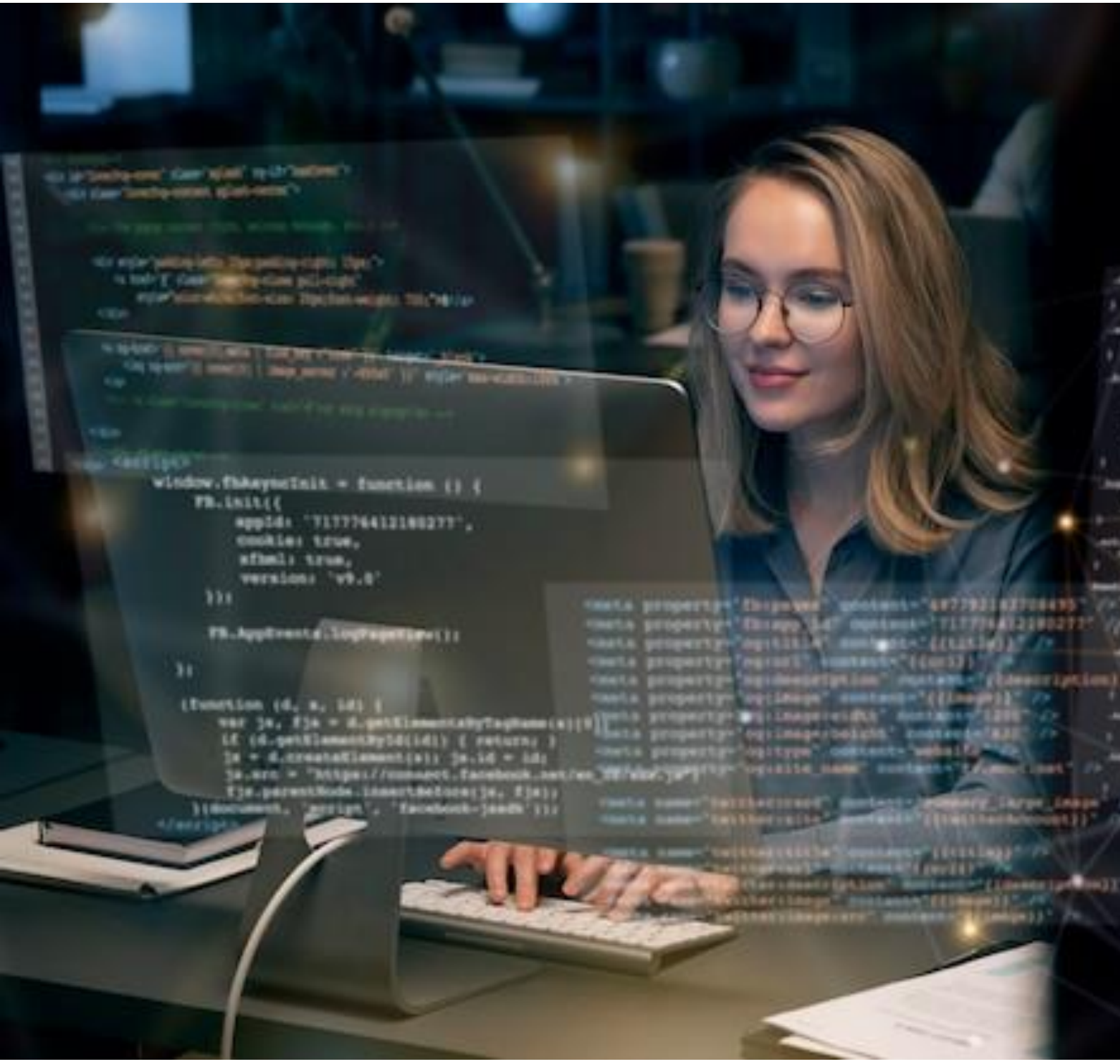
Web Application Security Assessment Sample Report



This document is a highly confidential which contains all the information regarding the red team engagement that was done by Infopercept Team on ABC Company.

