

# 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
```

```
root@ ?:~# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS
30f4e2199a4e   304038d216cf  "/bin/bash"             9 hours ago   Up 9 hours   0.0.0.0:888->888/tcp,
```

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

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

```
root@ ?:~# docker exec 30f4e2199a4e bt restart
Stopping Bt-Tasks... done
Stopping Bt-Panel... done
Starting Bt-Panel... done
Starting Bt-Tasks... done
root@ ?:~# docker exec 30f4e2199a4e bt default
=====
BT-Panel default info!
=====
Bt-Panel-URL: http://47.98. .206:2279/786ec2a4
username: tr4fvstu
password: 5fa0a808
Warning:
If you cannot access the panel,
release the following port (8888|888|80|443|20|21) in the security group.
=====
```

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）

应用搜索 支持应用名称、字段模糊搜索

应用分类 全部 已安装 运行环境 系统工具 宝塔插件 专业版插件 企业版插件 第三方应用 一键部署 更新软件列表

酷锐云最稳最便宜服务器提供商

空广告位

当前为专业版，专业版可以免费使用专业版插件，过期时间：永久授权

软件名称	开发商	说明	价格	更新时间	位置	状态	显示提示	操作
Nginx 1.18.0	官方	轻量级，占有内存少，开发能力强	免费	-		▶	▶	设置   卸载
MySQL 5.6.49	官方	MySQL是一种关系数据库管理系统	免费	-		▶	▶	更新   设置   卸载
php PHP-5.6	官方	PHP是世界上最好的编程语言	免费	-		▶	▶	设置   卸载
FTP Pure-FTPd 1.0.49	官方	PureFTPd是一款专注于程序健壮性和软件安全的免费FTP服务器软件	免费	-		▶	▶	设置   卸载
phpMyAdmin 4.4	官方	著名Web端MySQL管理工具	免费	-		▶	▶	设置   卸载
Linux工具集 1.4	官方	Linux系统工具，配置DNS、Swap、时区、IP配置、内存等！	免费	-		▶	▶	更新   设置   卸载
宝塔SSH终端 1.0	官方	完整功能的SSH客户端，仅用于连接本服务器	免费	-		▶	▶	设置   卸载
宝塔 CDN 静态文件加速 7.2	白	对静态文件进行CDN加速，加快页面加载速度，减轻用户服务器压力，自动选择最优线路！	免费	-		▶	▶	设置   卸载

1/11 从1-8款 共8条数据

访问[http://your\\_ip:888](http://your_ip:888)

## 403 Forbidden

nginx

Timeline Sec

至此，环境搭建完毕。

## 0x05 漏洞复现

直接访问[http://your\\_ip:888/pma](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/3ZjwFo5gWIJACskeYWQLXA>





**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](#)