GSNA Practical v4.0
Option 1
Topic 1

Auditing an Apache Tomcat Application Server Used For Credit Card Processing

Chris Bennett
03/19/2005

Abstract

The Apache Jakarta Tomcat web server is used to deliver many applications on the Internet today. The Tomcat web server can also be used to support e-commerce credit card transactions. This paper will describe an audit of the Apache Tomcat web server being used as an interface between an Oracle iPayment system and an Internet based credit card payment processor. This audit looks at testing for vulnerabilities that can lead to three of the important impacts to the organization. Audits are an important player in the security infrastructure of an organization. The audit will verify that the security controls that are implemented to control the risks to the system are functioning as planned. The application was designed to use SSL encryption during transmission and the server should be secure from local and remote access. The system will be tested using the defined testing procedure and the results will be recorded, highlighting the tests that fail and what can be done to mitigate the vulnerability.

Table of Contents

Introduction

Auditing of computer systems is an important piece of the Information Security Program of an organization. An audit, conducted at appropriate intervals, will contribute to the overall security of a system by verifying that the system was implemented and is being operated in a manner as expected by the organization. This is especially useful during the implementation of new systems that are not well understood by the organization. Policy and procedure define the requirements of an information technology uniquely in the organization. Applications and systems, as supplied by a vendor, are not configured to support your particular set of policies. The IT organization must translate the policies and procedures into effective security controls that protect the system at the level required for the classification of the information processed by the system. The process of researching and testing of the vulnerabilities of a system will verify the information security controls in place are working. The audit conducted here looks at a system implemented to allow for credit card authorizations. The audit begins with the definition of the scope of the audit and therein sets the expectations of the project. This audit will look at three major impacts to the organization and will discuss the vulnerabilities and threats that could cause that impact. Tests that determine the existence of the vulnerabilities that were identified will then be executed against the system. The tests will determine if controls are in place to mitigate the risk or if the vulnerabilities are present. The audit process provides a window on a point in time security stance of the system and does not remove the on-going requirement that system administrators must continually monitor changes to the threat environment. This audit will also only address a subset of the risks present in this system and therefore should not be referred to as a comprehensive audit of this system.

Audit Scope

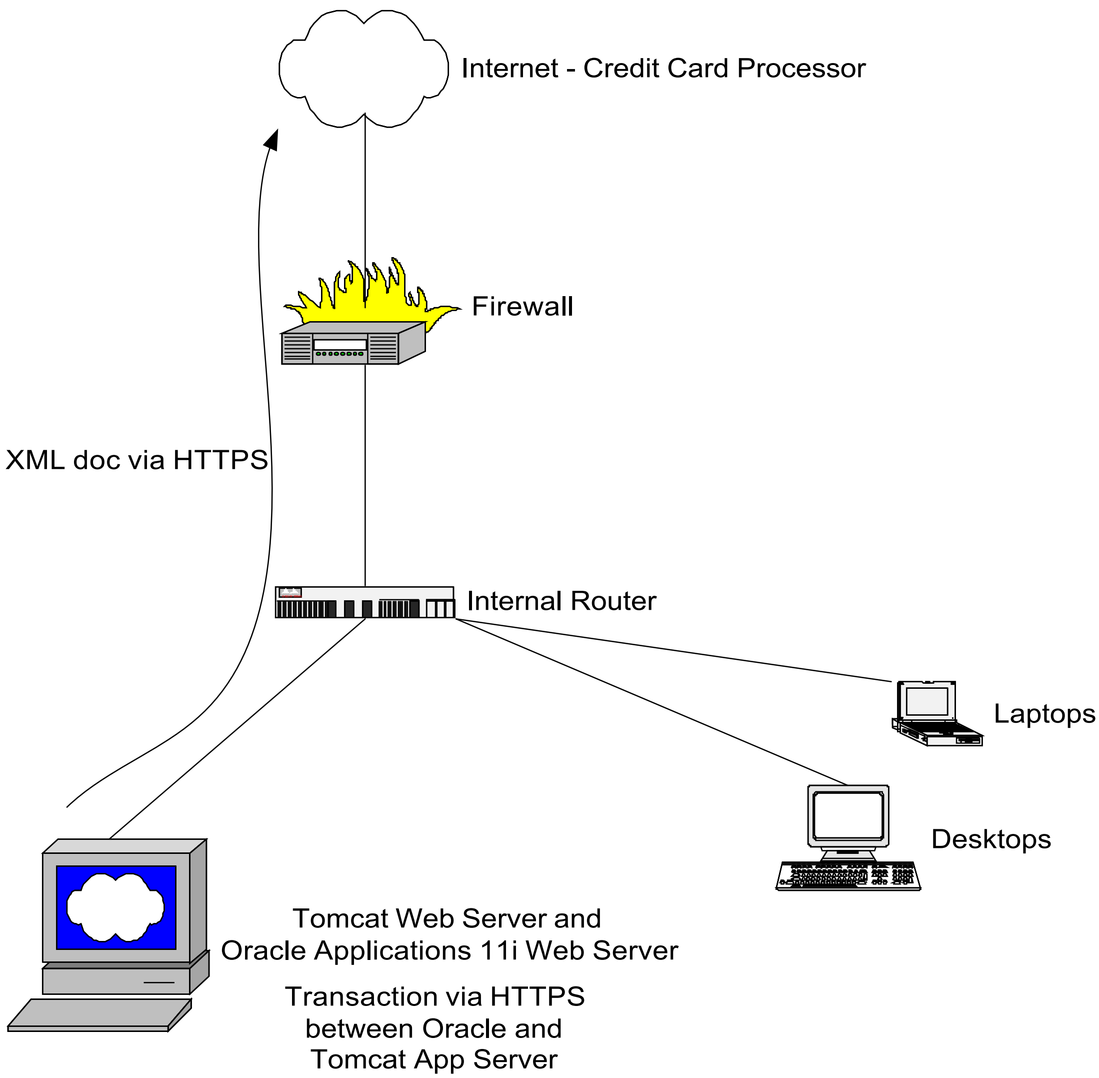
Identify the system to be audited

The system to be audited supports credit card transaction processing in an educational institution. Educational Due Diligence University, hereafter called EDDU, (A fictitious University) embarked on a project to implement credit card processing for the receipt of student tuition and to allow for the creation of an online spirit shop. The focus of the audit will be on the system that was implemented to authorize credit card transactions in real-time. The application is ClearLink Generic Servlet (CLGS) for Oracle iPayment developed by Clear Commerce. The application runs on an Apache Foundation Jakarta Tomcat 5.0.28 application server that is installed on an HP/UX server. The ClearLink Generic Servlet and the Apache Tomcat server are within the scope of this audit, while the HP/UX operating system is not within the scope. The HP server also runs an Oracle Applications 11i web server that is beyond the scope of this audit except to the extent that it is recognized to be a source of risk to the application. The ClearCommerce whitepaper on the Clearlink Generic Servlet (Kirchner, 1) states that “CLGS for iPayment provides a packaged integration between Oracle iPayment and ClearCommerce Merchant Engine or Hosting Engine”.

EDDU began the implementation of the new credit card system in cooperation with the implementation of a new student records system. The current student system from a different vendor had support for credit card payments of the student tuition and the new system must have that same capability. External consultants that were hired to assist with the student system configuration suggested the use of a third party application from ClearCommerce to interface between the Oracle Applications Student System using the Oracle iPayment module and the Credit Card Processor. The application is a Java Servlet and could be implemented in several ways in our environment. The application could be implemented on a standalone Microsoft Windows server running Tomcat 5.0 and J2SE 1.4. Oracle Applications 11i is based on the Apache web server and is a fully compliant J2EE server so the application could be install on Microsoft Windows server running Oracle Applications, with the application installed within Oracle Applications. The java application could also be installed within Oracle Applications that were already installed on a HP/UX operating system in the same way as described for the Windows environment. Another method would be to implement the application on the HP/UX operating system with a standalone Tomcat 5.0 web server with J2SE 1.4 for the application on the same machine as the existing Oracle Applications 11i install. This last method was selected because it would not introduce additional upgrade/patching issues to the Oracle applications, being that the application is using a totally standalone Tomcat web server. It was also one solution that the consultant did not have any technical issues implementing as a test server.

The audit will cover the accepting of the transaction via HTTPS, configuration and operation of the Tomcat Application Server and the transmission of the transaction to the Credit Card Processor via HTTPS. The Tomcat Application Server should only be accessible by the Oracle Application web server process that supports the Oracle iPayment credit card processing. The application will not accept input directly from a user browser and so the audit will not test for User Input tampering, but will verify the controls that limit the access. The laptops and desktops do have access to the Oracle Applications web server running on port 443 (https), but should not have access to the other services running on the server.

Through out this document the server that Tomcat is installed on is called server.eddu.edu to obfuscate its true name. Catalina_Home is used in the document to designate the installation directory for the Tomcat files and is usually set as an environment variable to designate the top of the Tomcat file system.



