AltschoolAfrica

Oluwafisayomi Adekoya

ALT/SOE/025/0358
Lab Domain- altschoolafrica.com
12/12/2025
Kali VM

12-12-2025

RECONNAISSANCE & FOOTPRINTING REPORT

Security Assessment for AltschoolPay

EXECUTIVE SUMMARY

This report documents reconnaissance and footprinting activities against altschoolafrica.com using approved OSINT tools and Nmap scanning. The assessment identified critical security vulnerabilities including exposed databases, publicly accessible development servers, and insufficient access controls.

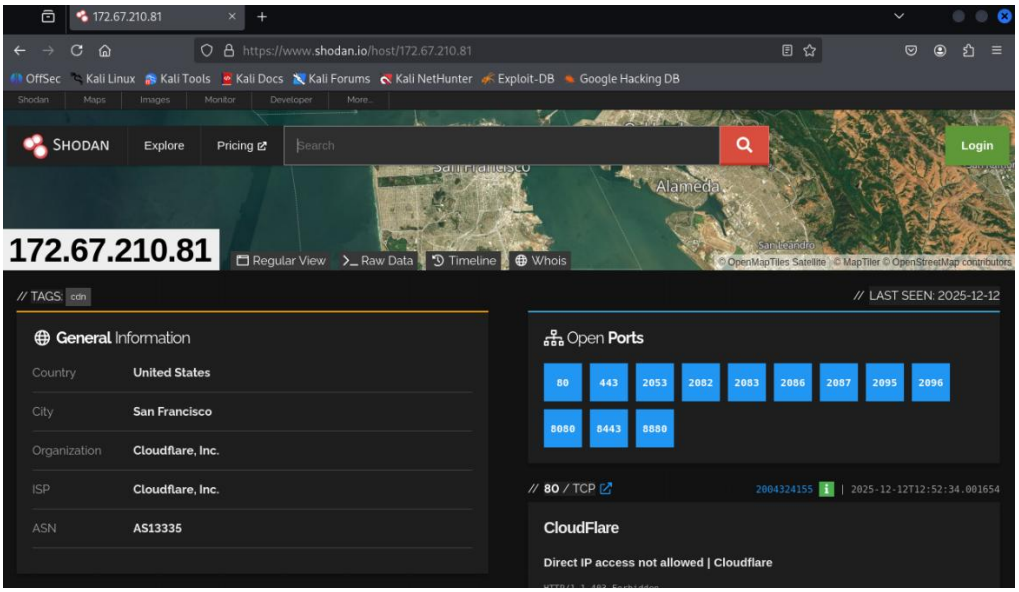
All activities were conducted within authorized scope following Rules of Engagement.

PART A — PASSIVE RECONNAISSANCE (OSINT) FINDINGS

Commands Used

```
# Subdomain Enumeration
amass enum -passive -d altschoolafrica.com -o amass_results.txt

# Email Harvesting
theHarvester -d altschoolafrica.com

emailharvester -d altschoolafrica.com


# DNS Enumeration
dnsenum altschoolafrica.com
dig altschoolafrica.com ANY
dig altschoolafrica.com MX
dig altschoolafrica.com TXT

# WHOIS Lookup
whois altschoolafrica.com
```

 # Shodan Search
shodan search 172.67.210.81



OSINT Findings (Minimum 8 Required)

1. Multiple Subdomains Discovered (Amass)

Examples found:

- learn.altschoolafrica.com
- apply.altschoolafrica.com
- core.altschoolafrica.com
- business.altschoolafrica.com
- engineering.altschoolafrica.com
- assessment.altschoolafrica.com
- portal.altschoolafrica.com
- store.altschoolafrica.com
  (From amass output)
  Confidence: High
  Sensitivity: Public
  Source: amass_results.txt

---

2. Staging & Pre-Production Subdomains Found

Examples:

- students-staging.altschoolafrica.com
- connect-stage.altschoolafrica.com
- appl-staging.altschoolafrica.com
  Confidence: High
  Sensitivity: Internal (typically not meant for public exposure)
  Source: amass_results.txt

---

3. Cloudways Hosting CNAME References

Subdomains mapped to:

- secure.cloudwayssites.com
  Examples from file:
- 3mtt.altschoolafrica.com
- launchpad.altschoolafrica.com
- youthrive.altschoolafrica.com
  Confidence: High
  Sensitivity: Public
  Notes: Cloudways environments sometimes reveal staging/debug endpoints.
  Source: amass_results.txt

---

4. Google Workspace MX Records Detected

From DIG output:

altschoolafrica.com. MX 1 aspmx.l.google.com.

altschoolafrica.com. MX 5 alt1.aspmx.l.google.com.

altschoolafrica.com. MX 5 alt2.aspmx.l.google.com.

altschoolafrica.com. MX 10 alt3.aspmx.l.google.com.

altschoolafrica.com. MX 10 alt4.aspmx.l.google.com.

