PenTech

F1 International Academy

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from F1 International Academy. (henceforth known as “F1 International Academy”). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

*Confidential information including but not limited to IP addresses, personnel, and website domains have been redacted and/or substituted with generic numbers and phrases for privacy purposes.

Table of Contents

Confidentiality Statement **2**
Contact Information **4**
Document History **4**
Introduction **5**
Assessment Objective 5
Penetration Testing Methodology **6**
Reconnaissance 6
Identification of Vulnerabilities and Services 6
Vulnerability Exploitation 6
Excluded Attacks 6
Reporting 6
Scope **7**
Included Systems, Networks, Applications, and Devices 7
Risk Management 7
Key Data Types and Assets to Be Protected 7
Executive Summary of Findings **8**
Grading Methodology 8
Summary of Strengths 9
Summary of Weaknesses 9
Executive Summary **10**
Summary Vulnerability Overview **13**
Vulnerability Findings **15**
Public Reconnaissance 15
Internal Investigations 31
Financial System Vulnerabilities 56
Unidentified Actors 61
Post-Test Actions **64**
Post-Test Activity Recommendations: 64
Prioritization and Timeline for Addressing Vulnerabilities 64

Contact Information

Company Name	The University of Utah edX Cybersecurity Bootcamp 'PenTech'
Contact Name	Auburn Ann Bertuccini
Contact Title	Penetration Test Team Lead / Primary Point of Contact

Document History

Version	Date	Author(s)	Comments
001	September 9th, 2024	Auburn A Bertuccini	Pages 1-8 Completed
002	September 9th, 2024	Sierra	Executive Summary Note Dump
003	September 22nd, 2024	Sarah Hill	Added vulnerability descriptions
004	September 23rd, 2024	Sarah Hill	Added vulnerability descriptions
005	September 23rd, 2024	Sarah Hill	Added vulnerability descriptions
006	September 25th, 2024	Auburn A Bertuccini	Expanded vulnerability descriptors and remediation
007	September 26th, 2024	Sarah Hill	Validated Links
008	September 26th, 2024	Auburn A Bertuccini	Executive Summary final draft rewrite
009	September 26th, 2024	Auburn A Bertuccini	Table of Contents Updated

Introduction

This penetration test report outlines the findings and assessments conducted by the cybersecurity team from the University of Utah's edX Cybersecurity Bootcamp for F1 International Academy from August 31st to 2024-September 7th, 2024. The test's primary objective was to evaluate and strengthen the security posture of F1 International Academy's digital infrastructure by identifying vulnerabilities that could expose the institution to external and internal threats.

For the testing, we focused on the following:

- **System-Level Vulnerabilities:** We sought to identify vulnerabilities that could be discovered and exploited with limited prior knowledge of the environment. This gray-box approach gave the penetration testing team some insider knowledge while allowing them to find vulnerabilities independently.
- **Exploitation of Identified Vulnerabilities:** We attempted to exploit vulnerabilities within the scope to determine if unauthorized access to confidential information, such as financial data and sensitive administrative records, was possible.
- **Comprehensive Documentation and Reporting:** All findings were thoroughly documented and reported, with a focus on providing actionable recommendations to mitigate identified risks.

During testing, careful consideration was given to the business processes supported by F1 International Academy's systems and their associated potential threats. Specific non-disruptive testing techniques were employed to ensure that F1 International Academy's operations were not negatively impacted. High-risk techniques, such as Denial of Service (DoS) attacks or persistent vulnerabilities (e.g., stored XSS on live systems), were excluded from the assessment to prevent any unintended disruptions. This approach allowed us to perform a comprehensive security evaluation while ensuring the safety and stability of F1 International Academy's environment.

Assessment Objective

The primary objective of this penetration test was to analyze and uncover security weaknesses in F1 International Academy's web applications, internal network, and system infrastructure. The assessment aimed to identify exploitable vulnerabilities, assess F1 International Academy's overall security posture, and offer actionable recommendations to remediate the vulnerabilities and enhance security across the institution.

Our team utilized a proven vulnerability testing methodology, customized for the specific needs and infrastructure of F1 International Academy, to conduct a thorough evaluation of all systems, networks, and applications included in the scope.

F1 International Academy has outlined the following objectives:

Table 1: Defined Objectives

Objective	Description
Administrative Systems	Conduct a thorough assessment of F1 International Academy's administrative systems to identify and address potential vulnerabilities that could disrupt operational efficiency or lead to unauthorized data access.
Financial Systems	Secure F1 International Academy's financial systems by identifying vulnerabilities that could expose the institution to financial fraud or data breaches.
Employee Security Practices	Evaluate the awareness and effectiveness of F1 International Academy employees in adhering to security best practices, particularly concerning social engineering and phishing attempts.

Penetration Testing Methodology

Reconnaissance

We began our assessments by conducting passive reconnaissance, gathering publicly available information (open-source intelligence) to aid in understanding the target environment. This included examining exposed credentials, metadata, and other accessible data sources. For internal assessments, we performed active reconnaissance using tools such as WHOIS, DNS Lookup, Nmap, Shodan.io, Nessus, and certificate information analysis. We also navigated through F1 International Academy's web applications to identify potential entry points and systems of interest. This comprehensive approach helped in pinpointing vulnerabilities and areas requiring further investigation.

Identification of Vulnerabilities and Services

To identify vulnerabilities and services within F1 International Academy's infrastructure, we utilized a combination of custom, open-source, and commercial tools. We employed Nmap for network scanning, Burp Suite for web application security testing, Metasploit for vulnerability exploitation, and Routersploit on F1 International Academy's internal WiFi network to assess router security. These tools provided a comprehensive view of the risks associated with F1 International Academy's current security posture and the effectiveness of existing controls. Our approach involved mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, and verifying the findings by eliminating false positives.

Vulnerability Exploitation

Once vulnerabilities were identified, our team followed a dual approach by performing both manual testing and automated exploitation of these vulnerabilities. Exploitation was carried out to determine whether vulnerabilities could lead to unauthorized access, privilege escalation, or the exposure of sensitive data. The exploitation phase focused on validating the potential impact of vulnerabilities while maintaining the integrity of F1 International Academy's systems by adhering to non-disruptive techniques.

Excluded Attacks

- **DoS Attacks**: Denial of Service (DoS) attacks were explicitly excluded from the scope of testing to prevent disruption to F1 International Academy's operations and avoid any negative impact on its infrastructure.
- **Persistence Techniques**: Techniques that allow attackers to maintain access to a system across restarts or other changes were not utilized. This ensures that the test concluded cleanly, without leaving any residual access that could later be exploited.

Reporting

After completing the exploitation phase or reaching the end of the allocated time, the assessment team compiled the results into a comprehensive report. This final deliverable provides F1 International Academy with a detailed overview of the identified vulnerabilities, exploitation attempts, and actionable recommendations for remediation. The report also includes risk prioritization to help F1 International Academy address the most critical security issues.

Scope

Prior to any assessment activities, F1 International Academy and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the F1 International Academy Point of Contact (POC) to determine which network ranges are in scope for the scheduled assessment.

It is F1 International Academy's responsibility to ensure that IP addresses identified as in-scope are controlled by F1 International Academy and are hosted in F1 International Academy-owned facilities (i.e., are not hosted by an external organization).

Included Systems, Networks, Applications, and Devices

Web Applications: All F1 International Academy web applications, focusing on input validation, session management, and data storage practices. This excludes third-party applications or services not directly managed by F1 International Academy.

Classroom Computers: Assess the security of classroom computers against unauthorized access, malware, and other threats, including an evaluation of installed software and user permissions.

Admin Network Router: An assessment of the admin network router, including attempts to retrieve router credentials, is included if time permits.

Excluded Assets or Resources

Third-party applications not directly controlled by F1 International Academy, such as external payment gateways and cloud services, will not be tested.

Risk Management

Penetration testers are required to avoid any actions that could lead to critical system failures, data loss, or substantial disruptions to F1 International Academy's operations. If an action poses a significant risk, it must only be undertaken with explicit approval from the Point of Contact (POC), Auburn Bertuccini, and written consent from the IT Administrator. All discovered vulnerabilities must be documented meticulously, with critical vulnerabilities escalated immediately to the IT Administrator for prompt remediation. All issues will be included in the final report. Critical vulnerabilities that present an immediate risk must be reported to the IT Administrator within one hour of discovery. The IT Administrator will have the authority to pause testing activities if necessary to address these critical issues.

Key Data Types and Assets to Be Protected

Financial data must be protected against unauthorized access and fraud to ensure its integrity and confidentiality. Attendance records need to be managed with precision to maintain accurate and secure documentation of student attendance. Test banks, which contain exam questions and answers, must be safeguarded to prevent academic dishonesty and uphold the integrity of academic assessments.

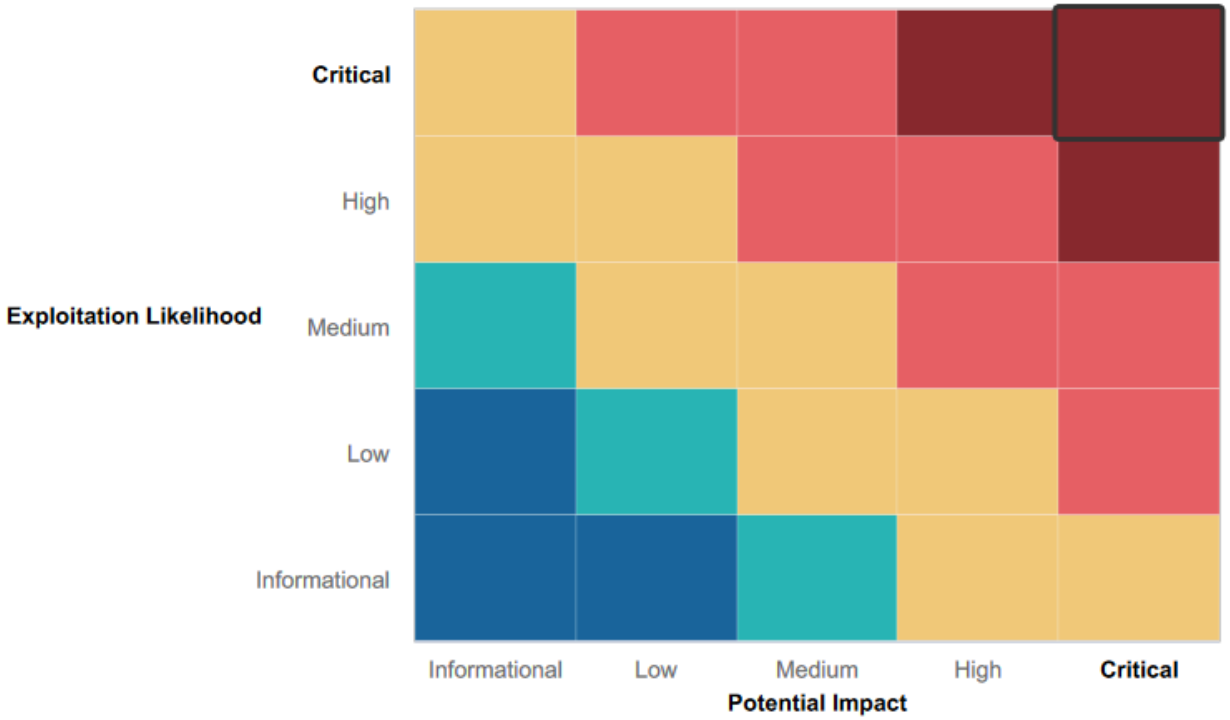
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

The assessment uncovered effective security measures that successfully prevented, detected, or mitigated various attack techniques. Key strengths include:

- WHOIS information for IP address 123.123.12.1 was redacted for privacy.
- No logins were found to utilize any of the "Most Common Passwords" from the rockyou.txt wordlist.
- Neither a robots.txt file nor a sitemap.xml file were found, reducing the exposure of sensitive URLs.
- The Windows server employs a separate admin account, distinct from the admin@f1schoolwebsite.edu email address.
- Student accounts cannot be independently created to access sensitive internal structures.
- Directory traversal attempts were unsuccessful, demonstrating robust protection against this attack vector.
- Captcha mechanisms are implemented for file submissions and emails directed to admin accounts, adding an extra layer of security.
- Simple command injection attacks on f1schoolwebsite.edu were ineffective.
- A moderate level of data privilege segregation is in place between instructor and admin accounts.
- Attempts to remotely connect to IP address 123.123.12.1 as the root user were unsuccessful, with the system stating the account was disabled and required administrator intervention.
- Ports 8088 and 8090 on IP 123.123.12.1 do not share credentials with other systems within F1 International Academy's network.
- Routersploit was unable to confirm any vulnerabilities on the router's network.

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Cyber security Safety Training Program
- Password lockout & requirements policy
- Remove admin privileges from local PC accounts
- Remove role-based admin privileges and adjust user privileges to "least privilege"
- Properly encrypt sensitive PII
- Remove old data
- Implement SSL certification
- Update physical security
- Create a data back-up and recovery plan
- Implement network segmentation for admins and student networks
- Secure VPN access for admin network
- Monitor unidentified devices in security logs
- Implement VPN on the financial Swagger UI website

Executive Summary

Between August 31 and September 7, 2024, a penetration test was conducted at F1 International Academy. This assessment involved public and internal reconnaissance, vulnerability scans, credential harvesting, social engineering, and on-site evaluations. While the findings identified critical vulnerabilities that need urgent attention, it is important to note that these discoveries should not be considered exhaustive. The environment showed several strong security measures that successfully detected, prevented, or mitigated various attack vectors.

Public Reconnaissance (August 31 - September 1, 2024)

We began by collecting publicly available information using WHOIS and DNS lookups. Notably, WHOIS data for IP address 123.123.12.1 was redacted for privacy. Additionally, we discovered outdated domains, such as `eslf1schoolwebsite.com`, and expired SSL certificates on subdomains, including `students.eslf1schoolwebsite.com`. The domain `f1schoolwebsite.edu` is hosted on Amazon AWS. Our team also collected available employee information from LinkedIn, presenting potential security concerns.

Strengths:

- WHOIS information for IP 123.123.12.1 was redacted, limiting exposure.
- No sensitive data, such as a `robots.txt` or `sitemap.xml`, was publicly accessible, reducing the risk of URL exposure.

Vulnerability Scanning (August 31 - September 1, 2024)

NMAP and Nessus vulnerability scans on the F1 International Academy domain uncovered several open ports, indicating potential entry points. Attempts to connect to IP 123.123.12.1 as the root user failed, with the system indicating that the account was disabled and required administrator intervention. Importantly, the credentials used for ports 8088 and 8090 on this IP did not overlap with other systems within F1 International Academy's network, demonstrating effective credential compartmentalization. This vulnerability scanning led to the discovery of all log-in pages on the IP and two versions of the Quickbooks API.

Strengths:

- Attempts to access IP 123.123.12.1 as the root user were unsuccessful.
- Port credentials on ports 8088 and 8090 did not share credentials with other systems, indicating compartmentalization.

Web Application and Credential Discovery (September 3, 2024)

During testing of login portals using Burp Suite, we observed the use of IP-based URLs, along with significant vulnerabilities in password management. We were able to attempt over 500 login attempts without triggering any lockout protections. Additionally, the lack of lockout features highlights the need for robust password management policies. However, we also confirmed that no passwords from the rockyou.txt wordlist were found in use, which suggests strong password hygiene in some areas.

