F1 SCHOOL

PENTEST REPORT

BY: AUBURN, JACOB, LIAN, SARAH, SAM, & SIERRA

DISCLAIMER

All findings including audio, visuals, and details presented have been anonymized. Real names, personally identifiable information (PII), and sensitive data from the pen test have either been hidden, censored, or changed completely.

We have adhered to strict confidentiality and data protection protocols to ensure that all information shared is compliant with our agreement and protects the privacy and security of the business involved.

CLIENT OVERVIEW

F1 School is a small business with a global presence.

The school maintains accreditation to issue F1 visas, which allow foreign students to study in the U.S.

Due to this responsibility, **F1 School** handles sensitive PII such as passports, IDs, and bank account information.

Students are required by law to maintain 80% attendance to keep their visa status.

F1 School must keep attendance records secure and maintain accreditation standards.

SCOPE EXCLUSION

01 Denial of Service Attacks

02 Stored Cross-Site Scripting

03 Persistence Techniques

04 Third-Party Applications/Services

05 Anything leading to data loss, critical system failure, or substantial disruption

Note: These were not tested and therefore remain potentially vulnerable.

METHODOLOGY GRAY BOX

01

RECONNAISSANCE

WHOIS, DNS lookup, port scanning, LinkedIn, certificate information analysis, f1.school and f1school.app.

02

IDENTIFICATION OF VULNERABILITIES AND SERVICES

Response codes, Burp Suite, Metasploit and Routersploit.

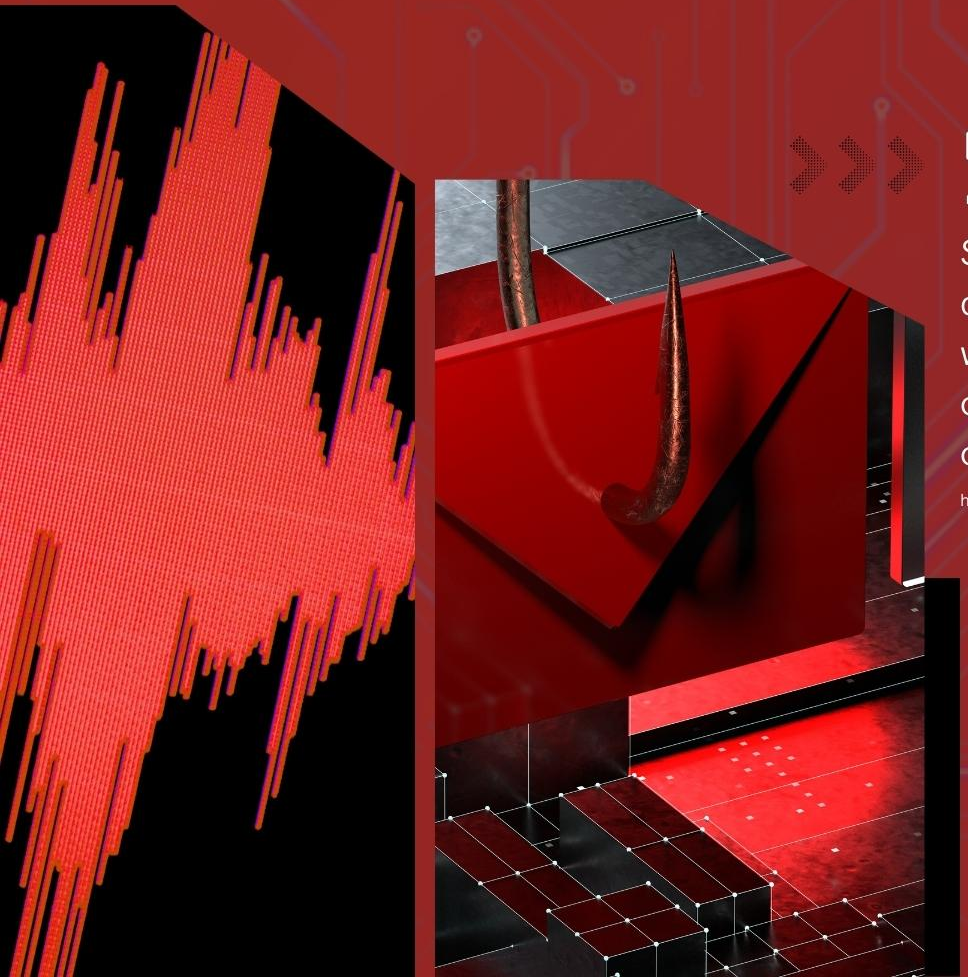
03

VULNERABILITY EXPLOITATION

Manual testing and automated exploitation, internal and external investigation.

OBJECTIVES

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



SOCIAL ENGINEERING

Social engineering attacks manipulate others into sharing confidential information, visiting compromised websites/links, sending money to criminals, or making other mistakes that compromise personal or organizational security.

