ALB漏洞修复

# 概述

本文档针对ALB敏捷版（alb-agile）的相关漏洞报告，参考Nginx的处理配置，提供相应的解决方案。

【**注意**】：下面的修复配置，是基于location /站点配置演示的，实际配置时请根据漏洞报告的实际站点（location）进行配置，另外关于请求及响应头处理的配置，若需全局生效（即所有location站点都生效），可在http模块中配置（全局生效），优先级顺序是：

“Server模块 > Http模块 > Location模块”

# **漏洞修复**

## 2.1 HTTP Strict-Transport-Security头缺失或不安全

【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的location / 模块中加入：

add\_header Strict-Transport-Security "max-age=63072000; includeSubdomains; preload";



## 2.2 “Content-Security-Policy”头缺失

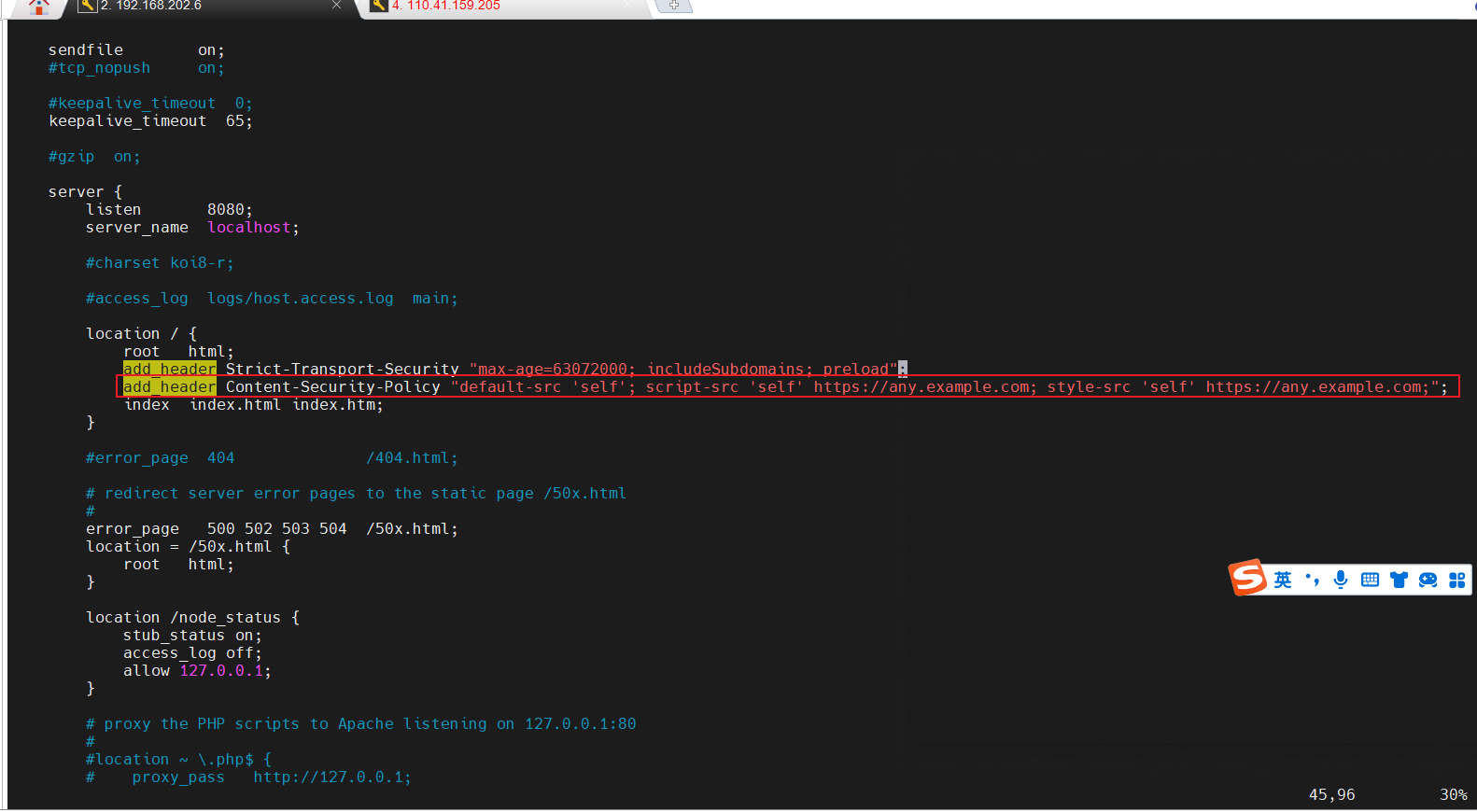
【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的location / 模块中加入（不一定能直接复用，需要根据资源响应慢慢配置）：