Table of Contents

Copyright

Disclaimer

By accessing and using this report you agree to the following terms and conditions and all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Infopercept Consulting Pvt Ltd (Infopercept). Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Infopercept or any third party. This document and its contents including, but not limited to, graphic images and documentation may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, without the prior written consent of Infopercept. Any use you make of the information provided, is at your own risk and liability. Infopercept makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information, products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Infopercept shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Infopercept agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

Document Authorities

Company	ABC Corporation Ltd.			
Document Title	Application Security Audit Report			
Date				
Reference				
Scope	Application Security Assessment			
Classification	☐Public	☐Internal	☐Confidential	☐ Secret
Document	☐Proposal	☐Deliverable	☐General	

Recipients

Name	Title	Company
Mr. XYZ	CIO	ABC Corporation Ltd.

Document History

Date	Version	Prepared by	Status
15/02/2021	1.0	Consultant 1	Draft Report
17/02/2021	1.1	Consultant 2	Final Report

Overview

ABC Corporation Ltd. engaged Activity to conduct a Web Application Security Assessment of its Internet facing MyApp. The purpose of the engagement was to utilize active exploitation techniques in order to evaluate the security of the application against best practice criteria and to validate its security mechanisms and identify application-level vulnerabilities.

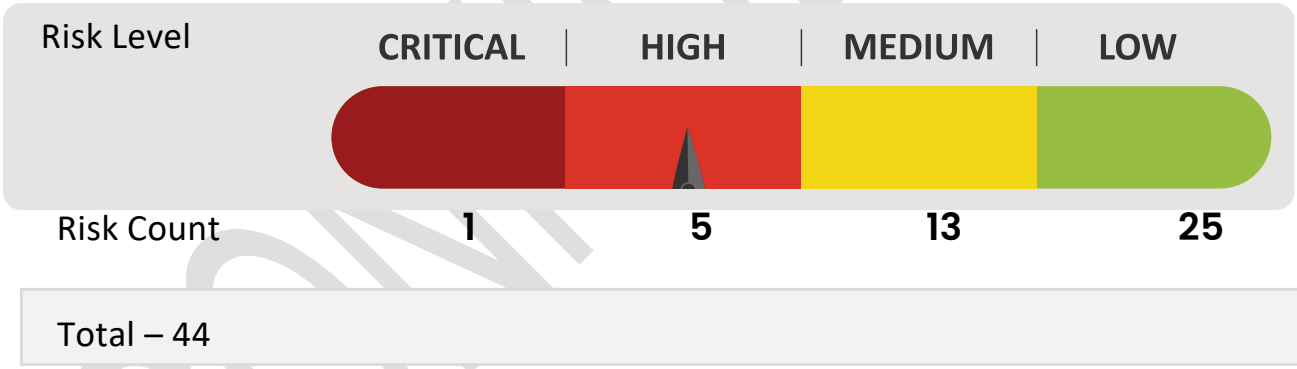
A Web Application Security Assessment provides ABC Corporation Ltd. with insight into the resilience of an application to withstand attack from unauthorized users and the potential for valid users to abuse their privileges and access. The assessment evaluates the security of the application against best practice criteria to validate security mechanisms and identify application-level vulnerabilities.

This report details the scope of testing conducted, all significant findings along with detailed remedial advice. The summary below provides a non-technical audience with a summary of the key findings and relates these back to business impacts. Section two of this report relates the key findings. Section three of this report highlights potential control areas where ABC Corporation Ltd. may want to invest further resources in order to improve the overall security posture of their systems. Section four of this report provides detailed narration and individual vulnerability findings that are aimed at a technical audience.

This document summarises the findings, analysis and recommendations from the assessment, which was conducted across the Internet from Activity offices in Farnborough, Hampshire.

Summary of Findings

The graph below shows a summary of the number of vulnerabilities found for each impact level for the Web Application Security Assessment. A significant number of high impact vulnerabilities were found that should be addressed as a priority.



The application has been deployed in a manner that is not in line with best practice guidelines for

application and web servers facing the Internet. The application was found to be vulnerable to a number of attacks related to the authentication mechanisms and implemented authorization controls that would result in unauthorized access to the application and compromise of the application and users' data.

