从攻击者角度浅析高校 Web 站点的安全①

白兴瑞　刘耀炎

(龙岩学院 现代教育技术中心 福建 龙岩 364000)

摘　要： 先简述了 WEB 攻击的种类，然后着重从攻击者角度，分别从 web 程序代码、文件目录权限、系统漏洞、web 验证漏洞、CGI 参数、SQL 注入、跨站点跟踪来浅析高校 WEB 站点的安全。

关键词： 校园网；Web 技术；网络安全；攻击

Analysis on the Security of College Web Sites from Attacker's Viewpoint

BAI Xing-Rui, LIU Yao-Yan

(Longyan University, Longyan 364000, China)

Abstract: In this paper, the category of web attacks is discussed. From attacker's viewpoint, the security of college Web sites is analyzed from many respects, such as web process code, permission of document catalog, system leak, validatory leak of web, CGI parameter, SQL injection and cross-site track.

Keywords: campus network; technology of Web; network security; attack

高校的主页代码通大多是网络上的一些开放性代码再修改而成，使其具有先天性的安全隐患，再加上高校 web 因其特殊性，及其容易受到非法篡改、破坏、攻击。安天实验室的一份高校网站黑客入侵统计显示，在国内 121 个重点大学和 487 个普通大学中，86%的高校网站因为存在漏洞而遭到黑客入侵[1]。因此如何来防止 web 入侵是高校网络安全的首要问题，这里从攻击者角度来对高校 Web 入侵浅析，通过发现其存在的缺陷和漏洞达到 WEB 的安全。从攻击者角度来对 Web 入侵分析可以保证检测的高效可靠，另外，从某个角度来说对手是最好的老师。

攻击者对 Web 的攻击一般分为三种：一是依赖于由输入错误数值所产生的错误，例如 SQL 注入攻击就是很好的例子；二是能生成应用程序可接受的值，例如模板机可使用 login.html 作为参数，攻击者把 login.html 替换为/etc/passwd；三是利用应用程序算法中的错误，最简单的是有些程序虽能防止攻击者上传.asp 的文件，但却允许上传其它文件，这样攻击者可以把上传后的文件类型再更改为.asp。其实，不管哪种攻击，攻击者都必须提交一些 WEB 程序不能正确解释的数值(程序设计员未考虑到的)，这样，WEB 程序就可能产生意想不到的错误，甚至允许攻击者执行任意命令。

攻击的预备阶段之一是收集潜在目标的公共信息，此过程称为足印[2]。攻击者常通过 Google 等搜索引擎构造一些查找关键字，去查找有漏洞的 web 应用程序。最经典的源代码泄露漏洞包括 IIS 上的“+.htr”漏洞，Apache Tomcat 和 BEA WebLogic 也存在类似问题，只是这次是在请求 Java Server Pages(JSP)页面的请求尾部追加几个特殊的字符而已[3]。

1　Web程序代码带来的入侵

Web 程序代码带来的入侵主要有：HTML 代码中的注释、HTML 代码中的敏感信息、WEB 服务器端的出错信息和 HTTP 响应、应用程序出错信息。攻击会仔细阅读 HTML 代码中的注释和敏感信息，寻找如密码、用户名、数据库名等非常有价值的信息。web 应用程序的源代码通常会被发送到每个客户机上，客户

① 收稿时间:2009-09-10;收到修改稿时间:2009-10-21

机上的用户可以通过浏览器来查看源代码。攻击者常用 wget 或 offline explorer pro，也就是我们常说的离线浏览器把目标网站上的全部内容下载到本地，然后再去寻找路径信息、后端服务器的名字和 IP 地址、SQL 查询字符串中的口令字、以及有价值的代码注释和其它敏感数据等。因此，源代码和错误信息在某个方面能帮助攻击者入侵 Web。

