一种采用MD5加密算法防止URL攻击的方法

张 杰[1] ， 李华伟[2] ， 周立军[1]

(1. 海军航空工程学院，烟台 264001；2 山东商务职业学院，烟台 264001)

摘 要：在简要分析当前URL攻击手段的基础上，提出一种使用MD5加密算法有效防止URL攻击的方法，按照URL合法性检测流程，设计基于Java MVC轻量级框架Struts的测试方案，比较MD5和DES算法在URL参数加密过程中的性能。

关键词：URL攻击；MD5算法；Struts；DES算法

0 引 言

由于Web B/S瘦客户端应用具有免安装等优点，同时Web应用程序逐步采用富应用程序模型和交互个性化内容，Web应用展现形式更加多样化。伴随着网络的日益普及，在网络主机上部署越来越多的Web应用，用户获取网络资源通常通过对应的URL，如果涉及重要资源或者权限的URL可以很容易地被用户猜出，资源(Web应用)的安全性将很难保证，当前URL攻击方式很多，例如SQL注入、语义URL攻击、XSS URL攻击、畸形URL攻击、URL溢出攻击等[1]。

1 方法思路

在网络上Web应用遭受URL攻击非常普遍，如何保证系统提供给用户的URL才能被访问，屏蔽用户伪造或篡改的URL访问，就能很好地防止URL攻击。一种防范URL攻击简单而有效的方法是采用加密技术对部分URL进行加密获取到字符串，并以附加参数方式传递给Web服务器，服务器接受用户URL请求后，根据密钥同样对URL进行加密进行处理，与附加参数进行对比判断URL是否合法(篡改)。

2 关键技术

以J2EE Web应用为例，实现采用MD5加密算法有效防止URL攻击。

当前J2EE Web应用多采用MVC架构，以Struts、Webwork为控制器，控制器接收来自浏览器的请求，并决定将这个请求发往何处。就Struts而言，Struts控制器组件负责接收用户的请求，更新模型以及选择合适的视图组件返回给客户端。采用ActionServlet统一拦截用户URL请求并进行验证。

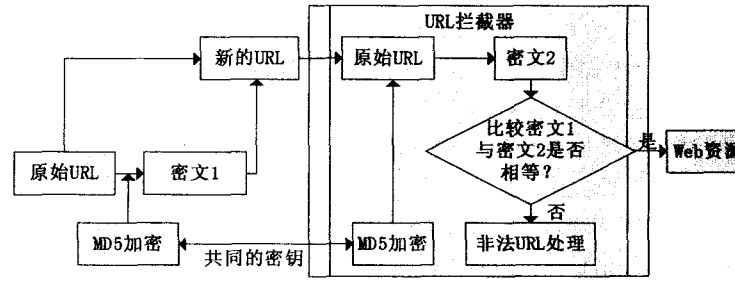

图1 URL合法性检测流程

2.1 MD5算法实现

MD5信息-摘要算法(Message Digest Algorithm 5)将任意长度的“字节串”变换成一个128bit的大整数，并且它是一个不可逆的字符串变换算法，Java语言实现MD5算法基于Java安全类库，该类库提供了一个java.security.MessageDigest类，此MessageDigest类为应用程序提供信息摘要算法的功能，例如MD5或SHA算法。信息摘要是安全的单向哈希函数，它接收任意大小的数据，并输出固定长度的哈希值[2]。

收稿日期：2011-03-05 修稿日期：2011-03-25

作者简介：张杰(1983-)，男，山东日照人，硕士，研究方向为J2EE、软件工程

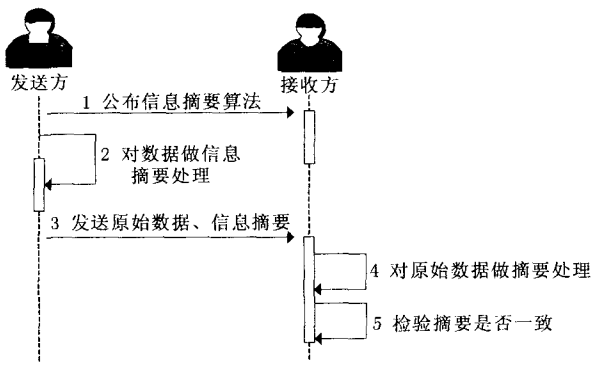

图 2 MD5 摘要校验过程

```
public class MD5 {
public static String crypt(String str) {
try {
MessageDigest md = MessageDigest.getInstance ("MD5"); //所用的加密算
mdupdate(str.getBytes());
byte[] digestArr = md.digest(); //计算摘要,加密
return byte2hex(digestArr);
}catch (Exception e) {
return "error! ";
}
}
public static String byte2hex(byte[] b) {
String hs = "";
String stmp = "";
for (int n = 0; n < b.length; n++) {
stmp = (java.lang.Integer.toHexString(b[n] & 0XFF));
if (stmp.length() == 1) {
hs = hs + "0" + stmp;
}else {
hs = hs + stmp;
}
}
return hs.toUpperCase();
}
}
```

2.2 Struts ActionServlet 拦截 URL 请求

ActionServlet 类是 Struts 框架的内置核心控制器组件，它继承了 javax.servlet.http.HttpServlet 类，Struts 的启动一般从加载 ActionServlet 开始，它在 MVC 模型中扮演中央控制器的角色。ActionServlet 是一个标准的 Servlet，在 web.xml 文件中配置，该 Servlet 用于拦截所有的 HTTP 请求[3]。因此，应将 Servlet 配置成自启动 Servlet，即为该 Servlet 配置 load-on-startup 属性，在 web.xml 中添加如下配置：

```
<servlet>
<servlet-name>action</servlet-name>
<servlet -class >com.platform.CheckActionServlet </servlet -class>
<init-param>
<param-name>config</param-name>
<param-value>/WEB-INF/struts-config.xml</param-value>
</init-param>
<init-param>
<param-name>debug</param-name>
<param-value>3</param-value>
</init-param>
<init-param>
<param-name>detail</param-name>
<param-value>3</param-value>
</init-param>
<load-on-startup>0</load-on-startup>
</servlet>
<servlet-mapping>
<servlet-name>action</servlet-name>
<url-pattern>*.do</url-pattern>
</servlet-mapping>
```

其中，CheckActionServlet 继承 ActionServlet。

3 测试与比较

采用 MVC 轻量级框架 Struts 涉及一测试 Web 应用程序，系统提供的合法 URL 包括两部分：原始 URL 与加密 URL 生成的附加参数，Struts ActionServlet 中对 URL 请求进行验证是否被非法篡改，加密方法分别采用 MD5 与 DES 算法，其中，DES 算法是一种单钥密码体制加密算法，信息的发送方和接收方共同使用同一把密钥进行加解密，具有简便高效，密钥简短，加解密速度快，破译极其困难，但是加密的安全性依靠密钥保管的安全性。

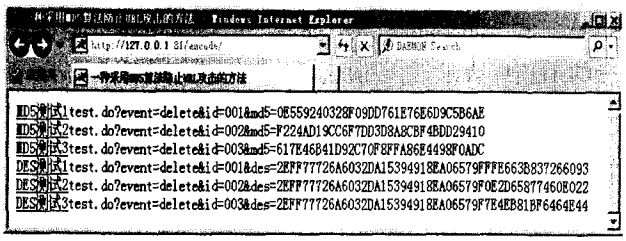

图 3 MD5 与 DES 算法对 URL 加密

通过运行程序并分析运行结果，得出以下结论：对 URL 参数 “event=delete&id=001” 进行加密 10000 次，MD5 算法花费的时间为 140 毫秒，DES 算法为 329 毫秒；同时，MD5 生成附加参数共 32 个字符，DES 算法生成 48 个字符的附加参数，且 MD5 生成的附件参数的字符个数不会随着 URL 的长度变化而变化，DES 算法则会不断增长。

4 结 语

URL 是用户获取网络资源的一种重要方式，如何识别 URL 是否被篡改是控制资源访问的有效途径，本文提出了一种基于 MD5 加密算法的防止 URL 攻击的方法，并使用 Java 安全类库实现了对 URL 的 MD5 加密，同时给出了 URL 检测流程，设计基于 Java MVC 轻量级框架 Struts 的测试方案，最后比较了 MD5 和 DES 算法在 URL 参数加密过程中的性能，得出 MD5 在 URL 加密方面性能优于 DES 算法的结论。

参考文献

[1]杜恩宽. URL 攻击防范和细粒度权限管理的安全链接方法[J]. 计算机应用，2008,29(8):2230~2231

[2]林晶，黄青松，张晶. 基于改进 MD5 算法的数据篡改检测方法[J]. 计算机工程与应用，2008,44(33):148~150

[3]孙卫琴. 精通 Struts:基于 MVC 的 Java Web 设计与开发[M]. 电子工业出版社，2004

A Method that Preventing URL Attack Based on MD5 Encryption Algorithm

ZHANG Jie[1] , LI Hua-wei[2] , ZHOU Li-jun[1]

(1. Naval Aeronautical and Astronautical University, Yantai 264001; 2. Shandong Business Institute, Yantai 264001)

Abstract: Based on brief analysis of the current URL attack means, puts forward a method using MD5 encryption algorithm effectively prevent URL attack.According to the URL legitimacy detecting process, designs a test scheme based on Java MVC lightweight framework Struts, then compares the performance between the MD5 and DES algorithm in URL parameter encryption process.

Keywords: URL Attack; MD5 Encryption Algorithm; Struts; DES