8、XCTF simple_php

原创

山兔1 于 2021-09-16 23:14:01 发布 28 收藏 1

分类专栏： CTF 文章标签： php

本文链接：https://blog.csdn.net/m0_53008479/article/details/120339673

小宁听说`php`是最好的语言,于是她简单学习之后写了几行`php`代码。

打开网站，就看到了下面这个

```php
<?php
show_source(__FILE__);          //查看源文件
include("config.php");           //包含config,php
$a=@$_GET['a'];                  //变量a通过参数a get方式获取
$b=@$_GET['b'];                  //变量b通过参数b get方式获取
if($a==0 and $a){                //变量a的值=0，用md5方式来比较
    echo $flag1;                     //输出flag1
}
if(is_numeric($b)){                      //检测变量b是否为数字串
    exit();                                      //是的话，并退出脚本
}
if($b>1234){                             //当变量b大于1234
    echo $flag2;                           //输出flag2
}
?>
```

`F12`，没搞头。

上代码审计，构造`payload`。

```
http://111.200.241.244:52351/?a=0e1&b=1235a
```

基础知识：

`is_numeric` — 检测变量是否为数字或数字字符串

`exit` — 输出一个消息并且退出当前脚本

`0e1`的`MD5`值是`0`， `1235a`是字符串，直接就绕过`is_numeric`的检测，并且大于`1234`。