证书部署常见问题

一、安全检测中涉及证书常见问题

1、 Q：安全检测中，出现缺少证书链问题，如何处理？

A：若出现证书链问题，证书链文件单独引用一行

以 Apache 配置文件为例，配置文件中证书引用如下：

```
#公钥文件
SSLCertificateFile /etc/httpd/conf.d/server.crt
#私钥文件
SSLCertificateKeyFile /etc/httpd/conf.d/server.key
#证书链文件（如：DigiCertCA.crt)
SSLCertificateChainFile /etc/httpd/conf.d /CA.crt
```

以 Nginx 配置文件为例，配置文件中证书引用如下：

```
#公钥文件
ssl_certificate /etc/nginx/domain.com.pem;
#私钥文件
ssl_certificate_key /etc/nginx/domain.com.key;
# 证书链文件，CA.crt 是中间证书， 一般存放于压缩包中。
ssl_trusted_certificate /etc/nginx/CA.crt;
```

2、 Q：安全检测中，出现使用 SSLV2、SSLV3、TLSv1 协议导致网站不安全，如何修改？

A：Apache、Tomcat、Nginx 修改配置文件中含 protocol 字段的协议，至少使用 TLSv1.1 及以上协议；IIS 中使用的协议需在注册表中添加/修改。

3、 Q：安全检测中，出现安全套件相关漏洞，如何处理？

A：使用检测网站推荐的安全套件，或参考 https://ssl-config.mozilla.org/ 所列安全套件

4、Q：安全检测中出现漏洞 HTTP 响应头未设置 Strict-Transport-Security

A：在相关域名例如 www.domain.com 的 server 块加入以下参数：

nginx 配置如下参数：

```
server {
    listen 443 ssl  ;
    listen [::]:443 ssl  ;
    server_name www.domain.com;
… …
 # HSTS (ngx_http_headers_module is required) (63072000 seconds)
add_header Strict-Transport-Security "max-age=63072000" always;
… …
}
```

Apache 配置如下参数：

```
<VirtualHost _default_:443>
DocumentRoot "/var/www/html"
ServerName www.domain.com:443
.... ...
Header add Strict-Transport-Security "max-age=63072000"
.... ...
</VirtualHost>
```

5、安全检测中出现漏洞的处理办法

1)、Q：安全检测中出现漏洞 HTTP 响应头未设置 X-XSS-Protection

Q：安全检测中出现漏洞 HTTP 响应头未设置 X-Frame-Options

Q：安全检测中出现漏洞 HTTP 响应头未设置 X-Content-Type-Options

A：

Nginx：编辑 /etc/naginx/nginx.conf 文件在 http 块加入以下参数：

```
http {
 … …
  add_header X-XSS-Protection "1; mode=block";
  add_header X-Frame-Options "SAMEORIGIN";
  add_header    X-Content-Type-Options：nosniff;
… …
}
```

Apache:

修改 httpd.conf 或者 /etc/httpd/conf.modules.d/00-base.conf 文件，确保启用了 mod_headers.so。以下行取消注释符号"#"。

```
LoadModule headers_module modules/mod_headers.so
```

修改 httpd.conf 在文件末尾添加以下参数：

```
<IfModule mod_headers.c>
  Header set X-XSS-Protection "1; mode=block"
  Header always append X-Frame-Options SAMEORIGIN
   Header set X-Content-Type-Options nosniff
</IfModule>
```

2)、Q：禁止显示 WEB 服务器版本

A:

Nginx:编辑 /etc/naginx/nginx.conf 在 http 块加入以下参数：

```
http {
 ……
    server_tokens off;
……
```

}

Apache: 编辑/etc/httpd/conf/httpd.conf

在文件末尾加入以下参数：

ServerTokens Prod

二、IIS 部署证书常见问题

1、 Q：IIS 服务器部署 SSL 证书，如何配置完成访问 http 跳转到 https？

A：1、根据 IIS 版本备份以下文件：

IIS6.0 路径：C：\Windows\Help\iisHelp\common\403-4.htm

IIS7.0 以上 路径：C：\inetpub\custerr\zh-CN\403.htm

IIS 服务中如有 URL 重写，可直接在 URL 重写中添加规则完成 http 跳转到 https

2、低版本 IIS 需修改文件完成 https 跳转的，参考以下内容：

把以下 script 脚本全部拷贝替换(403-4 或 403)文件<body>……</body>中内容，保存即可

```
<script type="text/javascript">
 var url=window.location.href;
  if(url.indexOf("https")<0){
        url=url.replace("http:","https:");
        window.location.replace(url);
 }
</script>
```

