Salesforce Application Security Audit

Case Study

Prepared by

Kurudunje Deekshith Shetty

Security Analyst / Student

Date:	April 27, 2025
Version:	1.0
Status:	Final Report

Contents

1 Introduction 3
1.1 Background 3
1.2 Objectives 4
1.3 Scope and Limitations 4

2 Problem Statement 4

3 Security Audit Methodology 4
3.1 Pre-Audit Planning 4
3.1.1 Scope Definition 4
3.1.2 Tools and Resources 5
3.2 Audit Procedures 5
3.2.1 Access Control Review 5
3.2.2 Authentication Review 5
3.2.3 Vulnerability Scanning 5
3.2.4 Log Analysis 5
3.2.5 Incident Response Review 5
3.2.6 User Awareness Assessment 6

4 Discoveries and Findings 6
4.1 Critical Findings 6
4.1.1 Weak Authentication Controls 6
4.2 High-Severity Findings 6
4.2.1 Over-Privileged Accounts 6
4.2.2 Vulnerable Custom Code 6
4.3 Medium-Severity Findings 7
4.3.1 Inadequate Monitoring 7
4.3.2 Poor Incident Response 7

5 Risk Analysis 7
5.1 Threat Modeling 7
5.2 Risk Matrix 7

6 Recommendations 8
6.1 Critical Priorities (0-30 Days) 8
6.1.1 Enforce MFA 8
6.1.2 Implement Least Privilege 8
6.2 High Priorities (30-60 Days) 8
6.2.1 Enhance Monitoring 8
6.2.2 Secure Custom Code 8
6.3 Medium Priorities (60-90 Days) 8
6.3.1 Strengthen Incident Response 8
6.3.2 User Awareness Training 8

7 Implementation Guide 9
7.1 MFA Implementation Steps 9
7.2 Least Privilege Implementation 9

8 Conclusion 9
8.1 Key Takeaways 9
8.2 Future Considerations 10

A Appendix A: Audit Methodology Details 11
A.1 Tools and Techniques 11

B Appendix B: Sample Security Controls 11
B.1 Sample MFA Configuration 11
B.2 Sample Monitoring Rules 11

C Paper Statement 12

Executive Summary

This study analyzes a recent cybersecurity incident where the threat actor "betway" compromised multiple Salesforce Cloud portals through stolen credentials. The key vulnerabilities exploited included weak authentication mechanisms, excessive user privileges, and inadequate monitoring systems. Our findings suggest implementing robust multi-factor authentication, enforcing least privilege principles, and enhancing monitoring capabilities as critical mitigation strategies. Organizations using Salesforce should prioritize these security controls to prevent similar breaches in the future.

Key Impact: Stolen data from 6 organizations was offered for sale at prices ranging from $5,000 to $75,000, demonstrating the significant financial motivation behind these attacks and their potential business impact.

Abstract

This case study examines a cyber campaign targeting Salesforce Cloud portals, as reported by ReliaQuest in their April 2025 report. The breach, attributed to stolen credentials, exposed vulnerabilities in authentication, access controls, and monitoring. Without direct Salesforce access, this study applies security audit procedures theoretically, drawing on online sources and best practices to identify weaknesses and propose mitigations. Key findings include weak authentication, over-privileged accounts, and inadequate monitoring, with recommendations for multi-factor authentication, least privilege, and enhanced monitoring. While this example was the most recent one, the study evaluates several salesforce application case studies over the past 3 years through various articles thus creating a hypothetical environment for an audit that extends past the current case study's scope. Recommendations are general and should be tailored to specific organizational needs and Salesforce implementations.

1 Introduction

In April 2025, ReliaQuest reported a cybercriminal campaign targeting public-facing Salesforce Cloud portals, where a threat actor, "betway," offered stolen data from six organizations for $5,000 to $75,000 [6]. The breach resulted from compromised credentials, likely obtained through infostealer malware. Lacking direct access to Salesforce, this study hypothetically applies security audit procedures, leveraging online articles, industry reports, and best practices to analyze the incident and propose mitigation strategies.