add\_header Content-Security-Policy "default-src 'self' data: 'unsafe-inline' 'unsafe-eval' 'unsafe-hashes'; script-src 'self' data: 'unsafe-inline' 'unsafe-eval' 'unsafe-hashes'; ";



【**注意**】Content-Security-Policy头的配置，是会对请求资源做拦截的，所以能不配建议就不配，配置地不合理会影响到正常资源的加载，也有可能上面的配置不一定能完全生效，可以根据响应的异常提示进行参数配置，具体参数说明参考下方：

参数说明：[Nginx配置Http响应头安全策略\_nginx content-security-policy-CSDN博客](https://blog.csdn.net/qq_32808455/article/details/133969833)

## 2.3 “X-Content-Type-Options”头缺失或不安全

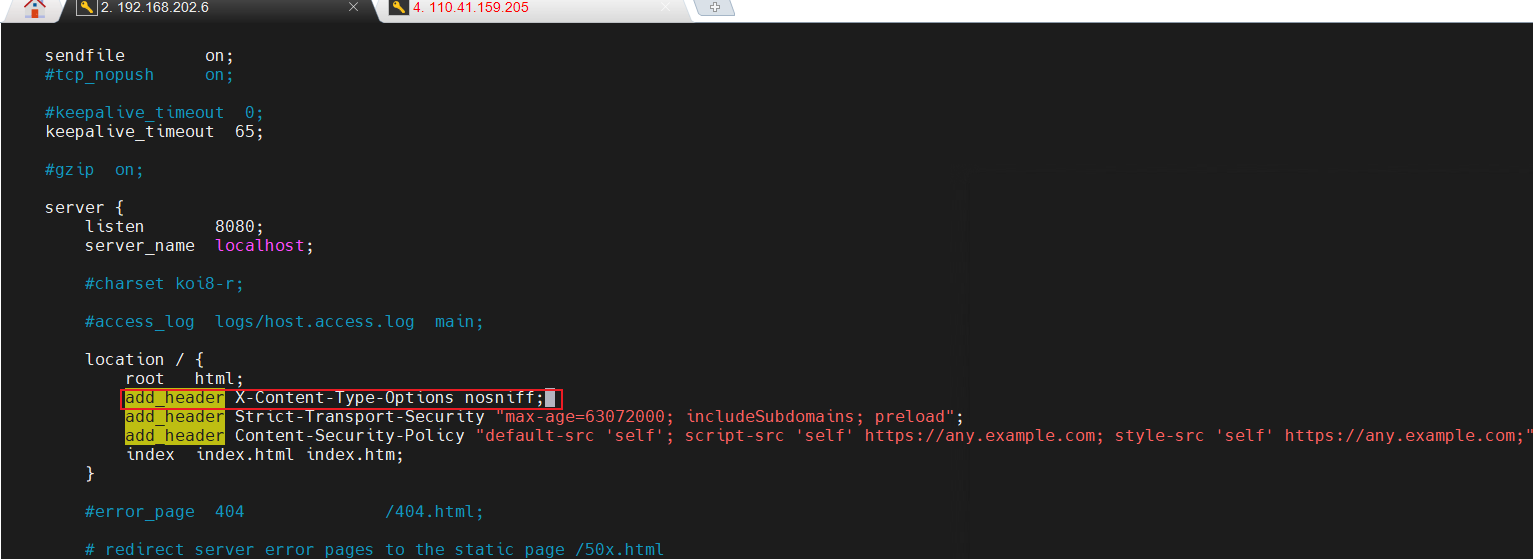
【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的location / 模块中加入：

add\_header X-Content-Type-Options nosniff;