注释：IIS6 中，站点属性-》目录安全性-》编辑中把"要求安全通道(SSL)"勾选上即可。IIS7、8 中，SSL 设置-》把"要求 SSL"勾选即可。

2、 Q：如果在 IIS 平台安装 cer 证书，提示“如果与申请证书的服务器不是同一台”，怎么办？

A：直接导入 pfx 格式证书

pem 证书转换 pfx 证书命令：

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.pem

3、 Q：IIS、IIS7 不支持多站点部署 HTTPS 怎么办？

A：有两种解决方案供选择：

1、至少升级到 Windows2012+IIS8 解决。

2、使用 Nginx 反向代理解决。

三、Apache 部署证书常见问题

1、 Q：Windows 下 Apache 默认安装不含 mod_ssl.so 模块，如何处理？

A：http://www.openssl.org/

根据系统选择 32 位或者 64 位版本下载安装

增加环境变量：OpenSSL_HOME 值：C：\Program Files\OpenSSL-Win64

在 path 环境变量的最后增加 ;%OpenSSL_HOME%

需要重启服务器生效。

四、Tomcat 部署证书常见问题

1、 Q：如何从制作 CSR 文件时生成的 JKS 文件中提取私钥 key 文件？

A：参考如下两步，其中文件名、密码按实际情况进行修改

1、jks 文件中的私钥不能直接得到，需要通过 OpenSSL 将 jks 文件转换成 pfx 格式后再进行提取。

执行如下命令将 server.jks 文件转换成 server.pfx 文件：

keytool -v -importkeystore -srckeystore server.jks -srcstoretype jks -srcstorepass jksfilepassword -destkeystore server.pfx -deststoretype pkcs12

2、执行如下命令便可以将 servers.pfx 的私钥导出：

OpenSSL pkcs12 -in server.pfx -nocerts -nodes -out server.key

2、 Q：Tomcat 上中使用 jks 格式证书如何转换？

A：1、Pem 格式证书转换 pfx 证书命令，会让设置密码，请记住设置的密码

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.pem

2、 pfx 文件转换为 jks 文件命令

keytool -importkeystore -srckeystore server.pfx -destkeystore server.jks -srcstoretype PKCS12 -deststoretype JKS

注：请替换成相应证书、私钥文件名。

五、证书部署后常见问题

1、 Q：证书已部署，443 端口已打开，https 访问证书仍不生效，为何？

A：1、检查服务器、防火墙上 443 端口是否都已打开。

2、检查服务器上 443 端口是否被其他应用程序占用。

2、 Q：证书已部署，443 端口均已打开，且未被占用，网站 https 访问仍不生效，为何？

A：检查网站是否做了负载均衡存在多台服务器部署的情况，或者部署位置是否错误（一般存在多个 tomcat 情况下，部署在舍弃不用的 tomcat 上但该 tomcat 也是正常运行状态）。

3、 Q：证书部署后内网 https 访问正常，外网 https 无法访问？

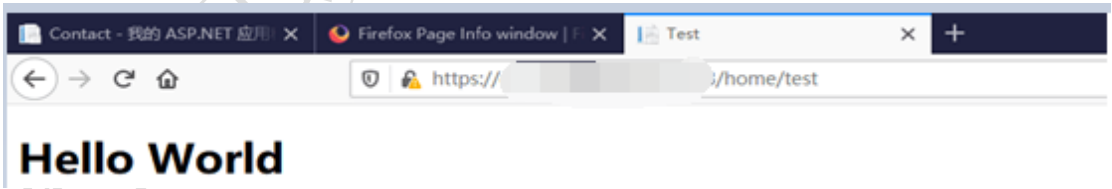
A：检查网站是否加入了各种安全网盾，如已加入安全网盾，需在网盾中针对各网站有对应的证书。

4、 Q：证书已部署，但是网站证书的颁发机构不是颁发证书的机构？

A：证书颁发机构被篡改，检查网络出口设备是否篡改了信息。

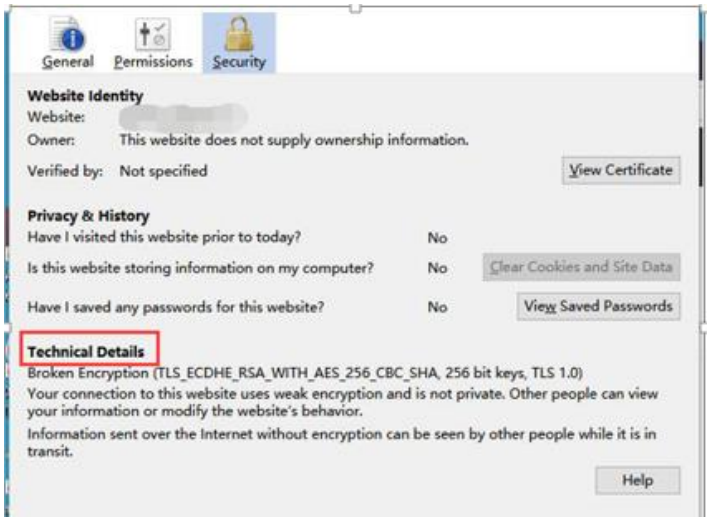
5、 Q：证书已部署，但为何浏览器上仍显示不安全？

A：不同浏览器呈现不安全的方式不同，有的直接显示“不安全”，有的在安全小锁上带有感叹号，如下图：



点击小锁，查看详情中可以查看“技术细节”，

根据提示具体问题具体分析，如下图：



6、 Q：原网站 http 访问正常，但 https 无法访问？

A：此问题多出现在 Windows XP 操作系统，使用 IE 或 IE 内核浏览器（如：360 浏览器），建议解决方案有二种：

1、升级操作系统

2、更换为 Chrome（谷歌浏览器）或 Firefox（火狐浏览器）