https://www.ibm.com/topics/social-engineering

ACTIONS ON OBJECTIVE

01 PRETEXTING

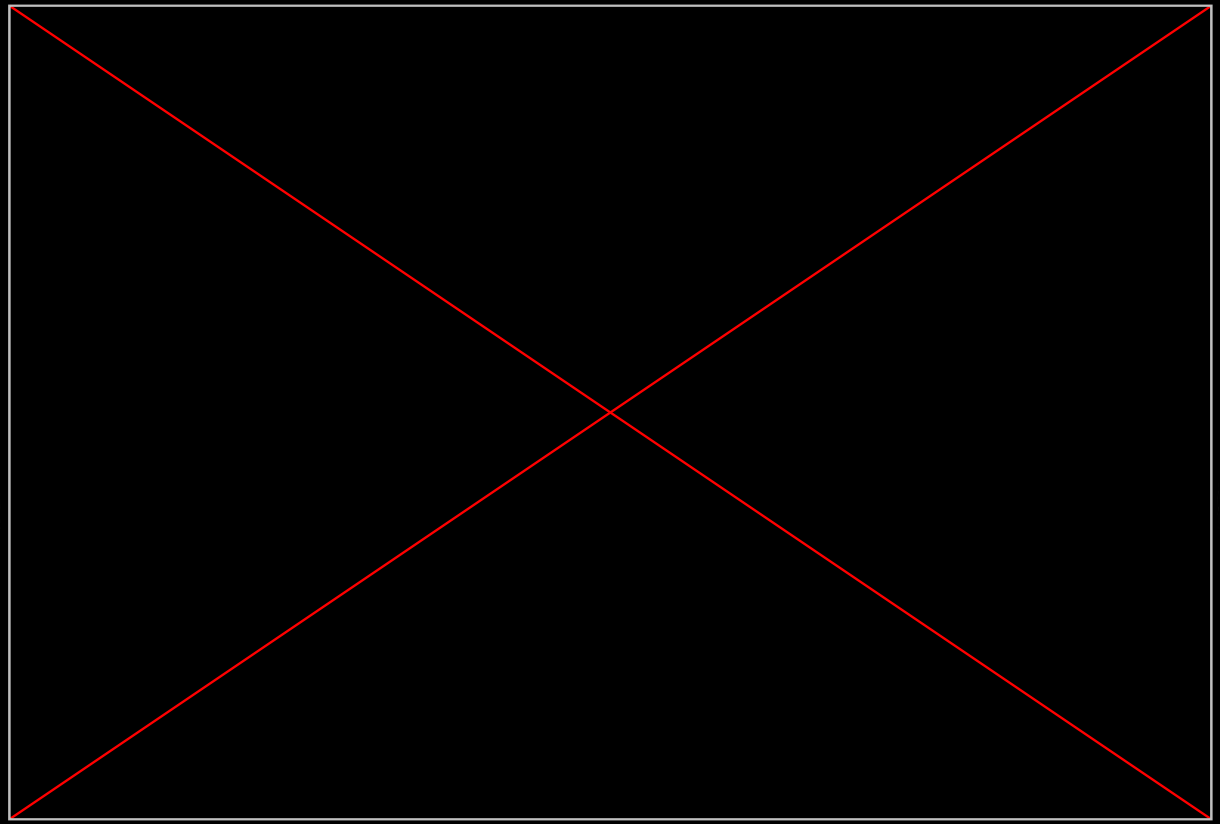
02 PHISHING

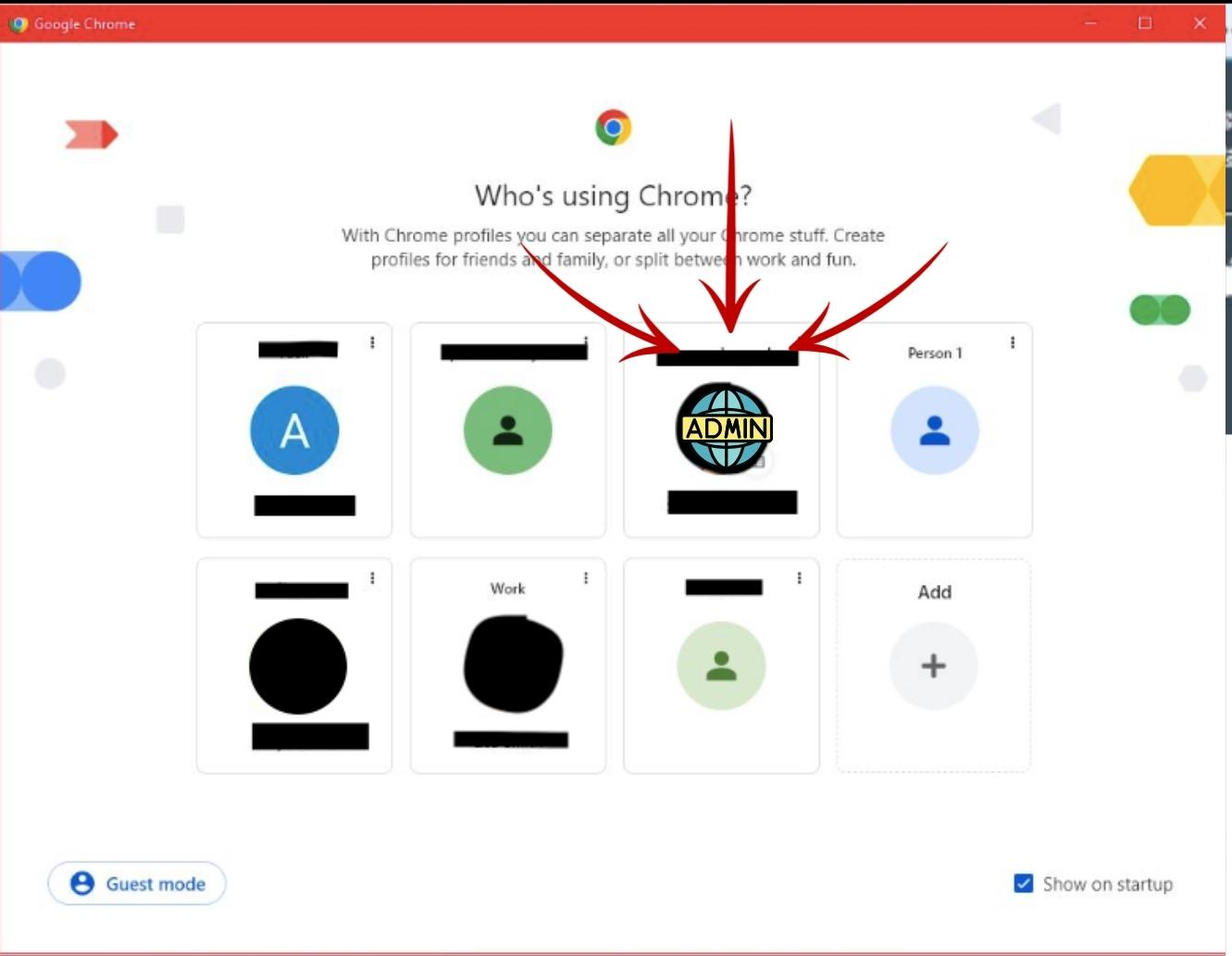
PRETEXTING

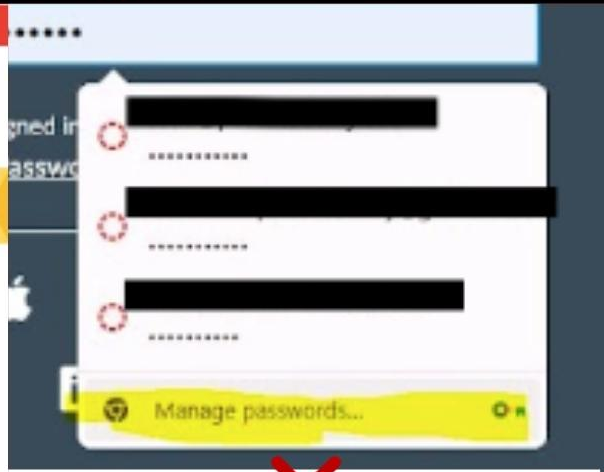
An attacker creates a fake scenario and pretends to be a legitimate source to trick victims into giving away confidential data.

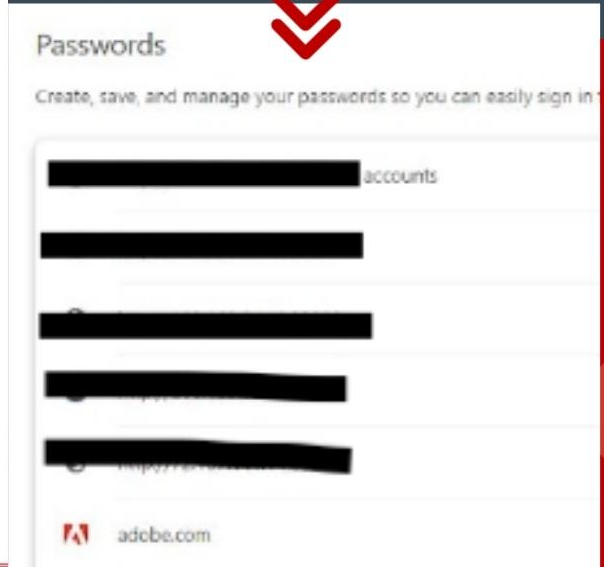
GOAL	PROCEDURES	FINAL RESULT
• Identify on-site vulnerabilities with employee security practices.	• Pose as a new teacher on the first day of class • Request credentials from employees • Record the conversation for evidence-gathering	• This client uses a universal password for all on-site computers; obtained 3/3 times. • Teachers use personal Chrome profiles. • Google Chrome accounts remained always logged in. • Universal password unlocks ALL saved Chrome passwords (bank accounts, 401k, canvas-test banks)