## 2.4 主机头注入攻击

【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的server模块中添加对于非server\_name的判断（具体以配置的server\_name为准）：例我这里是192.168.202.6

if ($http\_host !~\* ^192.168.202.6$ ) {

return 444;

}



## 2.5 具有不安全、不正确或缺少 SameSite 属性的 Cookie

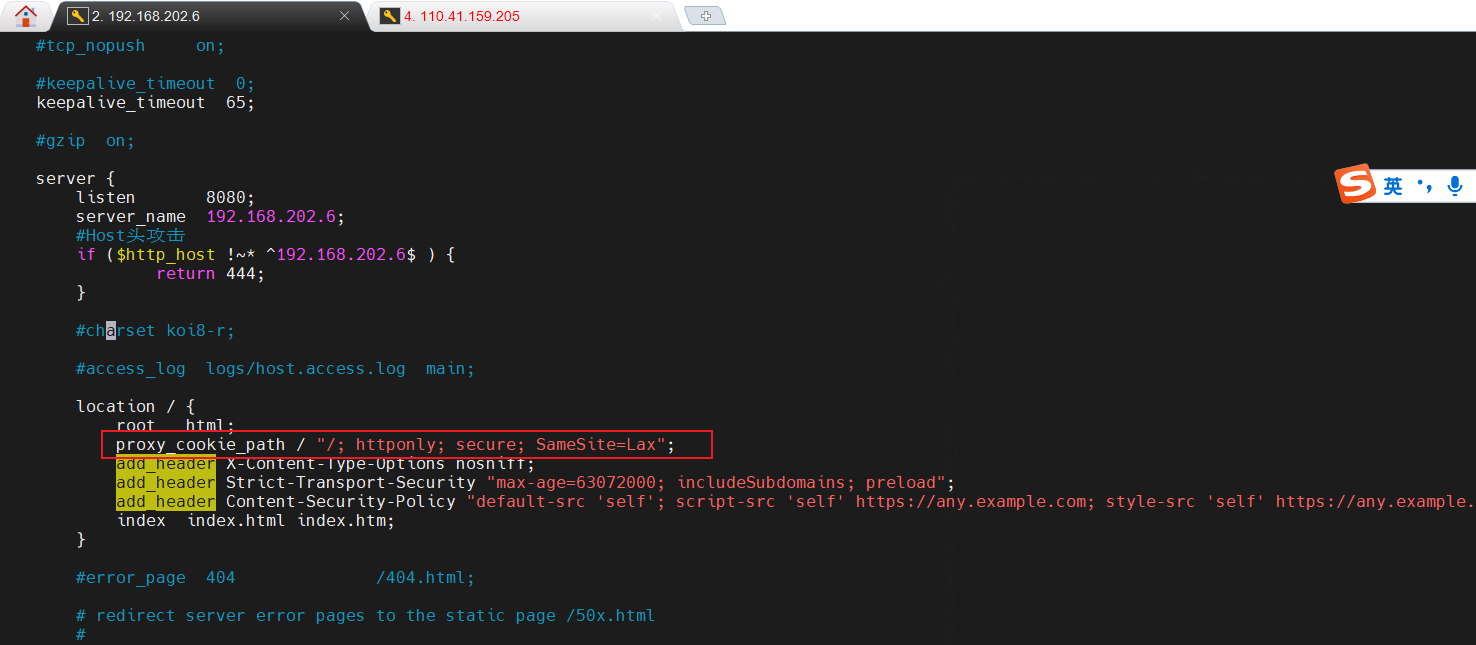
【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的location / 模块中加入（这个前后端都可以配置一下策略试试）：

proxy\_cookie\_path / "/; httponly; secure; SameSite=Strict";



【说明】：

1、proxy\_cookie\_path参数中的两个路径/ /表示将cookie原先path为/改为/,这个请根据实际站点cookie的path进行配置，一般原先的path是什么，就还是改为什么，例如: proxy\_cookie\_path /test "/test; httponly; secure; SameSite=Strict";

2、SameSite策略有None、Lax、Strict，一般浏览器默认用Lax，限制非Get请求的跨域请求，Strict是最严格的，一般Strict才能过扫描工具，但这个策略对cookie权限保存可能有一定的影响；

3、后端安全配置（tomcat的安全配置）：https://bwisebi-doc.biaopu.cloud/devops/install/tomcat/#security