Strengths:

- Passwords used across F1 International Academy systems did not appear in common password lists, indicating some level of secure password practices.

- CAPTCHA mechanisms were implemented for file submissions and emails directed to admin accounts, adding an additional security layer.

Social Engineering and Phishing Campaign (September 4 - 5, 2024)

Our social engineering campaign focused on evaluating staff awareness of pretexting and phishing attacks.

A pretexting attack was executed, wherein our team member posed as a new teacher to request computer credentials. This revealed the use of a universal password for all on-site computers, which also unlocked personal accounts such as bank accounts and 401k access through Chrome's auto-save feature. The fact that teachers were using personal Chrome profiles and passwords that were universally shared across multiple systems further compounded the security risks.

We were also able to gather critical information about instructor and admin emails, preparing the groundwork for our phishing campaign. Our phishing campaign, conducted via `f1schoolwebsite.net`, successfully sent targeted phishing emails, replicating internal communication methods. The phishing attack yielded multiple credentials, and employees provided alternative passwords when they couldn't log in, revealing additional security flaws. This uncovered weak user education and inadequate password management practices.

Strengths:

- A moderate level of data privilege segregation between instructor and admin accounts was observed, limiting the potential damage of a compromised account via the instructor pathway.

Administrative Web Portal and Data Access (September 4-7, 2024)

Using harvested credentials, we gained access to the administrative web portal, which contained several critical vulnerabilities, including:

- Functional "delete" buttons that did not require authentication.
- Plain-text passwords and predictable patterns that allowed us to guess others.
- Active accounts for terminated employees, posing a risk of unauthorized access to sensitive systems, including the ability to modify student visa statuses.

Sensitive student records, including passport and financial information, were also found to be accessible without encryption. However, attempts to exploit directory traversal vulnerabilities were unsuccessful, reflecting some resilience against this type of attack.

Strengths:

- Directory traversal attempts were successfully blocked.
- Admin accounts on Windows servers were distinct from the general `admin@f1schoolwebsite.edu` account, indicating adherence to basic account separation practices.

Onsite Router Investigation (September 6 - 7, 2024)

Our on-site evaluation included connecting to the Admin Wi-Fi, where we discovered multiple IoT devices and routers with known vulnerabilities. Using brute-force techniques and credentials obtained from plain-text password storage within the web app, we were able to guess the Admin Wi-Fi password. However, routersploit testing revealed no confirmable vulnerabilities on the router's network.

Additionally, we noted that the Admin and Student Wi-Fi networks were interconnected, posing an unnecessary exposure risk.

Strengths:

- Routersploit was unable to confirm any vulnerabilities on the router's network.

Conclusion

Our penetration test uncovered several critical vulnerabilities within F1 International Academy's infrastructure, as well as notable strengths in several areas:

- **Strengths:**
  - Robust protection against directory traversal attacks.
  - No use of common passwords from the rockyou.txt wordlist.
  - Successful CAPTCHA implementation for admin-related email security.
  - Effective separation of admin accounts on Windows servers.
  - Unsuccessful command injection attempts on the primary domain.
- **Vulnerabilities:**
  - Weak password management practices, including shared and easily guessable passwords.
  - Lack of encryption for sensitive student records and financial data.
  - Expired certificates and publicly accessible subdomains.
  - Exposure to phishing and social engineering attacks.
  - Poor network segmentation between the Admin and Student networks.

Recommendations: To mitigate these risks, we recommend the following actions:

- Implement a **password lockout and complexity policy** to prevent brute-force attacks (CWE-521).
- **Remove admin privileges** from local PCs and enforce least privilege policies across all accounts.
- **Encrypt all sensitive PII** and ensure proper encryption standards are followed for stored data.
- Remove outdated data and implement **SSL certification** for all subdomains.
- Enhance **physical security** controls and policies to prevent unauthorized access to critical infrastructure.
- Establish a **data backup and recovery plan** to safeguard against data loss.
- Isolate the **Admin and Student networks** through proper network segmentation.
- Implement **VPN access** for all administrative and financial portals, including Swagger UI.
- Continuously monitor logs for unidentified devices and network activity.

By implementing these measures, F1 International Academy can significantly reduce the risk of future breaches and protect the integrity of both student and organizational data.

Summary Vulnerability Overview

Vulnerability	Severity
1. DNS and WHOIS Data	Informational
2. Implement SSL certification	High
3. Public Employee Information Disclosure	Informational
4. Open Connections	Critical
5. Certificates and Infrastructure	Low
6. Public Login Pages - Web Application	Critical
7. Shodan.io - Public Information Disclosure	Informational
8. Physical Security	High
9. Password Lockout Policy	Critical
10. Password Requirements Policy	Critical
11. User/Admin Privileges	Critical
12. Auto-Fill Password Vulnerabilities	Critical
13. Unencrypted Sensitive Information	Critical
14. Outdated Data	Moderate
15. Phishing Campaign	Critical
16. File Upload Vulnerability	Low
17. Directory Traversal	Low
18. Router and Network Vulnerabilities	Moderate
19. Credential Harvesting	Critical
20. QuickBooks API Exposure	Critical
21. Swagger UI Exposure	Critical
22. Unidentified websites	Moderate

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total	Identifiers
Hosts	10	**f1schoolwebsite.app** 123.123.12.1 --- **f1schoolwebsite.edu** 22.22.22.222 --- **Router Connections** OFFICE-ITADMIN - 10.0.0.001 Unknown hostname - 10.0.0.01 Apple-TV.local - 10.0.0.02 WAP EAP245 - 10.0.0.002 WAP EAP245 - 10.0.0.003 WAP EAP245 - 10.0.0.004 WAP EAP245 - 10.0.0.005 WAP EAP245 - 10.0.0.006
Ports	25	**f1schoolwebsite.app 123.123.12.1** 53, 80, 443, 3306, 3389, 5001, 5002, 6002, 7001, 8000, 8010, 8050, 8060, 8088, 8090, 33060 --- **f1schoolwebsite.edu 22.22.22.222** 22, 80, 443, --- **OFFICE-ITADMIN 10.0.0.001** 5357 --- **Unknown hostname 10.0.0.01** 80 --- **Apple-TV.local 10.0.0.02** 5000, 7000, 7100, 49152, 49153, 49154, 62078 --- **WAP EAP245** 22, 80, 443

Exploitation Risk	Total
Critical	11
High	2
Moderate	3
Low	3
Informational	3

Vulnerability Findings

PUBLIC RECONNAISSANCE

Vulnerability # 1	Findings
Concern	DNS and WHOIS Data
Common Weakness Enumerations	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-610: Externally Controlled Reference to a Resource in Another Sphere
Risk Rating	Informational
Description	A DNS lookup for `f1schoolwebsite.edu` returns the IP address `22.22.22.222`, which is registered under Amazon AWS Network Operations. WHOIS information for this IP indicates the network type as "direct allocation," and the provider is described as follows: *"Amazon Web Services, Inc. is a subsidiary of Amazon that provides on-demand cloud computing platforms and APIs to individuals, companies, and governments, on a metered, pay-as-you-go basis. Clients often use this in combination with autoscaling."* Additionally, a DNS PTR record lookup for the IP address `123.123.12.1` returns the domain `1.12.123.123.host.secureserver.net`. The WHOIS information for this IP indicates it is registered to GO-DADDY-COM-LLC, with the network type also marked as "direct allocation." WHOIS data for the domain `f1schoolwebsite.edu` lists the contact information for an owner of the company. The associated email address appears to be linked to an outdated domain, `eslf1schoolwebsite.com`, which no longer has ties to the current operations of F1 International Academy, as indicated by its WHOIS records. This exposure provides unauthorized actors with detailed insights into the Academy's infrastructure, potentially enabling targeted attacks or exploitation of the identified information.
Affected Hosts	22.22.22.222, 123.123.12.1
Remediation	**Update WHOIS Information:** Ensure that the contact information for all domains, especially `f1schoolwebsite.edu`, is current and reflects the active operations of F1 International Academy. Replace outdated email addresses and contact details to avoid the risk of impersonation or unauthorized access attempts.

	Harden DNS Configurations: ● Review DNS records to ensure that only necessary information is publicly available. ● Implement DNSSEC (Domain Name System Security Extensions) to protect against DNS spoofing and ensure the integrity of DNS responses. ● Minimize exposure by limiting unnecessary subdomains and entries in DNS records. **Decommission Legacy Domains and IPs:** ● Properly decommission or transfer outdated domains, such as `eslf1schoolwebsite.com`, and ensure they no longer reference current contact details. ● Remove any unused IP addresses from DNS configurations to reduce the attack surface. **Monitor and Audit DNS and WHOIS Data:** ● Implement regular monitoring of DNS and WHOIS records for any changes or unauthorized modifications. ● Use alerting mechanisms to quickly respond to any detected anomalies or exposure of sensitive information. **Strengthen Domain Management Practices:** ● Review and improve domain management processes to adhere to industry best practices. ● Implement strong access controls and multi-factor authentication for all domain management accounts. ● Conduct periodic audits of domain configurations and WHOIS data to ensure compliance with security standards.

Vulnerability # 2	Findings
Concern	Implement SSL certification
Common Weakness Enumeration	CWE-295: Improper Certificate Validation CWE-311: Missing Encryption of Sensitive Data CWE-319: Cleartext Transmission of Sensitive Information CWE-522: Insufficiently Protected Credentials CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
Risk Rating	High
Description	The domain `www.f1schoolwebsite.edu` correctly uses the HTTPS protocol to secure its communications. However, login applications associated with the IP address `http://123.123.12.1` are using the unencrypted HTTP protocol, which poses a significant security risk by potentially allowing cleartext transmission of sensitive information (CWE-319). This means that data such as login credentials and personal information can be intercepted by malicious

	actors. Additionally, the subdomain `students.eslf1schoolwebsite.com` is using an outdated SSL certificate, which can lead to insufficiently protected credentials (CWE-522) if users unknowingly interact with an insecure connection. The primary domain, `f1schoolwebsite.edu`, is using a valid SSL certificate issued by Let's Encrypt (Common Name: R11, Organization: Let's Encrypt) with a validity period from August 7, 2024, to November 5, 2024. It is important to note that Let's Encrypt certificates are only domain-validated, meaning the Certificate Authority (CA) verifies domain ownership but does not perform extensive identity checks. This limited validation level could potentially be exploited by malicious actors who gain unauthorized access to the domain account, allowing them to create subdomains and issue certificates for malicious purposes (CWE-295). Moreover, some session cookies in the application are being transmitted without the `Secure` attribute, making them vulnerable to being sent over unencrypted connections (CWE-614). This increases the risk of sensitive information being exposed or manipulated by attackers, especially in a mixed-content environment.
Affected Hosts	f1schoolwebsite.edu, http://123.123.12.1, students.eslf1schoolwebsite.com
Remediation	**Implement HTTPS for All Communications:** ● Transition all services, including the login portal and any subdomains, to HTTPS with a valid and up-to-date SSL certificate. This will prevent sensitive information from being transmitted in cleartext and protect against Man-In-The-Middle (MITM) attacks. ● Use HTTP Strict Transport Security (HSTS) to enforce the use of HTTPS and prevent protocol downgrade attacks. **Encrypt and Secure Credentials:** ● Ensure that all credentials are transmitted over HTTPS and are not exposed in plaintext (CWE-319). ● Implement secure storage for credentials using strong, one-way hashing algorithms such as bcrypt or Argon2. Avoid storing any sensitive data, including passwords, in plaintext (CWE-522). ● Use Multi-Factor Authentication (MFA) for all critical accounts to add an extra layer of security. **Update Outdated Certificates:** ● Replace the outdated certificate on `students.eslf1schoolwebsite.com` with a valid and current certificate. Automate the renewal process to avoid future lapses. **Secure Cookie Management:** ● Mark all cookies that contain sensitive information, such as session cookies, with the `Secure` attribute to ensure they are only sent over HTTPS connections (CWE-614).

- Use the `HttpOnly` attribute to prevent client-side scripts from accessing cookies, reducing the risk of XSS attacks.
- Implement the `SameSite` attribute set to `Strict` or `Lax` to protect against cross-site request forgery (CSRF) attacks.

Use Higher Levels of Certificate Validation:

- For sensitive services, consider using Organization Validation (OV) or Extended Validation (EV) certificates, which provide a higher level of identity verification and increase trustworthiness (CWE-295).

Implement Secure Configuration for SSL/TLS:

- Use strong ciphers and protocols. Disable outdated and insecure versions like SSLv3 and TLS 1.0/1.1, enforcing TLS 1.2 or higher.

Regular Security Audits and Monitoring:

- Perform regular security audits and penetration testing to identify any vulnerabilities in your SSL/TLS implementation and overall security posture.
- Set up monitoring for certificate validity and expiration, and configure alerts for any certificate anomalies.

Regular Security Audits and Penetration Testing:

- Perform regular security audits and penetration testing to identify any vulnerabilities in your SSL/TLS implementation and overall security posture.

Monitor Certificate Validity and Security:

- Set up monitoring for certificate validity and expiration. Implement alerts for any certificate anomalies, such as unexpected changes in certificate issuers or validation errors.

Implement Secure Configuration for SSL/TLS:

- Use strong ciphers and protocols for SSL/TLS configuration. Disable weak ciphers and protocols such as SSLv2, SSLv3, and TLS 1.0/1.1. Ensure TLS 1.2 or higher is enforced.

Use Secure Cookie Attributes:

- If cookies are being used for session management, ensure they are marked as `Secure` and `HttpOnly` to prevent them from being transmitted over unencrypted connections and accessed by JavaScript.

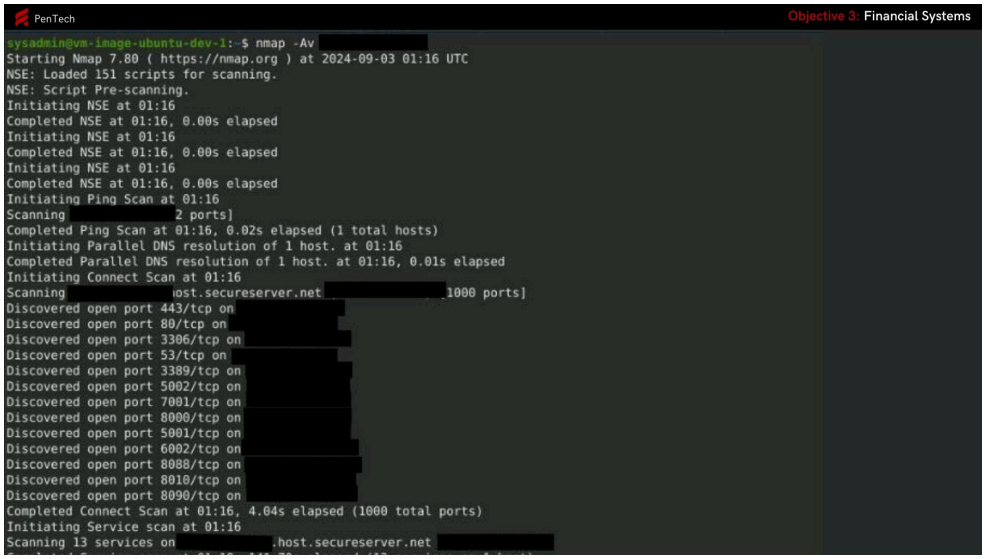
Educate and Train Staff:

- Educate IT and development teams on the importance of certificate management and secure communication practices. Regular training can help prevent configuration mistakes and improve security awareness.

