链滴

Web 建站安全防护建议

作者：sides
原文链接：https://ld246.com/article/1512475925240
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

最近自己建了个网站，网站安全搞了一阵，闲来没事就写写总结，方便以后查看。

建议

1. 服务器上能少开的端口就少开

2. 服务器最好禁ping

3. 服务器最好使用秘钥登录，禁止root账号登录

4. 应用程序千万不要使用root启动！！mysql、nginx、java程序这些最好用其他用户启动。还有，行的用户不允许对源代码有修改的权限！

5. 程序如果有上传文件的功能，相应的目录不能有执行的权限。

6. 关于暴露服务器真实ip的问题，如果作为web网站，除了购买高仿IP，好像别无选择。。 我的网站前没管，用cdn好像也没多大作用

7. 对于公开访问的网站，一定要做好防xss、CSRF、sql注入攻击，具体如何防御，请百度。对于ddo攻击，就别想防了，不过阿里云有5G的免费防御可以用，超了没法，早点洗洗睡吧！有钱人另说

8. 千万不要以为用户的输入是合法的，一定要控制输入的内容。要采取防御式的方式去处理应用。确应用的安全。一般我们提倡的是：防御式架构和防御式编程

9. 服务器最好装个fail2ban，开启sshd、sshd-ddos、mysql防护，另外配合nginx监控日志来防护目前记得的就这些

10. nginx做好网站限流配置

11. 修改linux系统内核参数配置，sysctl.conf

现在的技术已经很发达了，网络安全防不胜防，没有百分百的安全，上面的建议对于一般的公司网站说，差不多够用了。暂时想到这么多，后面想到再补充吧！