（三） Nginx

1、文件解析

2、目录遍历

3、CRLF 注入

4、目录穿越

1.

文件解析

主要结合上传漏洞

个人以前的总结：

<http://www.youknowi.xin/2018/09/%e5%85%b8%e5%9e%8b%e6%bc%8f%e6%b4%9e%e5%bd%92%e7%ba%b3%e4%b9%8b%e4%b8%8a%e4%bc%a0%e6%bc%8f%e6%b4%9e%ef%bc%88%e8%bd%ac%e8%bd%bd%ef%bc%89/>

http://www.youknowi.xin/2018/10/%e6%96%87%e4%bb%b6%e4%b8%8a%e4%bc%a0%e7%9a%84%e5%a7%bf%e5%8a%bf/



2.

目录遍历

即index of

预防：

在配置文件中删除autoindex on即可

3.

可参考：

<https://blog.csdn.net/think_ycx/article/details/50267801>

http://www.youknowi.xin/2019/01/crlf%e6%b3%a8%e5%85%a5/

crlf 注入

\r\n

浏览器会根据第一个CRLF把HTTP包分成头和体，然后将体显示出来

xss利用补充：把数据包中http头含有X-XSS-Protection并且值为0的时候，浏览器不会开启filter

预防：

过滤\r 、\n之类的换行符

修改配置文件使用不解码的url跳转

4.

目录穿越

其成因除去目录遍历漏洞中开启的autoindex on;选项，同时在配置文件/etc/nginx/conf.d/error2.conf中，没有闭合跳转目录