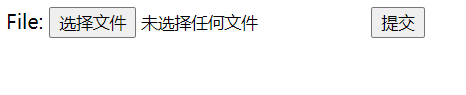
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问ip地址，可查看到上传文件接口

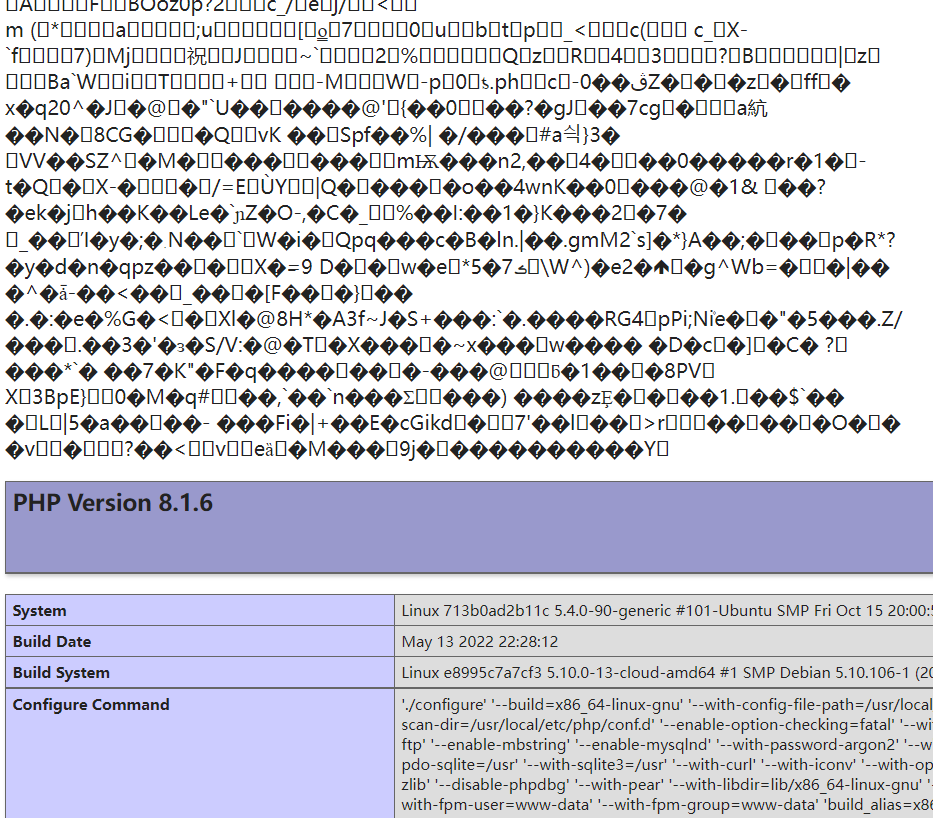


**二、漏洞复现**

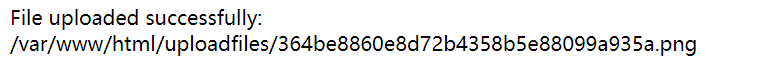
1、访问<http://your-ip/uploadfiles/nginx.png>



2、访问<http://your-ip/uploadfiles/nginx.png/.php>，此时被解析成php文件



3、访问http://your-ip/index.php，上传带有phpinfo代码的test.png



4、访问<http://your-ip/uploadfiles/364be8860e8d72b4358b5e88099a935a.png/.php>，成功被解析