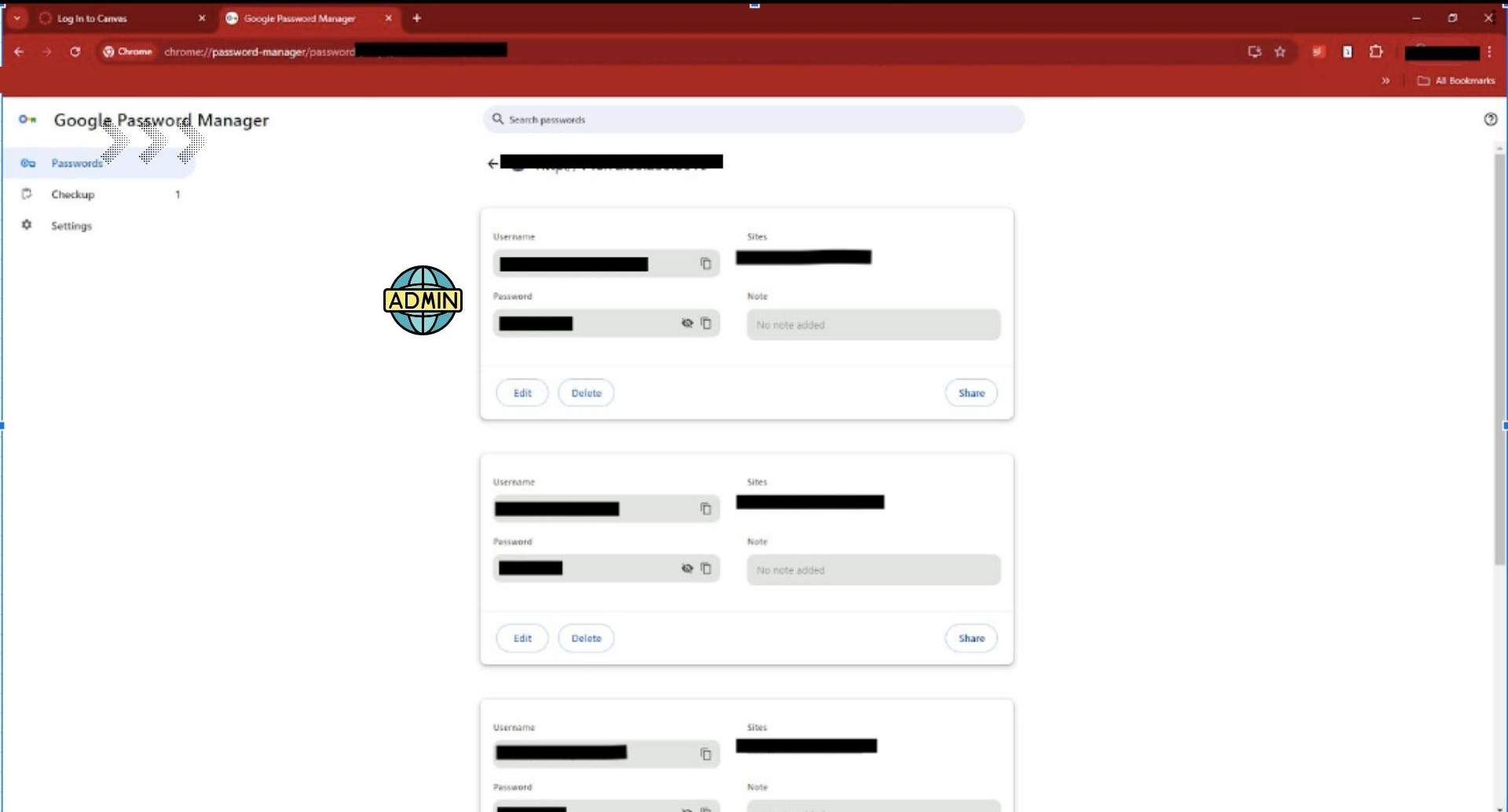
PRETEXTING DEMONSTRATION




Google Chrome
Who's using Chrome?
With Chrome profiles you can separate all your Chrome stuff. Create profiles for friends and family, or split between work and fun.
A
ADMIN
Person 1
Work
Add
Guest mode
Show on startup


Manage passwords...

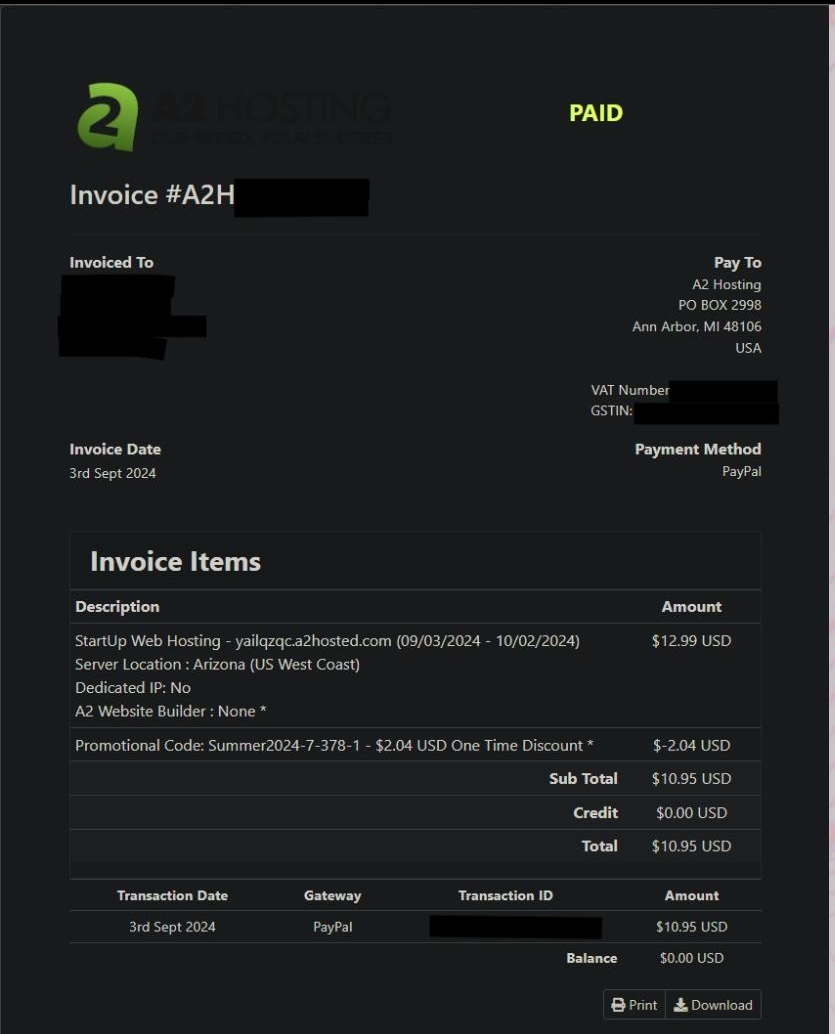

Passwords
Create, save, and manage your passwords so you can easily sign in
accounts
adobe.com


Log In to Canvas
Google Password Manager
Chrome
chrome://password-manager/password
All Bookmarks
Google Password Manager
Search passwords
Passwords
Checkup
1
Settings
ADMIN
Username
Sites
Password
Note
No note added
Edit
Delete
Share
Username
Sites
Password
Note
No note added
Edit
Delete
Share
Username
Sites
Password
Note

PHISHING

The attacker pretended to be one of the staff administrators to send emails letting the employees know about an update on their login portal website.

GOAL	PROCEDURES	FINAL RESULT
• Obtain credentials such as usernames and passwords from employees.	• Duplicate login portal. • Create Web Hosting (A2 Hosting). • Modify website and send emails to the employees.	• Phishing attack successful • Obtained several credentials • Employees use personal information (i.e. names, initials) as passwords.



A2 HOSTING

PAID

Invoice #A2H[redacted]

Invoiced To
[redacted]

Pay To
A2 Hosting
PO BOX 2998
Ann Arbor, MI 48106
USA

VAT Number [redacted]
GSTIN: [redacted]

Invoice Date
3rd Sept 2024

Payment Method
PayPal

Invoice Items

Description	Amount
StartUp Web Hosting - yailqzqc.a2hosted.com (09/03/2024 - 10/02/2024) Server Location : Arizona (US West Coast) Dedicated IP: No A2 Website Builder : None *	$12.99 USD
Promotional Code: Summer2024-7-378-1 - $2.04 USD One Time Discount *	$-2.04 USD
Sub Total	$10.95 USD
Credit	$0.00 USD
Total	$10.95 USD

Transaction Date	Gateway	Transaction ID	Amount
3rd Sept 2024	PayPal	[redacted]	$10.95 USD
		Balance	$0.00 USD

Print Download

Invoice Date
3rd Sept 2024

Attack Date
5th Sept 2024

Amount
$10.95 USD

We purchased a domain and web server from a popular hosting site (A2 Hosting). The company had not purchased any domain besides its main one, so we were able to obtain

<company-name>.net

New Login Portal!