Software version levels:
HP/UX 11.11
Tomcat 5.0.28
ClearLink Servlet 2.2

Tomcat listening port:
8443 HTTPS

Evaluation of Risks to the System

The risks facing a system that processes credit cards have been highlighted before in the news. A story from CNN on the loss of Social Security Number and Credit Card numbers (http://www.cnn.com/2004/EDUCATION/01/30/computer.breach.ap/) outlines the work that a University and 31,000 students were faced with as a result of a breach. In the NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, risk is defined as "a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability** and the resulting **impact** of that adverse event on the organization". The processing of Credit Card information could attract unwanted attention to the system because of the possibility for financial gain for the computer criminal and therefore the likelihood of attack will be much higher. The presence of Credit Card transactions changes the value of a system to possible attackers and greatly increases the impact to the University. The attacker will expend more effort on systems that are believed to have a larger reward. The attacker will be much more motivated and the resulting impact is much larger because of the impact to the University's reputation. Loss can be experienced in several ways including the loss of student and employee confidence in the University systems and the financial impact as EDDU must deal with the incident. The impact will also be felt by all of the customers that had their information stolen.

VISA has published a data security standard that lists the protections that are required to be in place for systems that handle credit card information. The VISA Cardholder Information Security Program web site is located at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html and provides a best practices guide to the security controls that should be in place. Also available are documents that help with verifying compliance with the security standards, a self-assessment questionnaire and an auditing document. These documents recommend controls for the many operational and technical risks present in information processing systems.

The vulnerabilities to applications running on a tomcat server have been well defined by groups like OWASP, which published "The Ten Most Critical Web Application Security Vulnerabilities". The vulnerabilities listed are for vulnerabilities that can be exploited on Internet-facing web application servers, but the application server being assessed is not Internet-facing and the top vulnerabilities must be evaluated in that context. For example, the tampering with parameters for form submissions and code injection are of a much lower risk since the server only needs to accept input from well defined application processes within the Oracle Applications environment and not directly from user browsers. By implementing the interface application in a stand-alone apache Tomcat server on the same server as the Oracle Applications installation, the application will only need to accept transactions from a process on the same server. The implementation of controls for limiting access will make the transmission of the information to the java application only internal to the server and therefore the information will not traverse the data network.

In the initial audit meeting to discuss the scope of this project, it was clear that EDDU had no experience running the Apache Jakarta Tomcat server in a production environment and so the vulnerabilities of the system were not well understood. The participants of the audit meeting had an understanding of the threats to the University, but had very little understanding of the vulnerabilities of the system.

The most serious impacts to the University are:

A. Loss of Confidentiality of information during Transmission:

Description: Information that is sent in the clear or using weak or low security encryption algorithms would possibly expose the credit card information to others. Transmitted information will travel across the Internet to the payment processor through network devices that the University has no control of and so the information transmissions must always be encrypted with high level ciphers. Importance: Users of the credit card systems are sold on the concept that if their information is SSL encrypted during transmission that they are safe in conducting business with you. This establishment of trust becomes a basis for future transactions. SSL encryption, if properly implemented, will safeguard the information, but the system should be verified often that it is maintaining that level of protection. This particular threat can also occur anywhere along the transmission path and that means that it can occur outside of your network infrastructure. Since the other networks may not have the same security controls in place, the encryption must be at a sufficiently high level to protect the information. A loss of confidentiality of the information would have the largest impact on the University.
Vulnerabilities (scenarios and means):

1. Use of a weak encryption or no encryption during transmission of the information. Communication to or from the Tomcat Application Server could be intercepted and monitored. If a weak encryption algorithm was being used then the monitored traffic could be decrypted to gather Names and credit card numbers. Traffic could be monitored at many points along the network path including at the servers network interface, on the Universities network, on the ISP network, or at the Credit Card Payment Processors network. A number of freely available tools for sniffing traffic can be used, if the attacker can gain access to any point along the network path.

B. Unauthorized access the Server configuration and log files:

Description: Access to the Tomcat Application Server configuration files, the applications configuration files or any of the system log files could provide valuable information or possibly unencrypted credit card numbers and names. The file system rights must be set correctly to minimize these risks.

Importance: The operating system, Tomcat Application Server, Oracle Application Server or any of the applications running could hold a vulnerability that would give an attacker access to the file system on the server. The level of access to the files in the Tomcat Application Server must be controlled to limit the risk of compromise. Configuration files give an attacker much information, either to use directly or to further compromise the security of the system. The ClearCommerce servlet properties file contains the userid and password used for authentication to the payment processor. Log files can also be source of direct information in the event that credit card transaction information gets logged in clear text to one of the logs. The File system only needs to be accessed by the user that is configured to run the Tomcat Application Server. Access by other users of the system should be removed. And it is not only an issue of confidentiality of the information, but could also affect the availability of the system, by interrupting the processes of the Tomcat web server.

Vulnerabilities (scenarios and means):

1. World-readable files that contain high-valued information. A user on the system should not be able to read the content of high-valued files, like configuration files that contain userids and passwords or log files that contain passwords or credit card information. One weak password on an operating system account or a vulnerability of another application that allows you to read files on the system could be used to gain access to these high-valued files and compromise your system.
2. Group-readable files for groups other than tomcat. A group file right allows access only to members of that group, but you must pick your group of friends carefully. Membership in the group that has access to the files in the Tomcat directories should be limit to only the required users for the application to function.
3. Configuration files that are writeable by other than tomcat. Tomcat Application Server may have a need to write to some files or file systems during operation, like a log file, but most files should not be allowed to be updated.

C. Improper configuration of the Web Servers access control:

Description: The ClearCommerce servlet and the Tomcat Web Server must be configured to limit access to the application and therein reduce the footprint for vulnerabilities of the system.

Importance: The application must be understood and all unnecessary features and functions should be removed. The ClearCommerce servlet should accept information only from the Oracle iPayment server. The test servlet provided (generic.htm) is not designed to be accessed by just any user with a web browser. The test servlet has several vulnerabilities in it and so it is all that more important that the access to the Tomcat server is limited. In addition, if an attacker could use a web browser to inject credit card transactions this could lead to fraud or other financial losses. The Tomcat server, if configured to only accept transactions from the local server ip address, will be less likely to be compromised. The Application Server should be checked for any known vulnerabilities that would allow a specially crafted packet to subvert the address controls in place. The configuration must be checked to make sure that vulnerabilities are not present that would allow an attacker to gain access to the ClearCommerce servlet and introduce unwanted credit card transactions into the system.

Vulnerabilities (scenarios and means):

1. Incoming transactions are not limited to specified IP addresses. This particular application server has a very well defined set of IP addresses that it is allowed to transact business with. It should only accept credit card authorizations from the same server it is on. All other connections from other computers should not be accepted.
2. Presence of known vulnerabilities. The presence of a known or discovered vulnerability should be checked to make sure that no unauthorized access is made to the Tomcat Application Server. Vulnerabilities in the Tomcat web server could subvert the access controls allowing access to the web server applications.

Audit Testing

Impact: Loss of Confidentiality of information during Transmission

Steps to determine the level of encryption used

<table>
<tr><th>#</th><th>Control Objective</th><th>Risk</th></tr>
<tr><td>A1.1</td><td>Verify that encryption is being used during transmission of the information</td><td>Errors in configuration or installation could cause the transfer of information without encryption resulting in a compromise of the confidentiality of personal information or credit card numbers</td></tr>
<tr><td colspan="3">Testing/Compliance: Debug trace of the JSSE handshakes within the Tomcat server.
Stop the Tomcat server ‘$CATALINA_HOME/bin/shutdown.sh’.
Enter ‘export CATALINA_OPTS=”-Djavax.net.debug=ssl:handshake”’.
Start the Tomcat server ‘$CATALINA_HOME/bin/startup.sh’.
The output of the debug will be located in $CATALINA_HOME/logs/catalina.out.
Look for “Cipher Suite” similar to
   Cipher Suite: SSL_RSA_WITH_RC4_128_SHA
   Compression Method: 0
   ***
   %% Created: [Session-2, SSL_RSA_WITH_RC4_128_SHA]
   ** SSL_RSA_WITH_RC4_128_SHA

The cipher suite should not be one of the following low strength ciphers. The openssl command can give you that information by typing:
openssl ciphers LOW:NULL:aNULL:EXP</td></tr>
<tr><td colspan="3">Reference: “JSSE Reference Guide J2SDK SE v1.4.2”, Debug Utilities
VISA, “Payment Card Industry Self-Assessment Questionnaire”, Req. 4.2, p. 5</td></tr>
</table>

After running this test you will need to restore the system back to running in normal mode:
Stop the Tomcat server ($CATALINA_HOME/bin/shutdown.sh)
Unset CATALINA_OPTS
Start the Tomcat server ($CATALINA_HOME/bin/startup.sh)

