

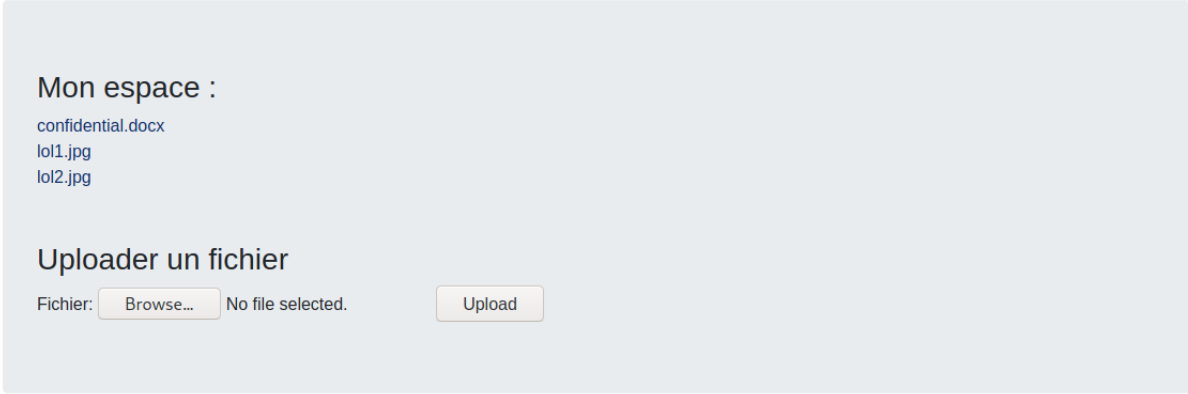
Faible 1

URL impactée :	http://10.54.101.67/resolver.php
CWE :	CWE-78 - Mauvaise utilisation des inputs sur des commandes OS
<div><h3>Testez la résolution d'un service</h3><div><input type="text" value="esdacademy.eu"/> <input type="button" value="Submit Query"/></div><p>esdacademy.eu has address 54.36.91.62 esdacademy.eu mail is handled by 10 alt4.aspmx.l.google.com. esdacademy.eu mail is handled by 5 alt1.aspmx.l.google.com. esdacademy.eu mail is handled by 5 alt2.aspmx.l.google.com. esdacademy.eu mail is handled by 1 aspmx.l.google.com. esdacademy.eu mail is handled by 10 alt3.aspmx.l.google.com. root:x:0:0:root:/root:/bin/bash</p></div>	
Description :	Il est possible de passer d'autres fonctions après l'adresse IP renseignée dans l'input. Exemple : <code>127.0.0.1 && cat /etc/passwd</code>
Remédiation :	<code>const clean = DOMPurify.sanitize(« your input »);</code>


Faible 2

URL impactée :	http://10.54.101.67/my_files.php?id=3
CWE :	CWE-434 - Mauvaise gestion d'upload de fichier
<div><p>Mon espace :</p><p>reverse.php</p><p>Uploader un fichier</p><div>Fichier: <input type="button" value="Browse..."/> No file selected. <input type="button" value="Upload"/></div></div>	
Description :	Les extensions de fichier ne sont pas vérifiées. Il est donc possible d'uploader du script et de l'exécuter.
Remédiation :	<code><input type="file" accept=".jpg,.png,.pdf" /></code>

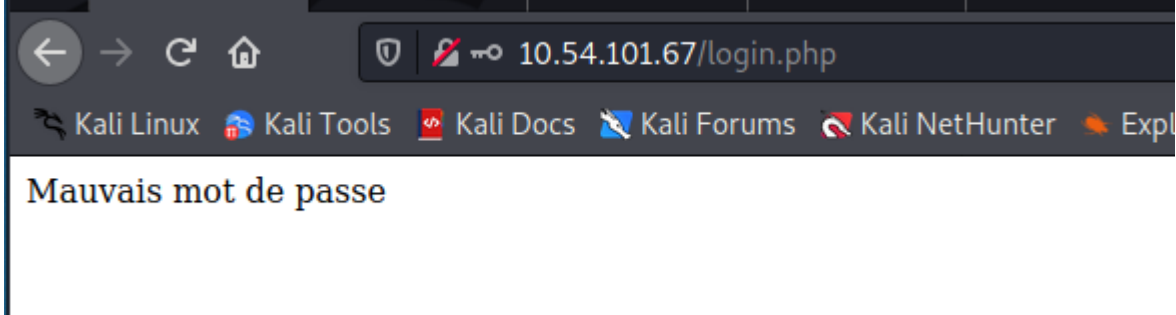
Faible 3

URL impactée :	http://10.54.101.67/my_files.php?id=2
CWE :	CWE-732 - Faiblesse de contrôles d'accès (data exposure, IDOR)
	