From admin[redacted]et
To [redacted] 12 more...
Date Today 07:00

Summary Headers Plain text

F1 School
Big News!

Just in time for the new semester, [redacted] has finally updated our login portal!

Our new login portal retains the same minimalist design we're all familiar with
while incorporating a more streamlined login process.

Moving forward, Admins and Instructors will both use the link below to access the Login Portal.
The home page of the login portal will let you choose whether you are an instructor or an administrator.
Click your appropriate role to be directed to your corresponding login page!

New Login Portal

If you run into any issues, be sure to click the link provided on each login page first.

If that doesn't resolve your issue, reply to this email and our IT team will assist you as soon as possible.

We hope this new update makes your work just a little bit easier!

From all of us at [redacted] we thank you for your hard work and look forward to an incredible semester!

NEW ATTENDANCE LINK YAY!

From [redacted].net
To [redacted]
[redacted], 5 more...
Date Today 07:09

Summary Headers Plain text

Hey, everyone! I hope you had a great first day!

[redacted] put out a fancy, new **Attendance Link** (called **Login Portal now!**):
https://[redacted].net

No more crazy numbers!! Yay!!

It's **still the same email and password**, with a slightly new design. If this doesn't work, or you **notice any issues that need fixing**, please submit them to the **same Google form link from yesterday**:
https://forms.gle/[redacted]

Let's finish up this week **STRONG!** You **GOT THIS!!**

--
[redacted]
Academic Coordinator
[redacted].net

"If you change the way you look at things, the things you look at change."
-Wayne Dyer

f1school.net/instructor-login.php

F1 School
Instructors

Welcome to [redacted]
Sign in to start your session.

email@domain.com

enter your password

Sign In

I forgot my password

Having trouble? Click here

Not secure 8010

F1 School
instructors

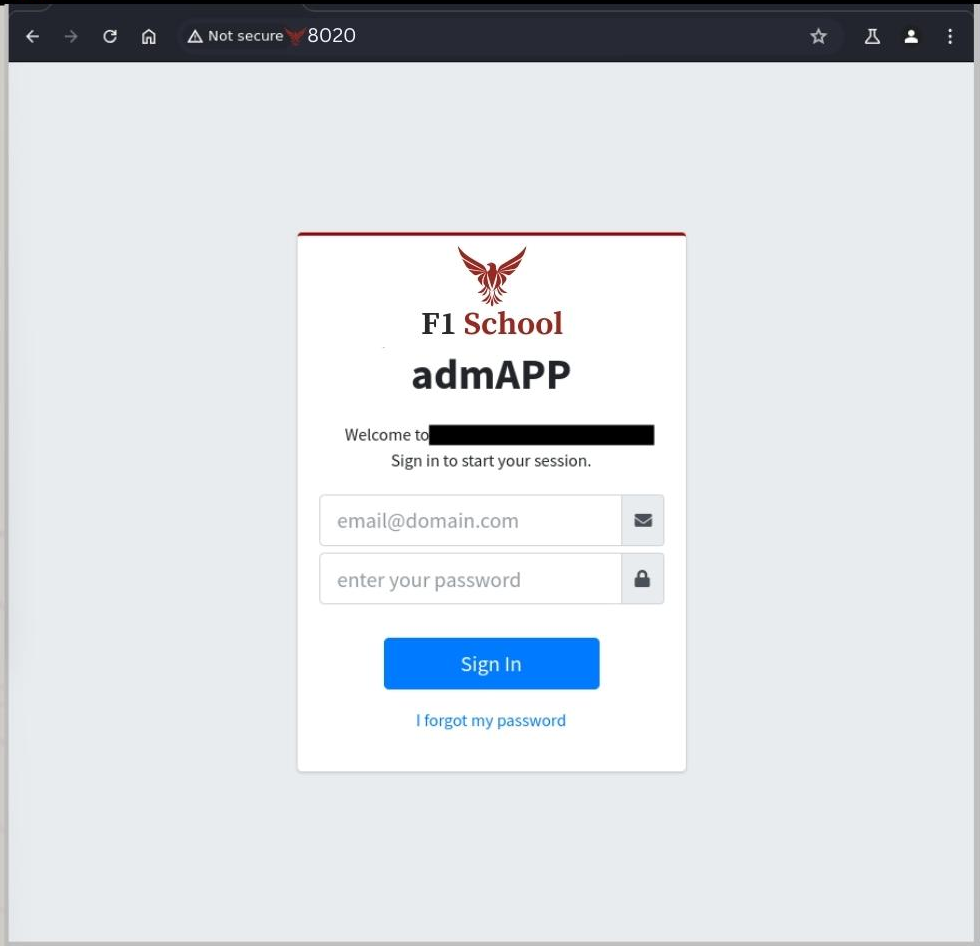
Welcome to [redacted]
Sign in to start your session.

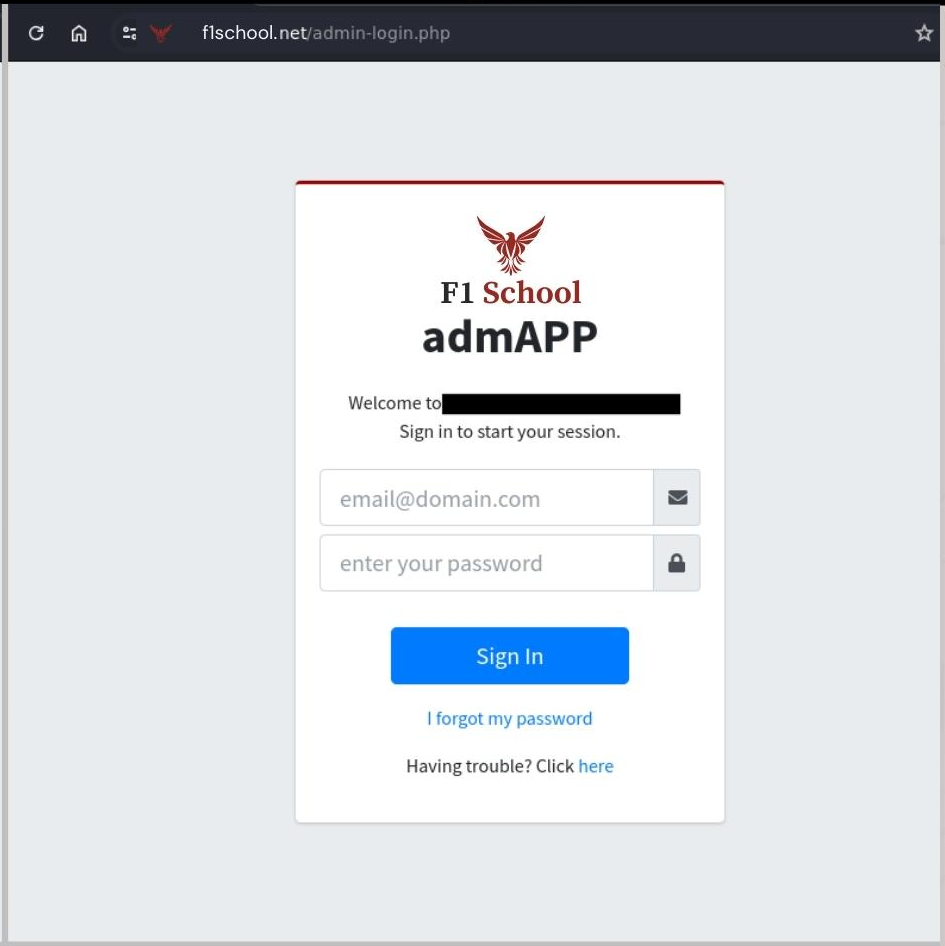
email@domain.com

enter your password

Sign In

I forgot my password


Not secure 8020
F1 School
admAPP
Welcome to [redacted]
Sign in to start your session.
email@domain.com
enter your password
Sign In
I forgot my password


f1school.net/admin-login.php
F1 School
admAPP
Welcome to [redacted]
Sign in to start your session.
email@domain.com
enter your password
Sign In
I forgot my password
Having trouble? Click here