To display what are the LOW or export levels of encryption are, you can use the openssl command from www.openssl.org.
openssl ciphers LOW:NULL:aNULL:EXP
KRB5-DES-CBC-MD5:KRB5-DES-CBC-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:DES-CBC-SHA:ADH-DES-CBC-SHA:RC4-64-MD5:DES-CBC-MD5:NULL-SHA:NULL-MD5:ADH-AES256-SHA:ADH-AES128-SHA:ADH-DES-CBC3-SHA:EXP-ADH-DES-CBC-SHA:ADH-RC4-MD5:EXP-ADH-RC4-MD5:EXP1024-DHE-DSS-RC4-SHA:EXP1024-RC4-SHA:EXP1024-DHE-DSS-DES-CBC-SHA:EXP1024-DES-CBC-SHA:EXP1024-RC2-CBC-MD5:EXP1024-RC4-MD5:EXP-KRB5-RC4-MD5:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-EDH-DSS-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:EXP-RC4-MD5:EXP-RC2-CBC-MD5:EXP-RC4-MD5

Steps to determine that no weak encryption methods can be used

<table>
<tr><th>#</th><th>Control Objective</th><th>Risk</th></tr>
<tr><td>A1.2</td><td>Verify that the remote payment processor does not support weak encryption methods</td><td>If the payment processor supported weak encryption methods the client to server negotiation could select one of the weak encryption methods and an attacker could capture traffic and decrypt the information within a period of time.</td></tr>
<tr><td colspan="3">Testing/Compliance: The OPENSSL package supports performing a client connection that allows you to specify the allowed ciphers. If a client tries to connect only using low or export strength ciphers, the server should reject the connection.
./openssl s_client –connect server.eddu.edu:8443 –ssl2 –cipher ‘LOW:NULL:aNULL:EXP’
./openssl s_client –connect server.eddu.edu:8443 –ssl3 –cipher ‘LOW:NULL:aNULL:EXP’

The output from the two commands should look similar to:
CONNECTED(00000003)
8374:error:1407F0E5:SSL routines:SSL2_WRITE:ssl handshake failure:s2_pkt.c:429:
A successful connection is completed only if the server negotiated and accepted one of the low strength encryption methods.</td></tr>
<tr><td colspan="3">Reference: Rhoades, “Auditing Web Servers and Applications”, p.120</td></tr>
</table>

Impact: Unauthorized access to the server configuration and log files

Steps to determine the existence of world-readable files

#	Control Objective	Risk
B1.1	Make sure other users of the operating system are unable to read files in the Tomcat web server file system.	If another account or application on the system is compromised, that account would have access to read the configuration or log files gaining access to valuable information.
Testing/Compliance: cd $CATALINA_HOME find . -type f -perm -0004 -xdev -print All files returned are world readable and should be reviewed for a requirement to be world readable.		
Reference: Turner, “Apache Tomcat Security Handbook”, p. 48 Curphey, “The OWASP Testing Project”, Phase 4B Configuration Mgmt, p. 22		

The Apache Tomcat Security Handbook [1] page 47 suggests that the following directory permissions be set for the UNIX file permissions.

Directory	Owner/Group	Permissions (numeric)
CATALINA_HOME	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/bin	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/bin/*.sh	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/common	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/conf	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/logs	root/tomcat	rwxrwx--- (770)
CATALINA_HOME/logs/*.*	root/tomcat	rw-rw---- (660)
CATALINA_HOME/server	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/shared	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/temp	root/tomcat	rwxrwx--- (770)
CATALINA_HOME/webapps	root/tomcat	rwxr-x--- (750)
CATALINA_HOME/work	root/tomcat	rwxrwx--- (770)

If not otherwise indicated, all files in the listed directories above should have the same ownership as its containing directory and have rw-r----- (640) permissions. The ls command (ls –lAR) could also be used to get a full listing and allow for manual review of all owner, group and permission settings. The owner and group rights are set for a web server running on port 80 and/or 443.

Steps to determine read access granted to another group

#	Control Objective	Risk

B2.1	No files should be group-readable by a group other than the tomcat group.	The group-readable rights should not be given to a group that includes other operating system users. This would expose the information in the configuration or log files to compromise by other applications or users of the system
Testing/Compliance: cd $CATALINA_HOME find . -type f ! -group tomcat -perm -0040 -xdev -print All files returned are group readable by a group that is not tomcat and should be reviewed for a requirement to be readable by other groups. All files in CATALINA_HOME should have a group ownership of the tomcat group. If your installation does not use tomcat as the group that the Tomcat server runs as, replace that group name in the command.		
Reference: Turner, “Apache Tomcat Security Handbook”, p. 47 Curphey, “The OWASP Testing Project”, Phase 4B Configuration Mgmt, p. 22		

Steps to determine the existence of world-writeable or group-writeable files

#	Control Objective	Risk
B3.1	Identify all world or group writeable files.	If any account on the system or other members of your group can make changes to files in the web server, an attacker could make changes that would affect the uptime or integrity of the server.
Testing/Compliance: cd $CATALINA_HOME find . -type f -perm -0002 -xdev -print (World-writeable) find . -type f -perm -0020 -xdev -print (Group-writeable) All files returned are world or group writeable and should be reviewed for a requirement to be writeable. Only files in CATALINA_HOME/logs, CATALINA_HOME/temp and CATALINA_HOME/work should have writeable files.		
Reference: Turner, “Apache Tomcat Security Handbook”, p. 47 Curphey, “The OWASP Testing Project”, Phase 4B Configuration Mgmt, p. 22		

Impact: Improper configuration of the Web Servers access control

Steps to check for limiting of access by IP address

#	Control Objective	Risk

C1.1	The Tomcat web server should return HTTP 403 (forbidden) to connections from ip addresses other than the servers own IP address.	Access to the application from computers other than those required increases the number of vulnerabilities that could be exploited. The control will reduce the target surface that an attacker would be able to target.
Testing/Compliance: A web browser should return a HTTP 403 or page forbidden message and no page should be accepted from a browser on a laptop. Use Achilles from http://www.mavensecurity.com/achilles, which is a web browser proxy to verify the returned web pages content. Start Achilles and select the 'Intercept Mode ON'. 'Intercept Server Data' and 'Ignore .jpg/.gif' check boxes. Press the triangle shape 'Start Proxy' button. Open a web browser. (Internet Explorer) Reconfigure the communications parameters of the browser to use a proxy with address 127.0.0.1 and port 5000. Enter 'http://server.eddu.edu:8443/servlet/generic.htm' into the address field Switch back to the Achilles application and see the returned http message. Switch back to the browser and enter 'http://server.eddu.edu:8443/' Switch back to the Achilles application and see the returned http message. Verify that the pages that are returned refer to HTTP error 403 or the word Forbidden.		
Reference: Turner, "Apache Tomcat Security Handbook", p. 17 VISA, "Payment Card Industry Data Security Standard", 2.2		

The Tomcat configuration should include a valve directive to limit access to the server and cause the web server to return the HTTP 403 (forbidden). The command added to the server.xml file within the Host directives should be:

<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="*server-ip*,127.0.0.1"/>

#	Control Objective	Risk
C2.1	Identify common web vulnerabilities in the Tomcat server using Nstealth	Known vulnerabilities and common web server problems could lessen the strength of the access controls that are put in place.

Testing/Compliance: Nstealth from http://www.nstalker.com/eng/products/nstealth/ is a windows program. The access restriction tested in test C1.1 must be expanded to include the host that will run the Nstealth application. The program when run requires the following parameters to be filled in. Host Address: server.eddu.edu Port: 8443 Protocol: https Click ‘Start Scan’ button. Any vulnerability should be verified for false positives.
Reference: VISA, “Payment Card Industry Data Security Standard”, 6.2 Rhoades, “Auditing Web Servers and Applications”, p. 62

#	Control Objective	Risk
C2.2	Identify common web vulnerabilities in the Tomcat server using Nessus	Known vulnerabilities and operating system problems could lessen the strength of the access controls that are put in place. The use of a second vulnerability scanner that looks at the vulnerabilities from a different angle will increase the accuracy of what vulnerabilities the server may really have.
Testing/Compliance: Nessus from http://www.nessus.org/ is a unix/linux program. The access restriction tested in test C1.1 must be expanded to include the host that will run the Nessus application. The program when run requires the following parameters to be filled in. Target Selection tab>Target(s): server.eddu.edu Scan options tab>Port Range: 22,4001,8009,8082,8090,8443 For the Plug-ins used for the run: the following plug-ins were disabled (unchecked) Plugins tab>Plugin selection: Windows, Cisco, Firewalls, Windows:User Management, Mac OS X local security checks, Windows:Microsoft Bulletins, Netware Click ‘Start the Scan’ button. Any vulnerability should be verified for false positives.		
Reference: VISA, “Payment Card Industry Data Security Standard”, 6.2 Rhoades, “Auditing Web Servers and Applications”, p. 55		

Audit Evidence

Loss of Confidentiality of information during Transmission

#	Control	Pass/Fail	Findings

A1.1	Determine the level of encryption used	Pass	The two encryptions used were SSL_RSA_WITH_3DES_EDE_CBC_SHA and SSL_RSA_WITH_RC4_128_SHA.
A1.2	Determine that no weak encryption methods can be used	Pass	The communication with the payment processor would not accept an SSL handshake with only LOW level encryption.