Vulnerability # 3	Findings
Concern	Public Employee Information Disclosure
Common Weakness Enumeration	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-359: Exposure of Private Information ('Privacy Violation')
Risk Rating	Informational
Description	It has been identified that employee email addresses are accessible through LinkedIn and other public databases, posing a potential risk for phishing attacks. Additionally, the “Contact Us” page on the f1schoolwebsite.edu website lists publicly available emails, which could be exploited by malicious actors. **Discovery Method:** A search for F1 International Academy employees was conducted on LinkedIn. By reviewing individual profiles, employees with publicly listed city and state information were identified. Further investigation using a free online people search tool, such as thatsthem.com, revealed associated email addresses linked to these LinkedIn profiles. This unintentional exposure of private information may result in privacy violations.
Sources Referenced	LinkedIn.com, thatsthem.com, f1schoolwebsite.edu
Remediation	**Remove Publicly Available Emails:** ● Employees should be encouraged to remove or obfuscate their work email addresses from public profiles, such as LinkedIn, and other social media platforms. **Restrict Email Visibility on the Website:** ● Modify the “Contact Us” page to use a contact form instead of listing direct email addresses. **Review and Strengthen Privacy Settings:** ● Guide employees on configuring their privacy settings on LinkedIn and other social media platforms to limit the exposure of personal information. ● Implement an internal policy restricting employees from listing sensitive information on public platforms. **Implement an Information Disclosure Policy:** ● Develop and enforce a policy that governs what information can be shared publicly by employees. ● Regularly review this policy and update it based on evolving security

	practices. **Internal Data Handling and Classification:** ● Classify employee information based on sensitivity and ensure that it is handled appropriately. ● Implement access controls to restrict who can view and share sensitive employee data. **Deploy Security Information and Event Management (SIEM):** ● Use SIEM tools to monitor and analyze security events related to employee email accounts, such as unusual login attempts or data access patterns.

Vulnerability # 4	Findings
Concern	Open Connections
Common Weakness Enumeration	CWE-601: URL Redirection to Untrusted Site CWE-693: Protection Mechanism Failure CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-284: Improper Access Control
Risk Rating	Critical
Description	A comprehensive security scan has revealed multiple vulnerabilities that could potentially be exploited by malicious actors. Details of the findings are as follows: ● **f1schoolwebsite.edu** An NMAP scan detected three open ports, which could serve as potential attack vectors. The open ports identified are: ○ **Port 22 (SSH)**: Used for secure shell access, it could be targeted for brute force attacks if not adequately protected. ○ **Port 80 (HTTP)**: An open web server port, susceptible to attacks such as cross-site scripting (XSS) or other HTTP-based vulnerabilities. ○ **Port 443 (HTTPS)**: While more secure than HTTP, improper configuration can lead to exposure of sensitive information.

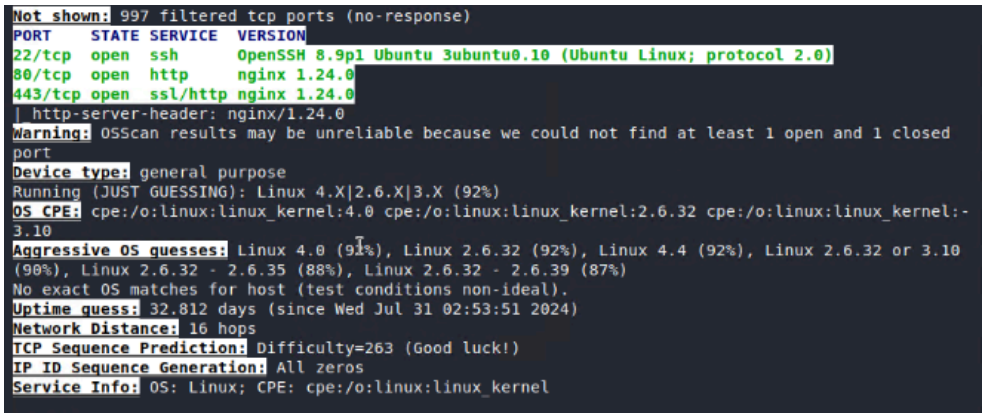


123.123.12.1
An NMAP scan on this host revealed 13 open ports, including:

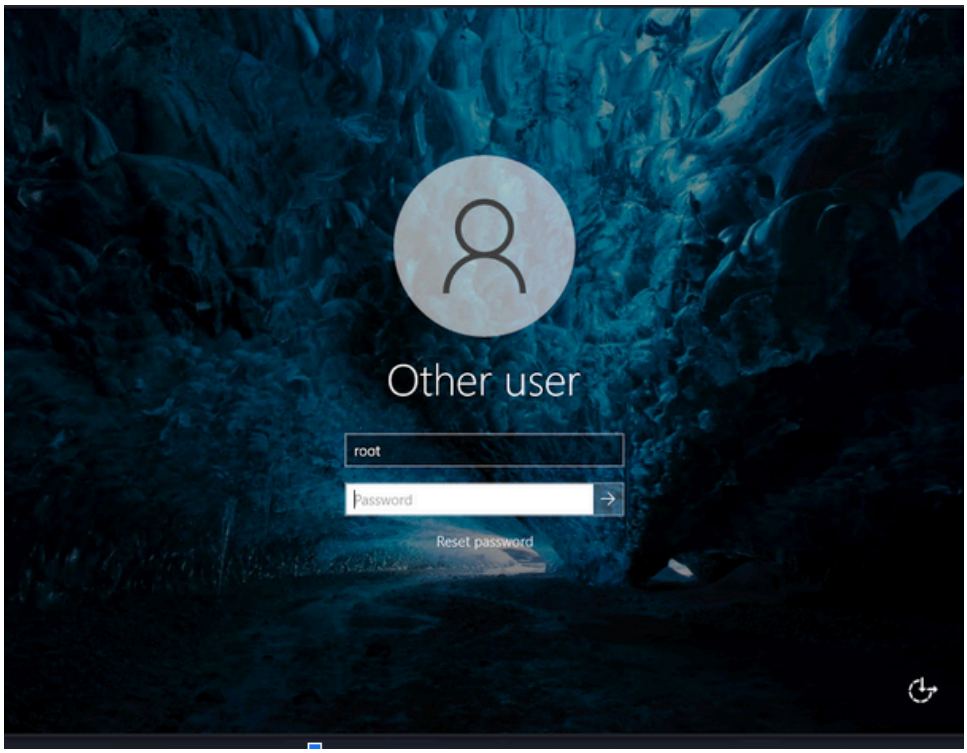
- **Port 443 (HTTPS)**
- **Port 80 (HTTP)**
- **Port 3306 (MySQL)**: Direct database exposure, which could lead to SQL injection attacks.
- **Port 3389 (RDP)**: Remote Desktop Protocol is a frequent target for unauthorized access attempts.
- **Ports 53, 5002, 7001, 8000, 5001, 6002, 8088, 8010, 8090**: Various other ports that could potentially be exploited for malicious activities.

22.22.22.222
A Zenmap scan detected the following open ports:

- **Port 22 (SSH)**
- **Port 80 (HTTP)**
- **Port 443 (HTTPS)**



Additionally, an attempt to connect to 123.123.12.1 using the `rdesktop` command in Kali Linux was made. Although the attempt was unsuccessful due to account lockout after multiple failed login attempts, this incident indicates a significant security concern regarding improper access controls (CWE-284).

	
Affected Hosts	**f1schoolwebsite.edu, 123.123.12.1, 22.22.22.222**
Remediation	**Close Unnecessary Ports:** ● Perform a thorough review of all open ports on the affected hosts. ● Close any ports that are not required for daily operations. ● Implement firewall rules to restrict inbound and outbound traffic to only necessary services. **Implement Proper Access Controls:** ● Review user permissions and ensure that only authorized personnel have access to sensitive resources. ● Use role-based access control (RBAC) to limit access based on user roles and responsibilities. **Secure Remote Access:** ● Limit remote access to specific, trusted IP addresses using firewall rules or a VPN. ● Disable remote access services (e.g., SSH, RDP) when not in use. ● Configure automated alerts for failed login attempts to detect potential brute-force attacks. ● Implement an account lockout policy to reduce the risk of unauthorized access. **Regular Monitoring and Updates:** ● Schedule regular vulnerability scans and penetration tests to identify and address new vulnerabilities. ● Ensure all systems and applications are regularly updated with security

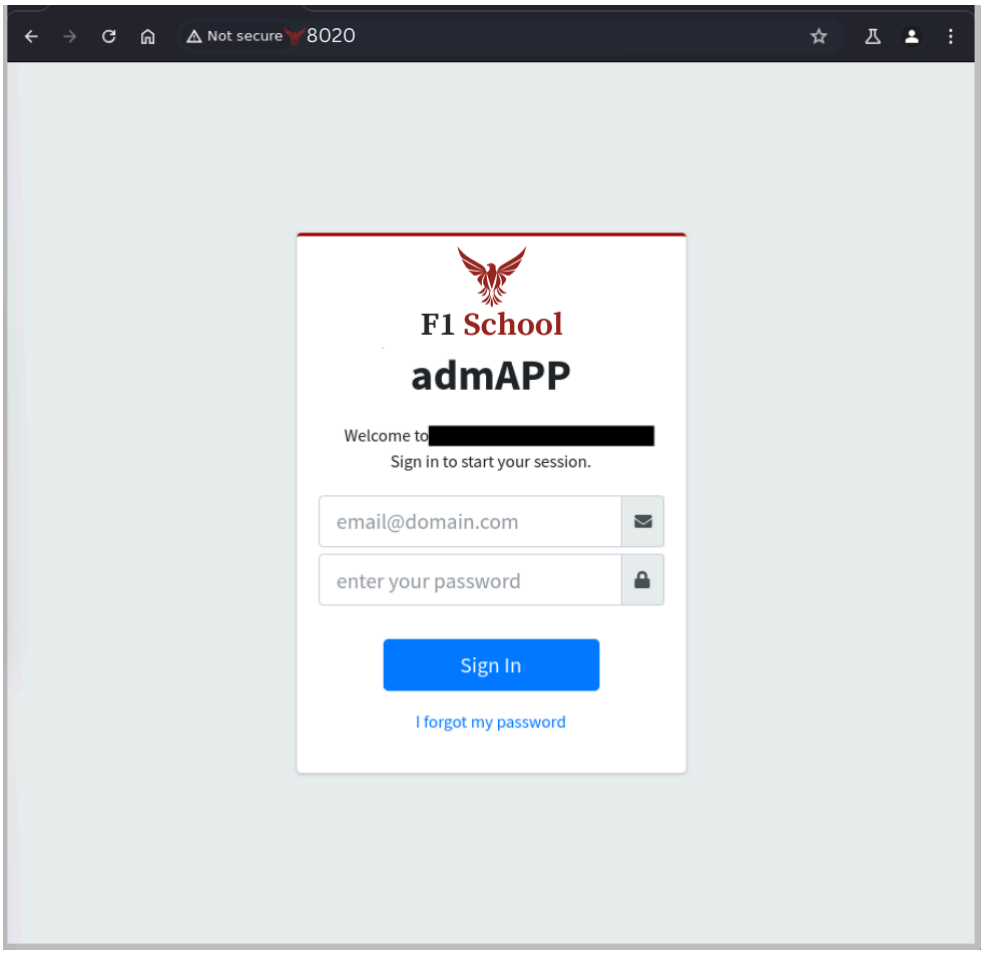
	patches. • Monitor logs for unusual activities and respond to potential security incidents promptly.

Vulnerability # 5	Findings
Title	CWE-937: Use of Outdated Software CWE-295: Improper Certificate Validation
Type	Certificates and Infrastructure
Risk Rating	Low
Description	An assessment of the security posture of `f1schoolwebsite.edu` revealed the use of outdated software and potential issues with certificate validation. Specifically, the investigation found the following: • **Outdated Software** The web server for `f1schoolwebsite.edu` is running nginx version 1.24.0, which is outdated. The use of obsolete software versions poses a risk as they may contain known vulnerabilities that could be exploited by attackers. It is crucial to update to the latest stable version to ensure the application benefits from the latest security patches and performance enhancements. • **Certificate Validation** The website utilizes a Let's Encrypt SSL/TLS certificate, valid from August 7, 2024, to November 5, 2024. While the certificate itself is valid, improper management or configuration could lead to vulnerabilities such as man-in-the-middle attacks. It is essential to ensure that certificates are correctly implemented and validated.
Affected Hosts	f1schoolwebsite.edu
Remediation	**Implement a Patch Management Policy:** • Establish a comprehensive patch management policy to ensure that all software, including web servers, operating systems, and applications, is regularly updated. • Regularly review software versions and apply patches as soon as they are released, particularly for critical applications and infrastructure. • Monitor for announcements from software vendors regarding vulnerabilities and update timelines. **Upgrade to the Latest Software Version:** • Update nginx to the latest stable version to mitigate any vulnerabilities present in version 1.24.0. • Ensure that all dependencies and libraries used by the web server are also updated to their latest compatible versions. **Enhance Certificate Management:**

	• Implement automated monitoring for certificate expiration and renewal to avoid service disruptions or security risks due to expired certificates. • Regularly review and test the SSL/TLS configuration using tools like SSL Labs to ensure best practices are followed, such as enabling only secure protocols and ciphers. **Regular Security Audits:** • Schedule periodic security audits to review the infrastructure for outdated software and improper configurations. • Conduct vulnerability scans and penetration testing to identify and rectify potential security issues before they can be exploited. **Documentation and Training:** • Document the patch management and certificate management processes, including roles and responsibilities. • Provide training for the IT staff on best practices for software updates, certificate management, and secure configuration.

Vulnerability # 6	Findings
Concern	Public Login Pages - Web Application
Common Weakness Enumeration	CWE-523: Unprotected Transport of Credentials CWE-308: Use of Single Factor Authentication CWE-284: Improper Access Control CWE-309: Use of Password System for Primary Authentication CWE-261: Weak Encryption for Passwords CWE-311: Missing Encryption of Sensitive Data
Risk Rating	Critical
Description	A security assessment of the web application infrastructure associated with the IP address `123.123.12.1` revealed several critical vulnerabilities related to public login pages: • **Unprotected Transport of Credentials (CWE-523):** The login portals were accessed through direct IP navigation rather than using fully qualified domain names (FQDNs). This practice indicates a potential lack of secure transport mechanisms, which could result in the unprotected transmission of user credentials. Such configurations are susceptible to interception by malicious actors, leading to unauthorized access and potential data breaches.