2 web文件与目录的权限带来的入侵

对用户提供包含动态或者静态内容的页面来自于 Web 服务器，Web 服务器和 Web 应用程序的作用就是对这些页面进行处理，同时将正在访问的用户限制在表示 Web 内容的那些文件中，而且还阻止非法者浏览和执行 Web 服务器端的任何其它文件。而攻击者往往会尝试访问 Web 根目录以外的文件，或是访问根目录下限制使用的文件以达到非法入侵，主要的途径就是 URL。

攻击者通过 Web 对外的信息预测到其它文件名和文件存放的位置，最常用的是对目标系统进行页面映射之后，可以很容易的知道页面命名转换的模式；通过对其目录附加“ ../ ”，或者是将其变形，曾经非常流行的 IIS 二次解码和 Unicode 解码漏洞都是利用其变形后的编码；有时可以直接在浏览器的地址栏里输入绝对地址和文件名来访问这些文件，如果访问的是密码文件就会引发安全问题。因此，这些文件如没有采取保护措施，攻击者很容易获取它们，从而利用这些文件绕过一些访问控制措施，获取目标系统的控制权。

另外，在微软提供的 asp1.0 的例程里面有一个 aspsamp/samples/code.asp 文件，专门用来查看其它*.asp 文件的源代码，攻击者常利用目录权限没有防范措施把这个程序上传，可以很容易查看其它程序。

3 Web服务器系统漏洞带来的入侵

如果底层的 Web 服务器软件有漏洞，那么 Web 应用程序的安全性状况会受到严重的影响，Web 服务器软件是运行 Web 应用程序时最容易发现和最容易暴露的组件[4]。Open Web Application Security Project 组织在一篇名为“ Insecure Configuration Management ”文章对 Web 程序漏洞做了非常细致的分类(详见 http://www.owasp.org/document-ation/topten/a10.html)。

攻击者需要确定被攻击的服务器上运行的是哪些类型的软件及其版本，这就是所谓的探测。攻击者利用 HTTPrint 工具，将不同的请求发送到服务器端，并且监测服务器返回的响应来得到这些服务器正在运行的软件和版本信息。两个最灵活的识别主机和服务的工具是 Nmap 和 Scanline，Nmap 是目前同时被 windows 和 UNIX 平台支持的最稳健和最有特色的扫描器。Scanline 是一款免费的命令行扫描器。然后攻击者再扫描其安全漏洞，常用的 Nikto 基于 lib-whisker 的 perl 库漏洞扫描器的改进版本，侧重于已知的 Web 服务器和 CGI 脚本的安全漏洞检测程序。也可以用开源工具 Nikto 来进行大范围的检测，以确定漏洞的所在，或使用 IISLockdown 这样的工具来实现。

攻击者还通过订阅这些漏洞有关的邮件列表和新闻组来了解这些公开的 bug，通常一个非常详尽的新闻组会给出问题的很多细节和对其进行攻击的方法，甚至包括一个详细的介绍和写好的例子。

4 较弱的输入验证和无力的会话处理带来的入侵

Web 的一个主要安全漏洞是由较弱的输入验证和无力的会话处理所造成的。输入验证可威胁到用户数据、应用程序数据或服务器本身的安全。无力的会话处理可威胁到用户数据的安全，导致应用程序管理权失去。攻击者通过提交错误的输入来产生 HTML 代码中的敏感信息、WEB 服务器端的出错信息和 HTTP 响应、应用程序出错信息，其体的措施是利用页面之间传递的参数迫使应用程序产生出错信息，或通过把参数修改为超出其正常值范围或数据类型限制之外的结果，以发现一些对攻击者非常有用的信息。

攻击者常用的输入验证漏洞攻击有：利用 HTML 输入流中有未经验证的输入，采用 XSS 攻击；利用生成 SQL 查询的输入未经验证，采用 SQL 注入攻击；利用依赖客户端的验证，客户端验证被忽略；利用输入文件名、URL 或用户名制定安全决策，攻击应用程序易出现规范化错误并导致安全漏洞；利用对恶意输入仅采用应用程序筛选器，这基本上不可能达到目的，原因是可能的恶意攻击范围太大，就用程序应对输入进行约束、拒绝和净化[5]。

