php 变量覆盖 ctf,CTF-代码审计(1)——parse_str()变量覆盖

转载

Yfjcc 于 2021-03-27 09:14:22 发布 73 收藏
文章标签： php 变量覆盖 ctf
题目连接：http://222.18.158.226:7000/iscc.php

考点：parse_str()变量覆盖

代码：

```php
<?php
$hashed_key = '79abe9e217c2532193f910434453b2b9521a94c25ddc2e34f55947dea77d70ff';
$parsed = parse_url($_SERVER['REQUEST_URI']);
if(isset($parsed["query"])){
    $query = $parsed["query"];
    $parsed_query = parse_str($query);
    if($parsed_query!=NULL){
        $action = $parsed_query['action'];
    }

    if($action==="auth"){
        $key = $_GET["key"];
        $hashed_input = hash('sha256', $key);
        if($hashed_input!==$hashed_key){
            die("GTFO!");
        }

        echo file_get_contents("/flag");
    }
}else{
    show_source(__FILE__);
}
?>
```

PHP知识点：

1.parse_url()

参照网址:https://www.php.net/manual/zh/function.parse-url.php

```
parse_url ( string $url [, int $component = -1 ] ) : mixed
```

本函数解析一个 URL 并返回一个关联数组，包含在 URL 中出现的各种组成部分。

本函数*不是*用来验证给定 URL 的合法性的，只是将其分解为下面列出的部分。不完整的 URL 也被接受，parse_url() 会尝试尽量正确地将其解析。

对严重不合格的 URL，parse_url() 可能会返回 FALSE。

如果省略了 component 参数，将返回一个关联数组 array，在目前至少会有一个元素在该数组中。数组中可能的键有以下几种：

- scheme - 如 http
- host
- port
- user
- pass
- path
- query - 在问号 ? 之后
- fragment - 在散列符号 # 之后

2.$_SERVER[]

参考网址：https://php.net/manual/zh/reserved.variables.server.php

3.parse_str()

参考网址：http://www.w3school.com.cn/php/func_string_parse_str.asp

4hash()

参考网址：https://www.php.net/manual/zh/function.hash.php

漏洞：

parse_str() 变量覆盖漏洞

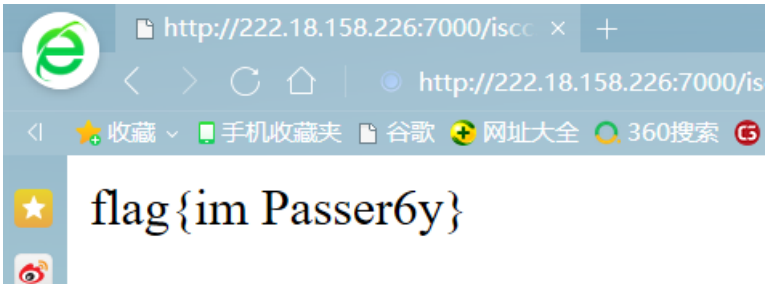
parse_str()函数往往被用于解析url得query_string,但是当参数值背用户所控制时，很可能导致变量覆盖。类似得有mb_parse_str()，想了解更多可以去网上查查资料

flag:

这里实则就是需要我们提交action=autu key要经过sha256加密过后与hashed_key相等，但是这里我想要去解密这个hased_ke却无果。

这道题考得就是变量覆盖，自己交一个自己知道结果得编码后hashed_key去覆盖最开始那个变量，实则最后就是自己与自己比较。

这里构造?
action=auth&key=abc&hashed_key=ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015
即可，提交则拿到flag



关于parse_str变量覆盖分析

这个漏洞有两个姿势.一个是不存在的时候一个是存在的时候. 经过测试该漏洞只在php5.2中存在,其余均不存在. 倘若在parse_str函数使用的代码上方未将其定义那么即存在变量覆盖漏洞否则不行. 还 ...

代码审计-MetInfo CMS变量覆盖漏洞

0x01 代码分析 安装好后是这样的 漏洞文件地址\include\common.inc.php 首先是在这个文件发现存在变量覆盖的漏洞 foreach(array('_COOKIE', '_POST ...