A1.1 - Determine the level of encryption used – Detailed Findings:

Communication between the Oracle iPayment process and Tomcat

```
Cipher Suites: [SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA,
SSL_RSA_WITH_RC4_128_MD5, SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5,
SSL_DH_anon_WI
TH_DES_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA, SSL_RSA_EXPORT_WITH_RC4_40_MD5,
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DH_anon_EXPORT_WITH_RC4_40_MD5,
SSL_DH_anon_EXPORT_WITH_DES40_CBC
_SHA, SSL_RSA_WITH_NULL_SHA, SSL_RSA_WITH_NULL_MD5]
Compression Methods:  { 0 }
***
%% Created:  [Session-1, SSL_RSA_WITH_3DES_EDE_CBC_SHA]
*** ServerHello, SSLv3
RandomCookie:  GMT: 1110690546 bytes = { 149, 78, 114, 25, 181, 233, 138, 213, 218, 27, 162, 224, 202, 200, 56, 196,
0, 193, 125, 105, 22, 120, 101, 225, 59, 78, 76, 143 }
Session ID:  {66, 52, 203, 242, 85, 238, 146, 29, 10, 59, 241, 139, 58, 71, 95, 114, 193, 60, 41, 53, 149, 67, 249, 93, 42,
93, 122, 116, 58, 197, 157, 93}
Cipher Suite: SSL_RSA_WITH_3DES_EDE_CBC_SHA
Compression Method: 0
***
```

Cipher suite: **SSL_RSA_WITH_3DES_EDE_CBC_SHA**

Server.eddu.edu connecting to card-processor.com

```
Cipher Suites: [SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH
_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC
_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_
DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_DES_CBC_SHA, SSL_DHE_RSA_WITH_DES_CBC_SH
A, SSL_DHE_DSS_WITH_DES_CBC_SHA, SSL_RSA_EXPORT_WITH_RC4_40_MD5, SSL_RSA_EXPORT_
WITH_DES40_CBC_SHA, SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, SSL_DHE_DSS_EXPORT_WI
TH_DES40_CBC_SHA]
Compression Methods:  { 0 }
***
http-8443-Processor24, WRITE: TLSv1 Handshake, length = 73
http-8443-Processor24, WRITE: SSLv2 client hello message, length = 98
http-8443-Processor24, READ: SSLv3 Handshake, length = 58
*** ServerHello, SSLv3
RandomCookie:  GMT: 1110332134 bytes = { 221, 254, 187, 18, 162, 182, 232, 216,
167, 213, 234, 245, 233, 248, 184, 19, 174, 188, 237, 218, 179, 219, 237, 246, 2
45, 242, 189, 17 }
Session ID:  {10, 138, 1, 79, 77, 194, 82, 133, 80, 169, 84, 182, 22, 132, 6, 76
}

Cipher Suite: SSL_RSA_WITH_RC4_128_SHA
Compression Method: 0
***
%% Created:  [Session-2, SSL_RSA_WITH_RC4_128_SHA]
** SSL_RSA_WITH_RC4_128_SHA
http-8443-Processor24, READ: SSLv3 Handshake, length = 1177
```

A1.2 - Determine that no weak encryption methods can be used
Result: Pass
Findings:
#./openssl s_client -connect secdev.virtualpay.com:11500 -ssl3 -cipher LOW:NULL:aNULL'
CONNECTED(00000003)
23141:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:524:

Unauthorized access to the server configuration and log files

#	Control	Pass/Fail	Findings
B1.1	Determine the existence of world-readable files	Fail	The majority of files were world readable including the configuration files for the application.
B2.1	Determine read access granted to another group	Fail	The application was installed with the group 'users' assigned as the group owner of all the files.
B3.1	Determine the existence of world-writeable or group-writeable files	Pass	No unexpected world or group writeable files were found in the Tomcat file system.

B1.1 Determine the existence of world-readable files detailed findings:

The output of the command to list all files in the CATALINA_HOME directory is included in Appendix A. Some subdirectory listings in the webapps directory were deleted for space reasons, because the sample applications should all be deleted in a production installation. The files that were found to be world-readable included configuration files that had application userids and passwords and the private SSL key. The files can be changed to no longer be world-readable by using the chmod command. (Chopra, 38)

Chmod o-rwx filename (use the –R option to recursively change all subdirectories)

The issue of finding a private SSL key set to world-readable should be handled by revoking that SSL certificate and starting the process of generating a new private key and certificate signing request (CSR). If you are not sure whether your private key is compromised, it is best to not accept that risk and to generate a new one.

B2.1 Determine read access granted to another group detail findings.

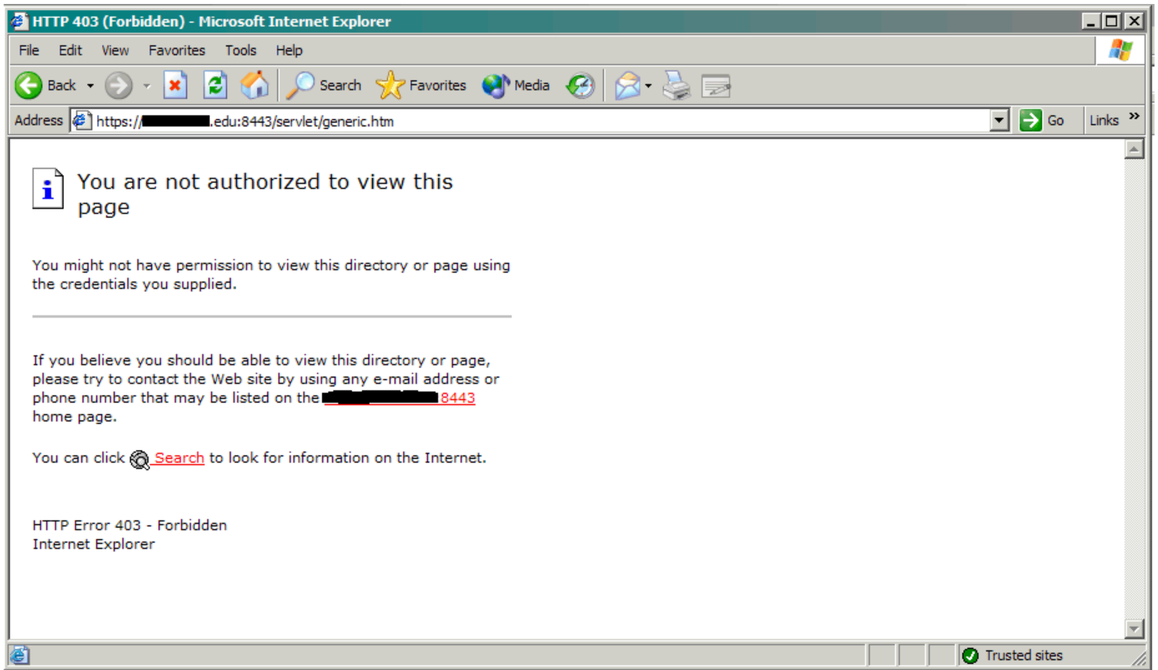
The system was found to have the Tomcat server software installed with group "users". This group does not appear to be used exclusively for running the Tomcat service and so it is likely that other users would be assigned to be members of that group. All of the findings of B1.1 would then apply, allowing access to the configuration files. The files could be protected by making sure that no other users of the system are members of the group "users" or to create a new group. The group owner of the file can then be changed using the chown command. (Chopra, 39)

