



链滴

基于 caddy 提升 https 安全等级

作者: [yuanhenglizhen](#)

原文链接: <https://ld246.com/article/1543153259670>

来源网站: 链滴

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

起因

最近由于工作无暇处理博客，昨天正好看了下博客，发现博客的https被降权到B,所以折腾一波，提高+

基础环境

web: caddy +jetty

降权原因

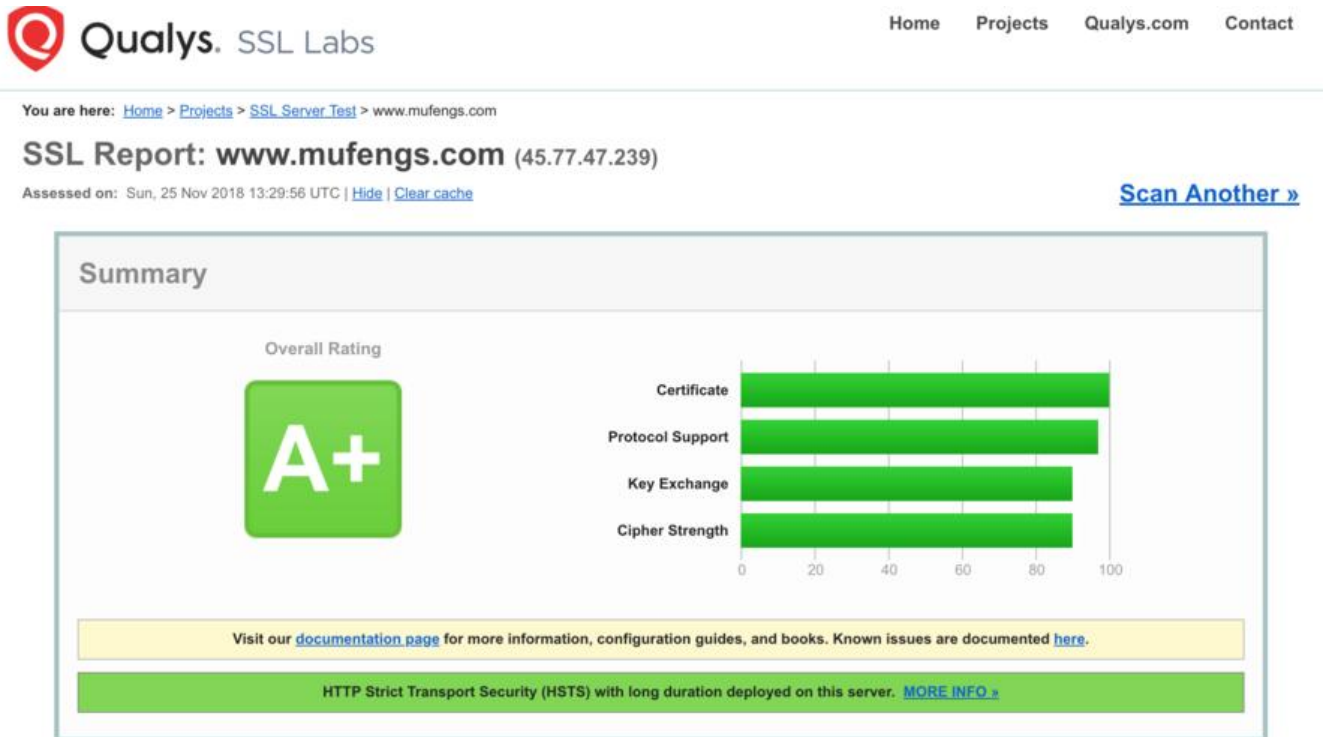
发到mysl那边提示的降权的主要原因是由于网站含有http的不安全链接，于是想起来，有个图片是接引用某网站的http链接，将http搞成https