Specifically, the application is vulnerable to a number of exploitable issues that are a direct consequence of either inadequate or non-existent input validation routines. The majority of these issues are a result of Cross Site Scripting vulnerabilities. The potential impacts of successful Cross Site Scripting attacks can be disclosure of user credentials and use of the site to fool users into accessing other compromised or malicious sites, which could damage brand and reputation which would ultimately have a financial cost.

In a multi user shared working environment such as the e-portal, it is feasible that attackers would use Cross Site Scripting attacks to steal other users' credentials and sessions, in order to masquerade as those users or elevate their privileges to perform actions that they may otherwise be unable to perform.

Cross site scripting attacks would require knowledgeable users to perform them. should review what the impact of a successful XSS attack on their users would be and its likelihood against the cost of remediation which would consist of sanitizing all user supplied data on its receipt and on its use. The lack of input validation within the application also resulted in the discovery and exploitation of a number of SQL injection vulnerabilities. It is possible for an attacker to access the database with administrative privileges and manipulate the data store in order to access, modify or delete its data. It is also possible to use the same attack to execute operating system commands on the database server providing access to the underlying server resources with administrative privileges allowing an attacker the ability to attack internal systems that are not directly exposed to the Internet. Many tools are available to automate the exploitation of the application in this manner and the Internet has many step-by-step guides to enable even the lowest skilled attacker to successfully execute an attack.

SQL injection targets the application's database and the infrastructure supporting that application and database. 's corporate network could be at risk depending how segregated the application is from the corporate environment. Given the ease of the attack, and what is at stake, should urgently address this vulnerability by sanitizing user supplied data. should note that sanitizing user supplied data addresses both the XSS and SQL injection issues at the same time if performed correctly.

The in house developed application should be re-engineered by in order to resolve all of the identified issues. It is evident to Activity that a secure and consistent application development framework or standard has not been adopted or followed by all of the developers responsible for the application. Given this inconsistent approach to application development, Activity cannot be certain that every vulnerability within this application has been identified. To remediate this risk, Activity recommends that a full application source code review be conducted of the application's source code. Additionally, a review of HTML and active content source code could uncover a variety of vulnerabilities that are not likely to be found during a blind assessment, yet would be exploitable via insider knowledge or in the event that application source code is exposed

1.Executive Summary

1.1 Introduction

Infopercept Cons Pvt. Ltd. conducted an Application Security audit activity for the internal network at ABC Limited. The assignment was carried out by Infopercept technical team between the 1st to the 10th of February 2015 with the following goals:

- Identifying security vulnerabilities in TESTAPP.
- Providing risk mitigation recommendations for the discovered vulnerabilities.
- Mapping the discovered vulnerabilities to ABC's Information Protection Policy.

This audit report contains:

- The description of the TESTAPP application and its business case
- The security vulnerabilities discovered as a result of the technical application security audit
- The security vulnerabilities discovered as a result of the application process audit
- The risk mitigation strategies that need to be implemented to ensure that the application meets information protection plan (IPP) control compliancy

1.2 Scope of The Audit

The application security audit has been conducted to provide a holistic picture of the security of the TESTAPP distribution application. In order to achieve this, one cannot consider only the technical aspects of security as this provides a one-sided depiction of the security. It is imperative that the processes, policies and procedures governing the accepted use of the application are also audited to ensure that information is protected entirely.

Bearing this in mind the audit was divided into a two-phase approach:

PHASE 1 – TECHNICAL AUDIT

The objective of this phase is to identify and provide remedies for all technical vulnerabilities in the application. The idea behind this audit is to discover whether an attacker can leverage flaws in the application to compromise the confidentiality, integrity or availability of ABC's distribution information. As the client side of the application will be operated by semi-trusted third parties. Specific attention has been given to the security mechanisms of the client application and the potential damage a malicious third party could cause, by exploiting flaws in the client-server architecture. The technical audit was conducted as a 'black-box' exercise, implying that the auditors were not given access to the source-code of the application, nor were they given any special privileges to connect to the application. This was done to simulate, as closely as possible, the access level granted to a normal user of the application.