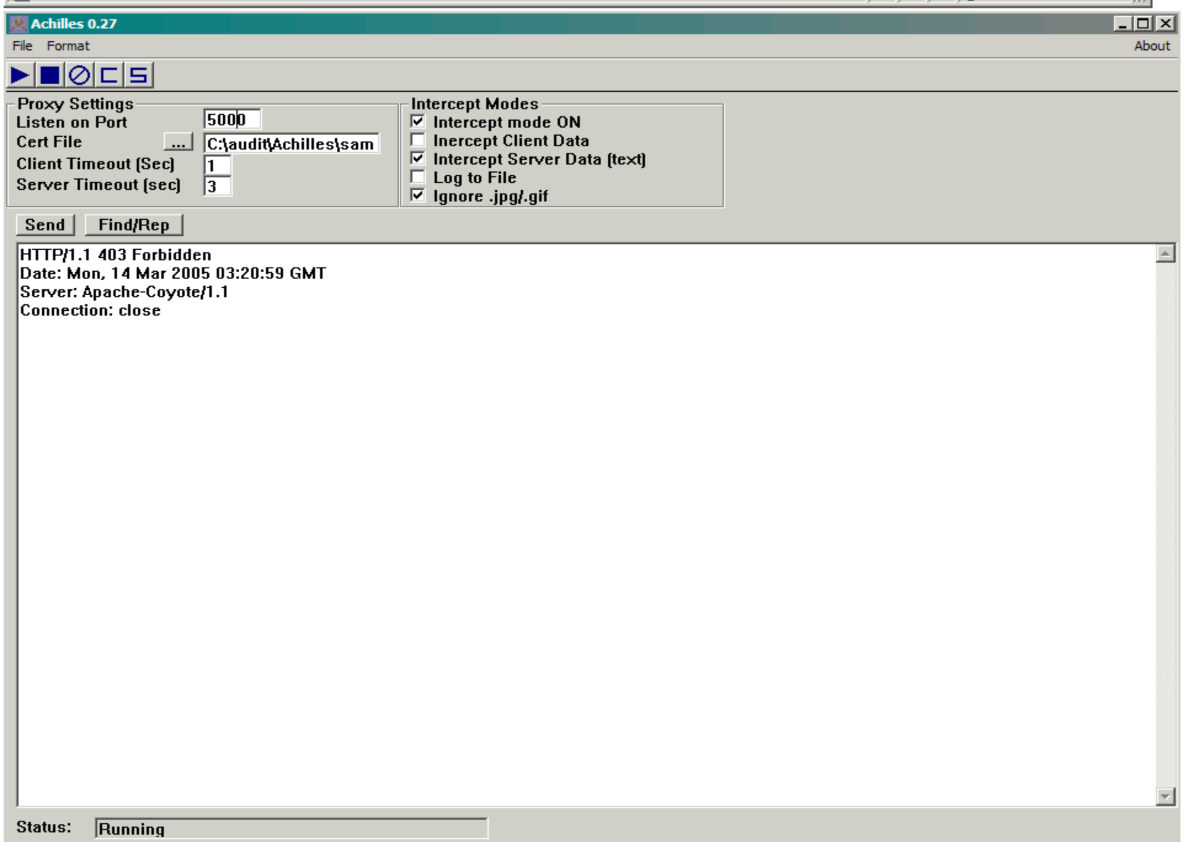
Chown tomcat:tomcat filename

Improper configuration of the Web Servers access control

#	Control	Pass/Fail	Findings
C1.1	The Tomcat web server should return HTTP 403 (forbidden) to connections from ip addresses other than the servers own IP address.	Pass	The Web Browser displayed the 403 Forbidden message and that was verified within the Achilles Proxy server intercept window. The test was tried from several source IP addresses.
C2.1	Identify common web vulnerabilities in the Tomcat server using Nstealth	Fail	The Nstealth scanner identified 5 vulnerabilities, but it was determined by later verification that 3 of the vulnerabilities no longer exist in this version of Tomcat. The vulnerabilities were all associated with the /admin application, which it is recommended that you remove this application since it is not used. The Nstealth scanner classifies the existence of the /admin application directory as a low level vulnerability and since it has not been removed this test fails.
C2.2	Identify common web vulnerabilities in the Tomcat server using Nessus	Fail	The Nessus scanner identified for the ports defined seven warnings and one hole. The hole was actually in the SSH software and not within the Tomcat web server. The vulnerabilities fell into two categories. The first is the existence of sample and documentation files and the second is the allowance of dangerous HTTP methods like delete and put.

C1.1 Check for limiting of access by IP address detailed findings:

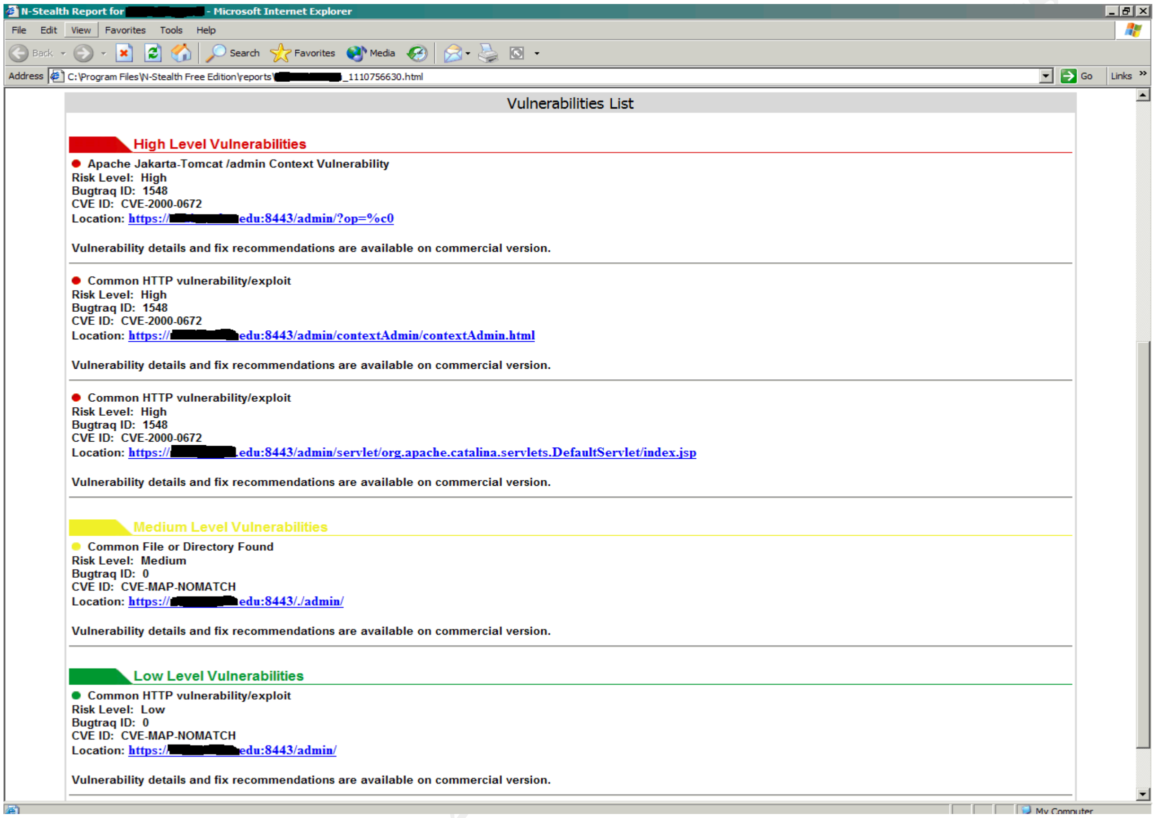




C2.1 Nstealth detail findings

The Nstealth scanner determined that the web server had 3 High Level

Vulnerabilities that were determined to be false-positives by researching the CVE ID: CVE-2000-0672. The installation still contained the /admin directory and that was the issue that needs to be addressed. The admin application can be removed by removing the admin.xml file located in the webapps directory.



C3.1 Nessus detail findings:

Nessus Scan Report (edited output to remove port information for services outside of audit scope and to reduce space)

TESTED HOSTS

server.eddu.edu (Security holes found)

DETAILS

+ server.eddu.edu :
. List of open ports :
o https-alt (8443/tcp) (Security notes found)
o unknown (8090/tcp) (Security warnings found)
o ajp13 (8009/tcp)
o ssh (22/tcp) (Security hole found)
o general/tcp (Security warnings found)
o unknown (8443/tcp) (Security warnings found)
o general/udp (Security notes found)

. Warning found on port unknown (8443/tcp)

The remote web server seems to be vulnerable to the Cross Site Scripting vulnerability (XSS). The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request). The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code. Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high).

Sample url : http://server.eddu.edu:8443/<SCRIPT>foo</SCRIPT>

Risk factor : Medium

Solutions:
. Allaire/Macromedia Jrun:
- http://www.macromedia.com/software/jrun/download/update/
- http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html
. Microsoft IIS:
- http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html
. Apache:
- http://httpd.apache.org/info/css-security/
. ColdFusion:
- http://www.macromedia.com/v1/handlers/index.cfm?ID=23047
. General:
- http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html
- http://www.cert.org/advisories/CA-2000-02.html
BID : 1462, 2478, 4687, 4689, 823

. Warning found on port unknown (8443/tcp)

Default files, such as documentation, default Servlets and JSPs were found on the Apache Tomcat servlet/JSP container.

Solution: Remove default files, example JSPs and Servlets from the Tomcat Servlet/JSP container.

These files should be removed as they may help an attacker to guess the exact version of Apache Tomcat which is running on this host and may provide other useful information.

The following default files were found :
/tomcat-docs/index.html

Risk factor : Low
BID : 1462, 2478, 4687, 4689, 823

. Warning found on port unknown (8443/tcp)

It seems that the PUT method is enabled on your web server. Although we could not exploit this, you'd better disable it
Solution : disable this method
Risk factor : High
BID : 1462, 2478, 4687, 4689, 823

. Warning found on port unknown (8443/tcp)

It seems that the DELETE method is enabled on your web server. Although we could not exploit this, you'd better disable it
Solution : disable this method
Risk factor : Medium
BID : 1462, 2478, 4687, 4689, 823

Summary

The audit process, allowing for an independent review of the system, assists the system administrators to secure the system. The audit for this limited set of vulnerabilities show that the vulnerabilities associated with the transmission of information are sufficiently controlled, but the access to the files or the web server show several vulnerabilities are present. The vulnerabilities discovered could cause great impact to the organization, but are easy to fix. The Credit Card industry has done a good job defining a standard that must be met for merchants to handle credit transactions. The standards, when implemented, will allow the organization to manage the risk as part of building an Information Security Program with scheduled vulnerability scans, audits and updated policies.