## 2.6 发现可高速缓存的 SSL 页面

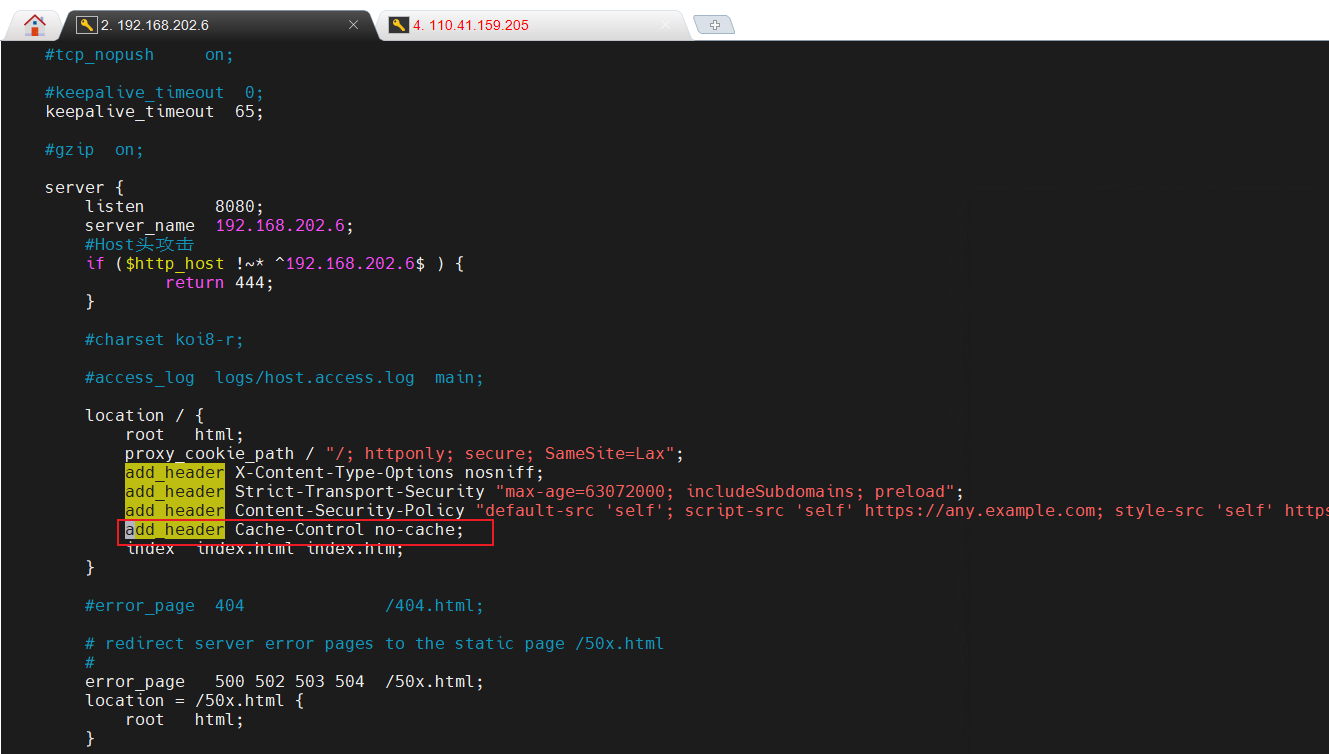
【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的location / 模块中加入：

add\_header Cache-Control no-cache;



