宝塔面板未授权访问数据库管理界面漏洞复现

原创 Sky Timeline Sec
2020-09-01原文

收录于话题
#漏洞复现 111
#宝塔 25
#漏洞复现文章合集 70

上方蓝色字体关注我们，一起学安全！

本文作者：Sky@Timeline Sec

本文字数：612

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

宝塔面板是一款服务器管理软件，支持windows和linux系统，可以通过Web端轻松管理服务器，提升运维效率。例如：创建管理网站、FTP、数据库，拥有可视化文件管理器，可视化软件管理器，可视化CPU、内存、流量监控图表，计划任务等功能。

0x02 漏洞概述

该漏洞是phpmyadmin未鉴权，可通过特定地址直接登录数据库的漏洞。

0x03 影响版本

宝塔Linux面板7.4.2版本
宝塔Linux测试版7.5.13
Windows面板6.8版本

0x04 环境搭建

为

在搭建环境的过程，遇到了宝塔面板自动升级的问题，导致无法停留在漏洞版本，为此，Sky师傅专门制作了docker镜像供大家复现。

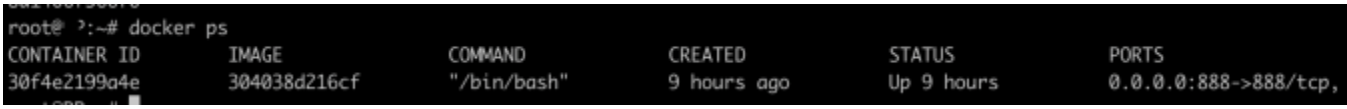
转发文章后后台回复“**宝塔靶场**”即可获得在线环境。

自行搭建方式如下：

```
# 配置加速器：

vi /etc/docker/daemon.json

# 替换为：

{

    "registry-mirrors":["https://docker.mirrors.ustc.edu.cn/"]

}

# 重启docker

sudo systemctl restart docker


# 拉取镜像启动docker环境：

docker pull tim2docker/baota2:v1

docker images
```

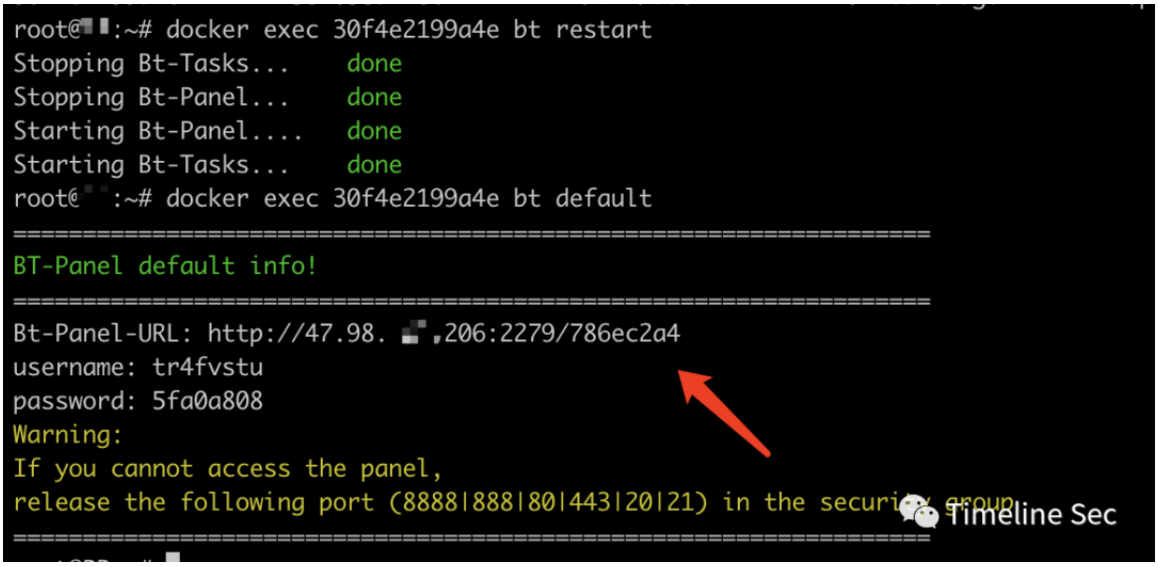
```
docker run -d -it -p 8888:8888 -p 888:888 -p 2279:2279 <your
IMAGE ID>
```

```
docker ps
```




```
docker exec <your CONTAINER ID> bt restart
```

```
docker exec <your CONTAINER ID> bt default
```



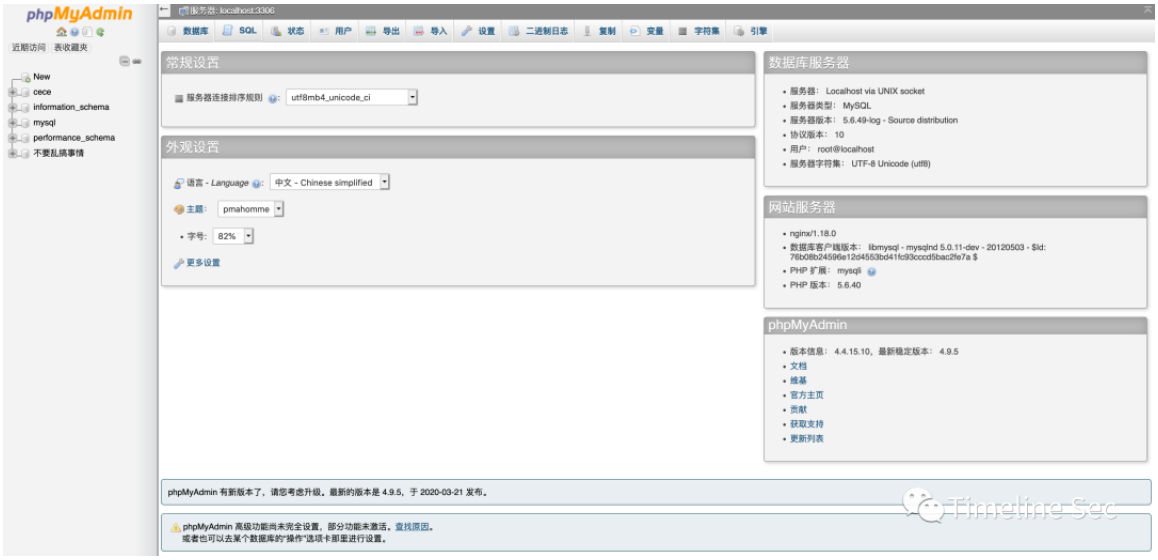
访问得到的url并输入username和password进入宝塔面板后台
启动Nginx、Mysql和PHP（设置中启动）

访问http://your_ip:888

至此，环境搭建完毕。

0x05 漏洞复现

直接访问http://your_ip:888/pma



0x06 漏洞分析

具体原因p牛已经分析得很清晰了：

宝塔面板phpMyAdmin未授权访问漏洞是个低级错误吗？

0x07 修复方式

更新至官方最新版本。

参考链接：

https://mp.weixin.qq.com/s/3ZjwFo5gWlJACSkeYWQLXA

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文