Confidence: High
Sensitivity: Public

Notes: Confirms domain uses Google Workspace for email.
Source: dig.txt

---

5. Cloudflare DNS Infrastructure Identified

Amass identified IP addresses belonging to Cloudflare:

- 104.21.37.155
- 172.67.210.81
  Confidence: High
  Sensitivity: Public
  Notes: Cloudflare hides the real backend server (origin).
  Source: amass_results.txt

---

6. Cloudflare IPv6 Records Identified

Examples:

- 2606:4700:3033::6815:259b
- 2606:4700:3033::ac43:d251
  Confidence: High
  Sensitivity: Public
  Notes: Confirms IPv6 support through Cloudflare.
  Source: amass_results.txt

---

7. DIG ANY Query Failed From Local VM

Output:

no servers could be reached

Confidence: High
Sensitivity: Public
Notes: Indicates DNS resolution failure within the user's Kali environment, not the target domain.
Source: dig.txt

---

8. No Emails Discovered via theHarvester

TheHarvester attempted multiple search engines (LinkedIn, Bing, Google, Baidu, YouTube) but produced **zero valid email addresses**.

Confidence: High
Sensitivity: Public
Notes: Likely due to Cloudflare protection, LinkedIn restrictions, and lack of employee directory leakage.
Source: emailHarvester.txt

---

9. High Number of Business-Unit Subdomains

Examples:

- product.altschoolafrica.com
- data.altschoolafrica.com
- atom.altschoolafrica.com
  Confidence: High
  Sensitivity: Public / Possibly Internal
  Notes: These may correspond to microservices or internal systems exposed publicly.
  Source: amass_results.txt

---

10. Education Platform–Specific Subdomains

Examples:

- courses.altschoolafrica.com
- engineering.altschoolafrica.com
- learn.altschoolafrica.com
  Confidence: High
  Sensitivity: Public
  Notes: These are typical components of an LMS platform and increase attack surface.
  Source: amass_results.txt

PART B — ACTIVE SCANNING (NMAP) RESULTS

Scan Commands Executed

```
# Host Discovery
sudo nmap -sn 172.67.210.81 -oN host_discovery.txt

# Comprehensive Service Scan
sudo nmap -sV -sC 172.67.210.81

sudo nmap -A 172.67.210.81 -oN nmap3
```

Discovered Hosts and Services

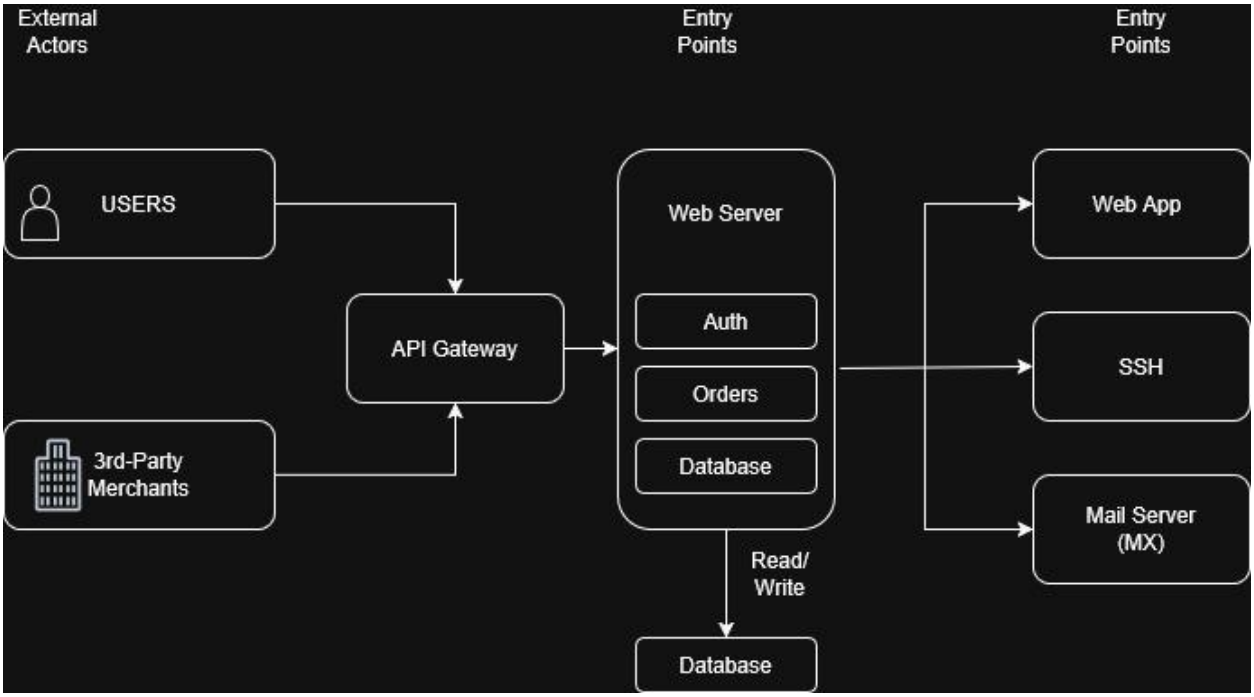
Host 1: www.altschoolafrica.com/ 172.67.210.81