## 2.7 在应用程序中发现不必要的 Http 响应头

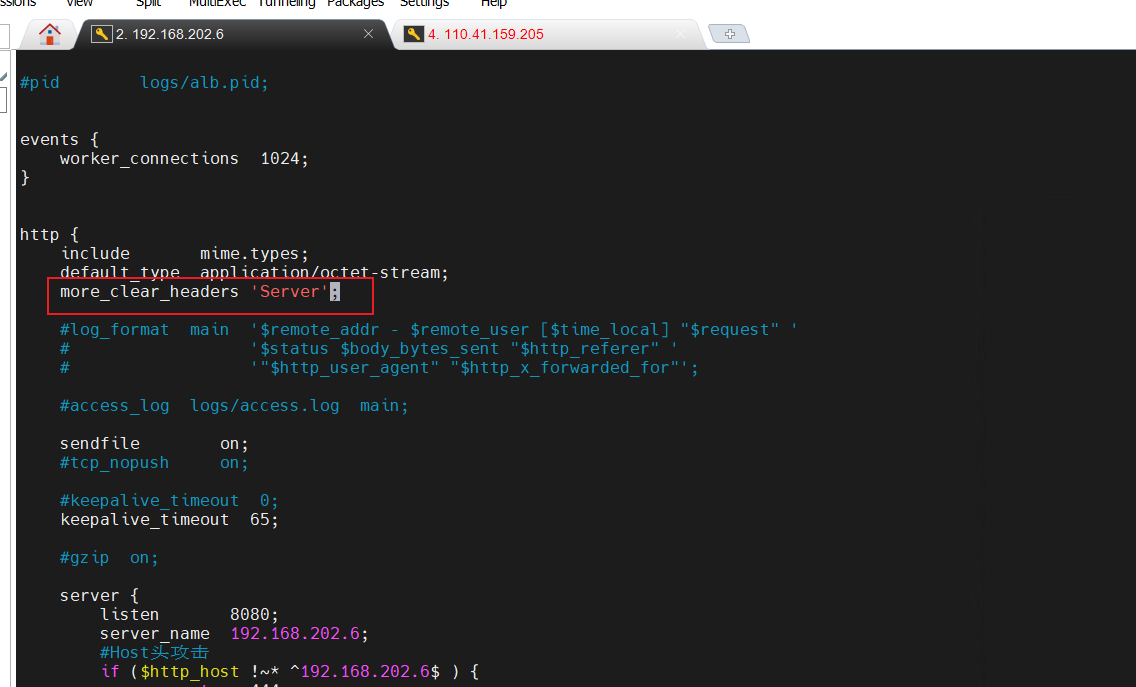
【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf的http模块加入：

more\_clear\_headers 'Server';



（但不确定alb与插件是否兼容）有可能需要另外安装插件：[nginx-在应用程序中发现不必要的Http响应头\_nginx剔除去掉server: nginx的响应头-CSDN博客](https://blog.csdn.net/u013008898/article/details/136168888)

