**Gym Management System 1.0远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

Gym管理系统版本1.0存在未经验证的文件上载漏洞，使得远程攻击者能够通过上载绕过图像上载过滤器的恶意构建的PHP文件，在宿主Web服务器上获得远程代码执行（RCE）

# 二、机理分析

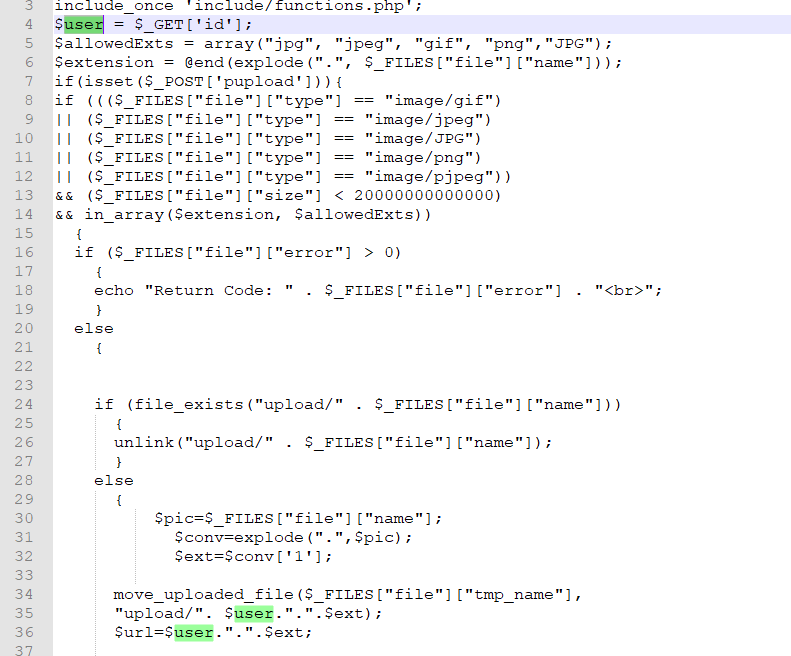
## 1、Gym Management System 1.0远程代码执行漏洞

**影响版本：**5.0.23</5.1.31<

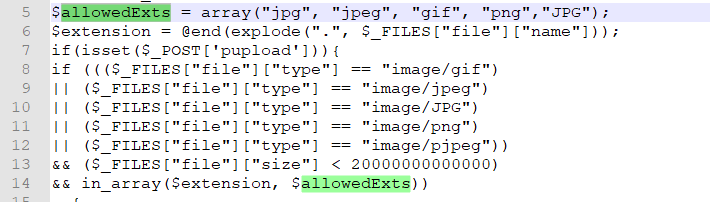
**漏洞编号：**1.0

1. 访问'/upload.php，因为它不检查经过身份验证的用户会话。
2. 将GET请求的“id”参数设置为上载的PHP文件所需的文件名。

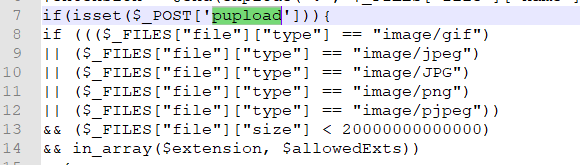
使用move\_uploaded\_file函数将id参数作为了文件名



1. 通过添加一个双扩展名来绕过扩展名白名单，最后一个扩展名是可接受的扩展名（png），比如shell.php.png



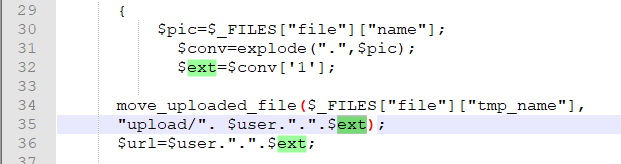
1. 在POST请求中将“file”参数的“Content type”修改为“image/png”，并将“pupload”参数设置为“upload”，从而绕过文件类型检查。



1. 在POST请求的“file”参数体中，插入恶意PHP代码：

<?php echo shell\_exec($\_GET["cmd"]); ?>

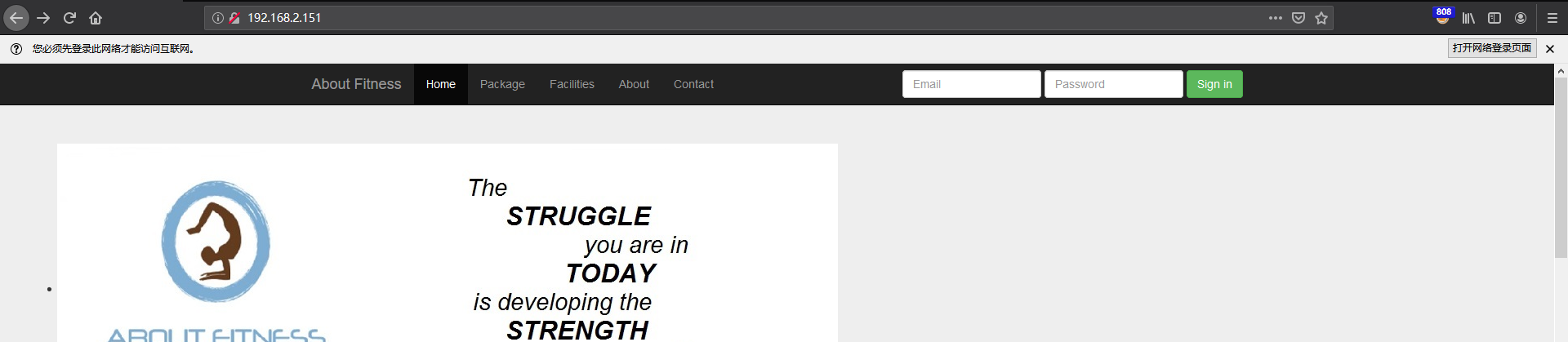
1. Web应用程序将重命名该文件，使其扩展名为从文件名创建的数组中的第二项；用“.”字符分隔。因为我们用的是双扩展名shell.php.png，所以用“.”字符分隔的数组的第二项为php，所以最终会被重命名为.php