Works Cited

Cheng, Derek. "Web Server Security Assessment", 2003. http://www.giac.org/certified_professionals/practicals/gsna/0157.php (03/01/2005).

Curphey, Mark, et al. "The OWASP Testing Project", Version 1.0. December 2004. http://cogent.dl.sourceforge.net/sourceforge/owasp/OWASPTesting_PhaseOne.pdf (03/01/2005).

"Java Secure Socket Extension (JSSE) Reference Guide for the Java 2 SDK, Standard Edition", Version1.4.2. 2004. http://java.sun.com/j2se/1.4.2/docs/guide/security/jsse/JSSERefGuide.html (03/01/2005).

Kirchner, John. ClearLink Generic Servlet and Oracle 11i Payment Integration, Version 2.2.9, July 2003.

Rhoades, David. Auditing Web Servers and Applications, Version 1.10, The SANS Institute, 2004.

Stonburner, Gary, el al. "Risk Management Guide for Information Technology Systems", NIST Special Publication 800-30, July 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (03/01/2005).

"The Ten Most Critical Web Application Security Vulnerabilities", July 2004. http://unc.dl.sourceforge.net/sourceforge/owasp/OWASP_Top_Ten_2004.doc (03/15/2005).

Turner, John, et al. Apache Tomcat Security Handbook, UK: Wrox Press Ltd., 2003.

Visa. "Payment Card Industry Data Security Standard", version 1.0. December 15, 2004. http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf (03/01/2005).

VISA. "Payment Card Industry Self-Assessment Questionnaire", Version 1.0. December 15, 2004. http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Self_Assessment_Questionnaire.doc (03/15/2005)

Appendix A.

