攻防世界mfw_攻防世界--web高级writeup

原创

拖狗老师 于 2021-01-14 06:44:30 发布 69 收藏
文章标签： 攻防世界mfw

根据大佬们的writeup作出来后，自我整理下知识点及分类php

目录html

mfw git泄露app

注意 page=about ，能够传数据

且用git写可能有git泄露

传flag为空，表明有文件，若是报错，是没有webstorm

git泄露函数

查看flag.php没有东西

查看index.php

page没有通过任何过滤和处理，因此能够传递参数闭合strpos函数

设置page为'.system("cat ./templates/flag.php").',查看源代码，可得到flag

分步理解

'.system("ls").'

'.system("ls templates").'

'.system("cat ./templates/flag.php").'

必定要查看源代码，否则就亏大了！

NaNNaNNaNNaN-Batman js代码审计

获得一个文件，打开后乱码，webstorm整理格式也不行，发现一个很长很长的字符串，name为_，可发现应该是一个函数function

eval()改为alert(_)可输出function的函数

或者改为console.log()

整理得

代码审计，对正则表达式不太熟悉

https://blog.csdn.net/lucky541788/article/details/81711711

以be0f23开头

以e98aa结尾

包含233ac

包含c7be9

而后重复的部分去掉

输入be0f233ac7be98aa

或者这部分可直接输出s获得flag

PHP2--phps

phps文件就是php的源代码文件，一般用于提供给用户(访问者)查看php代码，由于用户没法直接经过Web浏览器看到php文件的内容，因此须要用phps文件代替。其实，只要不用php等已经在服> 务器中注册过的MIME类型为文件便可，但为了国际通用，因此才用了phps文件类型。 它的MIME类型为：text/html, application/x-httpd-php-source, application/x-httpd-php3-source。

看大佬的writeup 能扫目录扫出来index.phps,我只能扫出两个，若是再赶上只能猜了

dirsearch命令复习一下：用python3

python dirsearch.py -u url -e*

要传入一个id而且这个id进行url解码后的值为admin

当咱们在浏览器输入admin时，浏览器会对admin进行一次url解码

因此须要对admin进行两次url编码才可

urldecode($_GET[id]) ------>url解码

找了半天终于找到能用的了

web2--加密解密

要对函数很熟悉

分析其中的PHP内置函数

strrev(string): 反转字符串

strlen(string): 返回字符串的长度

substr(string, start, length): 返回字符串的一部分

string: 所须要的字符串

start: 在字符串何处开始

length: 可选。规定被返回字符串的长度。默认是直到字符串的结尾

ord(string): 返回字符串首个字符的 ASCII 值

chr(): 从指定的 ASCII 值返回对应的字符

str_rot13(string): 对字符串执行 ROT13 编码。

ROT13 编码把每个字母在字母表中向前移动 13 个字母。数字和非字母字符保持不变

编码和解码都是由该函数完成的。若是把已编码的字符串做为参数，那么将返回原始字符串

base64_encode(string): 使用 MIME base64 对数据进行编码

```
$miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
$a = base64_decode(strrev(str_rot13($miwen)));
$fin = "";
for($x=0; $x
$c = substr($a,$x,1);
$_ = ord($c)-1;
$_c = chr($_);
$fin = $fin.$_c;
}
echo strrev($fin);
```

lottery