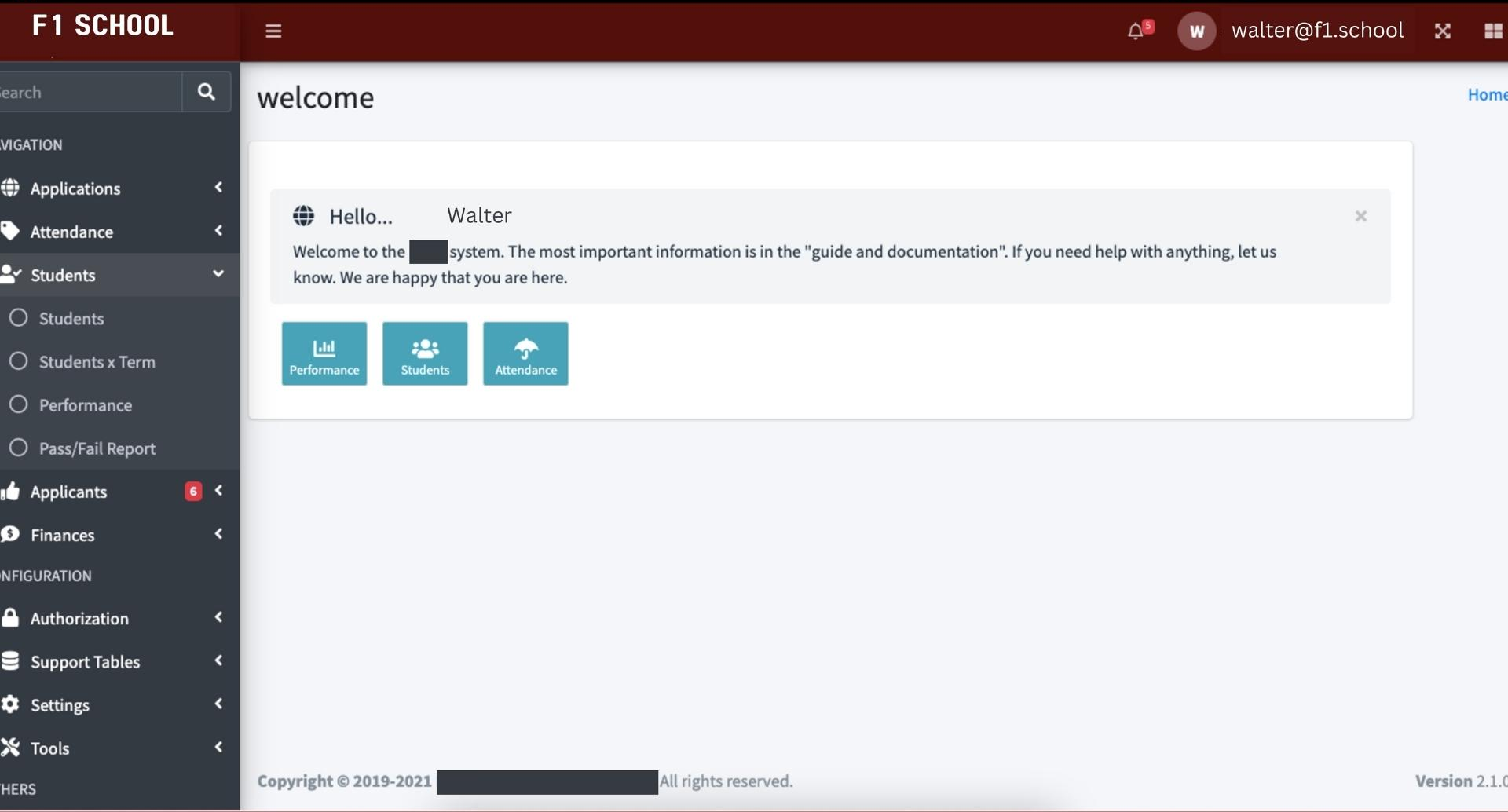
data.csv (ASCII text, with CRLF, LF line terminators)

```
Role,Email,Password
Instructor,c                .com,
Instructor,c                .com,
Instructor,c                .com,
Instructor,s                edu,
Instructor,o                com,
Admin,k              com,
Admin,k              com,
Instructor,a                com,
Instructor,,
Instructor,a                com
Admin,k              edu,
Instructor,a              com,
Instructor,a                com,
Instructor,o                com,
Instructor,o                com,
Instructor,o                com
Instructor,a                com
Instructor,a                com,
Instructor,o                com
Instructor,a                com
Instructor,o                com
Instructor,a                com
Instructor,a                com,
Instructor,o                com,
Instructor,a                com
Instructor,o                com
Instructor,a                com
Instructor,o                com,
Instructor,a                com
Instructor,a                com,
Instructor,o                com,
Instructor,a                com,
Instructor,a                com,
Instructor,a                com,
Instructor,a                com,
Instructor,,
Instructor,a                com,
Instructor,a                com,
Instructor,a                com,
Instructor,c                om,
Instructor,s                com,
Instructor,s                com,
Instructor,s                com
```

ADMINISTRATIVE SYSTEMS

01 OPERATIONAL EFFICIENCY

02 UNAUTHORIZED DATA ACCESS


F1 SCHOOL
walter@f1.school
Search
VIGATION
Applications
Attendance
Students
Students
Students x Term
Performance
Pass/Fail Report
Applicants
6
Finances
NFIGURATION
Authorization
Support Tables
Settings
Tools
HERS
welcome
Home
Hello... Walter
Welcome to the [redacted] system. The most important information is in the "guide and documentation". If you need help with anything, let us know. We are happy that you are here.
Performance
Students
Attendance
Copyright © 2019-2021 [redacted] All rights reserved.
Version 2.1.0

F1 SCHOOL

walter@f1.school

Search

NAVIGATION

- Applications
  - Courses
  - Instructors
  - Terms
  - Calendars
- Attendance
- Students
- Applicants 6
- Finances

CONFIGURATION

- Authorization
- Support Tables
- Settings
- Tools

OTHERS

Instructors

Home / Instructors / In

INDEX

create | refresh | download

	I...	LastNa...	FirstNa...	Email	Phone	Blocked	
	fil	filter...	filter...	filter...	filter...		
edit	1	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	2	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	3	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	4	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	5	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	6	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	7	[redacted]	[redacted]	[redacted]	[redacted]	☐	delete
edit	8	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	9	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete
edit	10	[redacted]	[redacted]	[redacted]	[redacted]	☐	delete
edit	11	[redacted]	[redacted]	[redacted]	[redacted]	☑	delete

javascript:;

F1 SCHOOL

walter@f1.school

Search

NAVIGATION

- Applications
  - Courses
  - Instructors
  - Terms
  - Calendars
- Attendance
- Students
- Applicants 6
- Finances

CONFIGURATION

- Authorization
- Support Tables
- Settings
- Tools

Instructors

Home / Instructors / In

INDEX

create refresh

Computed Properties
Name: "delete"
aria-labelledby: Not specified
aria-label: Not specified
Contents: "delete"
~~title: "1"~~
Description: "1"
Role: gridcell
Read-only: false
Required: false

