V 1.2 1 December 2015

CCB INC.

Web Application Security Policy Audit Plan

Mengyuan Wang

Shuaya Yang

Yue Zhang

Shiting Liu

Yi Wang

Executive Summary

This audit plan provides a proposed strategy to conduct an internal audit regarding the web application security controls across various departments of CCB, Inc. The security assessment is done to protect CCB's system from common potential threats including unauthorized access, excessive privilege abuse, misconfigurations, and network weakness. The overall company policy specifies the role of audit by:

- Monitoring security controls addressed in policies and ensuring the compliance of the security policy among various departments;
- Ensuring confidentiality, integrity, and availability of information; and
- Supporting managers as they work to identify the best way to mitigate a risk.

This report details the scope of testing conducted, auditors' resources allocation and responsibilities, the audit approach, and key control areas.

1. CCB Inc.

Contents

Purpose

The purpose of CCB internal IT audit is to provide an objective opinion whether CCB's web application security policy along with its IT management are put in place in a sufficient manner to achieve both CCB's IT and Business objects. Auditing activities include gaining understanding of the web application environment, identifying proper security controls has been put in place to mitigate risks, testing the sufficiency of these controls and finally issuing an objective IT audit report. CCB Internal Audit also plays a consultancy role independently to assist IT managers to improve IT governance and controls.

Scope

The scope of this review includes an assessment of CCB's web application security controls. The audit process provides reasonable assurance of CCB's web application environment and all systems and networks connected to it, ensuring internal controls are effective and users' information are properly secured and confidential. The assessment shall mostly consist in security issues of the web application, including in the policy: access controls, authentication, configuration management, and architecture and design.

Audit Team

The audit team consists of one internal audit manager and four internal auditors. The audit will take approximately 650 hours in an 8 hours a day and 5 days a week base. All internal auditors are required to maintain independence and objectivity in the conduct of their engagement. In carrying out the duties and responsibilities, the internal audit manager will issue reports to the executive team as well as the audit committee. The allocation of auditing resource based on planning, testing and reporting phases is listed below:

Team Members	Title	Time Allocation (in hours)			Total Time (in hours)
		Planning	Testing	Reporting	
Shiting Liu	Internal Audit Manager	50	30	50	130
Shuya Yang	Internal Auditor	30	80	20	130
Yi Wang	Internal Auditor	30	80	20	130

Mengyuan Wang	Internal Auditor	30	80	20	130
Yue Zhang	Internal Auditor	30	80	20	130
Total Time (in hours)		170	350	130	650

Responsibilities

Internal auditing is an independent, objective assurance and consulting activity. The team will perform the internal audit work to review and evaluate the risk management, control and governance arrangements that CCB has put in place, focusing in particular on how these arrangements help CCB to achieve its both IT and business objectives. The audit team will perform the following tasks in accordance with its overall objective:

- Assess compliance with the web application policy and procedures;
- Evaluate the adequacy of the system of internal controls;
- Recommend improvements in controls;
- Ensure the compliance of the security policy across all departments;
- Follow-up on significant findings from previous audit.

Audit Approach

The approach for the execution of this audit engagement is risk based and will consist of interviews with key employees, data extractions, review of documents, and system tests. Components of the audit are listed below:

- Identify risk areas;
- Perform a risk assessment in a particular area. Risks are classified as high, medium or low;
- The Internal Audit is primarily focused on the areas of key risks;
- Review and test current risk controls written in the security policy and evaluate whether these controls are in a sufficient manner;
- The previous CCB Internal Audit results would be used to identify areas that could benefit from the audit.

Control Areas

A review and a test will be performed based on key control areas. The estimated main control areas have been categorized and listed below:

- Access Control. The access of sensitive information should be granted on a least privilege principle. These privileges should be reviewed regularly and removed if no longer required.
- Authentication. Users of the web application must follow appropriate password management policies in order to prevent unauthorized access.
- Architecture and Design. The design of network and application security controls must be set appropriately against both internal and external threats.
- Configuration Management. Relevant parameters are set to recommended values which ensure optimum performance while maintaining security.

Issuing Audit Report

The audit report will include a summary of the findings from assessing the policy, controls, and results from the interviews held with the related employees. Recommendations for corrective actions shall be discussed immediately after the audit. Audit finding should be supported by the objective evidence. An official report summarizing the auditor's activities and findings will be distributed within two weeks. Signature is required from the department manager to accept the recommendations. The report shall contain following information:

- Audit Period
- Date of Audit
- Name of Auditee and Auditors
- Statement of findings
- Corrective Actions
- Statement of Recommendations

Summary of risk assessment and control evaluation:

Risk Areas Analysis with Controls	Test Steps and Summary of Evidence
1. Access Control	**Test Steps:** 1. Schedule a security drill with the IT personnel; 2. Select a security issue based on the Annual Rate of Occurrence (ARO); 3. IT personnel will call out tasks that will be performed; 4. Discuss with the IT group for possible mitigation methods with the help of the Information security group and the CIO; 5. Document and review the recovery processes discussed in the drill.
1.1 Unauthorized Execution of Administrative Functions	
Risk Description: Access to administrative functionality requires a user be authenticated and in possession of a valid session token, however execution of the ‘Add User’ functionality does not verify that the user requesting the action is an administrative user. The application does not correctly check that the user is authorized to execute the actions requested, meaning that the different privilege levels are not effectively enforced.	
Inherent Risk Assessment:	**Evidence:**

Impact	High	Security policies and procedures;
		Risk management process;
		IT risk management framework;
		Risk management process.