1.1 Background

Salesforce is a leading customer relationship management (CRM) platform used by organizations worldwide to manage customer data, sales processes, and marketing campaigns. As cloud-based systems become increasingly important for business operations, they also become attractive targets for cybercriminals seeking valuable data.

1.2 Objectives

This security audit aims to:

- Identify security vulnerabilities in typical Salesforce implementations
- Analyze attack vectors used in recent breaches
- Develop pragmatic recommendations to enhance security posture
- Provide a framework for ongoing security monitoring

1.3 Scope and Limitations

This study is limited to theoretical analysis based on publicly available information and best practices, without direct access to affected Salesforce environments. The findings and recommendations represent hypothetical scenarios derived from industry standards and published security guidelines.

2 Problem Statement

The incident involved unauthorized access to Salesforce Cloud instances via stolen credentials, leading to significant data breaches. Public reports indicate that weak authentication mechanisms, insufficient monitoring of public-facing portals, and poor credential management enabled attackers to exploit Salesforce CRM systems, compromising sensitive customer data. This hypothetical audit assesses the security posture of a typical Salesforce environment, identifies potential weaknesses, and recommends controls based on online research and established audit methodologies.

Critical Security Issue: The primary attack vector appears to be credential theft, with attackers using ”infostealer” malware to obtain valid Salesforce login credentials. Once obtained, these credentials provided direct access to sensitive customer data with minimal technical barriers.

3 Security Audit Methodology

The audit methodology was designed to systematically evaluate the security controls of a typical Salesforce environment, drawing on standard practices and tools described in online sources [1, 3, 5, 7–9].

3.1 Pre-Audit Planning

3.1.1 Scope Definition

The audit scope was defined to cover:

- Authentication mechanisms and credential security
- User permissions and access controls

- Public-facing portal configurations
- Monitoring and incident response capabilities
- Custom code security

3.1.2 Tools and Resources

The following tools were considered for the hypothetical audit:

- Salesforce Security Health Check
- OWASP ZAP for external portal vulnerability scanning
- Splunk for log analysis and correlation
- Checkmarx for static code analysis
- Burp Suite for session testing

3.2 Audit Procedures

The audit procedures were structured into six key areas:

3.2.1 Access Control Review

User profiles, roles, and sharing rules were evaluated for adherence to the principle of least privilege, using tools like Setup Audit Trail and Permission Set Analyzer to identify over-privileged accounts, as recommended by [5].

3.2.2 Authentication Review

Multi-factor authentication (MFA) implementation, password policies, and session management were assessed, leveraging tools such as MFA Configuration Scanner and Burp Suite for session testing, following best practices for credential security [3].

3.2.3 Vulnerability Scanning

Dynamic and static application security testing (DAST and SAST) were proposed for portals and custom Apex code, using OWASP ZAP, Metasploit, and Checkmarx to detect vulnerabilities like XSS, as emphasized by [1].

3.2.4 Log Analysis

Login logs, API calls, and audit trails were analyzed for suspicious activity, with Splunk and Salesforce Event Monitoring as hypothetical tools to review monitoring configurations [9].

3.2.5 Incident Response Review

Incident detection, containment, and recovery plans were evaluated, using Salesforce Security Center and Jira for tracking and workflow automation, in line with industry standards [5].

3.2.6 User Awareness Assessment

Training programs, phishing awareness, and security culture were evaluated to assess the human element of security controls.

Table 1: Criticality Index of Audit Procedures

Procedure	Scope	Criticality
Pre-Audit Planning	Environment Setup	High
Access Control Review	User Permissions	High
Authentication Review	Credential Security	Critical
Vulnerability Scanning	Application Security	High
Log Analysis	Monitoring	Medium
Incident Response Review	Response Preparedness	Medium
User Awareness Assessment	Training	High

4 Discoveries and Findings

Drawing on [6] and online research, the hypothetical audit identified several vulnerabilities. These findings are categorized by severity and potential impact.

4.1 Critical Findings

4.1.1 Weak Authentication Controls

The absence of mandatory MFA and weak password policies (e.g., 8-character minimum without complexity) likely facilitated credential theft via phishing or malware, allowing attackers to access CRM data undetected [6].