Description :	Le site utilise des id pour afficher les informations appartenant à l'utilisateur. Le changement de l'id dans l'url permet aux utilisateurs de récupérer les informations des autres comptes
Remédiation :	Utiliser un uuid a la place d'un id en base de données

Faible 4

URL impactée :	http://10.54.101.67/settings.php
CWE :	CWE-79 - Mauvaise ré-utilisation d'entrées
	
Description :	Le site interprète les entrées permettant ainsi d'exécuter du javascript directement dans les inputs. De plus, celui-ci est stocké et reste sur le profil utilisateur.
Remédiation :	<code>const clean = DOMPurify.sanitize(« your input »);</code>

Faible 5

URL impactée :	http://10.54.101.67/login.php
CWE :	CWE-200 - Exposition d'informations sensibles
	
Description :	L'application laisse fuiter des informations utiles à un attaquant. Ici je sais que l'utilisateur « xena » existe bien dans la BDD.
Remédiation :	Nettoyer le code pour ne pas afficher un texte trop explicite

Faible 6

URL impactée :	http://10.54.101.67/inscription.php
CWE :	CWE-20 - Mauvaise validation des inputs
	
Description :	L'application laisse la possibilité de réutiliser la même adresse mail pour plusieurs comptes.
Remédiation :	Demander au script de vérifier si l'adresse mail n'est pas déjà utilisée dans la BDD ou ajouter une contrainte unique dans la Table SQL

Faillle 7

URL impactée :	http://10.54.101.67/login.php
CWE :	CWE-352 - Cross-Site Request Forgery (CSRF)
	<pre> <div class="container"> <h1>Login</h1> <form method="POST" action="login.php"> <div class="form-group"> <label for="pseudo">Pseudo</label> <input type="text" class="form-control" id="pseudo" aria-describedby="pseudo" name="pseudo"> </div> <div class="form-group"> <label for="exampleInputPassword1">Password</label> <input type="password" class="form-control" id="password" name="password"> </div> </form> </div> </pre>
Description :	L'application ne vérifie pas de manière efficace, ou pas du tout la légitimité, consentement, à prétendre à une action donnée lors d'une requête.
Remédiation :	<pre> <?php //On démarre les sessions session_start(); //On génère un jeton totalement unique \$token = uniqid(rand(), true); //Et on le stocke \$_SESSION['token'] = \$token; //On enregistre aussi le timestamp correspondant au moment de la création du token \$_SESSION['token_time'] = time(); //Maintenant, on affiche notre page normalement, le champ caché token en plus </label> <input type="hidden" name="token" id="token" value="<?php //Le champ caché a pour valeur le jeton </pre>

Faillle 8

URL impactée :	http://10.54.101.67/login.php
CWE :	CWE-521: Weak Password Requirements
	<pre> POST /login.php HTTP/1.1 Host: 10.54.101.67 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 46 Origin: http://10.54.101.67 Connection: close Referer: http://10.54.101.67/login.php Cookie: PHPSESSID=31er9ltkqp7bk4mpgf8u40e7fu Upgrade-Insecure-Requests: 1 pseudo=administrateur&password=azerty&connect= </pre>
Description :	L'application ne vérifie pas de manière efficace la complexité des mots de passe.
Remédiation :	<pre> // Given password \$password = 'user-input-pass'; </pre>

	<pre>// Validate password strength \$uppercase = preg_match('@[A-Z]@', \$password); \$lowercase = preg_match('@[a-z]@', \$password); \$number = preg_match('@[0-9]@', \$password); \$specialChars = preg_match('@[^\w]@', \$password); if(!\$uppercase !\$lowercase !\$number !\$specialChars strlen(\$password) < 8) { echo 'Password should be at least 8 characters in length and should include at least one upper case letter, one number, and one special character.'; }else{ echo 'Strong password.'; }</pre>
--	---