	I...	Last	Blocked	
edit	1		☑	delete
edit	2		☑	delete
edit	3		☑	delete
edit	4		☑	delete
edit	5		☑	delete
edit	6		☑	delete
edit	7		☐	delete
edit	8		☑	delete
edit	9		☑	delete
edit	10		☐	delete
edit	11		☑	delete

javascript:;

F1 SCHOOL

walter@f1.school

Search

NAVIGATION

- Applications
- Attendance
- Students
- Applicants 6
- Finances

CONFIGURATION

- Authorization
  - Users
- Support Tables
- Settings
- Tools

OTHERS

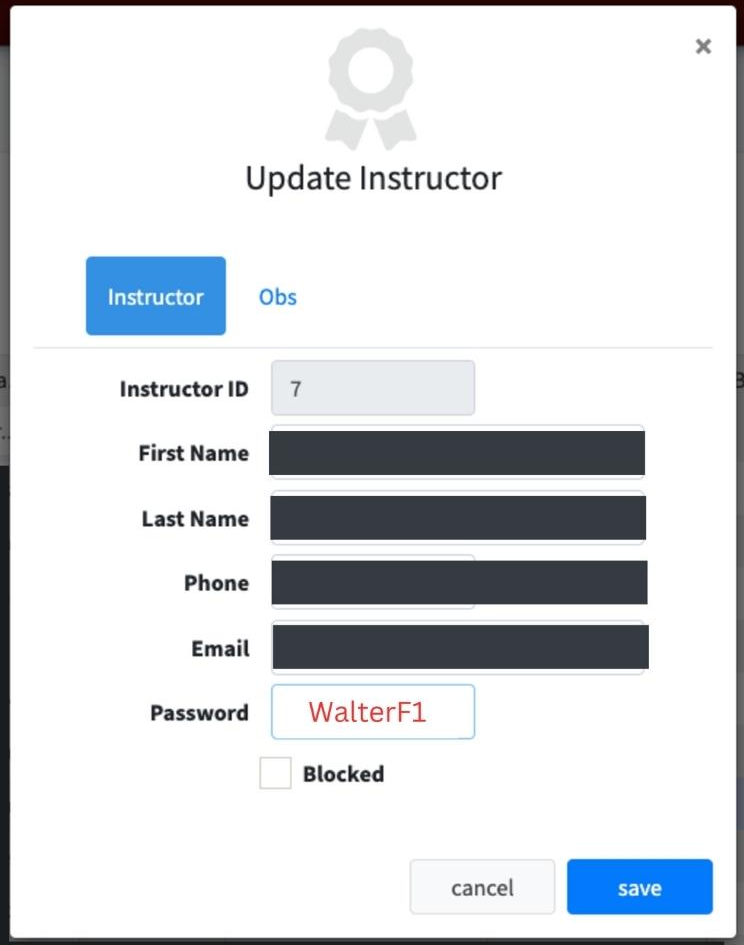
- Documentation

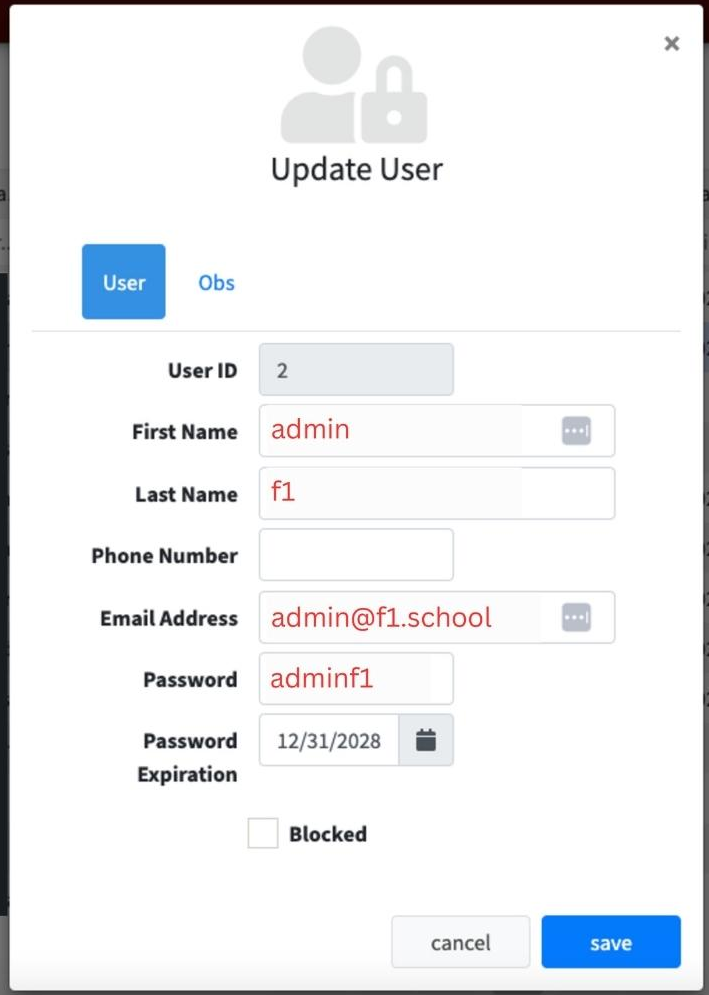
create | refresh | download

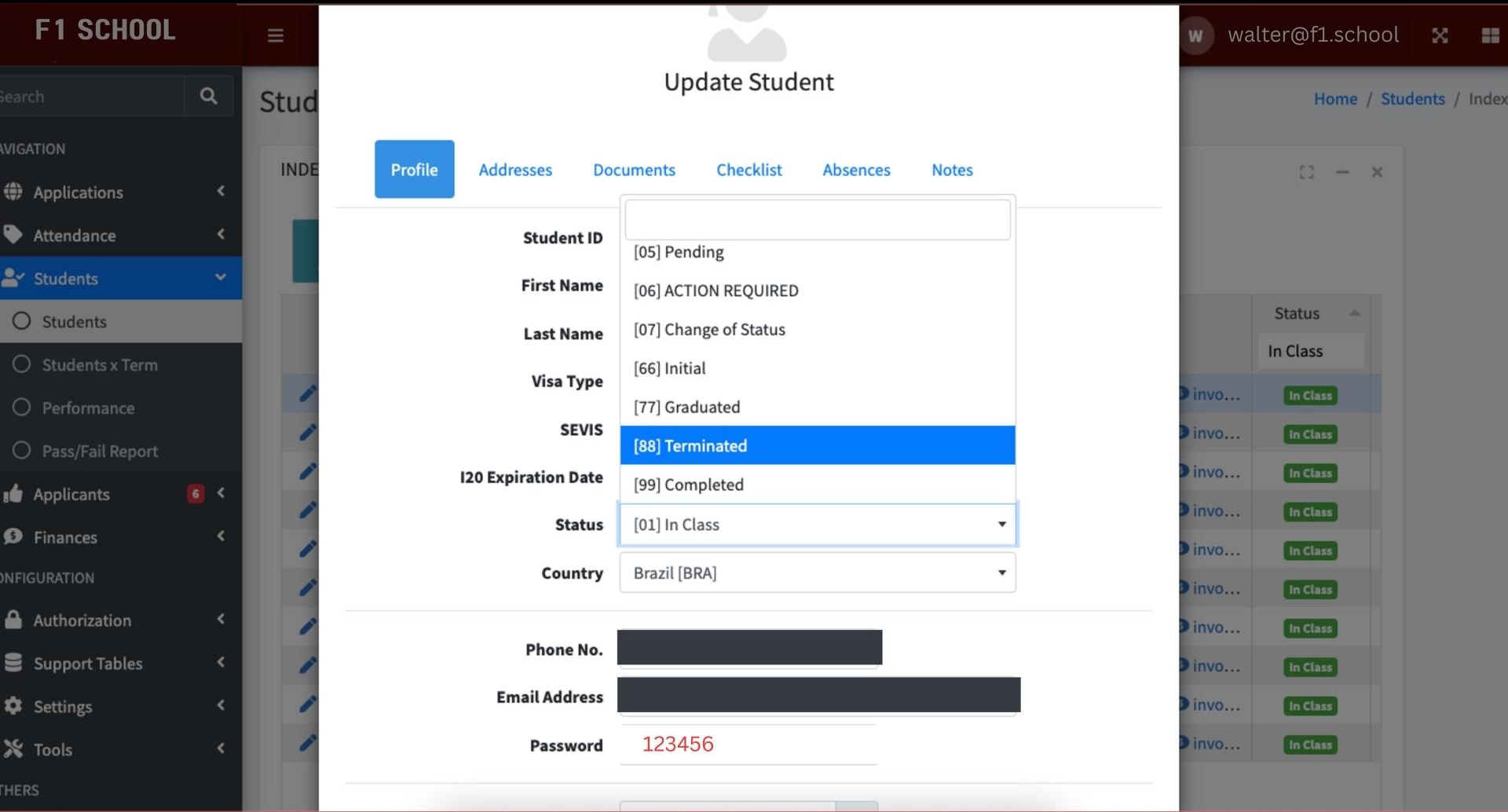
	U…	LastNa…	FirstNa…	Email	Phone	LastLogin		
	fil	filter...	filter...	filter...	filter...	filter...		
edit	1	[redacted]	[redacted]	[redacted]		2022-09-25 …	ACTIVE	delete
edit	2	[redacted]	[redacted]	[redacted]		2022-09-22 …	ACTIVE	delete
edit	3	[redacted]	[redacted]	[redacted]	[redacted]		ACTIVE	delete
edit	5	[redacted]	[redacted]	[redacted]			ACTIVE	delete
edit	6	[redacted]	[redacted]	[redacted]		2022-09-13 …	ACTIVE	delete
edit	8	[redacted]	[redacted]	[redacted]		2022-01-09 …	ACTIVE	delete
edit	9	[redacted]	[redacted]	[redacted]		2022-02-16 …	ACTIVE	delete
edit	10	[redacted]	[redacted]	[redacted]	[redacted]	2022-09-22 …	ACTIVE	delete
edit	11	[redacted]	[redacted]	[redacted]		2022-05-26 …	ACTIVE	delete
edit	12	[redacted]	[redacted]	[redacted]	[redacted]		ACTIVE	delete
edit	13	[redacted]	[redacted]	[redacted]	[redacted]		BLOCKED	delete
edit	14	[redacted]	[redacted]	[redacted]			ACTIVE	delete
edit	15	[redacted]	[redacted]	[redacted]	[redacted]		ACTIVE	delete

Page Size All | First | Prev | 1 | Next | Last

13 rows


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


F1 SCHOOL
walter@f1.school
Home / Students / Index
Update Student
Profile
Addresses
Documents
Checklist
Absences
Notes
Student ID
First Name
Last Name
Visa Type
SEVIS
I20 Expiration Date
Status
Country
[05] Pending
[06] ACTION REQUIRED
[07] Change of Status
[66] Initial
[77] Graduated
[88] Terminated
[99] Completed
[01] In Class
Brazil [BRA]
Phone No.
Email Address
Password
123456
Status
In Class
Applications
Attendance
Students
Students x Term
Performance
Pass/Fail Report
Applicants
Finances
Authorization
Support Tables
Settings
Tools

F1 SCHOOL

walter@f1.school

Home / Attendance / Index

- Applications
- Attendance
- Calculator
- Students
- Applicants 6
- 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

Tardies	Abse...	% Curre
0	12	90
1	65	44
4	21	81
4	21	81
5	17	84
0	0	0
0	0	0
0	0	0