PHASE 2 – PROCESS AUDIT

The purpose of Paper / Office documents audit was to assess and evaluate the existing security controls vis-à-vis controls laid down by ABC's information protection plan (IPP) control in response to risk assessment undertaken as per Information Protection management guideline (IPMG).

The scope of the above audit was limited to the TESTAPP application and information available pertaining to infrastructure, people, contract documents, process and agreements associated with the use of TESTAPP application.

The methodology involved was discussions, personal interviews and review of documents available.

An audit plan was laid down after understanding the IPP controls. The list of documents and procedures required for fulfilling these controls was prepared. After gathering the requisite information, a process of compliance and substantive testing was undertaken. Substantive testing was done for alleviating doubts related with completeness accuracy or validity of desired IPP controls.

1.3 Key Findings

Following is a point-wise key finding of all the vulnerabilities discovered. This list is categorized according to vulnerabilities in the following aspects:

- **Authentication Mechanism:** The features of the application that ensure that a non-authorized user cannot gain access to the application.
- **Data Security:** The features of the application that ensure the confidentiality and integrity of the data that is being processed.
- **Configuration Security:** The parts of the application that control its configuration parameters.
- **Communication Security:** The parts of the application that ensure that data is secure when communicate over a network.
- **Auditing Mechanism:** The mechanisms in the application that record and maintain an audit trail of what activities were performed, by whom and at what time.
- **Architectural Concerns:** The design decisions made in the development of the application.

Authentication Mechanism

The application login screen disallows special characters; however this can be bypassed by pasting the required characters.

- An attacker can login without valid credentials, bypassing the authentication mechanism.
- The login screen allows attackers to harvest valid usernames.
- Password complexity requirements are not properly enforced.
  - Passwords are not case sensitive.
  - Usernames are allowed as passwords.
  - Special characters are allowed when changing a password, but not at login, locking out a valid user.
- The account lockout feature can be bypassed, allowing an attacker to mount brute force attacks.
- Passwords are not hidden behind *'s in the password change dialog box.

- The user should be asked for the current password before being allowed to change it.
- The password ageing mechanism is not enforced.
- The default as well as test accounts are present on the server allowing easy access to the application.

Data Security

- The entire database including usernames / passwords is stored unencrypted.
- An attacker can take full control of all the data in the database including:
    - Customer details
    - Invoicing and transaction details
    - Product information.
    - Usernames / passwords
- The database is accessed through the default super-user account with a blank password.
- An attacker can poison any data that is waiting to be synchronized with the server.
- The file system does not support access control for the locally stored data.

Configuration Security

- FTP server IP address, username and password are stored in the client registry unencrypted.
- FTP server usernames / passwords are stored on the server encrypted with a proprietary
- encryption algorithm which does not withstand basic cryptanalysis.

Communication Security

- Client-side certificates are not enabled, thus there is no way to verify the source of a
- transaction.
- CFA systems are unprotected and provider CFA access is via insecure dial-up lines.
- The FTP server allows the client to use weak encryption algorithms which do not provide
- adequate communications security.

Auditing Mechanism

- The application does keep a record of login failures. Brute force attacks on the login will not be detectable.
- An attacker can erase all the audit logs,
- The user activity log can be controlled to
    - Inject fake entries
    - Modify existing entries including the date & time
    - Delete specific entries

Architectural Concern

- The CFAs fall outside ABC's security domain.
- The CFAs are vulnerable to remote attacks and provide a potential attack vector to the main ABC network.
- An unnecessary amount of confidential information is stored locally on the unprotected CFA systems.
- Encryption is not used at multiple levels in the application, violating the principle of defense-in-depth.
- The application security can collapse in a domino effect. The different vulnerabilities can be chained together to create different attack scenarios.