另外，隐藏域的实际验证过程是在服务器端进行的。这些字段通常用来保存客户的会话的信息，以便减少服务器端复杂的数据库处理工作。有时隐藏的 HTML 格式字段被用来保存系统口令，而攻击者却往往能读出隐藏域，最简单的办法是在网页的源代码中查找字符串“ Hidden ”，然后从源代码中去掉(如：type= ” hidden ”，再把相对链接改成绝对链接，这样就把隐藏域改成了标准的控件，可以在浏览器里对它进行修改)。因为大多数应用没有对返回网页进行验证，它们认为输入数据和输出数据是一样的，所以攻击者通过修改 HTML 源文件中的这些字段达到攻击行动的成功。另一种隐藏域的方法是使用浏览器的文件对象模型(DOM)，这个功能用于动态的 HTML，它可以像 JavaScript 或 VBScript 脚本实现动态 UI 的功能。攻击者通过 PageSpy 工具列出页面中所有允许修改的隐藏域，然后修改隐藏的表单域中的内容，通过后继的页面发生的变化来决定攻击策略。另外隐藏域也是客户端传递给 web 服务器的数据，由于其没有相关的数据类型，因此攻击者有时利用过长的字符串和特殊的字符串来造成 web 报务的瘫痪或者产生某些不利的影响。

5　CGI参数

用 CGI 脚本编写的程序涉及远程用户从浏览器中输入表格并进行检索或 Form-Mail 之类在主机上直接操作和命令时，会给 web 主机系统造成危险[6]。如果 CGI 脚本中有安全方面的失误，如口令文件、私有数据及任何其他敏感内容，就能使攻击者方便侵入到计算机。CGI 参数是通过页面请求的 URL 地址来传递的，跟在“ ？ ”符号之后，并用“ & ”符号进行“ 变量名＝结果 ”的分组。攻击者的攻击取决于页面之间传递的参数种类和内容，最直接的方法是可以编辑页面的代码或它的 URL 地址来修改 CGI 参数。另外，没有过滤 ”$ ”的会导至泄露网页中的敏感信息；没有过滤“ ;” 的会导致执行任意系统指令；没有过滤“ | ”或“ \t ”经常导致文本文件攻击；没有过滤“ ’”和“ # ”经常导致 SQL 数据库攻击；没有过滤“ < ”和“ > ”导致 Cross-Site Scripting 攻击。

CGI 参数的另一个常见的用途是记录用户成功访问的页面的路径，如用户进行注册后才能访问的页面，这种参数的名字一般赋值为 1 表示真，0 表示假，攻击者往往会修改这些值来使 web 程序误认为攻击者完成了注册。

6　SQL注入攻击

SQL 攻击都是利用某些可以提交或修改数据的页面里的漏洞,恶意构造 SQL 语句,让系统执行此类特殊的 SQL 指令,从而获取用户名、密码等敏感信息，并获取主机控制权限[7]。

SQL 命令是前端 Web 和后端数据库之间的接口，使得数据和 web 应用程序互相传递。很多 web 站点都会利用用户输入的参数动态的生成 SQL 查询请求，攻击者通过在 URL、表格域，或者其他的输入域中注入一些额外的特殊符号或攻击者的 SQL 语句，以此改变查询属性，骗过应用程序，从而可以对数据库进行不受限制的访问。

攻击者一般会通过加'、and 1=1、and 1=2 判断其是否存在注入；通过 and ord(mid(version (),1,1))>51 判断版本，并用 union 查询；利用 order by 暴字段，在网址后加 order by N ，如果返回正常说明字段大于 N，再利用 union 来查询准确字段，如: and 1=2 union select 1,2,3,.....，直到返回正常，达到猜到准确字段数，如过滤了空格可以用/**/代替；通过 and (select count(*) from mysql.user)>0 判断数据库连接帐号有没有写权限，如果返回正常，则可以通过 and 1=2 union select 1,2,3,4,5,6,load_file(char(文件路径的 ascii 值，用逗号隔开)),8,9,10 ，load_file(char(文件路径的 ascii 值，用逗号隔开))也可以用十六进制，通过这种方式读取配置文件，找到数据库连接等。攻击者常利用 paros proxy 工具对已知服器配置错误和常见应用程序缺陷（比如“ SQL 注射 ”漏洞）进行扫描，paros proxy 工具提供了一个表单形式的输入注射界面。另外攻击者通过 web-sleuth 也可以让轻而易举地对 http/cookie 的会话 ID 进行蛮力攻击、尝试进行各种“ SQL 注射 ”攻击或者对 http 连接的口令字进行蛮力攻击。