0	0	0
1	23	80

F1 SCHOOL

walter@f1.school

Home / Students / Inde

Update Student

Profile | Addresses | Documents | Checklist | Absences | Notes

+ Add new File

	Description	Date	
open file	Divorce Decree	2024-04-11 14:31:22	delete
open file	I-20/ 23-2024/ Bank statement	2023-05-08 16:47:34	delete
open file	F23 Doctor's Note	2023-11-09 16:39:56	delete
open file	F23 Doctor's Note	2023-12-04 10:57:13	delete
open file	I-20 2025 / F2 dependents / Bank statem…	2024-04-09 17:40:34	delete
open file	F23 Doctor's Note	2023-11-20 19:48:51	delete
open file	I-20 2023 / Dependents I-20	2022-05-16 15:12:08	delete
open file	Medical Semester Note for W24	2024-01-10 16:40:45	delete
open file	F23 Doctor's Note	2023-11-15 10:50:12	delete
open file	Transcripts 2	2022-05-09 12:55:44	delete
open file	F23 Doctor's Note	2023-09-26 13:56:54	delete
open file	Transcripts	2022-05-09 12:55:21	delete

cancel save

Applications
Attendance
Students
Students
Students x Term
Performance
Pass/Fail Report
Applicants 6
Finances
Authorization
Support Tables
Settings
Tools

Status
In Class

PASSPORT INFORMATION

Attention - Please, Information as it appears on Passport.

Surname/Last Name [redacted]

Given Name/First Name [redacted]

Gender (•) Male ( ) Female

Date of Birth [redacted]

Country of Birth Brazil

Country of Citizenship Brazil

Passport Number [redacted]

Upload Passport — Copy of the passport page with your photo and information. Acceptable uploads are **jpg** or **pdf** files of **5MB or less**.

[redacted] PASSPORT_0000000007.jpg

General | Address | Passport | Emergency | Dependent | Financial

EMERGENCY CONTACT INFORMATION

First Name [redacted]

Last Name [redacted]

Relationship Parent

Email Address [redacted]

Phone [redacted]

format: +XXX (999) 999-9999 ..

- Please **agree to continue** .

☑ The data is correct and the invoice for payment will be created.

← Back to Financial

Save and Continue →

FINANCIAL SYSTEMS

01 DATA BREACH

02 FINANCIAL FRAUD

General Address Passport Emergency
Dependent Financial

FINANCIAL INFORMATION

For how many semesters do you want your I-20?

1 semester only

			Surname	Given Name	A
1		[redacted]	[redacted]	[redacted]	

- Please agree to continue .

The data is correct and the invoice for payment will be created.

Back to Financial

Save and Continue

Applicant Type Transfer

General Address Passport Emergency Dependent
Financial Payment Status

FINANCIAL INFORMATION

For how many semesters do you want your I-20?