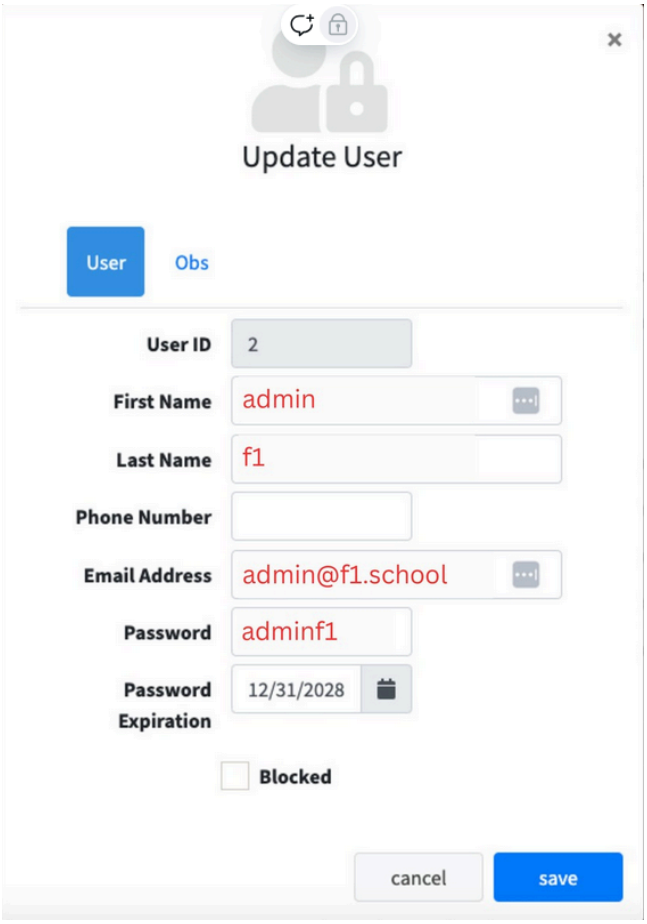
- **Use of Single-Factor Authentication (CWE-308):**
  The login portals identified appear to rely solely on single-factor authentication (i.e., username and password), which significantly increases the risk of unauthorized access. Single-factor authentication is generally considered inadequate for protecting sensitive systems, as it is vulnerable to brute-force attacks, credential stuffing, and phishing.



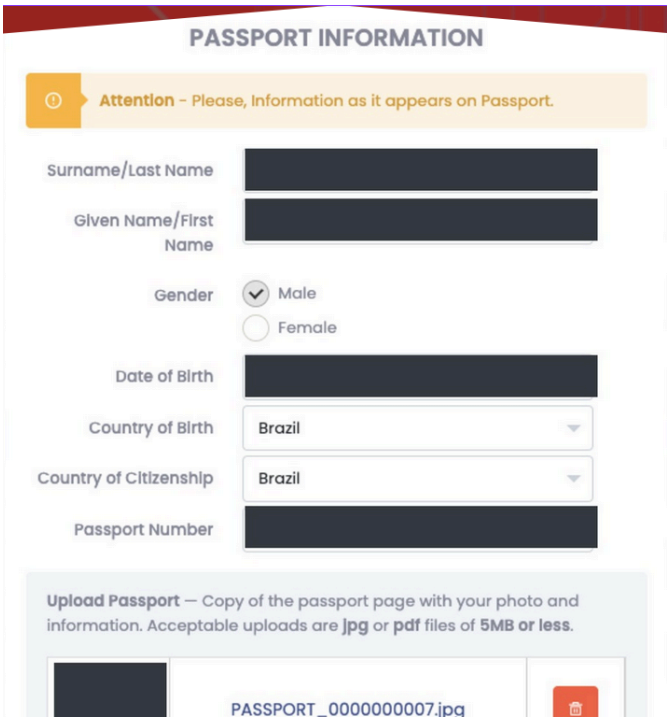
- **Improper Access Control (CWE-284):**
  Using direct IP addresses for login portals rather than FQDNs can bypass domain-based access controls, weakening the security framework intended to protect the application. This practice exposes internal functions and resources to potential exploitation by unauthorized users, increasing the risk of sensitive information being accessed or compromised.

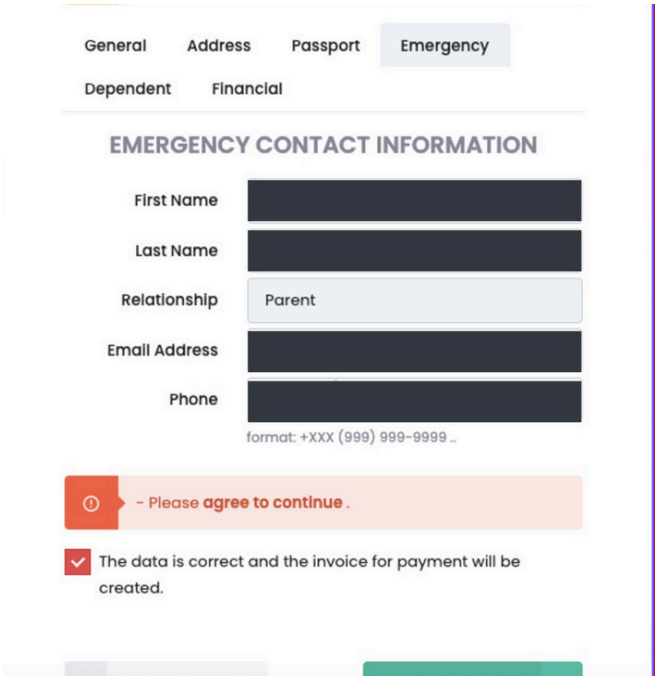
- **Use of Password System for Primary Authentication (CWE-309):**
  The reliance on a password-based authentication system as the primary means of access makes the application vulnerable to various attacks. Passwords can be stolen, guessed, or otherwise compromised, especially if not coupled with additional authentication mechanisms.

- **Weak Encryption for Passwords (CWE-261):**
  If passwords are stored using weak encryption algorithms, they can be easily compromised if the underlying database is accessed by unauthorized users. This vulnerability emphasizes the need for robust hashing and salting practices to protect stored credentials.



- **Missing Encryption of Sensitive Data (CWE-311):**
  If sensitive information, including user credentials and personal data, is transmitted or stored without adequate encryption, it may be exposed to interception or unauthorized access, increasing the risk of data breaches.





Affected Hosts	**123.123.12.1; Affected ports: 8010, 8020, 8030, 8040, 8050, 8060**
Remediation	**Implement Fully Qualified Domain Names (FQDNs):** • Configure all login portals to use FQDNs instead of direct IP addresses. This practice will ensure that domain-based security policies are effectively applied.

- Implement strict DNS configurations to prevent unauthorized changes to FQDNs and enforce the use of HTTPS with valid SSL/TLS certificates for all login portals.

Secure Transmission of Credentials:

- Ensure that all login pages use HTTPS with secure configurations to encrypt credentials during transmission.
- Implement HTTP Strict Transport Security (HSTS) to enforce the use of secure connections and prevent downgrade attacks.

Enhance Authentication Mechanisms:

- Implement multi-factor authentication (MFA) for all login portals to provide an additional layer of security beyond traditional username and password methods.
- Regularly review and update password policies to enforce complexity, expiration, and uniqueness requirements.

Strengthen Access Controls:

- Review and refine access control policies to ensure that only authorized users have access to login portals and sensitive resources.
- Implement role-based access control (RBAC) to limit access based on user roles and responsibilities.

Improve Password Security:

- Use strong hashing algorithms (e.g., bcrypt, Argon2) to securely store passwords, incorporating unique salts for each password to protect against rainbow table attacks.
- Regularly review and update encryption methods to ensure they meet current security standards.

Ensure Proper Encryption of Sensitive Data:

- Implement robust encryption mechanisms for both data in transit and data at rest, ensuring that sensitive information is adequately protected from unauthorized access.
- Regularly audit the encryption processes to verify compliance with best practices and regulatory requirements.

Conduct Regular Security Audits and Penetration Testing:

- Perform regular security audits and penetration tests to identify and mitigate vulnerabilities in the login portals and associated infrastructure.
- Review logs and monitor for any unusual login attempts or patterns that may indicate malicious activity.

User Awareness and Training:

- Educate users about the importance of using strong, unique passwords and the risks associated with single-factor authentication.

	• Provide training on recognizing phishing attempts and the importance of securing login credentials.

Vulnerability # 7	Findings
Concern	Shodan.io - Public Information Disclosure
Common Weakness Enumeration	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Risk Rating	Informational
Description	An analysis conducted using Shodan.io has identified the domain `f1schoolwebsite.app` mapped to the IP address `123.123.12.1`. This assessment confirms that the same IP address is associated with multiple subdomains utilized for login portals. The exposure of this information poses potential security risks, as it may inadvertently disclose sensitive information regarding the infrastructure and operational structure of the organization. The following points highlight the implications of this finding: • **Exposure of Sensitive Information:** The mapping of multiple subdomains to a single IP address can provide malicious actors with insights into the architecture of the web application and its associated services. If attackers can correlate subdomains and their functions, they may devise targeted strategies to exploit vulnerabilities or gain unauthorized access. • **Lack of Proper Domain Management:** The presence of direct IP references, rather than fully qualified domain names (FQDNs), can further expose the system to various attack vectors. It may bypass certain security mechanisms designed to restrict access based on domain policies, leading to potential unauthorized access and data breaches.
Affected Hosts	**f1schoolwebsite.app, 123.123.12.1**
Remediation	**Implement Fully Qualified Domain Names (FQDNs):** • Transition all login portals and associated services to utilize fully qualified domain names rather than direct IP addresses. This practice will enhance security by ensuring that domain-based security policies are effectively enforced and will help obscure the underlying infrastructure from potential attackers. • Ensure that all domain configurations are correctly set up to minimize the risk of DNS spoofing or hijacking. **Limit Public Exposure of Sensitive Information:** • Conduct a comprehensive audit of the web application and associated services to identify any unnecessary exposure of information,

	particularly regarding IP addresses and system architecture. ● Remove or restrict access to any non-essential public-facing information that could aid attackers in their reconnaissance efforts. **Enhance Security Posture:** ● Regularly review and update security policies and protocols to align with best practices for web application security. ● Implement robust logging and monitoring systems to detect and respond to unauthorized access attempts or anomalies in user behavior. **User Education and Awareness:** ● Provide training for staff on the importance of securing sensitive information and the potential risks associated with public information disclosure. ● Encourage best practices for security awareness and response among all team members involved in managing the web application infrastructure.

INTERNAL INVESTIGATIONS

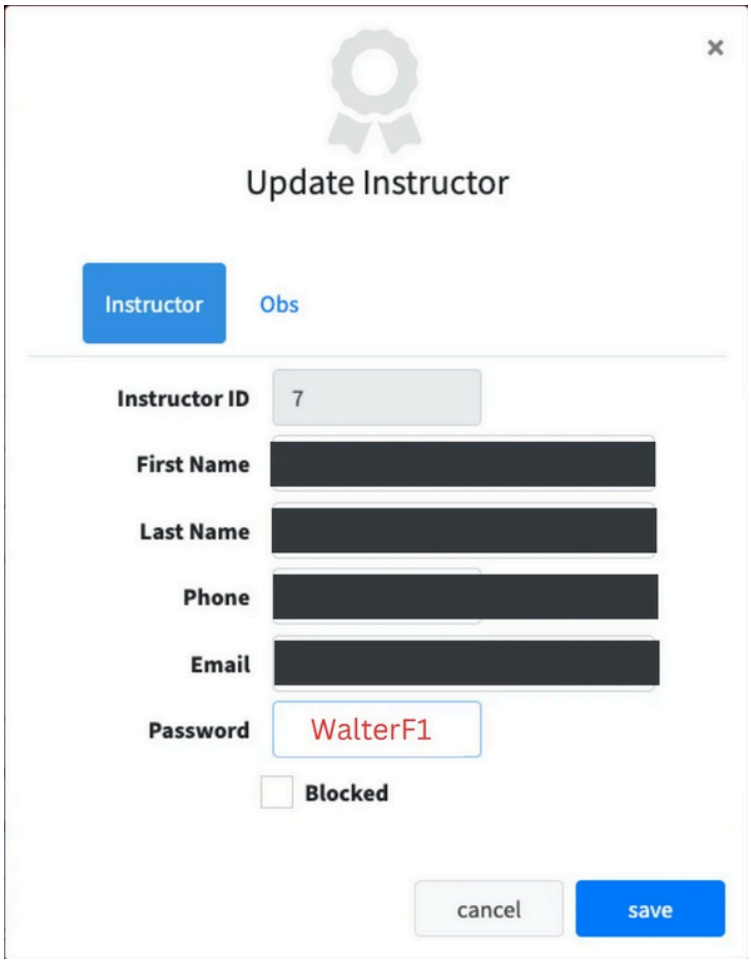
Vulnerability # 8	Findings
Concern	Physical Security
Common Weakness Enumeration	CWE-1263: Improper Physical Access Control CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Risk Rating	High
Description	During a recent social engineering assessment, it was identified that both a former employee and a non-employee successfully gained unauthorized access to the premises. The non-employee specifically solicited sensitive information from current faculty members, obtaining the universal password for teachers' computers on three separate occasions. This incident highlights significant vulnerabilities in our physical access control protocols.
Affected Hosts	Physical location
Remediation	**Access Control Protocols**: ● Restrict access to the premises to only authorized personnel, enrolled students, and prospective students. ● Implement robust identification measures, such as ID badges or biometric scanning, to ensure that only verified individuals can enter the facility. **Security Measures**:

	• Establish physical barriers such as security gates or locked doors in conjunction with monitored access points. • Utilize surveillance systems to monitor entry points and identify unauthorized access attempts. **Social Engineering Awareness Training**: • Conduct regular training sessions for all employees on identifying and responding to social engineering tactics. • Reinforce the protocol that any request for sensitive information, such as passwords, must be directed to a trusted administrator or IT security personnel.

Vulnerability # 9	Findings
Concern	Password Lockout Policy - Web Application
Common Weakness Enumeration	CWE-307: Improper Restriction of Excessive Authentication Attempts
Risk Rating	Critical
Description	An assessment revealed that multiple incorrect login attempts were executed using harvested credentials via BurpSuite, without triggering any account lockout measures. This lack of a password lockout policy significantly exposes sensitive data to risks from brute force or similar attacks. The web application in question, accessible at the following URLs, currently lacks adequate defenses against unauthorized access attempts
Affected Hosts	http://123.123.12.1:8020/ http://123.123.12.1:8030/ http://123.123.12.1:8060/
Remediation	**Implement a Password Lockout Mechanism**: • Establish a policy that restricts users to a maximum of **5 unsuccessful login attempts within a 15-minute window**. • Upon exceeding this threshold, the user's account should be locked to prevent further login attempts. **Cooldown Timer**: • Implement a **30-minute cooldown period** post-lockout, during which the user cannot attempt to log in again. • As an alternative to direct IT intervention for unlocking, users may be allowed to wait until the cooldown period expires, reducing the administrative burden on IT while maintaining security. **Secure Account Recovery Process**: • Implement a secure process for users to recover their accounts after a lockout, which could involve sending a verification code to the user's registered email or phone number for identity confirmation.