Authentication Weakness: Organizations typically enforce only basic password requirements (8 characters) without MFA, making credential theft particularly damaging. When credentials are stolen through infostealer malware, there are no additional verification barriers to prevent unauthorized access.

4.2 High-Severity Findings

4.2.1 Over-Privileged Accounts

Approximately 10–20% of accounts had unnecessary admin privileges, such as "Modify All Data," enabling compromised accounts to extract large datasets [9].

4.2.2 Vulnerable Custom Code

Custom Apex code likely contained XSS vulnerabilities, affecting 15% of Salesforce applications and risking session token theft or user redirection [2].

4.3 Medium-Severity Findings

4.3.1 Inadequate Monitoring

The lack of real-time event monitoring and short log retention (e.g., 30 days) delayed detection of suspicious logins, prolonging data exposure [6].

4.3.2 Poor Incident Response

Average detection times of 48–72 hours indicated unpreparedness, exacerbating data loss due to slow containment [4].

Table 2: Criticality Index of Audit Findings

Finding	Scope	Criticality
Weak Authentication Controls	Credential Security	Critical
Over-Privileged Accounts	User Permissions	High
Inadequate Monitoring	Monitoring	Medium
Vulnerable Custom Code	Application Security	High
Poor Incident Response	Response Preparedness	Medium

5 Risk Analysis

5.1 Threat Modeling

Based on the identified vulnerabilities, we can model the threat landscape:

1. **Threat Actors:** Financially motivated cybercriminals targeting customer data for resale
2. **Attack Vectors:** Credential theft via phishing, malware, and social engineering
3. **Impact:** Data exfiltration, financial loss, regulatory penalties, reputational damage

5.2 Risk Matrix

The risks identified can be categorized by likelihood and impact:

Table 3: Risk Assessment Matrix

Risk	Description	Likelihood	Impact	Risk Score
Credential Theft	Unauthorized access via stolen credentials	High	High	Critical
Data Exfiltration	Bulk extraction of sensitive customer data	High	High	Critical
Regulatory Penalties	Fines due to compliance violations	Medium	High	High
Reputational Damage	Loss of customer trust	Medium	High	High

6 Recommendations

To address the identified risks, the following mitigation strategies were developed based on online research, including [1, 3, 5]. These recommendations are categorized by priority and implementation timeframe.

6.1 Critical Priorities (0-30 Days)

6.1.1 Enforce MFA

Mandate MFA for all users, including contractors, via Salesforce Authenticator or hardware tokens to prevent unauthorized access from stolen credentials [3].

MFA Implementation: Enable Salesforce's built-in MFA requirement at the organizational level, requiring both something users know (password) and something they have (authenticator app or physical key). This single control could have prevented the majority of credential-based attacks.

6.1.2 Implement Least Privilege

Audit and revoke excessive privileges using Salesforce Security Health Check, restricting public portal access to authenticated users with IP whitelisting [5].

6.2 High Priorities (30-60 Days)

6.2.1 Enhance Monitoring

Enable Salesforce Shield Event Monitoring and integrate logs with a SIEM system (e.g., Splunk) for real-time detection, extending log retention to 180 days [1].

6.2.2 Secure Custom Code

Use Checkmarx for continuous SAST scanning of Apex and Visualforce code, and train developers on secure coding to eliminate XSS vulnerabilities [2].

6.3 Medium Priorities (60-90 Days)

6.3.1 Strengthen Incident Response

Develop a Salesforce-specific incident response plan with playbooks for credential theft, and conduct regular tabletop exercises to reduce detection times [5].

6.3.2 User Awareness Training

Launch phishing awareness campaigns and MFA training to educate users, reducing susceptibility to credential theft [3].

