部分web题目题解

原创

buchiyexiao. 于 2019-05-24 19:17:21 发布 312 收藏

分类专栏： ctf 文章标签： writeup

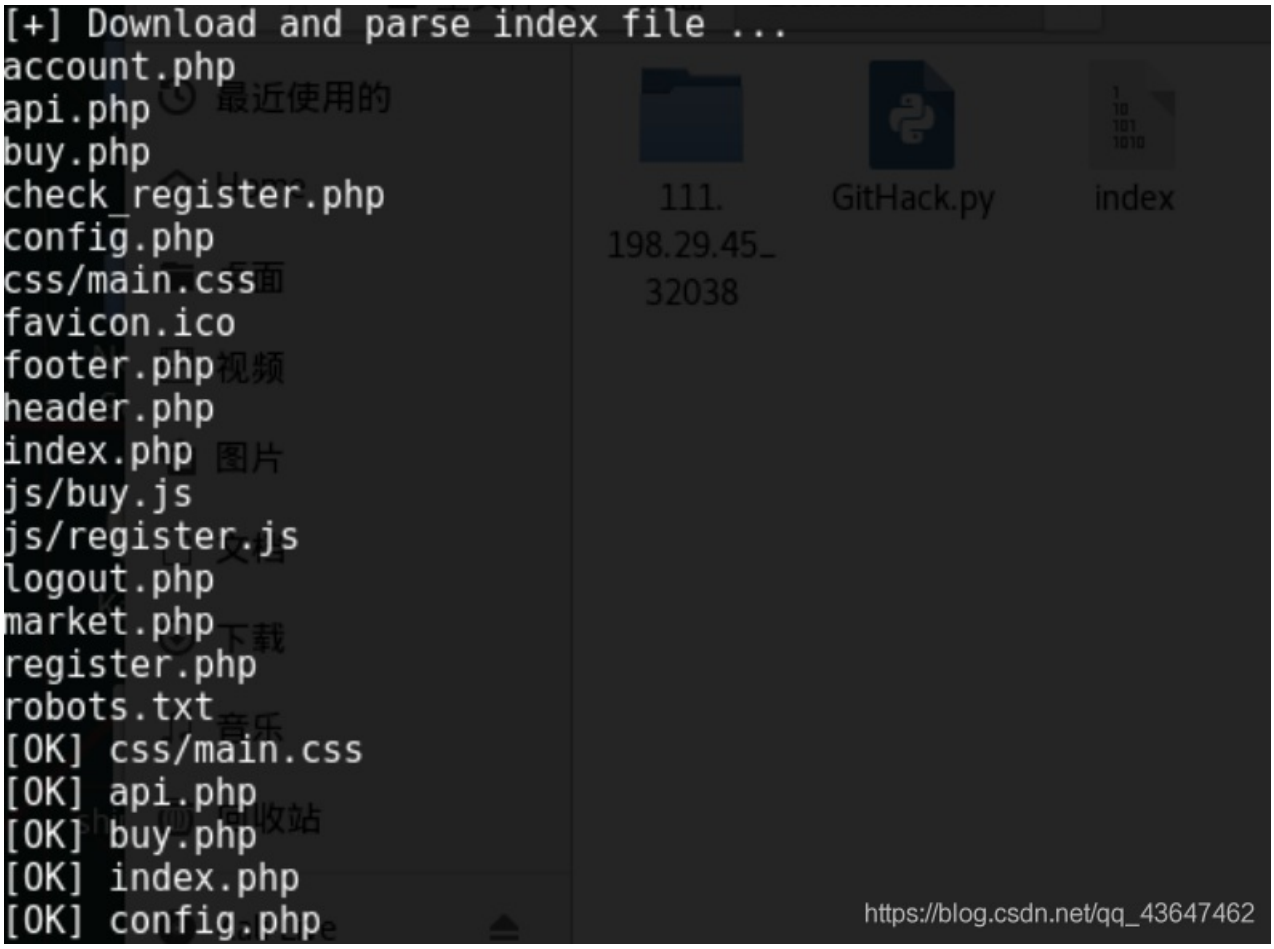
本文链接：https://blog.csdn.net/qq_43647462/article/details/90521796

XCTF WEB

Lottery！

首先看本题目，可以发现要求乐透彩票达到10w元，可以猜测应该是修改某些东西达到你可以获奖。

直接借助GitHack脚本对其进行.git/的源码获取



获取之后借助NotePad++进行代码审计，可以找到API.py中的原理

```
function buy($req){
    require_registered();
```

```php
require_min_money(2);

$money = $_SESSION['money'];
$numbers = $req['numbers'];
$win_numbers = random_win_nums();
$same_count = 0;
for($i=0; $i<7; $i++){
    if($numbers[$i] == $win_numbers[$i]){
        $same_count++;
    }
}
```


即win_num是随机产生的，num是我们输入的，判断num与win_num是否相同，哲理有一点需要我们格外注意，我们可以借助PHP弱类型松散比较，即向json传输bool类型条件，那么只要我们输入的数字全不为零那么久可以获得5w奖金
借助burpsuite进行抓包

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:32038
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://111.198.29.45:32038/buy.php
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 63
Connection: close
Cookie: PHPSESSID=84ce13bba4750340133162ce9da17b03

{"action":"buy","numbers":[true,true,true,true,true,true,true]}
```


然后多执行几次把钱拿到手，然后攒钱买Flag吧~

Training-WWW-Robots

题目告诉我们要学习robot协议的相关知识，robots文档简单理解就是勿扰，也就是类似于一个酒店内门前是否挂着请勿打扰的牌子，我们直接访问/robots.txt可以看到文中保护的一个是/fl0g.php，直接访问/fl0g.php即可得到flag

```
User-agent: *
Disallow: /fl0g.php


User-agent: Yandex
Disallow: *
```

NaNNaNNaNNaN-Batman

题目给了我们一个文件，用Notepad++打开后发现是一个html源码，所以我们直接用浏览器打开，最后一句eval(_)是执行一个名字为_的函数，我们直接把eval改成alert让函数体弹出，方便我们进行代码审计，然后我们审计代码

```
function
$(){var e=document.getElementById("c").value;
```

```
if(e.length==16)if(e.match(/^be0f23/)!=null)
if(e.match(/233ac/)!=null)
if(e.match(/e98aa$/)!=null)
if(e.match(/c7be9/)!=null)
{var t=["fl","s_a","i","e}"];
var n=["a","_h0l","n"];
var r=["g{","e","_0"];
var i=["it'","_","n"];
var s=[t,n,r,i];
for(var o=0;o<13;++o)
{document.write(s[o%4][0]);
s[o%4].splice(0,1)
}
}
}
document.write('<input id="c"><button onclick=$()>Ok</button>');
delete _
```


接下来有两种方法，一是通过match把匹配出来的16个字符写出来，二是通过程序把flag那一段跑一下，两种方法均可以，不予详述

Training-Get-Resourced

…这个题也太…tql

simple_php

```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

首先我们前半段flag1可以直接让a=a，因为这样的话比较会把a转换为数字0，然后进行判断；后半段flag2可以让b=1235abc，这样is_numeric判断其不是数字字符串，但是弱类型比较会让其忽略abc三个字母满足条件。