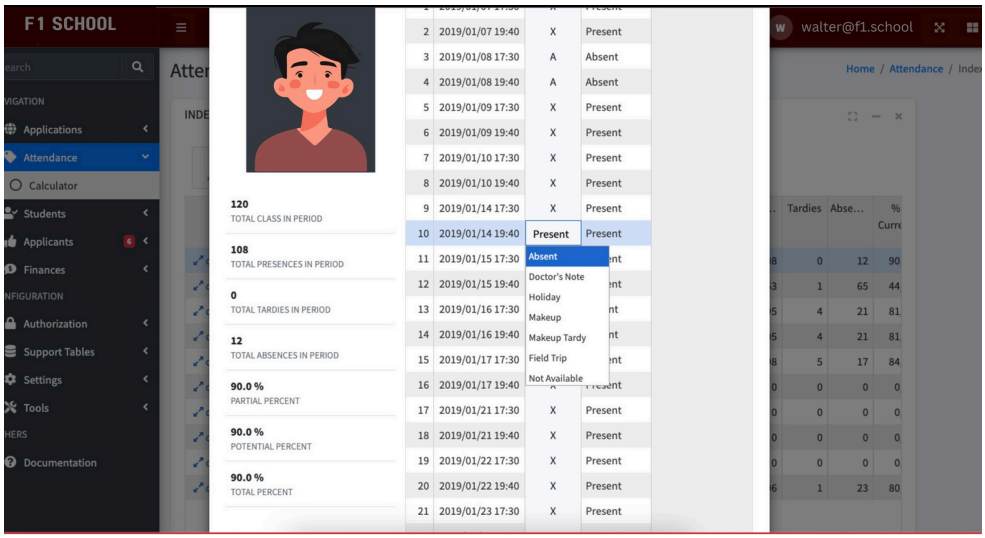
	Detailed Logging and Monitoring: ● Ensure that all authentication attempts, including successful and failed logins, are logged with timestamps, IP addresses, and user identifiers. ● Deploy real-time monitoring tools to alert the IT department of excessive failed login attempts, enabling immediate investigation and action. **Rate Limiting**: ● Implement rate limiting on login attempts, temporarily blocking an IP address after a specified number of failed attempts to mitigate the risk of brute force attacks. **User Alerts**: ● Notify users via email or SMS when their account is locked due to excessive login attempts, ensuring they are aware of potential unauthorized attempts to access their accounts. **Enhanced Security Measures**: ● Encourage or require users to set up security questions and enable multi-factor authentication (MFA) to further protect their accounts. MFA adds an additional layer of security, making unauthorized access significantly more difficult. **User Education and Awareness**: ● Provide training for users on best practices for password management and recognizing phishing attempts that could compromise their credentials.

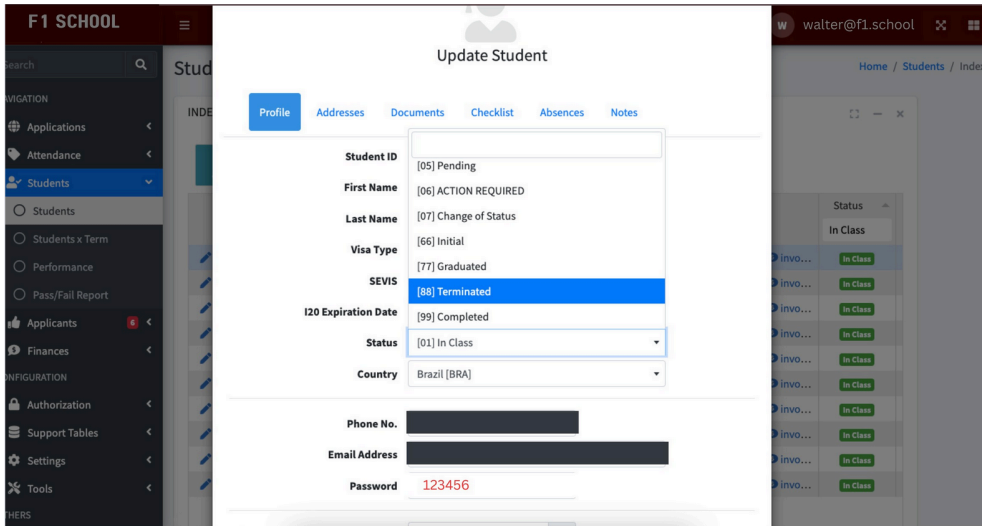
Vulnerability # 10	Findings
Concern	Password Requirements Policy
Common Weakness Enumeration	CWE-521: Weak Password Requirements
Risk Rating	Critical
Description	An evaluation of the current password practices revealed that users were employing easily guessed password formats, such as variations of their initials and last names (e.g., 'FirstInitialLastName'), common organizational references, and simplistic numerical sequences like '123456'. This indicates a significant vulnerability within the password management framework, exposing sensitive data to unauthorized access. The web applications under review, accessible via the following URLs, currently do not enforce adequate password security measures.

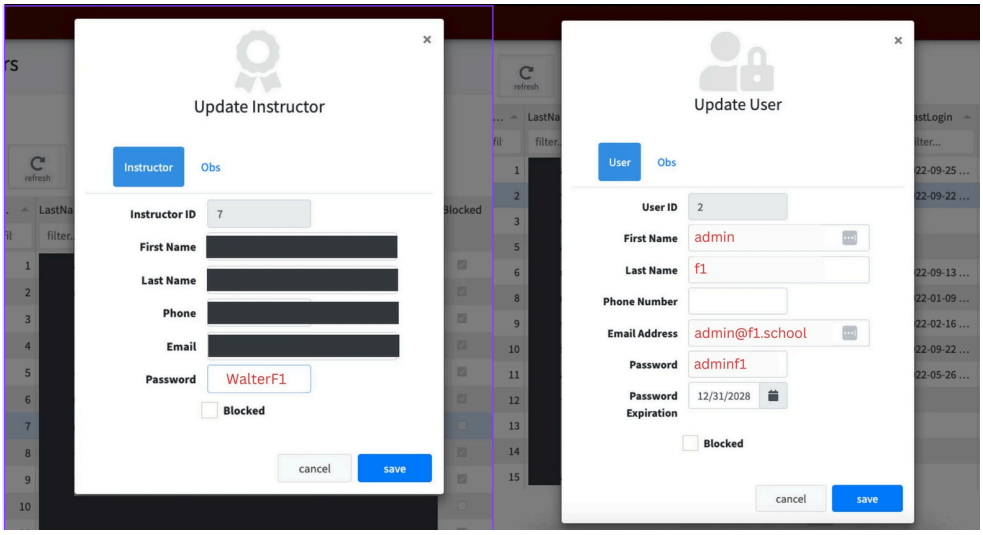
	
Affected Hosts	http://123.123.12.1:8020/ http://123.123.12.1:8030/ http://123.123.12.1:8060/ Physical Location
Remediation	**Implement Stricter Password Requirements**: ● Establish robust guidelines for password creation to ensure greater complexity and security. Passwords should not contain any personal information, such as usernames, real names, birth dates, or other easily accessible details. **Minimum Length and Structure**: ● Mandate that all passwords be at least **8 characters long**. While complexity is essential, it is also vital to promote memorable yet secure passwords. A recommended approach is to utilize a structure of **three random words separated by hyphens** (e.g., "Blue-Cat-Tree"), which is often more secure than random combinations of characters, especially those incorporating symbols. **Prohibit Common Patterns**: ● Develop policies that explicitly prohibit commonly used passwords and predictable patterns. This includes, but is not limited to, sequential numbers, repetitive characters, and easily guessable phrases. **Avoid Mandatory Password Resets**:

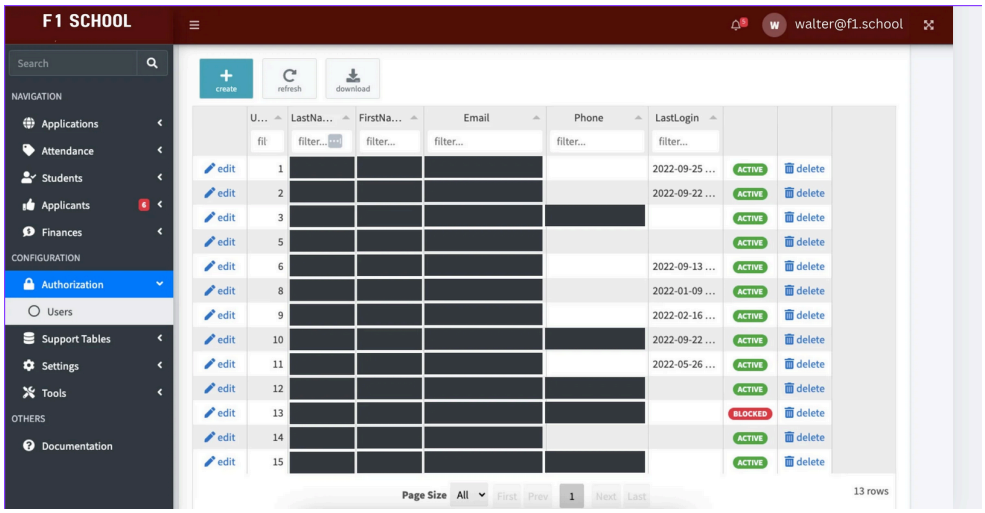
	• Reassess the necessity of mandatory password resets. Current guidance from the National Institute of Standards and Technology (NIST) suggests that enforced periodic changes can lead to weaker password choices as users may resort to easily remembered combinations. For more information on best practices, refer to NIST Password Guidelines. **User Education and Training**: • Implement training sessions and resources to educate users on the importance of strong password practices and the risks associated with weak passwords. This can enhance compliance and awareness of password security. **Utilize Password Managers**: • Encourage the use of password managers that can help users generate and store complex passwords securely. This can alleviate the burden of remembering multiple strong passwords while maintaining security. **Regular Audits and Monitoring**: • Conduct regular audits of password policies and user compliance. Monitoring password strength across the organization can identify areas for improvement and ensure adherence to security standards.

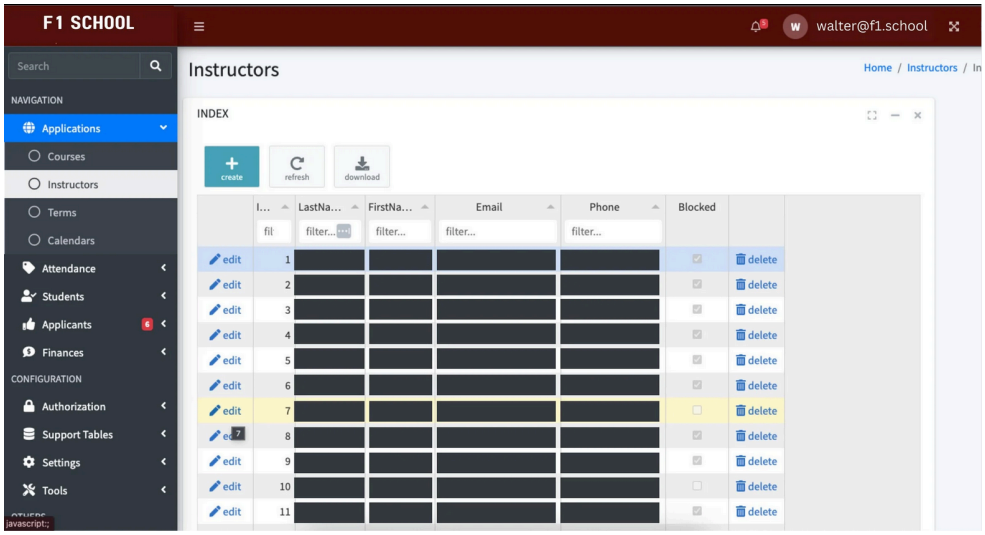
Vulnerability # 11	Findings
Concern	User/Admin Privileges
Common Weakness Enumeration	CWE-250: Execution with Unnecessary Privileges
Risk Rating	Critical
Description	An assessment of user and administrative privileges has identified critical vulnerabilities within the current access control framework. Various types and levels of administrative users possess unnecessary privileges, including the ability to view and edit administrative passwords, access sensitive student information, and download current student grades, government documentation, and medical, financial, and attendance records. Furthermore, it was observed that administrative account credentials are being stored using Google Password Manager on local PC accounts, which presents significant security risks.

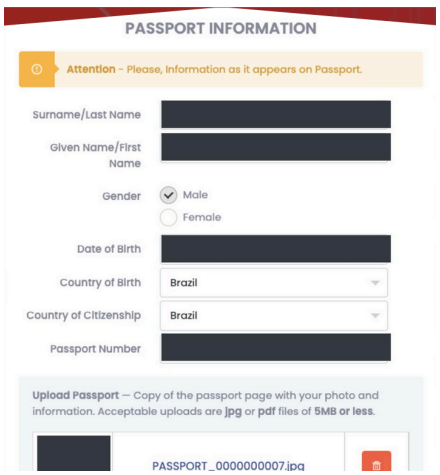

F1 SCHOOL
walter@f1.school
Home / Attendance
Applications
Attendance
Calculator
Students
Applicants
Finances
Authorization
Support Tables
Settings
Tools
Documentation
120
TOTAL CLASS IN PERIOD
108
TOTAL PRESENCES IN PERIOD
0
TOTAL TARDIES IN PERIOD
12
TOTAL ABSENCES IN PERIOD
90.0 %
PARTIAL PERCENT
90.0 %
POTENTIAL PERCENT
90.0 %
TOTAL PERCENT
2 2019/01/07 19:40 X Present
3 2019/01/08 17:30 A Absent
4 2019/01/08 19:40 A Absent
5 2019/01/09 17:30 X Present
6 2019/01/09 19:40 X Present
7 2019/01/10 17:30 X Present
8 2019/01/10 19:40 X Present
9 2019/01/14 17:30 X Present
10 2019/01/14 19:40 Present Present
11 2019/01/15 17:30
12 2019/01/15 19:40
13 2019/01/16 17:30
14 2019/01/16 19:40
15 2019/01/17 17:30
16 2019/01/17 19:40
17 2019/01/21 17:30 X Present
18 2019/01/21 19:40 X Present
19 2019/01/22 17:30 X Present
20 2019/01/22 19:40 X Present
21 2019/01/23 17:30 X Present
Absent
Doctor's Note
Holiday
Makeup
Makeup Tardy
Field Trip
Not Available

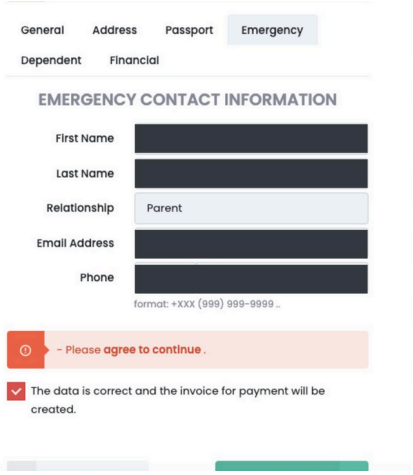

F1 SCHOOL
walter@f1.school
Home / Students
Update Student
Profile
Addresses
Documents
Checklist
Absences
Notes
Student ID
First Name
Last Name
Visa Type
SEVIS
I20 Expiration Date
Status
Country
Phone No.
Email Address
Password
123456
[05] Pending
[06] ACTION REQUIRED
[07] Change of Status
[66] Initial
[77] Graduated
[88] Terminated
[99] Completed
[01] In Class
Brazil [BRA]


Update Instructor
Instructor
Obs
Instructor ID 7
First Name
Last Name
Phone
Email
Password WalterF1
Blocked
cancel
save
Update User
User
Obs
User ID 2
First Name admin
Last Name f1
Phone Number
Email Address admin@f1.school
Password adminf1
Password Expiration 12/31/2028
Blocked
cancel
save