File system listing.

```
total 70
-rw-r--r--   1 appltcat   users        11357 Aug 28  2004 LICENSE
-rw-r--r--   1 appltcat   users          505 Aug 28  2004 NOTICE
-rw-r--r--   1 appltcat   users         9002 Aug 28  2004 RELEASE-NOTES
-rw-r--r--   1 appltcat   users         5887 Aug 28  2004 RUNNING.txt
drwxr-xr-x   2 appltcat   users         2048 Mar  8 13:51 bin
-rw-r--r--   1 root       sys              0 Mar 10 17:23 cab_files
drwxr-xr-x   5 appltcat   users           96 Sep 16 15:46 common
drwxr-xr-x   3 appltcat   users         1024 Mar  8 21:11 conf
drwxr-xr-x   3 appltcat   users         2048 Mar  9 10:21 logs
drwxr-xr-x   5 appltcat   users           96 Sep 16 15:46 server
drwxr-xr-x   4 appltcat   users           96 Sep 16 15:46 shared
drwxr-xr-x   2 appltcat   users           96 Aug 28  2004 temp
drwxr-xr-x   9 appltcat   users         1024 Sep 19 11:48 webapps
drwxr-xr-x   3 appltcat   users           96 Sep 17 11:46 work

./bin:
total 1650
-rw-r--r--   1 appltcat   users         4769 Aug 28  2004 LauncherBootstrap.class
-rw-r--r--   1 appltcat   users        29757 Aug 28  2004 bootstrap.jar
-rw-r--r--   1 appltcat   users         7340 Aug 28  2004 catalina.50.bat
-rw-r--r--   1 appltcat   users         9726 Aug 28  2004 catalina.50.sh
-rw-r--r--   1 appltcat   users         7512 Aug 28  2004 catalina.bat
-rwxr-xr-x   1 appltcat   users        10024 Aug 28  2004 catalina.sh
-rw-r--r--   1 appltcat   users         8835 Aug 28  2004 catalina.xml
-rw-r--r--   1 appltcat   users         9386 Aug 28  2004 commons-daemon.jar
-rw-r--r--   1 appltcat   users        41768 Aug 28  2004 commons-launcher.jar
-rw-r--r--   1 appltcat   users        26202 Aug 28  2004 commons-logging-api.jar
-rw-r--r--   1 appltcat   users          511 Aug 28  2004 cpappend.bat
-rw-r--r--   1 appltcat   users         1284 Aug 28  2004 digest.bat
-rwxr-xr-x   1 appltcat   users          848 Aug 28  2004 digest.sh
-rw-r--r--   1 appltcat   users       343900 Aug 28  2004 jmx.jar
-rwxr-x---   1 appltcat   users          187 Mar  8 14:22 jsse_handshake_debug.sh
-rw-r--r--   1 appltcat   users        73008 Aug 28  2004 jsvc.tar.gz
-rw-r--r--   1 appltcat   users         1356 Aug 28  2004 launcher.properties
-rw-r--r--   1 appltcat   users         3694 Aug 28  2004 service.bat
-rw-r--r--   1 appltcat   users         2017 Aug 28  2004 setclasspath.bat
-rwxr-xr-x   1 appltcat   users         2055 Aug 28  2004 setclasspath.sh
-rw-r--r--   1 appltcat   users         1246 Aug 28  2004 shutdown-using-launcher.bat
-rwxr-xr-x   1 appltcat   users          770 Aug 28  2004 shutdown-using-launcher.sh
-rw-r--r--   1 appltcat   users         1273 Aug 28  2004 shutdown.bat
-rwxr-xr-x   1 appltcat   users          787 Aug 28  2004 shutdown.sh
-rw-r--r--   1 appltcat   users         1225 Aug 28  2004 startup-using-launcher.bat
-rwxr-xr-x   1 appltcat   users          766 Aug 28  2004 startup-using-launcher.sh
-rw-r--r--   1 appltcat   users         1274 Aug 28  2004 startup.bat
-rwxr-xr-x   1 appltcat   users          788 Aug 28  2004 startup.sh
-rw-r--r--   1 appltcat   users        94208 Aug 28  2004 tomcat5.exe
-rw-r--r--   1 appltcat   users       131072 Aug 28  2004 tomcat5w.exe
-rw-r--r--   1 appltcat   users         1260 Aug 28  2004 tool-wrapper-using-launcher.bat
-rwxr-xr-x   1 appltcat   users          784 Aug 28  2004 tool-wrapper-using-launcher.sh
-rw-r--r--   1 appltcat   users         2195 Aug 28  2004 tool-wrapper.bat
-rwxr-xr-x   1 appltcat   users         2510 Aug 28  2004 tool-wrapper.sh
-rw-r--r--   1 appltcat   users         1280 Aug 28  2004 version.bat
-rw-r--r--   1 appltcat   users          790 Aug 28  2004 version.sh

./common:
total 2
drwxr-xr-x   2 appltcat   users           96 Aug 28  2004 classes
drwxr-xr-x   2 appltcat   users           96 Sep 16 15:46 endorsed
drwxr-xr-x   2 appltcat   users         1024 Sep 16 15:46 lib

./common/classes:
total 0
```

```
./common/endorsed:
total 2218
-rw-r--r--   1 appltcat   users      1010675 Aug 28  2004 xercesImpl.jar
-rw-r--r--   1 appltcat   users       124724 Aug 28  2004 xml-apis.jar

./common/lib:
total 4866
-rw-r--r--   1 appltcat   users         8412 Aug 28  2004 ant-launcher.jar
-rw-r--r--   1 appltcat   users       958858 Aug 28  2004 ant.jar
-rw-r--r--   1 appltcat   users       559366 Aug 28  2004 commons-collections-3.1.jar
-rw-r--r--   1 appltcat   users       107631 Aug 28  2004 commons-dbcp-1.2.1.jar
-rw-r--r--   1 appltcat   users       112341 Aug 28  2004 commons-el.jar
-rw-r--r--   1 appltcat   users        42492 Aug 28  2004 commons-pool-1.2.jar
-rw-r--r--   1 appltcat   users       351903 Aug 28  2004 jasper-compiler.jar
-rw-r--r--   1 appltcat   users       105502 Aug 28  2004 jasper-runtime.jar
-rw-r--r--   1 appltcat   users        50491 Aug 28  2004 jsp-api.jar
-rw-r--r--   1 appltcat   users        27968 Aug 28  2004 naming-common.jar
-rw-r--r--   1 appltcat   users        14870 Aug 28  2004 naming-factory.jar
-rw-r--r--   1 appltcat   users         2059 Aug 28  2004 naming-java.jar
-rw-r--r--   1 appltcat   users        42308 Aug 28  2004 naming-resources.jar
-rw-r--r--   1 appltcat   users        97689 Aug 28  2004 servlet-api.jar

./conf:
total 256
drwxr-xr-x   3 appltcat   users           96 Sep 16 15:46 Catalina
-rw-------   1 appltcat   users         6954 Aug 28  2004 catalina.policy
-rw-------   1 appltcat   users         2754 Aug 28  2004 catalina.properties
-rw-------   1 appltcat   users          778 Aug 28  2004 jk2.properties
-rw-------   1 appltcat   users         1128 Sep 17 17:05 server-minimal.xml
-rw-------   1 appltcat   users        18988 Mar  8 10:37 server.cab
-rw-------   1 appltcat   users        18988 Mar  8 21:11 server.xml
-rw-------   1 appltcat   users        18872 Dec  1 15:51 server.xml.20050308
-rw-------   1 appltcat   users        18876 Nov 30 17:47 server.xml.orig
-rw-r--r--   1 appltcat   users          310 Mar  8 21:11 tomcat-users.xml
-rw-------   1 appltcat   users        38793 Aug 28  2004 web.xml

./conf/Catalina:
total 0
drwxr-xr-x   2 appltcat   users           96 Sep 16 15:46 localhost

./conf/Catalina/localhost:
total 6
-rw-------   1 appltcat   users          687 Aug 28  2004 admin.xml
-rw-------   1 appltcat   users          321 Aug 28  2004 balancer.xml
-rw-------   1 appltcat   users          428 Aug 28  2004 manager.xml

./logs:
total 5002
drwxr-xr-x   2 appltcat   users         1024 Nov 30 15:51 archive
-rw-r--r--   1 appltcat   users       218253 Mar  9 10:21 catalina.out
-rw-r--r--   1 appltcat   users        24447 Nov 30 17:51 localhost_log.2004-11-30.txt
-rw-r--r--   1 appltcat   users        79356 Dec  1 16:52 localhost_log.2004-12-01.txt
-rw-r--r--   1 appltcat   users       105724 Dec  2 15:03 localhost_log.2004-12-02.txt
-rw-r--r--   1 appltcat   users       445971 Dec  3 15:24 localhost_log.2004-12-03.txt
-rw-r--r--   1 appltcat   users        34033 Dec  8 11:30 localhost_log.2004-12-08.txt
-rw-r--r--   1 appltcat   users        33994 Dec 10 14:54 localhost_log.2004-12-10.txt
-rw-r--r--   1 appltcat   users        17010 Dec 13 20:53 localhost_log.2004-12-13.txt
-rw-r--r--   1 appltcat   users        17010 Dec 14 15:54 localhost_log.2004-12-14.txt
-rw-r--r--   1 appltcat   users        76360 Dec 15 16:47 localhost_log.2004-12-15.txt
-rw-r--r--   1 appltcat   users        17011 Dec 16 10:06 localhost_log.2004-12-16.txt
-rw-r--r--   1 appltcat   users      1054867 Dec 17 11:09 localhost_log.2004-12-17.txt
-rw-r--r--   1 appltcat   users        27768 Jan  5 15:42 localhost_log.2005-01-05.txt
-rw-r--r--   1 appltcat   users        17009 Jan  7 17:13 localhost_log.2005-01-07.txt
-rw-r--r--   1 appltcat   users        17009 Jan  9 21:50 localhost_log.2005-01-09.txt
-rw-r--r--   1 appltcat   users        34018 Jan 10 11:45 localhost_log.2005-01-10.txt
-rw-r--r--   1 appltcat   users         9747 Jan 14 12:00 localhost_log.2005-01-14.txt
-rw-r--r--   1 appltcat   users        27743 Jan 25 13:01 localhost_log.2005-01-25.txt
```

```
-rw-r--r--   1 appltcat   users        9748 Jan 26 15:27 localhost_log.2005-01-26.txt
-rw-r--r--   1 appltcat   users       52041 Jan 31 16:19 localhost_log.2005-01-31.txt
-rw-r--r--   1 appltcat   users       17010 Feb  1 11:10 localhost_log.2005-02-01.txt
-rw-r--r--   1 appltcat   users         205 Feb  2 15:54 localhost_log.2005-02-02.txt
-rw-r--r--   1 appltcat   users        9748 Feb  4 11:51 localhost_log.2005-02-04.txt
-rw-r--r--   1 appltcat   users        6305 Feb  9 17:31 localhost_log.2005-02-09.txt
-rw-r--r--   1 appltcat   users        9751 Feb 22 14:56 localhost_log.2005-02-22.txt
-rw-r--r--   1 appltcat   users        9746 Feb 25 00:24 localhost_log.2005-02-25.txt
-rw-r--r--   1 appltcat   users       11007 Feb 28 12:32 localhost_log.2005-02-28.txt
-rw-r--r--   1 appltcat   users       18021 Mar  1 13:20 localhost_log.2005-03-01.txt
-rw-r--r--   1 appltcat   users       68053 Mar  3 11:53 localhost_log.2005-03-03.txt
-rw-r--r--   1 appltcat   users       16997 Mar  4 13:53 localhost_log.2005-03-04.txt
-rw-r--r--   1 appltcat   users       30409 Mar  8 21:11 localhost_log.2005-03-08.txt
-rw-r--r--   1 appltcat   users       17996 Mar  9 10:21 localhost_log.2005-03-09.txt

./logs/archive:
This directory listing intentionally left out.

./server:
This directory listing intentionally left out.

./shared:
total 0
drwxr-xr-x   2 appltcat   users          96 Aug 28  2004 classes
drwxr-xr-x   2 appltcat   users          96 Aug 28  2004 lib

./shared/classes:
total 0

./shared/lib:
total 0