1.4 Recommendations Summary

Infopercept's consultants have addressed each of the identified security concerns and provided recommendations to mitigate the risk involved. While many of the vulnerabilities discovered are at the programming level and may be easily mitigated by a consultant with skilled expertise, there are residual risks in the overall architecture of the application, which need, either to be treated as an accepted risk due to the logistical difficulties of such an implementation, or addressed at the foremost design level of the application.

There is another major flaw in the architecture of the application. This is that the security is in the hands of CFA who can knowingly, intentionally or accidentally transfer data which could access the ABC network and can create major Operating System, Application level or Middleware security threats. Though vital and sensitive information is protected by access controls, these are not available at all CFA's.

Many other recommendations have been made, to enhance the security of the policies and procedures governing the use of the applications and the handling of ABC's confidential information. All recommendations have been made to ensure that the application is fully compliant with the ABC Information Protection Policy (IPP) controls. Certain recommendations are not included in the ABC IPP; these represent the industry best-practices

2. Application Description & Architecture

2.1 Description & Business Case

The TESTAPP application has been designed to provide ABC, India with an automated processing system for the management of distribution and sales. The application development has been out-sourced to a software development company, 'XYZ Technologies'. Currently, the application is in the development phase and is awaiting roll-out into a production environment.
The application programming platform is Microsoft Visual Basic 6 and the application consists of three parts:

- The TESTAPP Client – Where all data-processing and transaction creations will be done. It will be installed at the third-party clearing & forwarding agents (CFA) locations, where operators will enter the relevant data. The client has a local database that is modified and then synchronized with the master server.
- The TESTAPP SFTP Server – This is the server installed at the Internet Data Center. This server will accept synchronization requests from different clients and store the synchronization data for multiple locations. The SFTP server component is provided by a third-party ActiveX control.
- The TESTAPP Configurator – This is a master database creation tool designed to administer the databases sent to the different CFA locations. It is to be installed only at the ABC Limited, India's Head Office.

2.2 Process Flow

- The ABC Limited, India Head Office creates 'database masters' that are sent to each of the CFA locations on an installation CD along with the TESTAPP client application.
- The CFA's install the application on the systems designated for data-processing. One system has to act as a local database server and this contains all the information that the CFA's need to work with.
- Transactions are entered into the client application, which make changes to the local database. The transactions relate to stock, invoicing, customer, transaction and payment processing information.
- A manual synchronization must be performed, to upload the changes made in the local database to the TESTAPP SFTP server. The CFAs connect to the Internet via regular ISP connections and synchronize their database changes with the SFTP server.
- These changes are stored on the SFTP server and passed to other CFA locations as per the requirements, when they synchronize.

3. Vulnerability Information Details

For each vulnerability, the following information is provided:

URL Information:

- URL Title – This title shows the scanned URL's role as shown below:

http://www.xyz.com/xyz.xyz

Vulnerability Information:

Below is the vulnerability table

Vulnerability Title	
Risk	
Abstract	
IPMG Control Violation	
Reference	
Ease of Exploitation	
Impact	
Recommendations	

- **Vulnerability Title –** A short title that describes the vulnerability. For each vulnerability, the title bar is color coded for a quick identification of the risk level. Title bar color codes are as follows:

CRITICAL

HIGH

MEDIUM

LOW

INFORMATION

Externally

- **Abstract –** Describes the flaw or bugs that cause the vulnerability.
- **IPMG Control Violation –** Provides the ABC IPMG control numbers that are violated.
- **Reference –** Describes the reference for the respective vulnerability found.
- **Ease of Exploitation –** Provides a metric for the skill level required to exploit the vulnerability

Metric Skill-level	Metric Skill-level
Easy	Casual user
Medium	Computer-savvy individual
Hard	Determined hacker

- **Impact –** Describes the possible business impact to ABC if this vulnerability is successfully exploited by an attacker.
- **Recommendation –** Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- **Proof of Concept –** Screenshots / supporting evidence showing the vulnerability being exploited.