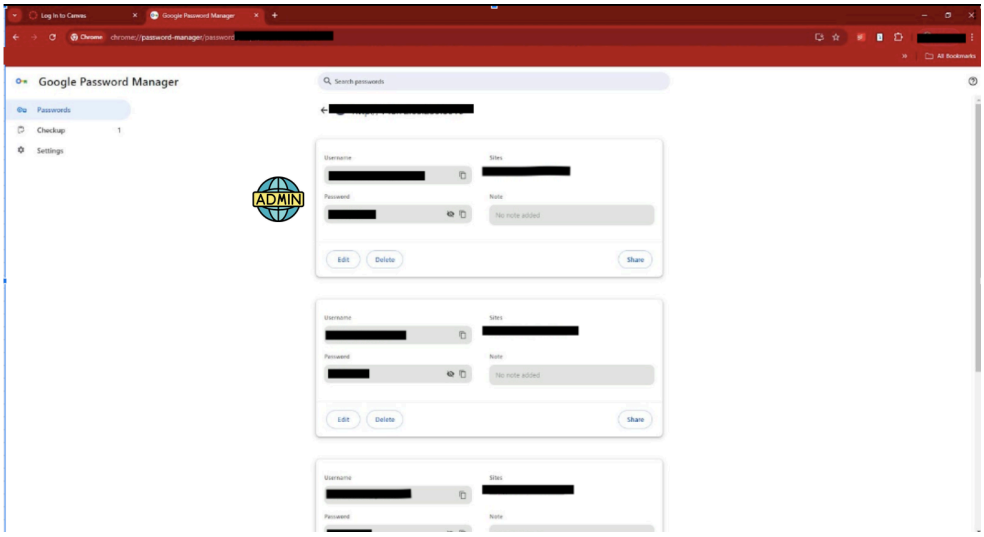




Affected Hosts	Physical location, local PC accounts, http://123.123.12.1:8020/,
Remediation	**Implement Least Privilege Policies**: • Restrict administrative privileges exclusively to IT personnel and other designated users who require access for their job functions. This principle of least privilege will minimize the risk of unauthorized

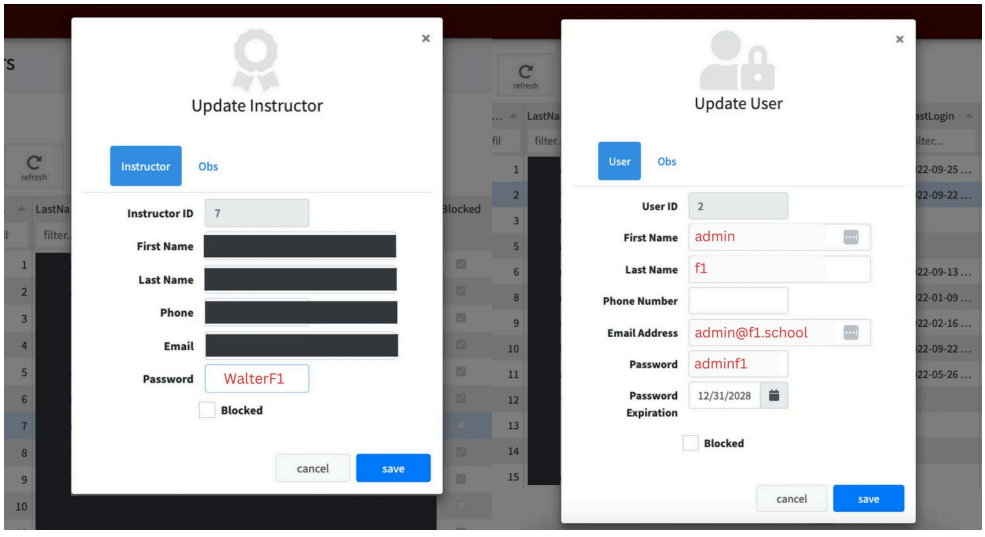
	changes and protect sensitive information. **Review and Reassess Privileges Regularly**: ● Conduct regular audits of user roles and privileges to ensure compliance with the least privilege principle. Promptly revoke any unnecessary privileges that are identified. **Secure Administrative Accounts**: ● Prohibit the use of personal email accounts (e.g., Gmail) for official business. Establish IT-managed email accounts using the organization's domain (e.g., "f1schoolwebsite.edu") for all staff members to ensure secure access and maintain control over sensitive information. **Implement Two-Factor Authentication (2FA)**: ● Enforce 2FA for all administrative accounts to provide an additional layer of security. This measure will significantly reduce the risk of unauthorized access, even if credentials are compromised. **User Behavior Analytics (UBA)**: ● Deploy UBA solutions to monitor user behavior for signs of abnormal or suspicious activities, such as unauthorized access attempts or irregular login patterns. Early detection of anomalies can help mitigate insider threats and identify compromised accounts swiftly. **Account Security Monitoring**: ● Encourage users to routinely review their account's security settings for unfamiliar devices or activities that could indicate unauthorized access. Promptly address any anomalies detected. **Regular Maintenance of Local Accounts**: ● Advise staff to refrain from storing administrative credentials in unsecured applications such as Google Password Manager on local PCs. Instead, utilize secure password management solutions endorsed by the organization. **Browser Security Hygiene**: ● Implement a policy requiring users to periodically clear their browser's cache and cookies. This practice helps mitigate the risk of cookie theft and other vulnerabilities associated with stored session information.

Vulnerability # 12	Findings
Concern	Auto-Fill Password Vulnerabilities

Common Weakness Enumeration	CWE-256: Plaintext Storage of a Password CWE-311: Missing Encryption of Sensitive Data CWE-640: Weak Password Recovery Mechanism for Forgotten Password
Risk Rating	Critical
Description	An evaluation of the current password management practices has revealed critical vulnerabilities associated with the use of auto-fill features in web browsers. Specifically, several Google Chrome accounts were found to have auto-fill enabled, resulting in the unencrypted storage of administrative credentials. This situation exposes sensitive information to potential access by unauthorized individuals due to inadequate password storage policies. Additionally, the use of auto-filled passwords often correlates with weak password recovery mechanisms, particularly when combined with insecure storage practices. 
Affected Hosts	f1schoolwebsite.edu, 123.123.12.1
Remediation	**Implement Active Directory Accounts**: • Establish an Active Directory (AD) account system for all users, linked to their "f1schoolwebsite.edu" email accounts. This account should be used for logging into local PCs, providing a centralized and secure authentication mechanism. **Eliminate Universal Passwords**: • Prohibit the use of universal passwords across multiple accounts or applications. Each account should have a unique password to mitigate the risk of widespread exposure in case of a breach. **Implement Windows Mobile Device Management (MDM)**: • Deploy Windows MDM to centrally manage and enforce password policies across all devices, ensuring compliance with organizational standards.

	Mandate Non-Personal Chrome Profiles: ● Require staff to use non-personal Chrome profiles for work-related activities, ensuring that sensitive information is not stored in personal accounts. **Encourage Creation of F1 International Academy-only Email Accounts**: ● Promote the use of dedicated F1 International Academy-only email accounts for all work-related communications to enhance security and streamline access management. **Enforce Logout Procedures**: ● Implement strict logout procedures to ensure that users sign out of applications when not in use. This will help prevent unauthorized access to sensitive information. **Strictly Enforce a No-Password-Sharing Policy**: ● Establish and enforce a no-password-sharing policy among staff. Provide clear guidelines and technical controls to assist in this enforcement, ensuring that all users understand the risks associated with sharing credentials. **Individual Accounts on Computers**: ● Ensure that each staff member has an individual account on shared computers. This will help maintain accountability and limit access to sensitive information. **Security Awareness Training**: ● Conduct regular security awareness training sessions to educate staff on best practices for password management and the importance of protecting sensitive data. **User Behavior Analytics (UBA)**: ● Deploy UBA solutions to monitor user activity for signs of abnormal or suspicious behavior. This includes tracking unauthorized access attempts and irregular login patterns, facilitating early detection of potential insider threats or compromised accounts. **Account Security Monitoring**: ● Instruct users to regularly review their account security settings for any unfamiliar devices or activities, which may indicate unauthorized access. Promptly investigate any anomalies identified. **Periodic Maintenance of Browser Security**: ● Establish a policy requiring users to periodically clear their browser cache and cookies. This routine maintenance helps to eliminate

	potentially compromised session data and reduces the risk of cookie theft. **Encryption of Sensitive Data**: ● Ensure that all sensitive data, including passwords, is stored using strong encryption protocols. This includes not only data at rest but also data in transit to protect against interception. **Strengthen Password Recovery Mechanisms**: ● Review and enhance password recovery mechanisms to ensure they are secure and reliable. This includes implementing multi-factor authentication (MFA) during the password recovery process to verify user identity before allowing access.

Vulnerability # 13	Findings
Concern	Unencrypted Sensitive Information
Common Weakness Enumeration	CWE-312: Cleartext Storage of Sensitive Information CWE-319: Cleartext Transmission of Sensitive Information CWE-311: Missing Encryption of Sensitive Data
Risk Rating	Critical
Description	A thorough security assessment has revealed critical vulnerabilities associated with the handling of sensitive information within the administrative portal. Specifically, it was discovered that passwords were stored in cleartext without any form of encryption, exposing all user accounts—including those of students, teachers, administrators, and employees—to significant security risks. Additionally, the current practices concerning the viewing of private documents, such as passports and bank statements, may also compromise sensitive information. 

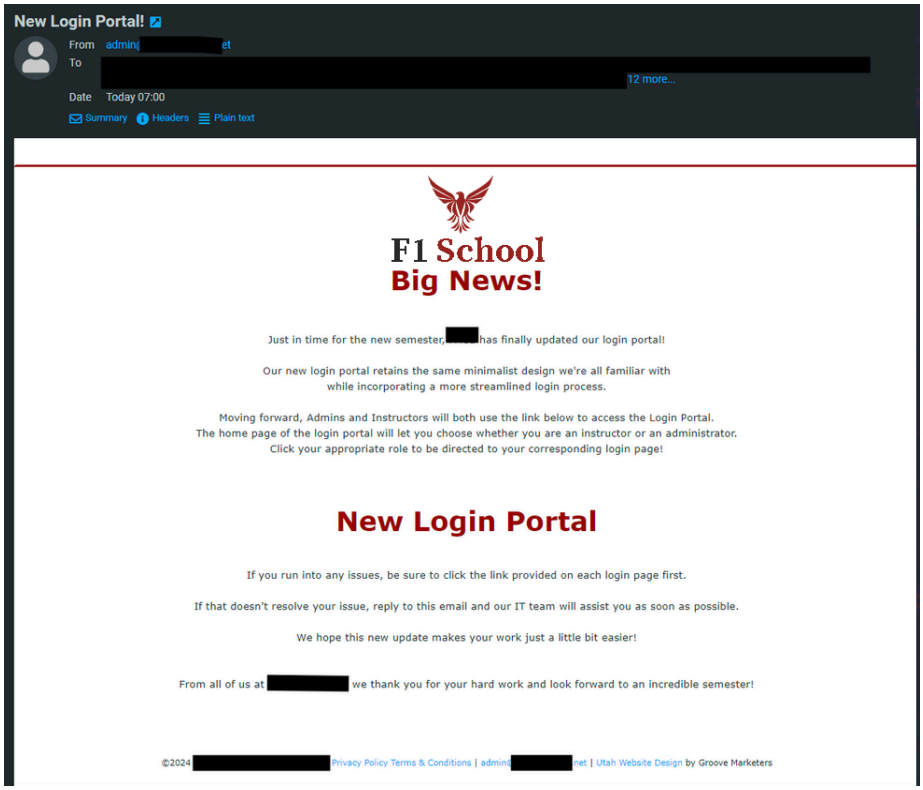
Affected Hosts	Physical location, local PC accounts, http://123.123.12.1:8020/
Remediation	**Implement Strong Encryption Practices**: ● Enforce the use of robust encryption protocols for storing passwords and sensitive information within the administrative portal. All user passwords should be hashed using industry-standard algorithms (e.g., bcrypt, Argon2) to ensure they are not stored in cleartext. **Ensure Secure Transmission of Data**: ● Utilize secure transmission protocols, such as HTTPS and TLS, for all data communications. This will protect sensitive information from interception during transmission, particularly when accessed over networks. **Restrict Access to Sensitive Documents**: ● Implement strict access controls to limit visibility of private documents (e.g., passports, bank statements) to only those individuals who absolutely require it for their job functions. This will help minimize the risk of unauthorized access to sensitive information. **Conduct Regular Security Audits**: ● Perform periodic security audits to assess compliance with encryption and data protection policies. This will help identify vulnerabilities and ensure that best practices are being followed consistently. **User Education and Training**: ● Provide training to all staff on the importance of data protection and the risks associated with handling sensitive information. This will raise awareness and promote adherence to security protocols. **Implement Data Loss Prevention (DLP) Solutions**: ● Deploy DLP solutions to monitor and protect sensitive data from unauthorized access and transmission. This technology can help identify and block potential data breaches before they occur. **Monitor for Anomalous Access**: ● Establish monitoring systems to detect unauthorized access attempts to sensitive information. Implement alerts for unusual access patterns that may indicate a security breach. **Develop an Incident Response Plan**: ● Create and maintain an incident response plan specifically addressing data breaches involving sensitive information. Ensure that all staff are familiar with the procedures for reporting and responding to such incidents. **Regularly Review and Update Policies**:

	• Conduct regular reviews of data handling and encryption policies to ensure they remain effective against evolving security threats. Update practices as necessary to maintain compliance with industry standards.

Vulnerability # 14	Findings
Concern	Remove any outdated or unnecessary data
Common Weakness Enumeration	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-359: Exposure of Private Personal Information to an Unauthorized Actor
Risk Rating	Medium
Description	A recent security assessment has uncovered significant vulnerabilities related to the retention of outdated or unnecessary data within the organization. Specifically, credentials for former employees remain active following their termination, which increases the risk of insider threats and potential exploitation by malicious actors. Furthermore, confidential information pertaining to former students continues to be stored, despite their departure from the institution. The risks associated with these practices are particularly concerning, as they expose sensitive data to unauthorized access.
Affected Hosts	123.123.12.1
Remediation	**Implement Data Retention Policies**: • Establish comprehensive data retention policies that define the duration for which different types of data (e.g., employee credentials, student records) may be stored. Ensure that data is retained only as long as necessary for operational and legal requirements. **Regular Data Audits**: • Conduct regular audits to identify and remove outdated or unnecessary data from servers. This includes deactivating and deleting accounts for instructors, students, administrators, and former employees who no longer require access to organizational resources. **Immediate Account Deactivation**: • Enforce a policy whereby accounts for staff members who are no longer employed are immediately deactivated upon termination. This practice will prevent potentially disgruntled or opportunistic former employees from exploiting access to sensitive information. **Secure Data Disposal Procedures**: • Implement secure data disposal procedures to ensure that any sensitive information, once deemed unnecessary, is irretrievably deleted. Utilize methods that comply with industry standards for secure

	data destruction. **Limit Data Access**: ● Restrict access to sensitive information on a need-to-know basis. Only personnel who require access for legitimate business purposes should be granted permission to view or manage sensitive data. **Enhance Monitoring and Alerting**: ● Develop monitoring systems to detect any unauthorized access attempts or unusual activities related to user accounts. Implement alerts for suspicious activities, especially involving accounts of former employees or students. **Employee Training and Awareness**: ● Provide training to current employees regarding the importance of data security and the potential risks associated with retaining unnecessary data. Encourage them to report any outdated or potentially vulnerable information they may encounter. **Legal Compliance Review**: ● Regularly review data retention policies to ensure compliance with legal and regulatory requirements related to data protection and privacy. Adjust practices as necessary to meet evolving legal standards. **Incident Response Planning**: ● Include procedures for addressing incidents involving outdated or unnecessary data in the organization's overall incident response plan. Ensure all staff are familiar with the steps to take in the event of a data breach.