Table 4: Implementation Roadmap for Recommendations

Recommendation	Priority	Timeframe	Estimated Cost
Enforce MFA	Critical	0-30 Days	Low
Implement Least Privilege	High	0-30 Days	Low
Enhance Monitoring	High	30-60 Days	Medium
Secure Custom Code	High	30-60 Days	Medium
Strengthen Incident Response	Medium	60-90 Days	Low
User Awareness Training	High	30-60 Days	Medium

7 Implementation Guide

For each key recommendation, specific implementation steps are provided:

7.1 MFA Implementation Steps

1. Navigate to Setup > Identity > Identity Verification
2. Enable "Require Multi-Factor Authentication for UI Logins"
3. Configure Session Settings to require verification at every login
4. Deploy Salesforce Authenticator to all users
5. Monitor MFA adoption and exceptions

7.2 Least Privilege Implementation

1. Run Salesforce Security Health Check
2. Review all Permission Sets with "Modify All Data" rights
3. Identify and revoke excessive permissions
4. Implement role-based access controls
5. Configure IP restrictions for sensitive operations

8 Conclusion

This hypothetical audit, informed by [6], underscores the critical need for robust authentication, least privilege, and monitoring in Salesforce environments. The proposed recommendations, grounded in online sources, provide a roadmap for organizations to strengthen their Salesforce security posture and prevent future breaches.

8.1 Key Takeaways

- Multi-factor authentication is the single most effective control against credential theft

- Regular permission reviews are essential to minimize the impact of compromised accounts
- Proactive monitoring reduces detection time and limits data exfiltration
- A security-first approach to custom code development prevents application vulnerabilities

8.2 Future Considerations

As threat actors continue to evolve their tactics, organizations should:

- Evaluate emerging authentication technologies beyond traditional MFA
- Explore AI-powered behavior analytics for anomaly detection
- Consider zero-trust architecture for Salesforce implementations
- Develop collaborative threat intelligence sharing within the Salesforce ecosystem

A Appendix A: Audit Methodology Details

A.1 Tools and Techniques

Detailed descriptions of the audit tools and techniques considered for this analysis:

- **Salesforce Security Health Check:** Built-in tool that assesses organization security against Salesforce standards
- **OWASP ZAP:** Open-source web application security scanner for finding vulnerabilities
- **Splunk:** SIEM tool for log aggregation, correlation, and analysis
- **Checkmarx:** Static application security testing tool for code analysis

B Appendix B: Sample Security Controls

B.1 Sample MFA Configuration

Example Salesforce MFA configuration settings:

- Require verification method registration
- Set session timeout to 2 hours
- Require verification for high-risk operations
- Allow backup verification methods

B.2 Sample Monitoring Rules

Example monitoring rules for Salesforce Shield:

- Alert on login from new geographic locations
- Monitor bulk data exports exceeding 1,000 records
- Track changes to permission sets
- Alert on failed MFA attempts

References

[1] CapStorm: *Your go-to guide for conducting a Salesforce data audit*. June 26 2023. – URL https://www.capstorm.com/blog/conducting-a-salesforce-audit/

[2] Checkmarx: *Salesforce code scanning best practices*. 2025. – URL https://www.checkmarx.com

[3] FoundHQ: *Conducting a Salesforce audit (2024 updates)*. January 16 2025. – URL https://www.foundhq.com/blog/conducting-a-salesforce-audit

[4] National Institute of Standards and Technology: *Computer security incident handling guide (SP 800-61)*. 2024. – URL https://nvlpubs.nist.gov

[5] Onilab: *Salesforce audit: A complete guide*. February 28 2024. – URL https://onilab.com/blog/salesforce-audit-guide

[6] ReliaQuest: *Cybercriminal campaign targeting Salesforce portals*. April 25 2025. – URL https://reliaquest.com/resources/research-reports/annual-threat-report-2025/. – Retrieved from X posts

[7] Salesforce: *Security Health Check documentation*. 2025. – URL https://help.salesforce.com

[8] SentinelOne: *10 security audit tools for 2025*. December 16 2024. – URL https://www.sentinelone.com

[9] Sonar Software: *How to audit Salesforce access: Ensuring compliance and security*. February 20 2025. – URL https://sonarsoftware.com

C Paper Statement

"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my electronic signature."

Signature : KURUDUNJE DEEKSHITH SHETTY