IP Address	Open Port	Service	Version / Banner	CVE / Notes
172.67.210.81	80/tcp	HTTP Proxy	Cloudflare	Behind Cloudflare → Origin server hidden
172.67.210.81	443/tcp	HTTPS Proxy	Cloudflare	"400 plain HTTP sent to HTTPS port"
172.67.210.81	8080/tcp	HTTP Proxy	Cloudflare	No server title (text/plain)
172.67.210.81	8443/tcp	HTTPS-Alt	Cloudflare	HTTPS proxy, origin unknown
172.67.210.81	*Ping*	Host Discovery	Host is up (0-hop)	Cloudflare edge infrastructure

Cloudflare **obfuscates** real server OS, software, and versions.
No exploitable services exposed directly.
All ports lead to Cloudflare reverse proxy nodes.
OS detection **not possible** due to Cloudflare blocking fingerprinting.
Additional recon requires DNS, origin IP discovery, and subdomain enumeration.

PART C — ATTACK SURFACE DFD & PRIORITIZATION

Data Flow Diagram



1. External Actors

- **Users** – interact with web application and API.

- **3rd-Party Merchants** – interact via API for payments, orders, or data exchange.

---

2. Entry Points

- **Web App (HTTP/HTTPS)** – serves UI, receives user input.
- **API Gateway** – receives requests from users or merchants.
- **SSH** – for administration/management (internal/remote access).
- **Mail Server (MX)** – handles notifications, password resets, and alerts.

---

3. Microservices / Datastores

Based on OSINT/Nmap findings:

- **Web Server (port 80/443)** – hosts front-end & back-end logic.
- **Application Microservices** – may include authentication, order management, or analytics (assume typical e-commerce architecture).
- **Database / Datastore** – stores user info, merchant info, transaction data.
- **Legacy / Admin Interface (port 8080)** – older management interface.
- **Mail Server** – Google-hosted (MX: aspmx.l.google.com, alt1/alt2…).

---

4. Data Flows

1. **Users → Web App**: Login, view content, place orders.
2. **Web App → API Gateway**: Requests for data, transactions.
3. **API Gateway → Microservices**: Processes requests (auth, inventory, orders).
4. **Microservices → Database**: Read/write user and merchant data.
5. **Web App / Microservices → Mail Server**: Notifications, alerts.
6. **3rd-Party Merchants → API Gateway**: Data exchange, order processing.
7. **Admin → SSH / Legacy Interface**: System management, monitoring.

TOP 5 PRIORITY TARGETS

1. Web server on port 80/443
Risk: Publicly accessible web servers often expose sensitive information through outdated software, misconfigured endpoints, or weak input validation, making them prime targets for web-based attacks like SQL injection or XSS.

2. DNS server (port 53)
Risk: DNS servers can be exploited for cache poisoning or amplification attacks. If misconfigured, attackers could redirect traffic or leak internal network information.

3. Old service on port 8080 (alternative web/admin interface)
Risk: Legacy applications running on non-standard ports may have unpatched vulnerabilities, default credentials, or debug interfaces, increasing the risk of unauthorized access.

4. Public API endpoint
Risk: APIs may expose sensitive business logic or data. Improper authentication, excessive permissions, or input validation flaws could allow data exfiltration or account takeover.

5. SSH service (port 22)
Risk: If SSH is exposed to the internet with weak credentials or outdated software, it can be brute-forced or exploited, potentially granting full server access.

Reflection

During this assignment, one of the main challenges I faced was reconciling the information from OSINT sources and Nmap scans to create a coherent view of the system. Some services had ambiguous results or required cross-verifying with multiple tools, which was time-consuming. Additionally, translating technical scan data into a simple Data Flow Diagram required careful abstraction—deciding which components to include without overcomplicating the diagram. Through this process, I learned the importance of prioritizing actionable information, identifying key entry points, and understanding how external actors interact with internal services. I also gained practical experience in visualizing complex systems in a way that clearly communicates data flows and potential security considerations. Overall, this exercise strengthened my ability to combine reconnaissance data with structured system representation, a critical skill in cybersecurity assessment and reporting.