3.1 List Of URL

The following list defines the systems to be scanned for vulnerabilities:

No	Site URL	Web Server	Database	Front End
01	http://www.abccorp.com/abc.aspx	IIS 7		ASP

3.2 Vulnerability Overview

Vulnerability overview

The application was found to be unsafe to some of the critical vulnerabilities as identified in OWASP

Sr No.	Vulnerabilities	Audit Status
01	Injection	Open
02	Cross Site Scripting (XSS)	Closed
03	Broken Authentication and Session Management	Open
04	Insecure Direct Object References	Closed
05	Cross Site Request Forgery (CSRF)	Closed
06	Security Misconfiguration	Closed
07	Failure to Restrict URL Access	Closed
08	Unvalidated Redirects and Forwards	Closed
09	Insecure Cryptographic Storage	Open
10	Insufficient Transport Layer Protection	Open

3.3 Vulnerabilities Discovered

1. Improper Session Management	
Risk	Medium
Abstract	Proper authentication and session management is critical to web application security. Flaws in this area most frequently involve the failure to protest credentials and session tokens through their lifecycle.
IPMG Control Violation	
Reference	http://www.technicalinfo.net/papers/WebBasedSessionManagement.html http://msdn.microsoft.com/enus/library/aa480476.aspx#pagexplained0002_aspnetforms
Ease of Exploitation	Low
Impact	These flaws can lead to the hijacking of user or administrative accounts, undermine authorization and accountability controls, and cause privacy violations.
Recommendations	Regenerate a new session upon successful authentication. Any session token used prior to login should be discarded and only the new token should be assigned for the user till the user logs out. This session token should be properly invalidated when the user logs out.

Proof of Concept:

Go to the 'Login' page and enter user ID and password, capture the request using proxy tool. Observe the session token.

2. Auto complete feature of the browser	
Risk	Medium
Abstract	For websites that user frequently visit, user find it helpful to have Firefox or Internet Explorer store commonly entered information such as usernames and passwords, email addresses, phone numbers and more. With the information stored, the web browser will then insert the information into the appropriate fields when completing forms. All mainstream web browsers have a built-in auto complete function.
IPMG Control Violation	
Reference	http://msdn.microsoft.com/library/default.asp?url=/workshop/author/forms/autocomplete_ovr.asp#security http://www.securityfocus.com/infocus/1882
Ease of Exploitation	Low
Impact	Password can be steeled from auto complete feature.
Recommendations	Set autocomplete to OFF. < form autocomplete="off"> - for all form fields,< input autocomplete="off" /> - for just one field

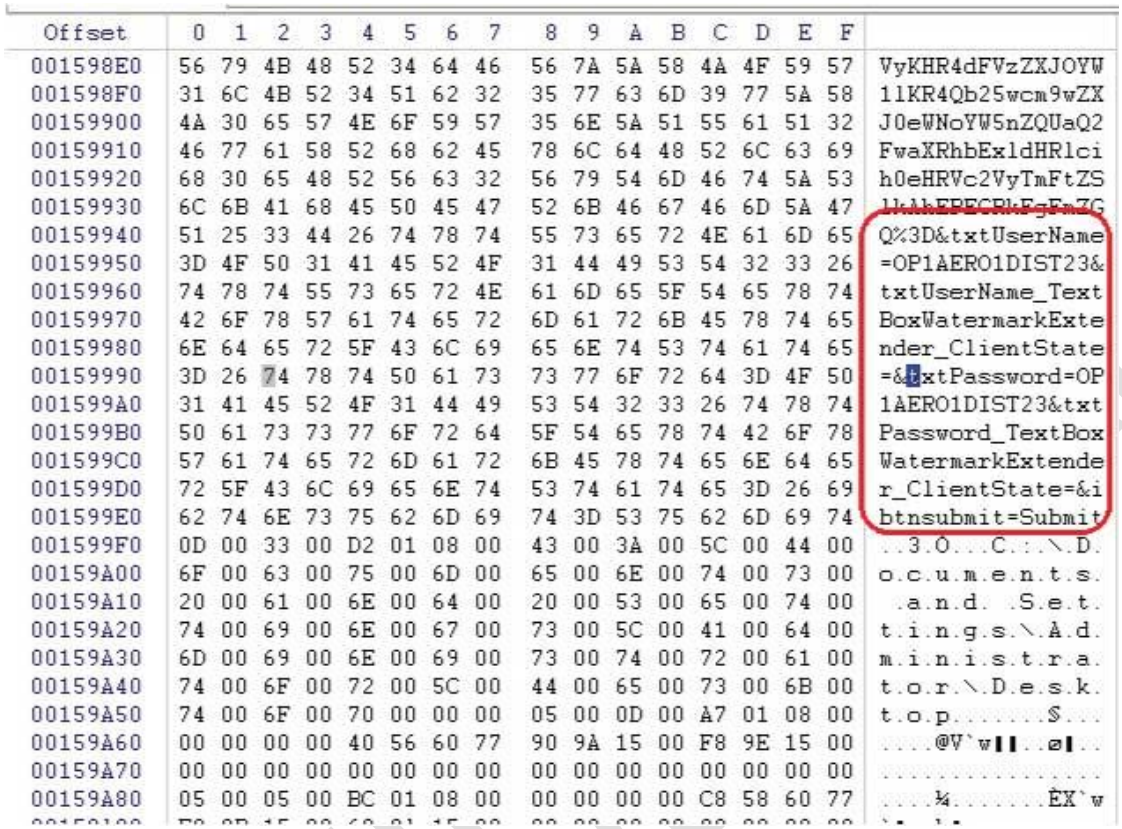
Proof of Concept:

