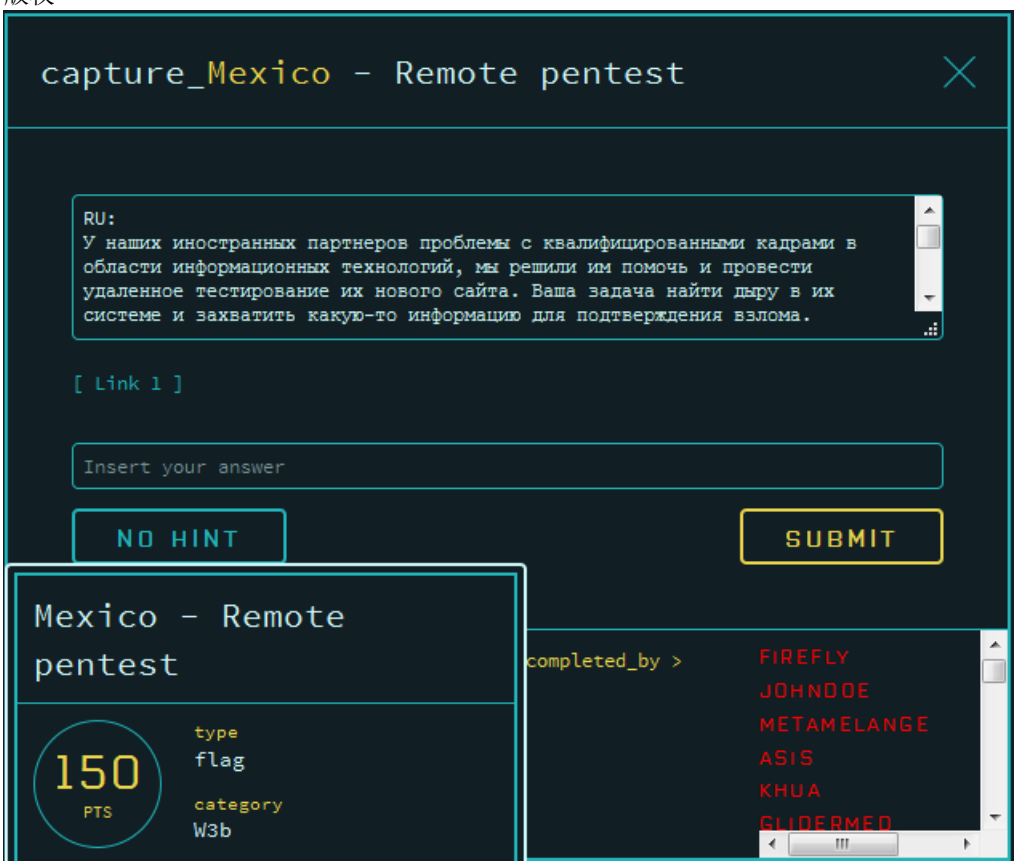
H4CK1T CTF 2016 Mexico-Remote pentest writeup

转载

BAM9090 于 2016-09-24 18:10:00 发布 142 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wocalieshenmegui/p/5903774.html



进去网站之后发现连接都是包含类型的，就能想到文件包含漏洞(话说刚总结过就能遇到这题，也算是复习啦)

这里用php://filter/read=convert.base64-encode/resource=方法读源码，明面上一共有4个文件，index.php,about.php,services.php,contact.php

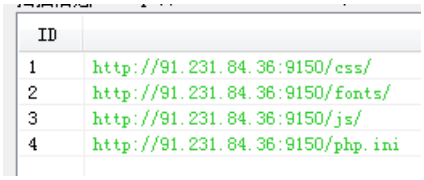
但是里面的flag都是假的，其中index.php有部分源码是这样的

```php
<?php
   if ($_GET["page"]) {
   $file = $_GET["page"].".php";
   // simulate null byte issue
   $file = preg_replace('/\x00.*/',"",$file);
      include($file);
   }
```

包含限制了php后缀，并且%00截断被过滤了(话说这里这样过滤和不过滤没差别吧)

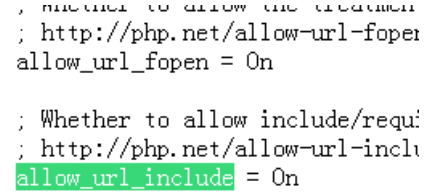
既然4个文件都没有flag，那么就拿出扫描器扫吧

然后扫到了根目录下存在php.ini



ID	
1	http://91.231.84.36:9150/css/
2	http://91.231.84.36:9150/fonts/
3	http://91.231.84.36:9150/js/
4	http://91.231.84.36:9150/php.ini

然后就想到看看allow_url_include

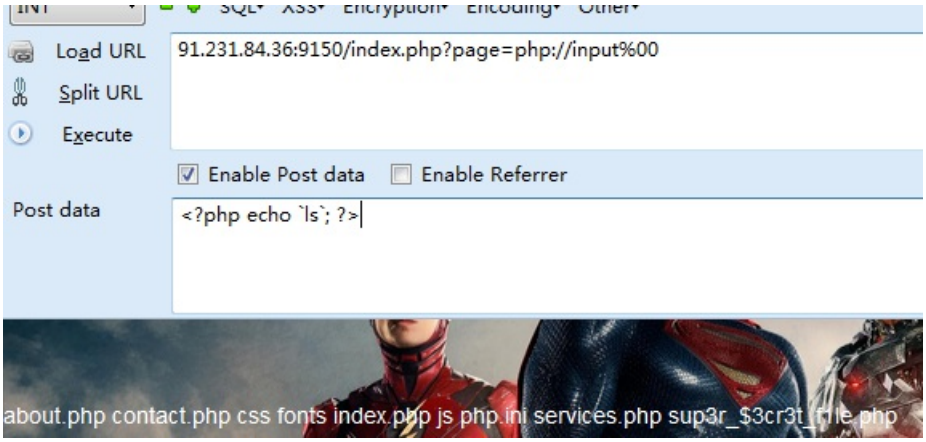


```
; Whether to allow the treatment
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/requ
; http://php.net/allow-url-inclu
allow_url_include = On
```

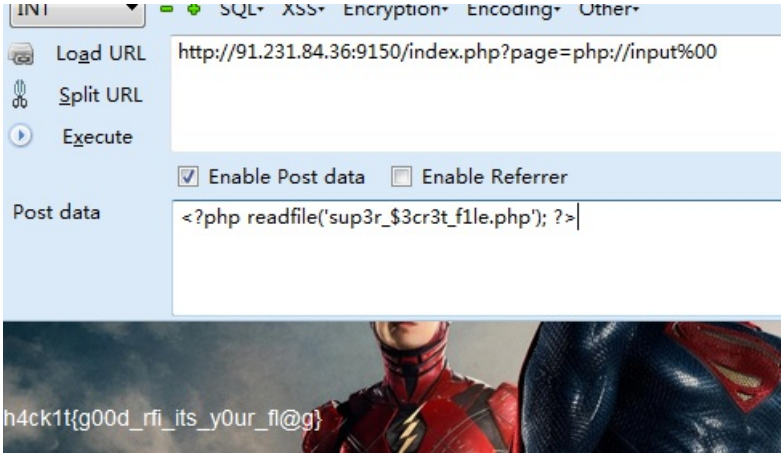
发现是On的，那么就可以远程包含，利用php://input或者远程服务器上的文件

直接用php://input



看到有个sup3r_$3cr3t_f1le.php文件

读取



转载于:https://www.cnblogs.com/wocalieshenmegui/p/5903774.html