Likelihood	Medium	
Overall	Medium	
Inherent Risk Rating Rationale	The overall is medium because the functionality is exposed only to Administrative users after successfully authenticating to the application. An attacker would need to be in possession of valid user credentials, an associated session token and have knowledge of the correct URL for the administrative functionality.	
Risk Controls:		
1.1.1 Preventive Control: Role Based Access Controls		

1.1.2 Preventive Control: Granting access to IT system users based on the principle of least privilege.	
1.1.3 Preventive Control: Applications must prevent users from directly accessing internal objects, API's, files, and databases.	
1.1.4 Corrective Control: Review the logical access process	
1.1.5 Corrective Control: Review the process for security monitoring	
Assessment the Control of Design: Insufficient. **Recommendation: Re-engineer the application logic and authorisation/access controls to ensure that requests to execute privileged functions require that the calling user have sufficient permission to do so.**	
1.2 File Upload Functionality Allows Potentially Dangerous File Types	
Risk Description: That would allow an attacker to upload arbitrary files and have users of the system download the files to their local machine. This could potentially be used as a vector to distribute Trojans and	

attack users of the system, including for example Visual Basic Script (VBS) macro viruses.		
Inherent Risk Assessment:		
Impact	Medium	
Likelihood	High	
Overall	Medium	
Inherent Risk Rating Rationale	The overall risk is medium because there was no evidence of file type filtering or any content or virus checking of the uploaded files.	
Risk Controls:		
1.2.1 Preventive Control: Scan networks for Trojans, eavesdropping programs or bugs.		
1.2.2 Preventive Control: Corporate files servers and workstations will be protected with virus scanning software.		

1.2.3 Preventive Control: Virus update patterns will be updated regularly on corporate servers and workstations.	
1.2.4 Preventive Control: All drive and disk (USB, cd-drive) which brought in from outside of corporation is forbidden to be used.	
1.2.5 Preventive Control: Restrict the file types to only those dictated by business requirements.	
Assessment the Control of Design: Sufficient. The IT system monitored the process and implemented a process to automatically disable inappropriate accounts.	
2. Authentication	**Test Steps:** 1. Inquire if only authorized individuals are able to access CCB's systems; 2. Inspect if two-factor authentication is required for all individuals accessing the bank's systems; 3. Observe if users are only able to access data assets and systems that are approved for remote access; 4. Inspect if logging in for access performed and are the logs regularly reviewed for irregular activities.
2.1 No Account Lockout for End-User Accounts	
Risk Description: The application does not impose an account lockout threshold. An attacker could perform unlimited login attempts. An attacker able to successfully brute force entry into an account would be able to masquerade as that user within the application.	
Inherent Risk Assessment:	

Impact	Medium	**Evidence:** Minutes from board meetings; IT risk management reports; Escalation and follow-up process for monitoring IT risk; Set of IT policies and procedures for risk management.
Likelihood	Medium	
Overall	Medium	
Inherent Risk Rating Rationale	The overall risk is medium because an attacker is able to successfully brute force entry into an account would be able to masquerade as that user within the application.	
Risk Controls:		
2.1.1 Detective Control: Authorization and approval processes: automatic locking of accounts if the accounts not used for 30 days.		
2.1.2 Preventive Control: Implement an account lockout mechanism that restricts the number of login attempts. Industry best practice suggests a maximum figure of failed logon attempts to be between 3 and 5 attempts.		

2.1.3 Detective Control: All unsuccessful login attempts should be tracked in a database or other stateful component and should not be tracked in a session variable.	
2.1.4 Preventive Control: The account lockout should either be implemented as a random period of time i.e. between 1 and 5 minutes to defeat automated brute force tools or should remain locked until unlocked by an administrator or through an account reset process that can be initiated by a user through the implementation of which is subject to security policy requirements.	
2.1.5 Preventive Control: Employees’ logon IDs will be terminated after they resigned.	
Assess the Design of the Controls: Sufficient. Those security controls limit attackers’ login attempts and disable attackers to successfully brute force into an account.	
2.2 Weak Password Complexity	
Risk Description: The application does not implement minimum complexity rules for passwords. This results in the user being able to select weak and easily guessed passwords that could be as simple as “password” or “123”.	

Inherent Risk Assessment:		
Impact	Medium	
Likelihood	High	
Overall	High	
Inherent Risk Rating Rationale	The overall risk is high because if an attacker was able to guess a user’s password, they would be able to masquerade as that user within the application.	
Risk Controls:		
2.2.1 Preventive Control: Use individual username and password to access network, servers and applications.		
2.2.2 Preventive Control: User IDs and passwords are required to gain access to CCB’s networks and applications. Password issuing, strength requirements, changing and control will be managed through formal processes.		