Go to login page enter user credentials and click on submit button. Observe the popup box will appear asking for saving the password.

3. Password staying in browser memory	
Risk	Low
Abstract	The request on the login page containing the username and password of the user is also stored in the browser's memory. The browser's memory can be read with the use of memory reading tools. In this application the encryption is same every time for a particular password, so if a user left his browser window open after logout, an adversary can steal the password from the memory.
IPMG Control Violation	
Reference	http://www.owasp.org/index.php/Cryptography http://www.owasp.org/index.php/Guide_to_Cryptography
Ease of Exploitation	Low
Impact	Password can be gained by an attacker.
Recommendations	The password can be read from the memory if it is being sent in clear text. Using the salted hash technique for password transmission will solve this issue. Do not create cryptographic algorithms. Only use approved public algorithms such as AES, RSA public key cryptography, and SHA-256 or better for hashing Do not use weak algorithms, such as MD5 / Sha1. Favour safer alternatives, such as SHA-256 or better Ensure that encryption is random Ensure that encrypted data stored on disk is not easy to decrypt

Proof of Concept:

Login into the application with valid username and password and browse the application. Now, log out from the application and leave the browser window open. Now Run the browser memory reading tool to read the browser's memory and observe that the username and password is visible in clear text



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
001598E0	56	79	4B	48	52	34	64	46	56	7A	5A	58	4A	4F	59	57	VyKHR4dFVzZXJOYW
001598F0	31	6C	4B	52	34	51	62	32	35	77	63	6D	39	77	5A	58	1lKR4Qb25wcm9wZX
00159900	4A	30	65	57	4E	6F	59	57	35	6E	5A	51	55	61	51	32	J0eWNoYW5nZQUaQ2
00159910	46	77	61	58	52	68	62	45	78	6C	64	48	52	6C	63	69	FwaXRhbExldHRlci
00159920	68	30	65	48	52	56	63	32	56	79	54	6D	46	74	5A	53	h0eHRVc2VyTmFtZS
00159930	6C	6B	41	68	45	50	45	47	52	6B	46	67	46	6D	5A	47	lkAhEPEGRkFgFmZG
00159940	51	25	33	44	26	74	78	74	55	73	65	72	4E	61	6D	65	Q%3D&txtUserName
00159950	3D	4F	50	31	41	45	52	4F	31	44	49	53	54	32	33	26	=OP1AERO1DIST23&
00159960	74	78	74	55	73	65	72	4E	61	6D	65	5F	54	65	78	74	txtUserName_Text
00159970	42	6F	78	57	61	74	65	72	6D	61	72	6B	45	78	74	65	BoxWatermarkExte
00159980	6E	64	65	72	5F	43	6C	69	65	6E	74	53	74	61	74	65	nder_ClientState
00159990	3D	26	74	78	74	50	61	73	73	77	6F	72	64	3D	4F	50	=&txtPassword=OP
001599A0	31	41	45	52	4F	31	44	49	53	54	32	33	26	74	78	74	1AERO1DIST23&txt
001599B0	50	61	73	73	77	6F	72	64	5F	54	65	78	74	42	6F	78	Password_TextBox
001599C0	57	61	74	65	72	6D	61	72	6B	45	78	74	65	6E	64	65	WatermarkExtende
001599D0	72	5F	43	6C	69	65	6E	74	53	74	61	74	65	3D	26	69	r_ClientState=&i
001599E0	62	74	6E	73	75	62	6D	69	74	3D	53	75	62	6D	69	74	btnsubmit=Submit
001599F0	0D	00	33	00	D2	01	08	00	43	00	3A	00	5C	00	44	00	..3.Ò...C.:.\.D.
00159A00	6F	00	63	00	75	00	6D	00	65	00	6E	00	74	00	73	00	o.c.u.m.e.n.t.s.