Semester

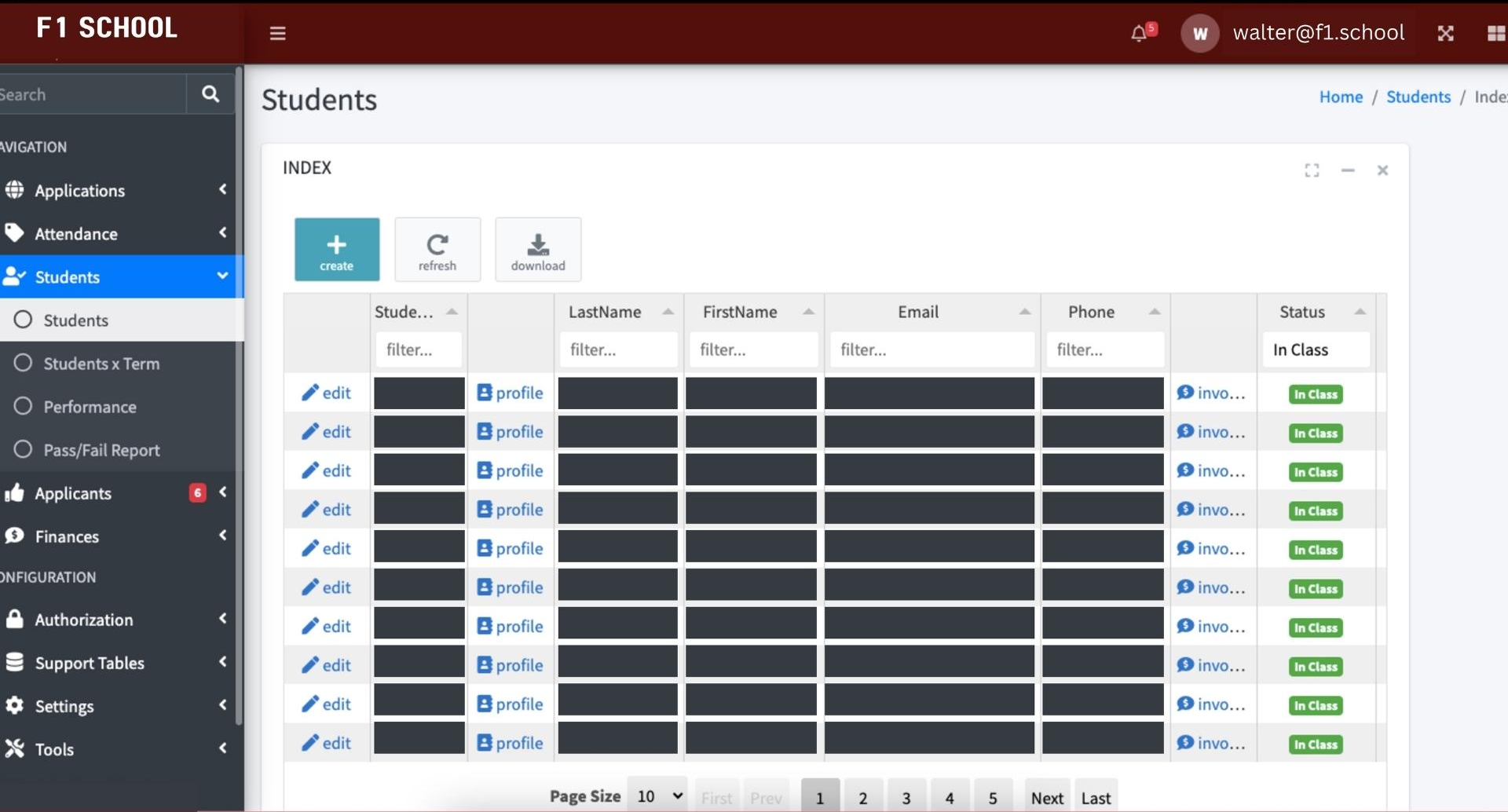
SPONSOR AMOUNT

$5,227.97

					Surname
1				[redacted]	[redacted]

Add sponsor

Close Save Changes


F1 SCHOOL
walter@f1.school
Search
AVIGATION
Applications
Attendance
Students
Students
Students x Term
Performance
Pass/Fail Report
Applicants
6
Finances
ONFIGURATION
Authorization
Support Tables
Settings
Tools
Students
Home / Students / Inde
INDEX
create
refresh
download
Stude...
LastName
FirstName
Email
Phone
Status
filter...
In Class
edit
profile
invo...
In Class
Page Size
10
First
Prev
1
2
3
4
5
Next
Last

INTUIT quickbooks

Sign in

BALANCE DUE

$150.00

Looking for a way to pay? We can let [redacted] know you're not sure how.

Yes, let them know | No thanks

[redacted]

Invoice [redacted]
Due date
Invoice amount
Status

View invoice

Merchant details
Email [redacted]

[redacted]

[redacted]

TRUSTe Certified Privacy

Information is protected and kept confidential

Feedback

PORT SCANNING

Is a common technique to discover open doors or any weak point and services available in a network device, use to find open ports and figure out whether those network devices are sending and receiving data from.

ACTIONS ON OBJECTIVE

01 Find any other vulnerable open port.

02 Look for any domain, host names and response code.

```
sysadmin@vm-image-ubuntu-dev-1:~$ nmap -Av [redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-03 01:16 UTC
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:16
Completed NSE at 01:16, 0.00s elapsed
Initiating NSE at 01:16
Completed NSE at 01:16, 0.00s elapsed
Initiating NSE at 01:16
Completed NSE at 01:16, 0.00s elapsed
Initiating Ping Scan at 01:16
Scanning [redacted]2 ports]
Completed Ping Scan at 01:16, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:16
Completed Parallel DNS resolution of 1 host. at 01:16, 0.01s elapsed
Initiating Connect Scan at 01:16
Scanning [redacted]ost.secureserver.net [redacted]1000 ports]
Discovered open port 443/tcp on [redacted]
Discovered open port 80/tcp on [redacted]
Discovered open port 3306/tcp on [redacted]
Discovered open port 53/tcp on [redacted]
Discovered open port 3389/tcp on [redacted]
Discovered open port 5002/tcp on [redacted]
Discovered open port 7001/tcp on [redacted]
Discovered open port 8000/tcp on [redacted]
Discovered open port 5001/tcp on [redacted]
Discovered open port 6002/tcp on [redacted]
Discovered open port 8088/tcp on [redacted]
Discovered open port 8010/tcp on [redacted]
Discovered open port 8090/tcp on [redacted]
Completed Connect Scan at 01:16, 4.04s elapsed (1000 total ports)
Initiating Service scan at 01:16
Scanning 13 services on [redacted].host.secureserver.net [redacted]
```

// TAGS: database self-signed

// LAST SEE

General Information

Hostnames	[redacted]:app [redacted]:app [redacted]secureserver.net
Domains	[redacted]APP SECURESERVER.NET
Country	United States
City	Phoenix
Organization	GoDaddy.com, LLC
ISP	GoDaddy.com, LLC
ASN	AS398101

Open Ports

53 80 443 3306 3389 5001 6002 8000

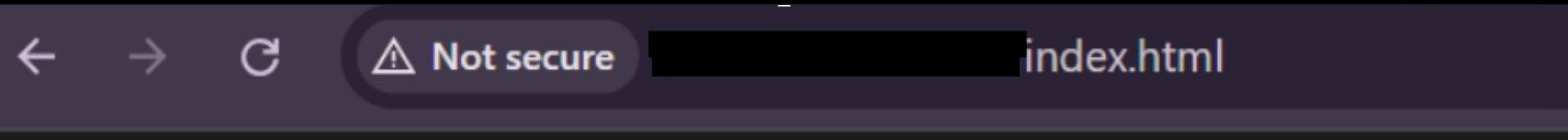
8050 8060 8088 8090 33060

// 53 / TCP -553166942 | 2024-08-2

```
Recursion: enabled
```

// 53 / UDP -553166942 | 2024-08-1

```
Recursion: enabled
```



Swagger
Supported by SMARTBEAR

[redacted]Services.QBO v1 OAS3

[redacted].json

This Api will be responsible for QuickBooks services.

[redacted] - Website
Send email to [redacted]

CRITICAL MITIGATIONS

01 **Principle of Least Privilege**
Employees should only be granted the minimum level of access necessary to perform their job functions effectively.

02 **Strong Password Policies**
User passwords need to be complex, long (12 to 14 characters in length), and unique.
Note: NIST recommends against password rotation policies.

03 **Basic Cybersecurity Training**
Employees need to be trained regularly in basic cybersecurity, such as recognizing phishing attempts, not sharing passwords, and reporting anything suspicious.

VPN 04 05 Logs

MEET OUR TEAM

SARAH HILL

SAMANTHA SUND

LIAN CHANCAY

JACOB COLLINGS

AUBURN BERTUCCINI

SIERRA MILLER