另外，在 Microsoft SQL 服务器上，攻击者常利用 xp_cmdshell 存储过程，这是一个从数据库软件到操作系统的接口，是数据库留给操作系统的一个后门[8]，充许命令行程序得以执行，如：exec_master .. xp_cmdshell “ net user name password /add ” --，执行存储过程 xp_cmdshell，用于调用系统命令，用 net 命令新建用户名为 name、密码为 password

的 windows 的帐号；exec_master..xp_cmdshell “net localgroup name administrators/add--，将新建的帐号 name 加入管理员组。其它危险的存储过程：xp_regreated 、xp_regwrite 、xp_regdeletekey 等，攻击者可以在注入点后加上：exec_master ..xp_regwrite ‘HKEY_LOCAL_ MACHINE’,’SOFTWAREMicrosoftJet4.0Engines’ ,’SandBoxMode’,’REG_DWORD’,0；开启沙盒模式，使用沙盒提权工具直接提权，获得网站最高权限，功击者就可以在网页中疯狂挂马。

7 跨站点跟踪

HTTP 有作为用于测试网络连接的一种机制一个方法叫做 TRACE，收到 TRACE 请求的服务器会把收到的报文信息原封不动的返回给客户机，但在某些情况下，服务器还需要在返回的报文当中添加一些信息。对于浏览器而言，由于 cookie 是根据其所设置的域而被自动包含在 HTTP 请求当中的，因此对 TRACE 请求的响应应当返回所有 cookie 的数值。攻击者常利用这一点（利用 paros proxy、fiddler 截获 HTTP 数据通信，利用 tamperIE 修改 GET 和 POST），达到可以越过客户端的 HTTP 保护措施，如果其中使用了 HTTP 认证机制，还可以由此得到用户名和密码。攻击者一般通过：%3Cscript%3Ealert(‘XSS’)%3C/script%3E、“><script>alert(‘XSS’)</script><”、‘><script>alert(document .cookie)</script> 、=’><script>alert(document .cookie)</script> 、<script>alert (document .cookie)</script> ，判断其是否存在跨站漏洞。

8 结语

高校 Web 网站的安全问题随着计算机技术和网络技术的发展，将是一个永无止境的话题，因此安全是没有绝对的，但有时从攻击者角度来考虑和管理我们的 WEB，也许是一个好的方法和策略。

参考文献

1 2009 上半年安天实验室信息安全威胁综合报告. http://www.antiy.com/cn/security/2009/antiy%20security%20report%202009(1-6).htm

2 Whitman ME, Mattore HJ.信息安全原理(第2版).北京:清华大学出版社, 2006. 241－242.

3 McClure S, Scambray J, Kurtz G. 黑客大曝光:网络安全机密与解决方案(第 5 版).北京:清华大学出版社, 2006. 543.

4 Horfon M, Mugge C.黑客札记——网络安全手册.北京:清华大学出版社, 2005. 138－139.

5 柳纯录主编.软件评测师教程. 北京:清华大学出版社, 2005.375.

6 杨云江.计算机网络管理技术.北京:清华大学出版社, 2005. 162－163.

7 郜激杨.基于 WEB 服务的数据库注入攻击与防范.华北水利水电学院学报.计算机工程与应用, 2007, 43(11):150－152.

8 张涛,阴东锋.网络安全管理技术专家门诊——黑魔方丛书.北京: