提高网络安全性的方法研究与实现

邹金慧[1], 田招选[2]
(1.昆明理工大学 信息工程与自动化学院,云南 昆明 650051; 2.文山州工商行政管理局,云南 文山 663000)

摘要: 通过对影响网络系统安全性的主要因素进行分析,提出了改进的用户验证、URL请求验证和抗 SQL注入式攻击等几种提高网络安全性的方法,并给出了每种方法的实现流程图和用户验证的部分代码,应用结果表明,这些方法能有效地提高网络系统的安全性.

关键词: 网络系统; 安全性; 用户验证; URL; SQL
中图分类号: TP309 文献标识码: A 文章编号: 1007-855X(2008)06-0032-03

Methods to Enhance Network Security and Their Realization

ZOU Jin-hui[1], TIAN Zhao-xuan[2]
(1. Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China;
2. Industrial and Commercial Bureau of Wenshan District, Wenshan, Yunnan 663000, China)

Abstract: Based on a comprehensive analysis of network security, this paper proposes such methods as improving user verification, URL test and anti-SQL. The flow charts of their realization and part of the user verification code of these methods are also presented respectively. It is indicated through the results that these methods can effectively enhance network security.

Key words: network; security; user verification; URL; SQL

0 引 言

网络安全是网络正常运行的前提,也是实现网络安全管理的基础.随着互联网的飞速发展,网络安全已逐渐成为一个潜在的巨大问题.因此,在各类网站的建设过程中,网站的设计者必须充分考虑网络系统的安全性问题,所开发的系统必须能对敏感数据进行加密处理,严格区分各类用户的操作权限,跟踪用户的操作行为,具有防抵赖机制.同时,系统还要具备一定的抗恶意攻击功能,比如 SQL注入式攻击、非法URL(Uniform Resource Locator,统一资源定位符)请求、恶意全文检索数据库等.此外,系统必须对有可能产生的异常进行必要的处理,且异常的出现不能影响正常的浏览.

1 提高网络系统安全性的几种方法

网络安全防范与保护的主要策略是访问控制,访问控制的主要任务是保证网络资源不被非法使用和非法访问,它是保证网络安全最重要的核心策略之一.传统的访问控制策略有入网访问控制、网络的权限控制和客户端安全防护策略等.其中,“入网访问控制”是控制哪些用户能够登录到服务器并获取网络资源,它通常包括用户名的识别与验证、用户口令的识别与验证以及用户账号的缺省限制检查等三关,只要任何一关未通过,该用户就不能进入网络.因此,对网络用户的用户名和口令进行验证是防止非法访问的第一道防线,也是用户入网的关键.下面介绍能进一步提高系统安全性的几种有效方法.

1.1 改进的用户验证流程

传统的用户验证过程是将客户端输入的验证信息进行 MD5加密形成“密文 1”,发送到服务器端,服

收稿日期: 2008-04-15.基金项目: 云南文山州工商行政管理局网站建设项目.
第一作者简介: 邹金慧(1963-),女,硕士,副教授.主要研究方向: 计算机应用、PLC、智能控制.
E-mail: km.zjh@163.com

务器端从数据库读出验证信息的 MD5值(密文 2), 然后“密文 1”与“密文 2”进行对比, 若相等则认证成功, 否则失败. 但是, 如果“密文 1”在传输过程中被非法获取, 非法用户即使不知道“密文 1”的内容, 直接向服务器发送“密文 1”并请求验证, 则验证有可能成功, 用户的真实性将无法保证[1]. 因此, 需要对传统的用户验证过程进行改进. 在用户要求开始身份验证时, 系统随机生成一个验证码并写入 Session, 当用户输入用户名和密码之后, 浏览器首先将用户名、密码和验证码分别进行两次 MD5加密, 然后再对用户名和密码的两次 MD5加密结果组合进行一次 MD5加密, 将上述加密结果提交给系统, 同时系统将服务器端的验证码也进行两次 MD5加密运算得到一个运算结果, 将此结果与用户提交的加密运算结果进行比较判断即可进一步保证入网用户的真实性, 如图 1所示.