2.2.3 Preventive Control: All built-in user IDs, testing user IDs, and IDs with default passwords been removed from the operating system, web servers and application itself before final production.	
2.2.4 Preventive Control: Use a minimum of 8 characters passwords that contains at least an uppercase, a lowercase character, a number and a non-alphanumeric character.	
2.2.5 Corrective Control: Review password complexity settings.	
Assessment the Control of Design: Insufficient. **Recommendation: Passwords should be set to expire on a regular basis and the application should maintain a history of at least the last 3 passwords to prevent password repetition. The accounts should be routinely audited in order to prevent and detect the use of weak passwords.**	
3. Configuration Management	**Test Steps:** 1. Remove all default content from the system in order to reduce its known signature footprint.;
3.1 .NET Version and HTTP Server Type and Version Information Leakage in HTTP Response Headers	

<table>
<tr><td colspan="2"><b>Risk Description:</b> The web server HTTP header responses displayed the type and version of software running on the host.
Knowledge of the specific web server version allows an attacker to quickly identify known vulnerabilities that may be present in that particular server.</td><td>2. Configure the server to provide false or no information;
3. Enable system security features on web server;
4. Build up secure processes manual</td></tr>
<tr><td colspan="2"><b>Inherent Risk Assessment:</b></td><td rowspan="5"><b>Evidence:</b>
Documentation about technology-related measures;
Risk appetite and tolerance level for the organization</td></tr>
<tr><td><b>Impact</b></td><td>Low</td></tr>
<tr><td><b>Likelihood</b></td><td>High</td></tr>
<tr><td><b>Overall</b></td><td>Low</td></tr>
<tr><td><b>Inherent Risk Rating Rationale</b></td><td>The overall risk is low because this vulnerability constituted information leakage and did not directly impact the security posture of the server however it is useful and time saving to an attacker.
An attacker can use common scanning tools or directly send valid HTTP requests to the</td></tr>
</table>

	server to cause it to reveal version information.	
Risk Controls:		
3.1.1 Preventive Control: Programmers should not believe and depend on HTTP REFERER headers, form fields or cookies to make security decision.		
3.1.2 Preventive Control: Specify the enable Version Header directive as false.		
3.1.3 Preventive Control: Remove all default, outdated, development and test content from production servers.		
3.1.4 Preventive Control: There are a number of web server hardening tools available for different web server types that automatically remove default content such as scripts and help pages i.e. IIS lockdown which is available from Microsoft.		
3.1.5 Preventive Control: If possible, configure the server to provide false or no information. Remove all default content from the system in order to reduce its known signature footprint.		
Assessment the Control of Design: Insufficient.		

Recommendation: Use the IIS Lock down tool from Microsoft and utilize the built in URL scan tool within IIS6.0 to prevent the information leakage; this can also be achieved by editing the machine.config configuration file.

4. Architecture and Design

4.1 Cookie HTTP-only Flag Not Set

Risk Description:

The cookie provided by the server for session maintenance is not marked for transmission over HTTP only. The HTTP-only attribute for cookies prevents them from being accessed through client-side script.

Web browsers that do not support the HTTP only cookie attribute either ignore the cookie or ignore the attribute, which means that it is still subject to cross-site scripting attacks. An attacker able to compromise a valid session cookie could masquerade as that user within the application without requiring knowledge of the users credentials.

Inherent Risk Assessment:

Impact	Medium

Test Steps:

1. Configure the application environment to only provide session cookies to that are marked as HTTP-only.

2. Ensure that the application is free of XSS vulnerabilities and support for the TRACE verb is disabled.

3. Current browsers block TRACE requests using the XML Http Request object.

Evidence:

Process to review and approve key events and impact;

Procedure to identify and evaluate relevant negative impacts;

Likelihood	Low	Significant events database (a copy of the structure and a sample of records); Risk monitoring process.
Overall	Low	
Inherent Risk Rating Rationale	The overall risk is low because for an attacker to gain access to the Document cookie object an exploitable XSS vector must exist. Launching an effective XSS attack against end users of the application requires a thorough knowledge of JavaScript and web application technologies.	
Risk Controls:		
4.1.1 Preventive Control: Can not put any sensitive information in client browser cookies.		
4.1.2 Preventive Control: CCB cannot believe the hidden parameters cannot be changed by the users, because hidden parameters can be easily affected by attackers.		

4.1.3 Preventive Control: Programmer should use strong cryptographic techniques to safeguard the confidentiality and integrity of the data.	
4.1.4 Preventive Control: Configure the application environment to only provide session cookies to that are marked as HTTP-only.	
4.1.5 Preventive Control: Current browsers block TRACE requests using the XML Http Request object.	
Assessment the Control of Design: Sufficient. Because newer edition browser will support the HTTP-only cookie attribute automatically.	