Vulnerability # 15	Findings
Concern	Phishing Campaign
Common Weakness Enumeration	CWE-601: URL Redirection to Untrusted Site CWE-640: Weak Password Recovery Mechanism for Forgotten Password

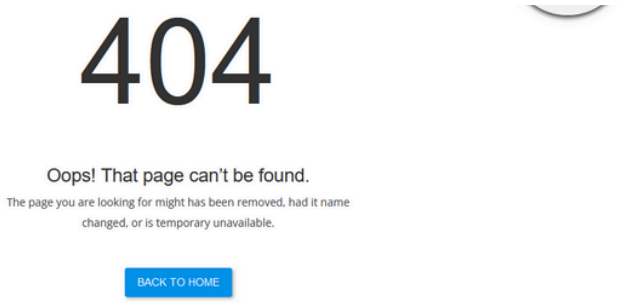
Risk Rating	Critical
Description	An orchestrated phishing campaign targeted F1 International Academy's employees, successfully harvesting credentials through an alternate domain (f1schoolwebsite.net) hosted on a private server. This attack highlights vulnerabilities in employee awareness and a susceptibility to social engineering tactics. 
Affected Hosts	Employees
Remediation	**Employee Training and Awareness** ● Conduct regular information security training for staff on identifying phishing attempts, recognizing suspicious links, and safeguarding sensitive information. ● Automatically mark any emails originating from outside the "@f1schoolwebsite.edu" domain as "EXTERNAL" to prompt users to exercise caution when interacting with these messages. **Phishing Simulations** ● Regularly conduct email phishing simulations to test staff's ability to detect and respond to phishing attempts. ● Provide immediate feedback to employees who fall victim to simulated attacks and offer additional, targeted training to improve phishing detection skills. **Email Policy and Configuration**

	• Require all employees to use official "@f1schoolwebsite.edu" email accounts exclusively for work-related communication; personal email accounts should not be used. • Have the IT team configure and manage these official email accounts to enforce spam filtering and phishing detection, enhancing email security across the organization.

Vulnerability # 16	Findings
Concern	File Upload Vulnerability
Common Weakness Enumeration	CWE-434: Unrestricted Upload of File with Dangerous Type CWE-20: Improper Input Validation
Risk Rating	Low
Description	During testing, it was discovered that the job application page (https://www.f1schoolwebsite.edu/job-application) allowed the upload of potentially malicious files, including a PHP shell, indicating improper input validation and insufficient file type restrictions. This vulnerability poses a risk of remote code execution, data compromise, or unauthorized system access if malicious files are executed on the server. `<?php` `// Path to the /etc/passwd file` `$file_path = '/etc/passwd';` `// Check if the file exists` `if (file_exists($file_path)) {` `// Read the file into an array, each line as an array element` `$file_contents = file($file_path);` `// Display the contents of /etc/passwd` `foreach ($file_contents as $line) {` `echo htmlspecialchars($line) . " ";` `}` `} else {` `echo "File not found!";` `}` `?>`
Affected Hosts	https://www.f1schoolwebsite.edu/job-application
Remediation	**Restrict File Types** • Implement strict file type validation to ensure that only permitted file formats (e.g., PDF, DOCX, or image files) can be uploaded. All other file types, especially executable files such as PHP, should be explicitly denied. **Server-Side Input Validation** • Enforce robust server-side input validation to prevent the upload of

	malicious files. This should include validating the file type based on its content (MIME type) and extension to ensure consistency. **File Size and Content Scanning** ● Set reasonable limits on file size to reduce the risk of malicious oversized uploads. Additionally, integrate content scanning mechanisms to detect potentially dangerous files, such as embedded scripts or executables, before storing them on the server. **Store Files Outside Web Root** ● Store all uploaded files outside the web root directory to prevent direct access to them through a browser. This will reduce the risk of remote execution if a malicious file is inadvertently uploaded. **Sanitize File Names** ● Implement filename sanitization to prevent malicious characters or scripts from being embedded in the file names. This will

Vulnerability # 17	Findings
Concern	Directory Traversal
Common Weakness Enumeration	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Risk Rating	Low
Description	Attempts to exploit directory traversal vulnerabilities were blocked during testing. However, it is important to note that the outdated Nginx version 1.24.0 in use on the server is known to be vulnerable to this type of attack. The following directory traversal attempts were made: ● **Command Injection to Access /etc/passwd:** Attempted via the URL: https://www.f1schoolwebsite.edu/form-submission-results?form=%22%22;%20system(%27cat%20/etc/passwd%27) This attack was designed to exploit directory traversal to view the system's password file. ● **Command Injection to List Directory Contents:** Attempted via the URL: https://www.f1schoolwebsite.edu/form-submission-results?form=;%20ls%20-la%20/var/www/html This attack aimed to list the files in the web root directory to gain insights into directory structure and potentially sensitive files.

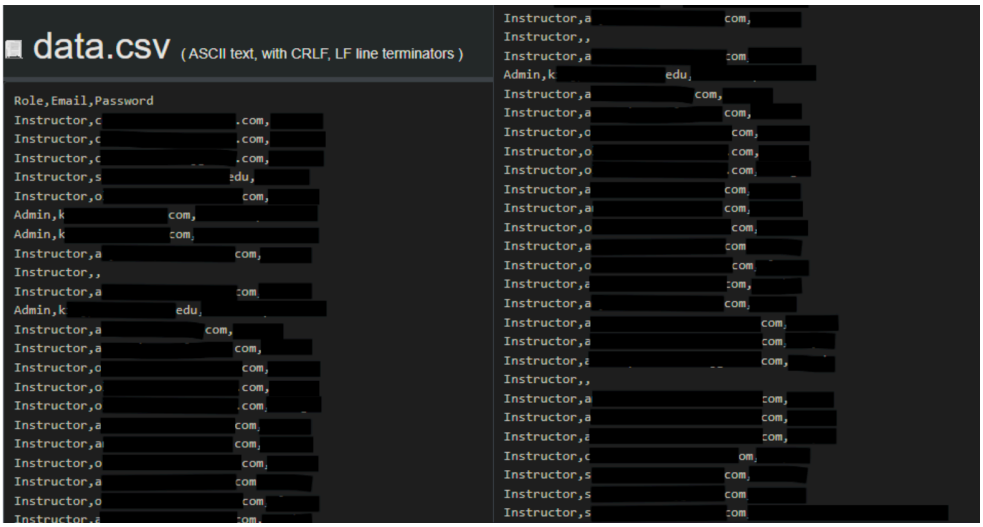
	
Affected Hosts	123.123.12.1, https://f1schoolwebsite.edu

Remediation	• **Update Nginx Version**
	  ○ Immediately update the Nginx web server to a version that is not susceptible to directory traversal vulnerabilities. Keeping the server up to date is essential to mitigate known vulnerabilities and exploits.
	• **Validate User Input**
	  ○ Implement proper input validation on all user-submitted data to ensure that commands or special characters that could be used for directory traversal attacks are properly sanitized or rejected.
	• **Ensure Secure File and Directory Permissions**
	  ○ Avoid storing sensitive configuration files, such as credentials or system data, within the web root directory. Sensitive files should be placed outside the accessible web directories to prevent unauthorized access in the event of a successful directory traversal attempt.
	• **Use the Principle of Least Privilege**
	  ○ Restrict permissions on directories and files to the minimum necessary for the web application to function. This reduces the impact of a successful attack by limiting what an attacker can access or modify.
	• **Understand File Processing Behavior**
	  ○ Ensure that developers and administrators fully understand how the underlying operating system processes filenames and paths handed off to it by the web application. This knowledge will help prevent directory traversal and other related attacks.
	• **For Windows IIS Servers**
	  ○ If using Windows IIS, the web root should not be located on the system disk. This configuration prevents recursive traversal attacks from accessing critical system directories by limiting what directories can be reached through traversal attempts.
	
	For more details on preventing directory traversal attacks, refer to the OWASP Path Traversal Guidelines.

Vulnerability # 18	Findings
Concern	Router and Network Vulnerabilities

Common Weakness Enumeration	CWE-284: Improper Access Control CWE-693: Protection Mechanism Failure CWE-400: Uncontrolled Resource Consumption (DoS) CWE-284: Improper Access Control
Risk Rating	Medium
Description	An internal network analysis using Routersploit exposed critical security issues in F1 International Academy's network. The student and admin networks are not properly segmented, creating a risk of unauthorized access to internal devices such as Apple TVs and Wireless Access Points (WAPs). Several devices were found with open ports, including port 22 (SSH), port 80 (HTTP), and port 443 (HTTPS), though no exploits were confirmed. Furthermore, the password for the admin Wi-Fi was manually brute-forced based on pattern recognition from unencrypted credentials found in the AdmAPP web application.
Affected Hosts	Physical F1 International Academy Router & Network, 10.0.0.1, 10.0.0.001, 10.0.0.01, 10.0.0.50, 10.0.0.02, 10.0.0.002, 10.0.0.003, 10.0.0.004, 10.0.0.005, 10.0.0.006
Remediation	**Network Segmentation** ● Immediate segmentation of the student and administrative networks is critical to protect sensitive systems. Isolating administrative resources from the student network minimizes the risk of internal attacks and unauthorized access to devices. **VPN or Encrypted Tunnel for Admin Network Access** ● Implement a secure VPN or encrypted tunnel for the admin network, ensuring only approved devices can connect. Administrative web applications and systems should only be accessible from within this secure network, blocking unauthorized access from external or unsecured devices. **Password Management and Encryption** ● Strong password policies must be enforced, and credentials for critical systems (such as the admin Wi-Fi) should be randomly generated and stored securely. Sensitive data, including passwords stored or transmitted within applications like AdmAPP, must be encrypted to prevent brute-force attacks and credential guessing. **Port Security and Device Hardening** ● Review and secure all devices with open ports, such as 22, 80, and 443. Restrict access by IP, disable unnecessary services, and ensure services are properly secured to prevent exploitation. **Physical Network Device Security**

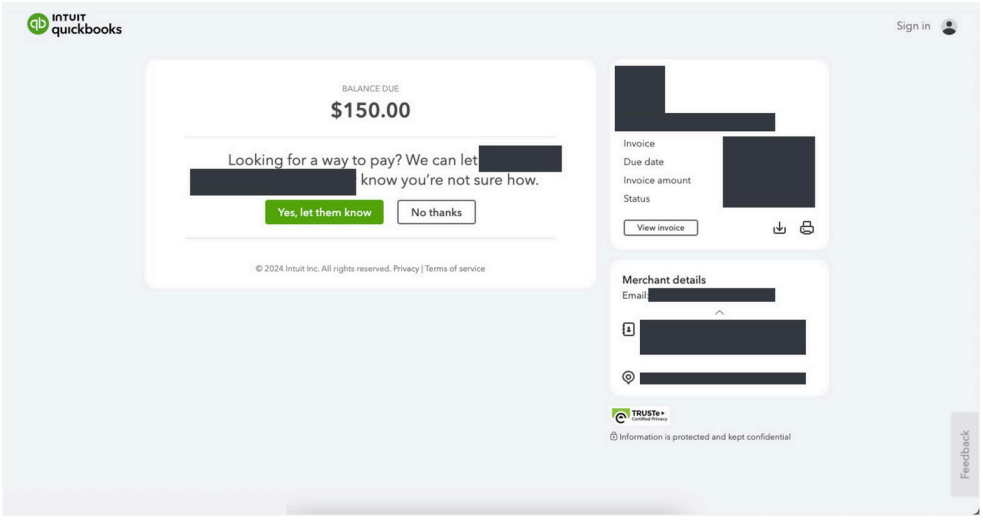
	• Secure routers and switches with strong, unique passwords and update their firmware regularly. Restrict access to these devices to authorized personnel only, ensuring that network infrastructure is protected from tampering. **Monitoring and Logging** • Deploy real-time monitoring tools to detect unauthorized access attempts or unusual traffic patterns. Logging tools should capture critical network events, with alerting mechanisms for rapid response to potential Denial-of-Service (DoS) attacks or intrusion attempts.

Vulnerability # 19	Findings
Concern	Credential Harvesting
Common Weakness Enumeration	CWE-522: Insufficiently Protected Credentials CWE-307: Improper Restriction of Excessive Authentication Attempts CWE-620: Unverified Password Change
Risk Rating	Critical
Description	During the investigation, over 100 administrative and instructor credentials were harvested, exposing critical security flaws within F1 International Academy's systems. While many of these credentials were obtained through social engineering techniques, the most concerning finding was that a single admin password provided access to all user passwords stored in plain text in the database. This flaw allowed any admin account to view sensitive credentials for systems such as financial databases and student records. 
Affected Hosts	Physical location, F1 International Academy employees, 123.123.12.1, f1schoolwebsite.edu

Remediation	**Encrypt Stored Passwords** • Immediately cease storing passwords in plain text. Implement secure password hashing algorithms such as bcrypt or Argon2 to store passwords in a way that prevents retrieval even by admin accounts. **Implement Stronger Password Policies** • Enforce password policies that require stronger, more complex passwords. Passwords should be at least 8 characters long and include a combination of short words, symbols, and numbers to prevent easily guessable combinations. Avoid using any personal identifying information within passwords. **Limit Admin Access to Credentials** • Restrict admin access to sensitive information such as passwords. Admins should not have the ability to view or retrieve stored passwords. Instead, implement secure password recovery mechanisms that do not expose actual credentials. **Prevent Excessive Authentication Attempts** • Introduce account lockout mechanisms after a predefined number of failed login attempts to prevent brute-force attacks. Excessive authentication attempts should be restricted to mitigate credential guessing attempts. **Strengthen Authentication Workflows** • Ensure that password changes are verified through secure channels, such as multi-factor authentication (MFA). Password change requests must be validated, and confirmation should be required before allowing any updates to user credentials. **Regular Employee Training** • Conduct regular information security training for employees, with a focus on recognizing and avoiding phishing, pretexting, and other social engineering tactics. Employees must be equipped to spot potential attacks and report them to IT before damage occurs.