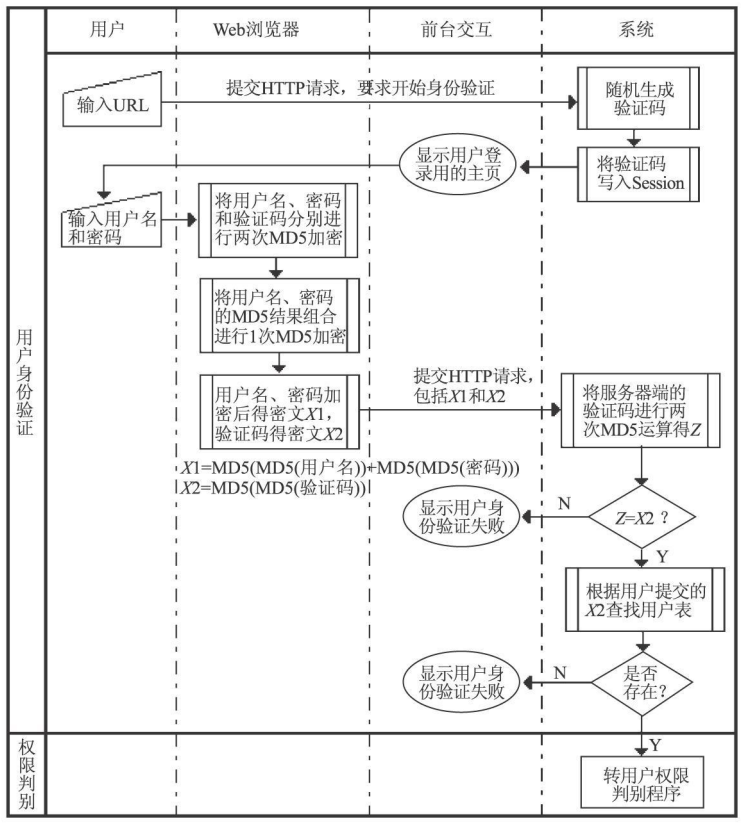

图1　改进的用户验证流程图

Fig.1　Flowchart of improving user verification

1. 2 URL请求验证流程

URL请求验证是防止用户非法请求的一种方法. 非法请求是用户直接向服务器发送 URL请求, 在请求中传递一些非法参数, 绕过系统的认证程序, 以达到入侵者的非法目的. 非法 URL请求是入侵系统的常用手段. 因此, 进行 URL请求的验证是提高系统安全性的一种有效方法. 为了进一步提高系统的安全性, 除了后台的 URL需要验证外, 前台的大多数页面也需要验证, 特别是处理过程的执行, 要求只能由指定的页面执行, 其它任何形式的请求都将被拒绝. 现以点击次数的统计为例, 说明URL请求的验证过程, 如图 2所示.

1. 3 抗 SQL注入式攻击流程

SQL注入式攻击是指在输入框或 URL中输入 SQL语句, 绕过验证程序, 非法获取用户的访问权, 进行非法操作的入侵方式. 防御 SQL注入式攻击的方法常用两种, 一种是使用数据库管理系统的存储过程, 另一种是对输入的信息和 URL进行必要的过滤. 开发网站时, 在 URL请求验证的基础上, 对输入的信息进行验证

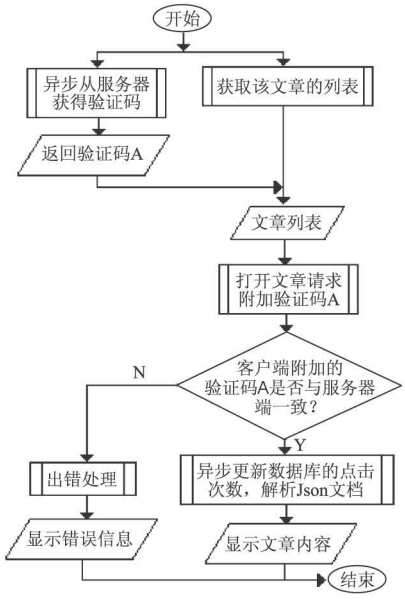

图2　URL请求验证流程图

Fig.2　Flowchart of URL test

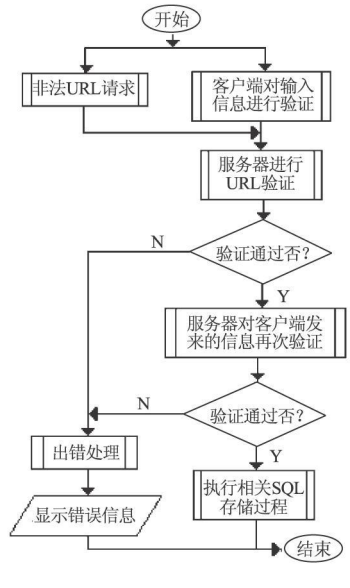

图3　抗SQL注入式攻击流程图

Fig.3　Flowchart of SQL method

(包括数据格式的合法性和非法 SQL语句检查),对敏感过程使用 SQL的存储过程,实行客户端与服务器端的双重认证,提高系统的安全性.抗 SQL注入式攻击流程如图 3所示.

2 实现用户验证的部分代码

用户验证包括客户端的验证和服务器端的验证.客户端的验证过程是向服务器发送获取验证码请求,从服务器得到验证码后,将用户输入的用户信息加密发送到服务器,由服务器进行下一步的验证;服务器端的验证包括 URL的验证和用户信息的验证.实现客户端的验证代码较多,主要有创建 XMLHttpRequest对象、获取验证码的值、以图片方式显示用户验证码、点击登录按钮时触发的事件、向服务器发送处理请求、判断服务器端验证是否通过等.以下代码是点击登录按钮时所触发的事件[2].

```
function dl()
  {
    var yhm = document.getElementById("yhm").value;
    var mm = document.getElementById("yhdMm").value;
    var yzm = document.getElementById("yhdYzm").value;
     if(yzm! = validate)
      {
        alert("验证码不正确,请重新输入.");
        createValidate("yhdYzm","yhdImage");
      }
     else
      {
        yhm = hexMD5(hexMD5(yhm));
        mm = hexMD5(hexMD5(mm));
        yzm = hexMD5(hexMD5(yzm));
        var userInfo = "userInfo = " + hexMD5(yhm + mm) + "&userYzm = ";
        userInfo + = yzm + "&time = " + new Date().getTime();
        yhdl(userInfo);
      }
  }
```

代码中,yhm是用户名的文本输入框 ID,yhdMm是用户密码的文本输入框 ID,yhdYzm是用户验证码的文本输入框 ID.

3 结 语

基于用户名和口令的识别与验证是入网访问控制的主要方法,本文将常规的验证方法进行改进,提出将用户名和密码分别进行二次 MD5加密后,再将它们进行组合加密,从而保证了入网用户的真实性.此外,通过采取 URL请求验证和抗 SQL注入式攻击等措施,进一步提高了系统的安全性.该技术已被成功应用于云南省某市的工商行政管理局的网站建设,实际应用结果表明,这些方法是行之有效的.

参考文献:

[1] 胡建伟.网络安全与保密[M].西安:西安电子科技大学出版社,2003
[2] 王宏宇.征服 ASP.NET 2.0 Ajax典型应用[M].北京:人民邮电出版社,2007.