## 2.8 检测到隐藏目录

【漏洞说明】：



【修复处理】：

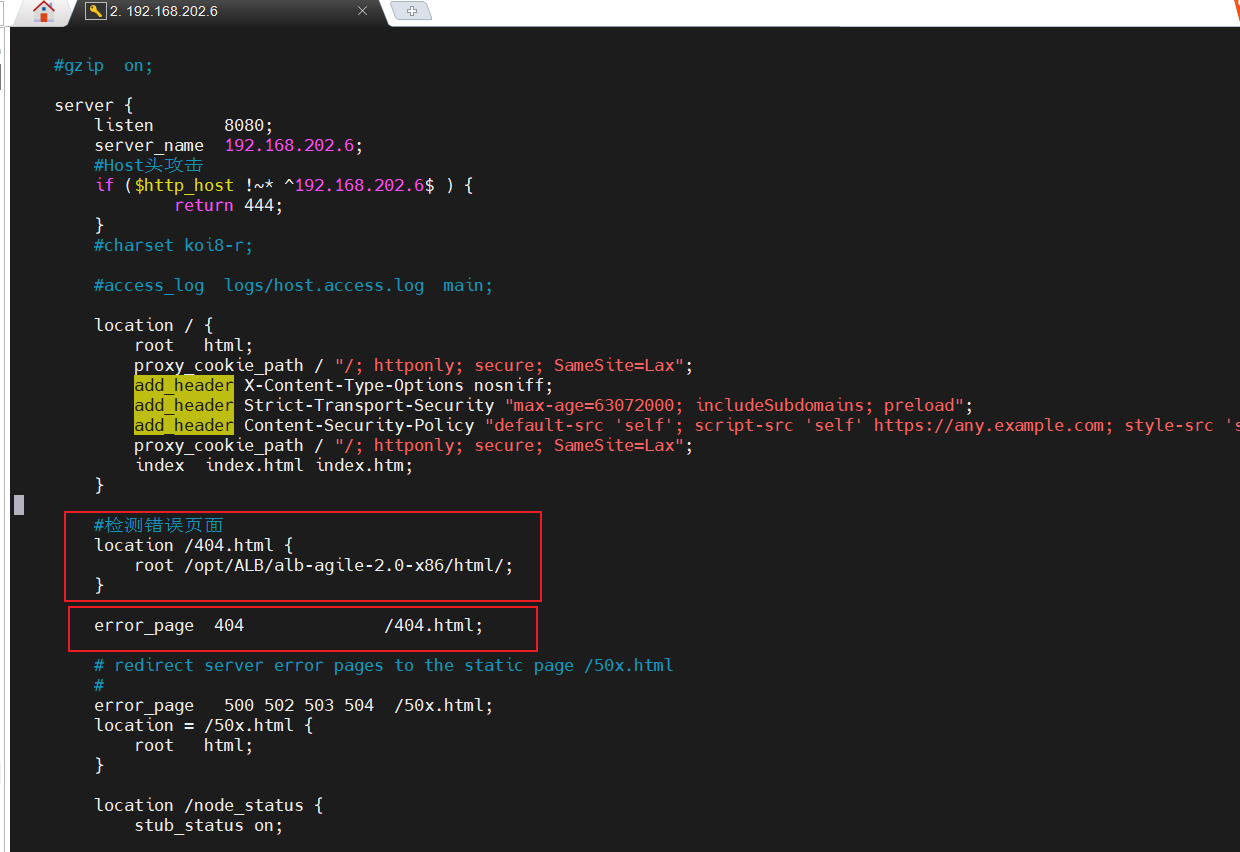
在{产品安装目录}/conf/alb.conf中引入404错误页面：

1、注释-启动404错误页面；

2、加入location /404.html

3、在{产品安装目录}/html目录下创建一个404.html，自行编写页面内容；

【**注意**】：一般隐藏目录访问的某个具体路径，确定这个路径不是业务需要的话，对这个路径访问进行拦截，并返回404



## 2.9 跨站点请求伪造

【漏洞说明】：



【修复处理】：

在{产品安装目录}/conf/alb.conf中server模块加入：

if ($http\_Host !~\* ^127.0.0.1$|^192.168.202.6$) {

return 403;

}

valid\_referers none blocked 127.0.0.1 192.168.202.6;

if ($invalid\_referer) {

return 403;

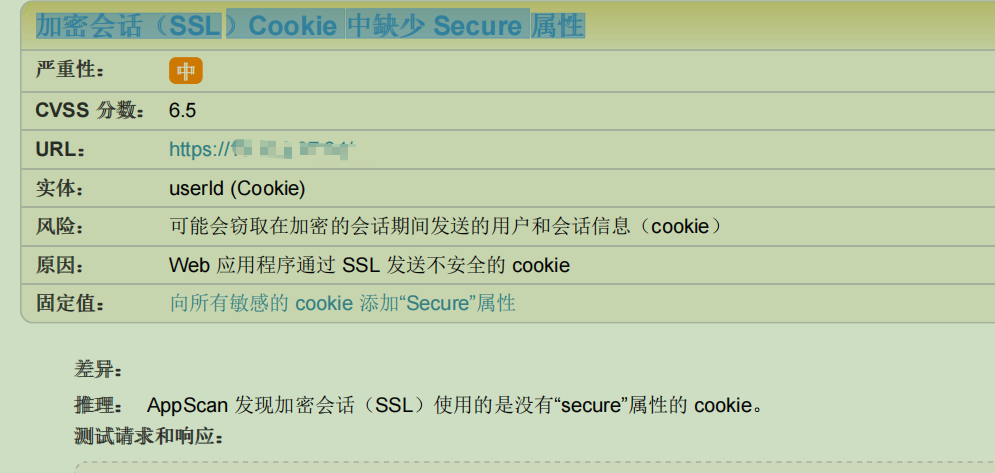
}

【**注意**】:这里红色部分是对应配置文件中server\_name的信息，有几个就写几个，具体的配置参考下文的连接

【参考链接】：<https://blog.csdn.net/liqun_super/article/details/124190824>

## 2.10 加密会话（SSL）Cookie 中缺少 Secure 属性

【漏洞说明】：



【修复处理】：可以在后端（应用服务器）端配置：

【参考链接】：https://blog.csdn.net/huaquan520/article/details/81358893