FINANCIAL SYSTEM VULNERABILITIES

Vulnerability # 20	Findings
Concern	QuickBooks API Exposure

Common Weakness Enumeration	CWE-284: Improper Access Control CWE-611: Improper Restriction of XML External Entity Reference (XXE) CWE-200: Information Exposure CWE-306: Missing Authentication for Critical Function CWE-307: Improper Restriction of Excessive Authentication Attempts CWE-770: Allocation of Resources Without Limits or Throttling CWE-400: Uncontrolled Resource Consumption CWE-20: Improper Input Validation CWE-79: Improper Neutralization of Input During Web Page Generation (XSS) CWE-89: Improper Neutralization of Special Elements Used in an SQL Command (SQL Injection) CWE-209: Generation of Error Message Containing Sensitive Information CWE-311: Missing Encryption of Sensitive Data CWE-319: Cleartext Transmission of Sensitive Information CWE-522: Insufficiently Protected Credentials CWE-613: Insufficient Session Expiration CWE-384: Session Fixation CWE-352: Cross-Site Request Forgery (CSRF) CWE-942: Permissive Cross-Origin Resource Sharing (CORS) Policy CWE-923: Improperly Controlled Creation of Process CWE-862: Missing Authorization
Risk Rating	Critical
Description	The exposed QuickBooks API presents several security vulnerabilities due to improper access controls and exposure of sensitive data. The issues identified span multiple Common Weakness Enumerations (CWEs), indicating a broad range of potential attack vectors. The QuickBooks API is exposed through publicly accessible ports (6002 and 5002), allowing unauthorized access to financial data. Publicly exposed API endpoints are vulnerable to various types of attacks due to inadequate access control and missing authentication. These vulnerabilities could lead to unauthorized data manipulation, information leakage, and exploitation of sensitive functions.  Risks include, but are not limited to: **1. Exposed API Endpoints on Public Ports (6002 and 5002)** ● **Risk**: Public exposure of API services can make the system vulnerable

to a variety of attacks, including brute force attacks, credential stuffing, and API enumeration.
- **Mitigation**: Restrict public access to sensitive endpoints by using a firewall, VPN, or API Gateway to limit access only to authorized users. Use TLS/SSL encryption to secure data in transit.

2. Unauthenticated Endpoints

- **Risk**: Some endpoints such as `/api/v1/auth/token` and `/api/v1/customers/query` might not require proper authentication, allowing attackers to retrieve sensitive information (e.g., customer data) or request an access token without valid credentials.
- **Mitigation**: Ensure strong authentication and authorization mechanisms (OAuth2, JWT, etc.) are in place for all endpoints, especially sensitive ones like `auth/token` and `customers`.

3. Lack of Rate Limiting

- **Risk**: APIs without rate limiting are susceptible to brute force attacks and denial of service (DoS) attacks, where an attacker floods the API with requests.
- **Mitigation**: Implement rate limiting and monitoring to restrict the number of API calls from a single IP or user over a period of time.

4. Insufficient Input Validation on Query Parameters

- **Risk**: The `email` parameter in the `/api/v1/customers/query` endpoint, along with the `id` parameter in `/api/v1/invoices/{id}`, might not have strict input validation. This could lead to SQL Injection, Cross-Site Scripting (XSS), or parameter manipulation attacks.
- **Mitigation**: Implement proper input validation and sanitization to ensure that user input does not contain malicious code. Use prepared statements for database queries to prevent SQL injection.

5. Sensitive Data Exposure via Error Responses

- **Risk**: If the API returns detailed error messages (e.g., stack traces or database errors) when a `204 No Content` response occurs, it could reveal system architecture or data structure details.
- **Mitigation**: Avoid exposing internal system details through error responses. Standardize and minimize the information returned by error messages.

6. No Clear Mechanism for Handling Sensitive Data

- **Risk**: The API handles sensitive customer information (PII) and QuickBooks authentication tokens, but there's no mention of how this data is secured (e.g., encryption).
- **Mitigation**: Encrypt sensitive data both at rest and in transit. Mask sensitive data such as email addresses or IDs in API responses, and ensure that tokens are stored securely.

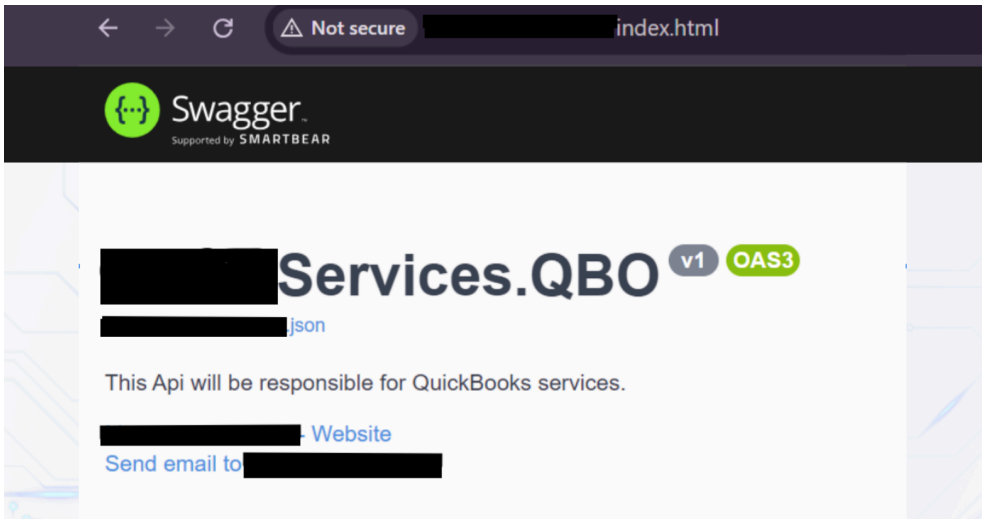
7. Potential for Improper Access Token Management

- **Risk**: The endpoint `/api/v1/auth/token` is used to retrieve a

	QuickBooks access token. If access tokens are not properly protected, stored securely, or rotated regularly, they could be exploited by attackers. ● **Mitigation**: Implement proper token management policies such as expiration times, refresh tokens, secure storage, and limiting token scope to reduce potential abuse. **8. No Mention of CORS or CSRF Protections** ● **Risk**: Without proper Cross-Origin Resource Sharing (CORS) or Cross-Site Request Forgery (CSRF) protections, attackers might be able to exploit the API by making unauthorized requests from other domains. ● **Mitigation**: Implement CORS policies to control which domains are allowed to make API requests. Additionally, use anti-CSRF tokens to validate the legitimacy of requests.
Affected Hosts	123.123.12.1:6002, 123.123.12.1:5002
Remediation	1. **Restrict Public Access:** ○ **Issue:** API endpoints on ports 6002 and 5002 are publicly accessible. ○ **Mitigation:** Close these ports and restrict access using a firewall or VPN. Ensure sensitive endpoints are not exposed to the public internet. 2. **Implement Strong Authentication and Authorization:** ○ **Issue:** Some endpoints may not require proper authentication. ○ **Mitigation:** Enforce strong authentication mechanisms (e.g., OAuth2, JWT) for all API endpoints, particularly those handling sensitive operations or data. 3. **Introduce Rate Limiting:** ○ **Issue:** Lack of rate limiting makes the API susceptible to brute force and DoS attacks. ○ **Mitigation:** Implement rate limiting and monitoring to control the volume of requests from a single IP address or user over a given period. 4. **Enforce Proper Input Validation:** ○ **Issue:** Insufficient input validation on query parameters could lead to SQL Injection or XSS attacks. ○ **Mitigation:** Validate and sanitize all user inputs rigorously. Use prepared statements for database interactions to prevent SQL injection. 5. **Protect Sensitive Data and Error Messages:** ○ **Issue:** Sensitive data might be exposed through error messages. ○ **Mitigation:** Avoid exposing internal details in error messages. Encrypt sensitive data both at rest and in transit, and mask data in API responses. 6. **Secure Access Tokens:** ○ **Issue:** Potential improper management of access tokens. ○ **Mitigation:** Implement proper token management practices, including secure storage, regular rotation, and limited scope of access tokens. 7. **Implement CORS and CSRF Protections:** ○ **Issue:** Absence of CORS and CSRF protections increases risk of unauthorized requests from other domains.

	○ **Mitigation:** Configure CORS policies to restrict API access to trusted domains and use anti-CSRF tokens to validate request legitimacy. 8. **Utilize VPN for API Access:** ○ **Issue:** Public IP exposure increases vulnerability. ○ **Mitigation:** A VPN can limit API access to authorized users, encrypt data in transit, and hide the API's public IP, reducing the risk of unauthorized access and attacks. **Additional Best Practices:** ● **TLS/SSL Encryption:** Secure all API communications with encryption protocols. ● **Regular Backups and Disaster Recovery:** Ensure regular backups of critical systems and data. Develop a disaster recovery plan to restore operations after data loss or attacks. ● **Comprehensive Security Policies:** Combine these measures with a robust security policy, including regular security reviews and updates. By addressing these vulnerabilities comprehensively, the security posture of the QuickBooks API can be significantly strengthened, mitigating the risk of data breaches and unauthorized access.

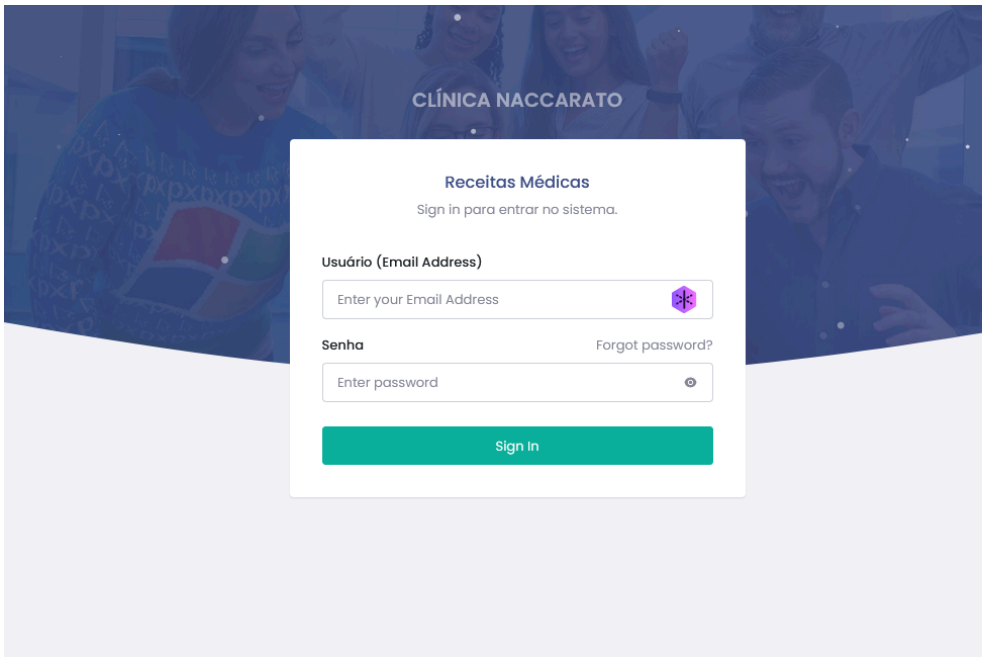
Vulnerability # 21	Findings
Concern	Swagger UI Exposure
Common Weakness Enumeration	CWE-923: Improperly Controlled Creation of Process ('exposing Swagger UI to manipulation') CWE-862: Missing Authorization (if the UI allows manipulation without proper authorization)
Risk Rating	Critical
Description	The Swagger UI interface, which was found to be exposed via open port 6002, significantly enlarges the attack surface of the QuickBooks API. This exposure potentially allows malicious actors to access and manipulate financial data. The open ports (6002 and 5002) not only provide a direct pathway to the API but also expose the Swagger UI, which can be a target for unauthorized access and exploitation.

	
Affected Hosts	123.123.12.1:6002, 123.123.12.1:5002
Remediation	**Immediate Closure of Exposed Ports:** • Close ports 6002 and 5002 to prevent public access. This action will eliminate the direct exposure of the Swagger UI and reduce the risk of unauthorized access and manipulation. **Implement Access Controls for Swagger UI:** • Ensure that access to Swagger UI is restricted and secured through authentication mechanisms. Implement role-based access control (RBAC) to ensure that only authorized personnel can access and interact with the Swagger UI. **Secure and Backup Critical Systems:** • Ensure regular backups of all critical systems and data. Store these backups securely, ideally in an offsite location, to protect against data loss or ransomware attacks. Establish a comprehensive disaster recovery plan that outlines procedures for restoring operations in the event of data loss or a security incident. **Review and Update Security Policies:** • Review and update security policies to include measures for securing API interfaces and management tools like Swagger UI. Incorporate best practices for securing sensitive data and interfaces into your organization's overall security strategy.

UNIDENTIFIED ACTORS

Vulnerability #	Findings

22	
Concern	Unidentified websites hosted on 123.123.12.1
Common Weakness Enumeration	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-610: Externally Controlled Reference to a Resource in Another Sphere CWE-284: Improper Access Control CWE-912: Hidden Functionality CWE-693: Protection Mechanism Failure
Risk Rating	Medium
Description	Ports 8088 and 8090 on IP address 123.123.12.1 are hosting websites that do not appear to be affiliated with F1 International Academy. The existence of these unidentified websites on the same IP address raises several security concerns: 1. **Sensitive Information Exposure:** The presence of unknown websites could potentially expose sensitive information to unauthorized actors, particularly if these sites are misconfigured or inadequately secured. 2. **Resource Segregation Issues:** If these external sites are capable of accessing internal resources, it indicates a possible failure in resource segregation, potentially leading to unauthorized access or control. 3. **Security Risks from Unknown Sites:** Hosting unknown or unauthorized websites on the same IP address increases the risk of unauthorized access, especially if these sites are not secured or monitored properly. 4. **Potential Hidden Functionality:** There is a risk that these websites could harbor hidden functionalities or malicious elements, which could compromise the infrastructure if these sites were not intended to be part of the network. 5. **Failure in Protection Mechanisms:** The unauthorized hosting of these websites suggests possible failures in existing security mechanisms, potentially allowing external entities to deploy and run services on the network without proper authorization.

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Affected Hosts</td><td>123.123.12.1:8088, 123.123.12.1:8090</td></tr>
<tr><td>Remediation</td><td>Immediate Action Required:
Close ports 8088 and 8090 on IP address 123.123.12.1 to prevent any further potential exposure and mitigate associated risks.
Future Prevention:
Use a verified domain address instead of an IP address for hosting purposes to improve security and ensure proper monitoring and management of web services.
Further Investigation:
Conduct a thorough review of network security policies and access controls to ensure that all resources are appropriately segregated and secured.
Monitoring and Securing:
Implement robust monitoring solutions to detect and prevent unauthorized access to all network resources and hosted services.</td></tr>
</table>

Post-Test Actions

The responsibility for addressing and remediating the identified vulnerabilities lies with F1 International Academy's IT department. This includes verifying that remediation efforts have effectively mitigated the risks and scheduling any necessary follow-up tests to confirm the success of these efforts. The penetration testing team may provide additional support and guidance as needed, but the primary responsibility for post-test actions will be managed internally by F1 International Academy.

Post-Test Activity Recommendations:

- **Remediation Validation:** Verifying that all critical and high-severity vulnerabilities have been successfully remediated.
- **Retesting:** Conducting follow-up tests to ensure that previously identified vulnerabilities have been effectively addressed and that no new issues have arisen.
- **Post-Engagement Review:** A debriefing session to review the test's outcomes, discuss lessons learned, and identify areas for improvement in future engagements.

Prioritization and Timeline for Addressing Vulnerabilities

The prioritization of vulnerabilities should be managed by F1 International Academy's IT department, based on the potential impact and urgency of each issue. Critical vulnerabilities should be addressed immediately, with high-severity issues following closely behind. Medium and low severity vulnerabilities can be scheduled for remediation based on available resources and operational considerations. F1 International Academy should establish clear timelines for each category to ensure timely and effective responses.