00159A10	20	00	61	00	6E	00	64	00	20	00	53	00	65	00	74	00	.a.n.d. .S.e.t.
00159A20	74	00	69	00	6E	00	67	00	73	00	5C	00	41	00	64	00	t.i.n.g.s.\.A.d.
00159A30	6D	00	69	00	6E	00	69	00	73	00	74	00	72	00	61	00	m.i.n.i.s.t.r.a.
00159A40	74	00	6F	00	72	00	5C	00	44	00	65	00	73	00	6B	00	t.o.r.\.D.e.s.k.
00159A50	74	00	6F	00	70	00	00	00	05	00	0D	00	A7	01	08	00	t.o.p.....§....
00159A60	00	00	00	00	40	56	60	77	90	9A	15	00	F8	9E	15	00	....@V`w..ø.....
00159A70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00159A80	05	00	05	00	BC	01	08	00	00	00	00	00	C8	58	60	77	....¼.....ÈX`w

4. IPMG Violation & Security Controls

Infopercept conducted an audit related with security control documents, which should be in place to enhance the protection mechanism. This task was undertaken by interviewing staff members and documents made available to auditors

IPMG VIOLATIONS HAVE BEEN REMOVED FOR THIS SANITIZED REPORT

5. Auditor's End Notes

During course of the audit, the auditors identified certain points that could be potential security concerns. As these points relate to the application architecture as a whole, they have not been included as individual vulnerabilities.

This section gives a brief description of each of these points.

5.1 Distributed Database Architecture

The architecture of the application relies on a 'distributed database' mechanism, where each CFA has a portion of the database stored locally. All updates are made to this database and then synchronized using the SFTP server as a medium. This raises a few concerns:

- The local databases contain more information than is required for the CFA to do their job.
- There is no automated process for performing synchronization. It is not specified when updates are supposed to be pushed to the server. This can result in disparities in the information available across locations.
- The confidential information in the local databases is completely outside ABC's security control.

5.2 CFA Client Security

The security of the CFA client infrastructure appears to be very weak. Specifically:

- A large number of the client systems are legacy Windows 98 systems, which do not have adequate security mechanisms at the operating-system level.
- The use of dial-up and regular ISP connections for the synchronization of data results in ABC's data traveling over insecure networks. Despite the use of SSL encryption, this poses a significant risk. The use of a proper VPN solution is recommended.

No.	Action Item	Responsibility	Time-line	Rating
01	The application must be modified to validate all user inputs so that only legitimate data can be entered.			
02	The application must ensure that password fields are hidden behind asterisks to prevent involuntary disclosure of the password.			
03	The application should ask the user to enter the old password before being allowed to change it.			

About Infopercept - Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Imprint
© Infopercept Consulting Pvt. Ltd.

Created Date
Oct 2023

Contact Detail
sos@infopercept.com
www.infopercept.com/sample-report