附件

江苏金坛图书馆

网络信息安全事件 (漏洞) 信息及处置建议

编号: JT-AQSJ-JTL-10

1 总体情况

经检测江苏金坛图书馆（URL 地址：www.jsjtlib.com）网站，发现存在不安全的 HTTP 请求方法等高危风险漏洞 1 个，为保证整个网站系统的安全性，请尽快修复该漏洞。

漏洞详情如下：

表 1: 漏洞列表

序号	漏洞类型	URL 网址	请求类型	参数	严重性
1	不安全的 HTTP 请求方法	http://www.jsjtlib.com/	OPTIONS		高

2 漏洞详情

2.1 不安全的 HTTP 请求方法

WEB 服务器默认是不开启 PUT 等方法的，出现该漏洞的原因主要是网站管理员对服务器的错误配置。常见的主要就是管理员错误地打开了 IIS 的服务器的 webDAV 而且没有开启权限验证，导致可以 PUT 文件到服务器再利用服务器的解析漏洞运行恶意代码或者用 webDAV 的 MOVE 方法将所上传的带有恶意代码的普通文件后缀修改为可执行文件后缀，运行恶意代码。

测试链接：http://www.jsjtlib.com/

测试语句：

```
OPTIONS / HTTP/1.1
Host: www.jsjtlib.com
Connection: Keep-alive
Accept: text/plain
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9.1) Gecko/20090624 Firefox/3.5
```

测试截图：

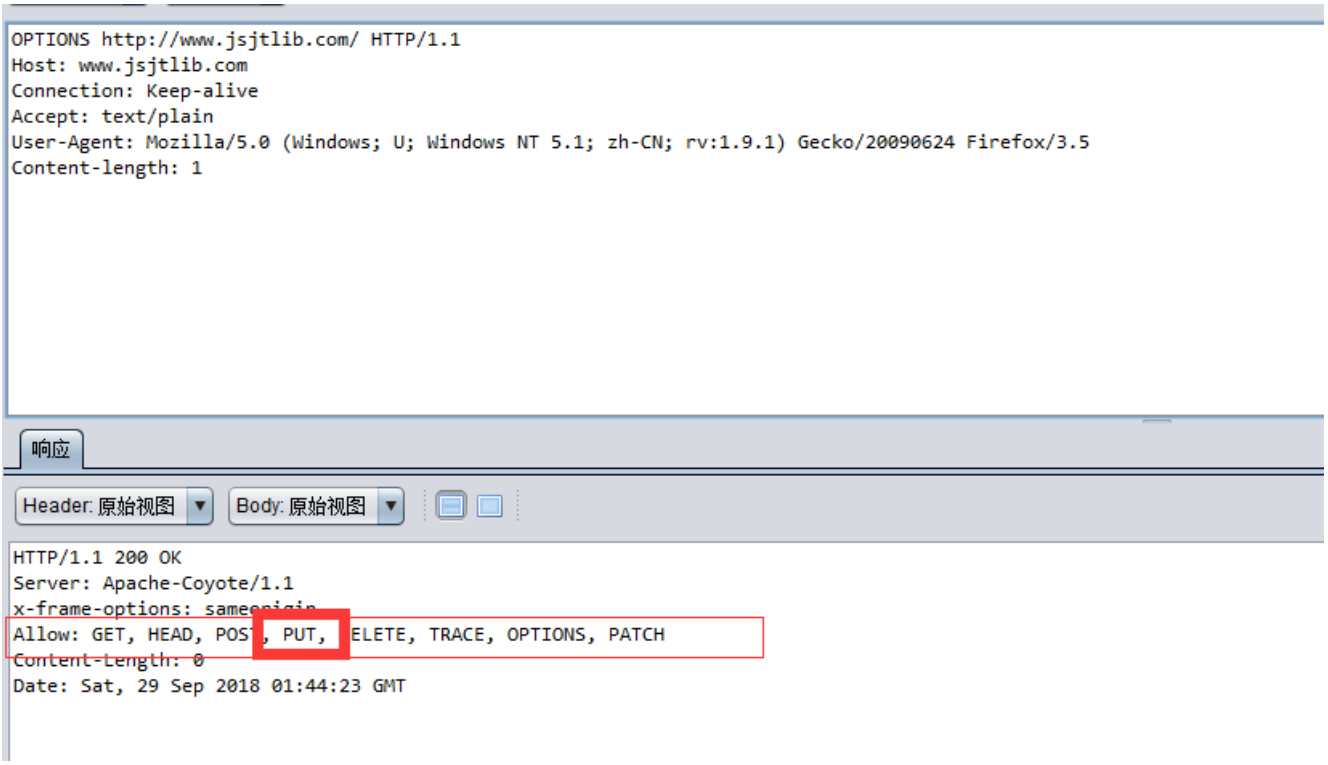

图 1: 不安全的 http 请求方法

3 处置建议

- 不安全的 HTTP 请求方法
  - 如果不是必要，禁用 WebDAV；
  - 如果要使用 WebDAV 的话，加上权限验证，并禁止 PUT、DELETE 等危险的请求方法。