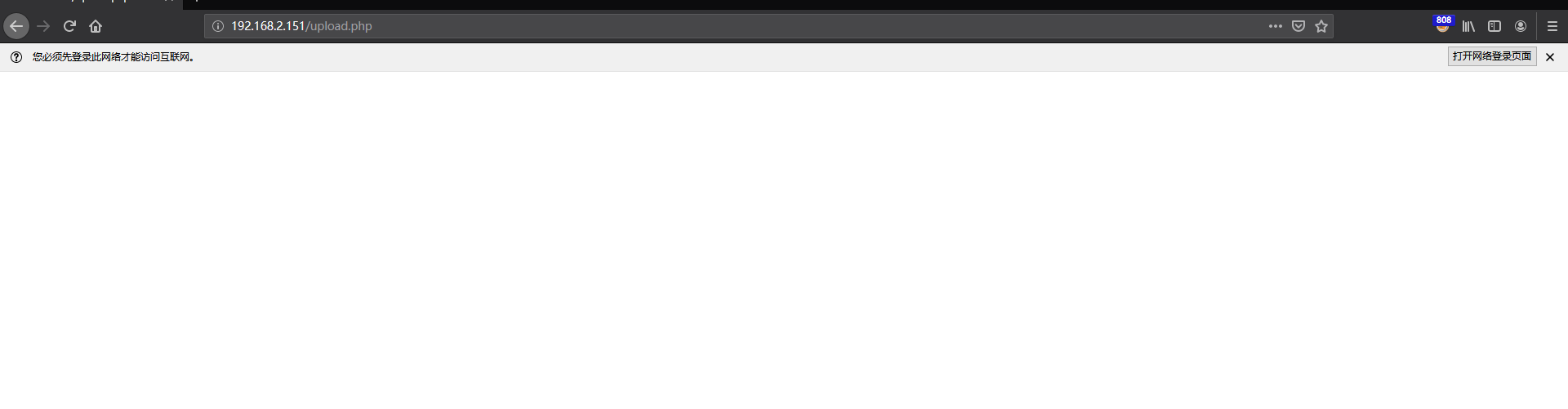
7. 访问websell执行任意命令

# 三、攻击路径

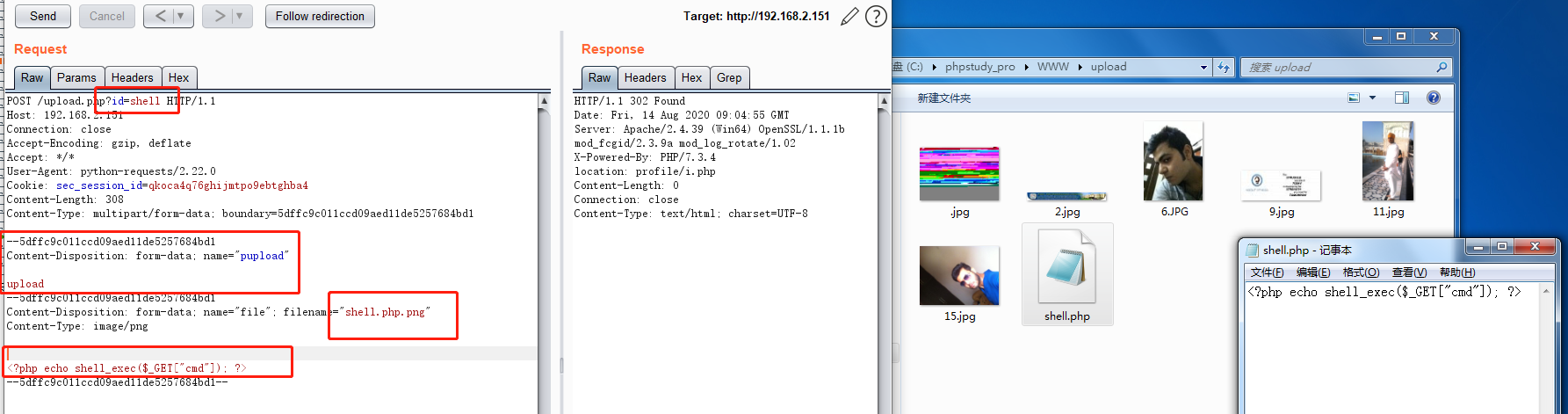
访问web



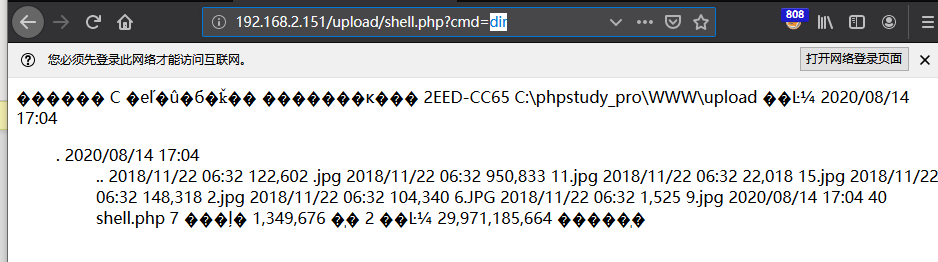
无需登录访问/upload.php



用burp构造payload



然后访问webshel



# 四、防御方案

使用最终扩展名来命名文件，而不是数组第二项