACL, mots de passe, pare-feu) | Niveau 3 |
| • Outils logiciels d'évaluation, de traçabilité de l'information, de tests, d'analyse de traitement et de rapport de l'incident (C11) | Niveau 3 |
| • Maîtrise des environnements de développement, d'intégration, de déploiement logiciel et des versions logicielles associées | Niveau 2 |

CONNAISSANCES OPÉRATIONNALISÉES

- | | |
|-----------------------------------------------------|----------|
| • Analyse Wireshark de la communication HTTP et UDP | Niveau 2 |
| • Mettre en place un chiffrement symétrique | Niveau 2 |
| • Versionner un code | Niveau 2 |

TP

Cryptage de la trame (AES)

Qu'est ce qu'un cryptage AES, est-il symétrique ou asymétrique ?

Créer un nouveau site WEB de test permettant de tester les codes JS et PHP donnés :

```
function AES_encryptage()
{
    // La clé
    var key = CryptoJS.enc.Hex.parse("0123456789abcdef0123456789abcdef");
    // Le vecteur d'initialisation
    var iv = CryptoJS.enc.Hex.parse("abcdef9876543210abcdef9876543210");
    var texte_encrypte=CryptoJS.AES.encrypt(document.getElementById("letexte").value, key, {iv:iv});
    document.getElementById("letexteAES").innerHTML = texte_encrypte;
    // Le texte encodé est convertit en base64 pour être envoyé
    encrypted = texte_encrypte.ciphertext.toString(CryptoJS.enc.Base64);
    var xh = new XMLHttpRequest();
    xh.onreadystatechange = function () {
        if (xh.readyState === 4 && xh.status === 200) {
            console.debug("REPONSE : " + xh.responseText);
        }
    }
    xh.open("POST", "decrypt_in_php.php", true);
    xh.setRequestHeader("Content-type", "application/json");
    xh.send('{"encrypted":"' + encrypted + '"}');
}
```

```
<?php
$postDataInJSON = file_get_contents ("php://input");
$data = json_decode($postDataInJSON, true);
// La clé
$key = pack('H*', '0123456789abcdef0123456789abcdef');
// Le vecteur d'initialisation
$iv = pack('H*', 'abcdef9876543210abcdef9876543210');
// La méthode de cryptage utilisée
$method = 'aes-128-cbc'; // C'est la méthode de cryptage utilisée par CryptoJS.AES.encrypt()
$decrypted=openssl_decrypt(base64_decode($data['encrypted']),$method,$key,OPENSSL_RAW_DATA,$iv);
echo '{"dechiffrement":"' . $decrypted . '"}'; // Sortie : 'Texte décrypté'
?>
```

Analyser les échanges à l'aide de Wireshark...

BONUS : intégrer à votre site WEB pilotage DMX le cryptage de la trame envoyée.

Versionner le code complet.