7. 由一道ctf学习变量覆盖漏洞

0×00 背景 近期在研究学习变量覆盖漏洞的问题,于是就把之前学习的和近期看到的CTF题目中有关变量覆盖的题目结合下进一步研究. 通常将可以用自定义的参数值替换原有变量值的情况称为变量覆盖漏洞.经常导 ...

PHP代码审计笔记--变量覆盖漏洞

变量覆盖指的是用我们自定义的参数值替换程序原有的变量值,一般变量覆盖漏洞需要结合程序的其它功能来实现完整的攻击. 经常导致变量覆盖漏洞场景有:$$,extract()函数,parse_str()函数, ...

2020/2/1 PHP代码审计之变量覆盖漏洞

0x00 变量覆盖简介 变量覆盖是指变量未被初始化,我们自定义的参数值可以替换程序原有的变量值. 0x01 漏洞危害 通常结合程序的其他漏洞实现完整的攻击,比如文件上传页面,覆盖掉原来白名单的列表,导 ...

php代码审计之变量覆盖

变量覆盖一般由这四个函数引起 <?php $b=3; $a = array('b' => '1'); extract($a,EXTR_OVERWRITE); print_r($b); / ...

Web安全之变量覆盖漏洞

通常将可以用自定义的参数值替换原有变量值的情况称为变量覆盖漏洞.经常导致变量覆盖漏洞场景有:$$使用不当,extract()函数使用不当,parse_str()函数使用不当,import_reques ...

[fortify] 变量覆盖漏洞

一.全局变量覆盖当register_global=ON时,变量来源可能是各个不同的地方,比如页面的表单,Cookie等. <?php echo "Register_globals: & ...

CTF——代码审计之变量覆盖漏洞writeup【2】

题目: 基础: 所需基础知识见变量覆盖漏洞[1] 分析: 现在的$a='hi',而下面的函数需满足$a='jaivy'才可以输出flag,那么需要做的事就是想办法覆盖掉$a原来的值. 那么出现的提示 ...

随机推荐

使用php+swoole对client数据实时更新(下)

上一篇提到了swoole的基本使用,现在通过几行基本的语句来实现比较复杂的逻辑操作: 先说一下业务场景.我们目前的大多数应用都是以服务端+接口+客户端的方式去协调工作的,这样的好处在于不论是处在何种终 ...

sql执行

一.提高sql执行效率---in与exist . where column in (select * from table where ...) . ...where exists (select ' ...

Linux内核中ioremap映射的透彻理解

几乎每一种外设都是通过读写设备上的寄存器来进行的,通常包括控制寄存器.状态寄存器和数据寄存器三大类,外设的寄存器通常被连续地编址.根据CPU体系结构的不同,CPU对IO端口的编址方式有两种: (1)I ...

unison + inotify 实现文件实时双向同步部署步骤

unison + inotify 实现文件实时双向同步部署步骤 一. Unison简介 Unison是Windows.Linux以及其他Unix平台下都可以使用的文件同步工具,它能使两个文件夹(本地或 ...

php程序员的开始

最近又懒惰了,博客没有更新,学习一直在停止,反思自己最近在学习什么了,但是脑子里面空白的一片,让我冒汗了.程序是一个不断的积累,最近在学习的路上,发现自己懂的越来越少,人就有点急躁了,什么都想学,导致 ...

QuickSort 递归 分治

QuickSort 参考, #include void swap(int v[], int i, int j); v ...

dojo事件

dojo.connect 和 dojo.disconnect /*建立连接*/ dojo.connect(/*Object|null*/ obj, /*String*/ event, /*Object ...

学JAVA第三天，JAVA第二章《JAVA数据类型》

---恢复内容开始--- 我们一般都用int类型,因为int类行一般的日常生活的数据都能满足了. 当然,想李嘉诚,马云这种有钱人,int类行就不能满足帮他记钱的了,像 ...

System.Security.Authentication.AuthenticationException：根据验证过程，远程证书无效。

好久没写博客了,今天突然遇到个神奇的问题. 做好的网站在win10上和Windows sever 2012 上都没有问题,搬到Windows sever 2003上就出现了这么一个错误: Server ...