去掉tls 1.0协议,添加hsts强制https

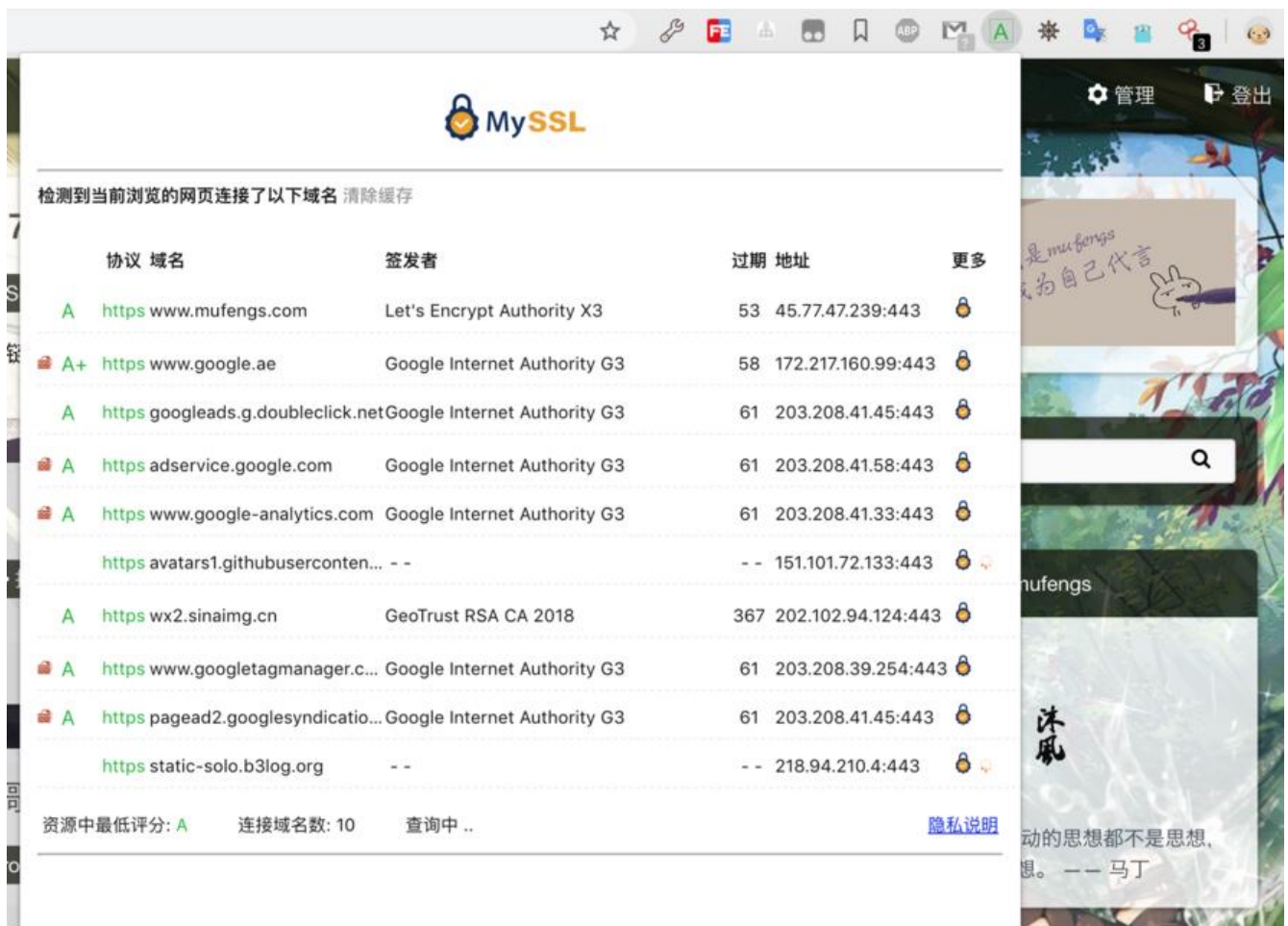
```
http://www.mufengs.com {
header / {
    # Enable HTTP Strict Transport Security (HSTS) to force clients to always
    # connect via HTTPS (do not use if only testing)
    Strict-Transport-Security "max-age=31536000;"
    # Enable cross-site filter (XSS) and tell browser to block detected attacks
    X-XSS-Protection "1; mode=block"
    # Prevent some browsers from MIME-sniffing a response away from the declared Content-Type
    X-Content-Type-Options "nosniff"
    # Disallow the site to be rendered within a frame (clickjacking protection)
    X-Frame-Options "DENY"
}
redir https://www.mufengs.com{url}
}
https://www.mufengs.com
{
header / {
    # Enable HTTP Strict Transport Security (HSTS) to force clients to always
    # connect via HTTPS (do not use if only testing)
    Strict-Transport-Security "max-age=31536000;"
    # Enable cross-site filter (XSS) and tell browser to block detected attacks
    X-XSS-Protection "1; mode=block"
    # Prevent some browsers from MIME-sniffing a response away from the declared Content-Type
    X-Content-Type-Options "nosniff"
    # Disallow the site to be rendered within a frame (clickjacking protection)
    X-Frame-Options "DENY"
}
# expires {
#     match .css$ 1m
#     match .js$ 1m
#     match .png$ 1m
#     match .jpg$ 1m
# }
gzip #开启gzip压缩
log /root/www/access.log #访问日志的配置
errors /root/www/error.log
tls mufeng5619@gmail.com {
    protocols tls1.1 tls1.2
}
proxy / http://127.0.0.1:8080 { #反向代理到82端口
    # transparent
    header_upstream Host {host}
    header_upstream X-Real-IP {remote}
    header_upstream X-Forwarded-For {remote}
    header_upstream X-Forwarded-Proto {scheme}
}
```

测试

Myssl那边由于vps所在地原因，一直更新不了。所以采用国外的SSL Server Test (Powered by Qualy SSL Labs)测试结果如下图



另外也附上myssl没有实时更新的图



原文链接: 基于 caddy 提升 https 安全等级

附录

1.获取caddy, 安装脚本

<https://getcaddy.com/>

2.caddy文档

[tls - Caddy User Guide](#)

3.myssl

<https://myssl.com/>