PHP 邮件 PHP 错误处理

PHP Secure E-mails

在上一节中的 PHP e-mail 脚本中，存在着一个漏洞。

PHP E-mail 注入

首先，请看上一章中的 PHP 代码：

```
<html>
<head>
<meta charset="utf-8">
<title>菜鸟教程(runoob.com)</title>
</head>
<body>

<?php
if (isset($_REQUEST['email'])) { // 如果接收到邮箱参数则发送邮件
    // 发送邮件
    $email = $_REQUEST['email'] ;
    $subject = $_REQUEST['subject'] ;
    $message = $_REQUEST['message'] ;
    mail("someone@example.com", $subject,
    $message, "From:" . $email);
    echo "邮件发送成功";
} else { // 如果没有邮箱参数则显示表单
    echo "<form method='post' action='mailform.php'>
    Email: <input name='email' type='text'><br>
    Subject: <input name='subject' type='text'><br>
    Message:<br>
    <textarea name='message' rows='15' cols='40'>
    </textarea><br>
    <input type='submit'>
    </form>";
}
?>

</body>
</html>
```

以上代码存在的问题是，未经授权的用户可通过输入表单在邮件头部插入数据。

假如用户在表单中的输入框内加入如下文本到电子邮件中，会出现什么情况呢？

```
someone@example.com%0ACc:person2@example.com
%0ABcc:person3@example.com,person3@example.com,
```

```
anotherperson4@example.com,person5@example.com
%0ABTo:person6@example.com
```

与往常一样，mail() 函数把上面的文本放入邮件头部，那么现在头部有了额外的 Cc:、Bcc: 和 To: 字段。当用户点击提交按钮时，这封 e-mail 会被发送到上面所有的地址！

PHP 防止 E-mail 注入

防止 e-mail 注入的最好方法是对输入进行验证。

下面的代码与上一章中的类似，不过这里我们已经增加了检测表单中 email 字段的输入验证程序：

```
<html>
<head>
<meta charset="utf-8">
<title>菜鸟教程(runoob.com)</title>
</head>
<body>
<?php
function spamcheck($field)
{
    // filter_var() 过滤 e-mail
    // 使用 FILTER_SANITIZE_EMAIL
    $field=filter_var($field, FILTER_SANITIZE_EMAIL);

    //filter_var() 过滤 e-mail
    // 使用 FILTER_VALIDATE_EMAIL
    if(filter_var($field, FILTER_VALIDATE_EMAIL))
    {
        return TRUE;
    }
    else
    {
        return FALSE;
    }
}

if (isset($_REQUEST['email']))
{
    // 如果接收到邮箱参数则发送邮件

    // 判断邮箱是否合法
    $mailcheck = spamcheck($_REQUEST['email']);
    if ($mailcheck==FALSE)
    {
        echo "非法输入";
    }
    else
```

```
    {
        // 发送邮件
        $email = $_REQUEST['email'] ;
        $subject = $_REQUEST['subject'] ;
        $message = $_REQUEST['message'] ;
        mail("someone@example.com", "Subject: $subject",
        $message, "From: $email" );
        echo "Thank you for using our mail form";
    }
}
else
{
    // 如果没有邮箱参数则显示表单
    echo "<form method='post' action='mailform.php'>
    Email: <input name='email' type='text'><br>
    Subject: <input name='subject' type='text'><br>
    Message:<br>
    <textarea name='message' rows='15' cols='40'>
    </textarea><br>
    <input type='submit'>
    </form>";
}
?>

</body>
</html>
```

在上面的代码中，我们使用了 PHP 过滤器来对输入进行验证：

- FILTER_SANITIZE_EMAIL 过滤器从字符串中删除电子邮件的非法字符
- FILTER_VALIDATE_EMAIL 过滤器验证电子邮件地址的值

您可以在我们的 PHP Filter 中阅读更多关于过滤器的知识。

← PHP 邮件 PHP 错误处理 →