./temp:
total 0

./webapps:
total 10
drwxr-xr-x   3 appltcat   users        1024 Sep 16 15:46 ROOT
drwxr-xr-x   4 appltcat   users          96 Sep 16 15:46 balancer
drwxr-xr-x  21 appltcat   users        1024 Sep 16 15:46 jsp-examples
drwxr-xr-x   4 appltcat   users        1024 Sep 17 11:46 servlet
drwxr-xr-x   4 appltcat   users        1024 Sep 16 15:46 servlets-examples
drwxr-xr-x  12 appltcat   users        1024 Sep 16 15:47 tomcat-docs
drwxr-xr-x   3 appltcat   users          96 Sep 16 15:47 webdav

./webapps/ROOT:
This directory listing intentionally left out.

./webapps/balancer:
This directory listing intentionally left out.

./webapps/jsp-examples:
******This directory and all its subdirectories removed for space reasons.  The contents of the jsp-examples directory
should be removed from a production server.

./webapps/servlet:
total 22
drwxr-xr-x   2 appltcat   users          96 Sep 17 11:46 META-INF
-rw-r--r--   1 appltcat   users        2118 Sep 17 11:46 PostAuth_generic_test4x_45.htm
-rw-r--r--   1 appltcat   users        1372 Feb 23 17:06 README
drwxr-xr-x   5 appltcat   users        1024 Sep 17 14:00 WEB-INF
-rw-r--r--   1 appltcat   users        4980 Sep 17 14:09 generic.htm

./webapps/servlet/META-INF:
total 2
-rw-r--r--   1 appltcat   users          71 Sep 17 11:46 MANIFEST.MF
```

```
./webapps/servlet/WEB-INF:
total 10
drwxr-xr-x   3 appltcat   users        1024 Sep 19 12:45 classes
drwxr-xr-x   2 appltcat   users          96 Sep 17 11:46 docs
drwxr-xr-x   4 appltcat   users        1024 Sep 17 11:46 lib
-rw-r--r--   1 appltcat   users        1115 Sep 17 14:00 web.xml
-rw-r--r--   1 appltcat   users         595 Sep 17 11:46 web.xml.orig

./webapps/servlet/WEB-INF/classes:
total 26
-rw-r--r--   1 appltcat   users         262 Dec  1 15:49 ClearCommerce.properties
-rw-r--r--   1 appltcat   users         201 Sep 17 11:50 ClearCommerce.properties.original
-rw-r--r--   1 appltcat   users         705 Sep 19 12:40 SampleServletOutput.class
-rw-r--r--   1 appltcat   users         836 Sep 17 11:46 SampleServletOutput.java
-rw-r--r--   1 appltcat   users        1595 Sep 19 12:41 SampleServletOutput2.class
-rw-r--r--   1 appltcat   users        2048 Sep 17 11:46 SampleServletOutput2.java
-rw-r--r--   1 appltcat   users         969 Sep 19 12:36 cc.class
-rw-r--r--   1 appltcat   users         420 Sep 19 12:37 cc.java
drwxr-xr-x   5 appltcat   users        1024 Sep 17 11:46 clearcommerce
-rw-r--r--   1 appltcat   users         626 Sep 19 12:45 make_env.sh
-rw-r--r--   1 appltcat   users         771 Sep 17 11:46 run.bat

./webapps/servlet/WEB-INF/classes/clearcommerce:
total 10
drwxr-xr-x   2 appltcat   users        1024 Sep 17 11:46 servlet
drwxr-xr-x   2 appltcat   users        2048 Sep 19 18:42 utilities
-rw-r--r--   1 appltcat   users          29 Sep 17 11:46 version_includes_https_pipeline
drwxr-xr-x   2 appltcat   users        1024 Sep 17 11:46 xmltools

./webapps/servlet/WEB-INF/classes/clearcommerce/servlet:
total 174
-rw-r--r--   1 appltcat   users       13462 Sep 17 11:46 ClrCmrcGenericServlet.class
-rw-r--r--   1 appltcat   users       20410 Sep 17 11:46 ClrCmrcGenericServlet.java
-rw-r--r--   1 appltcat   users        6749 Sep 17 11:46 ClrCmrcGenericServlet4x.class
-rw-r--r--   1 appltcat   users       11890 Sep 17 11:46 ClrCmrcGenericServlet4x.java
-rw-r--r--   1 appltcat   users         995 Sep 17 11:46 ClrCmrcMissingFieldException.class
-rw-r--r--   1 appltcat   users         690 Sep 17 11:46 ClrCmrcMissingFieldException.java
-rw-r--r--   1 appltcat   users       10459 Sep 17 11:46 ClrCmrcServletData.class
-rw-r--r--   1 appltcat   users       20794 Sep 17 11:46 ClrCmrcServletData.java

./webapps/servlet/WEB-INF/classes/clearcommerce/utilities:
total 576
-rw-r--r--   1 appltcat   users        3439 Sep 17 11:46 C_Order.class
-rw-r--r--   1 appltcat   users        3608 Sep 17 11:46 C_Order.java
-rw-r--r--   1 appltcat   users        2615 Sep 17 11:46 C_Request.class
-rw-r--r--   1 appltcat   users        3079 Sep 17 11:46 C_Request.java
-rw-r--r--   1 appltcat   users        5245 Sep 17 11:46 ClrCmrcConfig.class
-rw-r--r--   1 appltcat   users        7730 Sep 17 11:46 ClrCmrcConfig.java
-rw-r--r--   1 appltcat   users       12003 Sep 19 18:49 ClrCmrcConfigProvider.class
-rw-r--r--   1 appltcat   users       23851 Sep 19 18:34 ClrCmrcConfigProvider.java
-rw-r--r--   1 appltcat   users       32280 Sep 17 11:46 ClrCmrcConstants.class
-rw-r--r--   1 appltcat   users       48790 Sep 17 11:46 ClrCmrcConstants.java
-rw-r--r--   1 appltcat   users        2303 Sep 17 11:46 ClrCmrcCurrencyCodes.class
-rw-r--r--   1 appltcat   users        3745 Sep 17 11:46 ClrCmrcCurrencyCodes.java
-rw-r--r--   1 appltcat   users        3151 Sep 17 11:46 ClrCmrcData.class
-rw-r--r--   1 appltcat   users        4814 Sep 17 11:46 ClrCmrcData.java
-rw-r--r--   1 appltcat   users         738 Sep 17 11:46 ClrCmrcException.class
-rw-r--r--   1 appltcat   users        1018 Sep 17 11:46 ClrCmrcException.java
-rw-r--r--   1 appltcat   users        3852 Sep 17 11:46 ClrCmrcHttpServlet.class
-rw-r--r--   1 appltcat   users        4144 Sep 17 11:46 ClrCmrcHttpServlet.java
-rw-r--r--   1 appltcat   users       17393 Sep 19 18:50 ClrCmrcJ2XML.class
-rw-r--r--   1 appltcat   users       42645 Sep 19 18:34 ClrCmrcJ2XML.java
-rw-r--r--   1 appltcat   users         489 Sep 17 11:46 ClrCmrcPaymentProcessorInterface.class
-rw-r--r--   1 appltcat   users        1033 Sep 17 11:46 ClrCmrcPaymentProcessorInterface.java
-rw-r--r--   1 appltcat   users        2781 Sep 17 11:46 ClrCmrcUtils.class
-rw-r--r--   1 appltcat   users        3016 Sep 17 11:46 ClrCmrcUtils.java
-rw-r--r--   1 appltcat   users        3180 Sep 17 11:46 DateTimeTranslator.class
```

```
-rw-r--r--   1 appltcat   users         5365 Sep 17 11:46 DateTimeTranslator.java
-rw-r--r--   1 appltcat   users         1155 Sep 17 11:46 EchoServlet.class
-rw-r--r--   1 appltcat   users          809 Sep 17 11:46 EchoServlet.java
-rw-r--r--   1 appltcat   users          921 Nov 30 15:34 JPayment$1.class
-rw-r--r--   1 appltcat   users         9699 Nov 30 15:34 JPayment.class
-rw-r--r--   1 appltcat   users        13171 Nov 30 15:27 JPayment.java
-rw-r--r--   1 appltcat   users         4278 Sep 19 18:50 UrlTester.class
-rw-r--r--   1 appltcat   users         5600 Sep 19 18:34 UrlTester.java

./webapps/servlet/WEB-INF/classes/clearcommerce/xmltools:
total 224
-rw-r--r--   1 appltcat   users         3077 Sep 17 11:46 ClrCmrcConfigDoc.class
-rw-r--r--   1 appltcat   users         4958 Sep 17 11:46 ClrCmrcConfigDoc.java
-rw-r--r--   1 appltcat   users        19933 Sep 17 11:46 ClrCmrcDocument.class
-rw-r--r--   1 appltcat   users        61982 Sep 17 11:46 ClrCmrcDocument.java
-rw-r--r--   1 appltcat   users         2973 Sep 17 11:46 ClrCmrcXMLInterface.class
-rw-r--r--   1 appltcat   users         3838 Sep 17 11:46 ClrCmrcXMLInterface.java
-rw-r--r--   1 appltcat   users         2990 Sep 17 11:46 FraudInfo.class
-rw-r--r--   1 appltcat   users         3322 Sep 17 11:46 FraudInfo.java
-rw-r--r--   1 appltcat   users         3497 Sep 17 11:46 MsgResponse.class
-rw-r--r--   1 appltcat   users         3980 Sep 17 11:46 MsgResponse.java

./webapps/servlet/WEB-INF/docs:
total 440
-rw-r--r--   1 appltcat   users       224768 Sep 17 11:46 ClearLink Servlet 2.2.doc

./webapps/servlet/WEB-INF/lib:
total 440
-rw-r--r--   1 appltcat   users        33382 Sep 17 11:46 ClrCmrcCcTemplates.properties
-rw-r--r--   1 appltcat   users          684 Sep 17 11:46 ClrCmrcFDResources.properties
-rw-r--r--   1 appltcat   users         3267 Sep 17 11:46 ClrCmrcProcessorResources.properties
drwxr-xr-x   2 appltcat   users           96 Sep 17 11:46 META-INF
-rw-r--r--   1 appltcat   users        40481 Sep 17 11:46 Misc.jar
-rw-r--r--   1 appltcat   users       144852 Sep 17 11:46 ccc_ssl.jar
drwxr-xr-x   3 appltcat   users           96 Sep 17 11:46 com

./webapps/servlet/WEB-INF/lib/META-INF:
total 2
-rw-r--r--   1 appltcat   users           48 Sep 17 11:46 MANIFEST.MF

./webapps/servlet/WEB-INF/lib/com:
total 0
drwxr-xr-x   3 appltcat   users           96 Sep 17 11:46 clearcommerce

./webapps/servlet/WEB-INF/lib/com/clearcommerce:
total 2
drwxr-xr-x   2 appltcat   users         1024 Sep 17 11:46 utilities

./webapps/servlet/WEB-INF/lib/com/clearcommerce/utilities:
total 126
-rw-r--r--   1 appltcat   users         8906 Sep 17 11:46 ClrCmrcCcGenerator.class
-rw-r--r--   1 appltcat   users         6819 Sep 17 11:46 ClrCmrcCcTemplate.class
-rw-r--r--   1 appltcat   users         7049 Sep 17 11:46 ClrCmrcDefaultProcessor.class
-rw-r--r--   1 appltcat   users        20820 Sep 17 11:46 ClrCmrcFraudDemoProcessor.class
-rw-r--r--   1 appltcat   users          389 Sep 17 11:46 ClrCmrcIProcessable.class
-rw-r--r--   1 appltcat   users          870 Sep 17 11:46 ClrCmrcProcessor$HeldMsg.class
-rw-r--r--   1 appltcat   users        14485 Sep 17 11:46 ClrCmrcProcessor.class
-rw-r--r--   1 appltcat   users         1531 Sep 17 11:46 ClrCmrcProcessorData.class

./webapps/servlets-examples:
******This directory and all its subdirectories removed for space reasons.  The contents of the servlets-examples directory
should be removed from a production server.

./webapps/tomcat-docs:
******This directory and all its subdirectories removed for space reasons.  The contents of the tomcat-docs directory should
be removed from a production server.
```


./webapps/webdav:
This directory listing intentionally left out.

./work:
This directory listing intentionally left out.