CONFIDENTIAL

SECURITY AUDIT REPORT

Federal Republic of Somalia
eVisa System Security Assessment

Target System: immigration.gov.so

Assessment Date: October 2025

Classification: CONFIDENTIAL - GOVERNMENT ONLY

Severity Rating: **CRITICAL**

Security Researcher:
waryaX@proton.me
Somali Security Researcher
Independent Security Assessment

Prepared For:

Federal Government of Somalia

Ministry of Internal Security

Immigration & Naturalization Department

1. Executive Summary

⚠ CRITICAL SECURITY VULNERABILITIES DISCOVERED

This independent security assessment identified critical vulnerabilities in the Somalia eVisa system that allowed unauthorized access to sensitive government data. The system requires immediate security improvements to protect citizen and visitor information.

Assessment Overview

125,000+ Records Accessible	**5** Critical Issues
$795K Transaction Data	**145** Countries Affected

What Was Found

The security assessment revealed that the eVisa system had significant security gaps allowing unauthorized access to:

- **Visa Application Records:** Over 125,000 visa applications with personal details

- **Identity Information:** Names, passport numbers, dates of birth from 145 countries
- **Contact Details:** Thousands of email addresses and phone numbers
- **Biometric Data:** Uploaded photos and passport scans
- **Payment Records:** Financial transaction history totaling $795,000
- **System Access:** Administrative credentials and system configuration

> **Important Note:** This assessment was conducted for security research purposes only. No data was distributed, sold, or used maliciously. All findings are reported to facilitate immediate security improvements.

2. Critical Security Issues

Five critical security vulnerabilities were identified that require immediate attention:

Issue	Severity	Impact
1. System Files Publicly Accessible	**CRITICAL**	Database credentials exposed online
2. Unrestricted File Upload	**CRITICAL**	Allows unauthorized system access
3. Missing Access Controls	**CRITICAL**	Anyone can access visa records
4. Payment System Vulnerabilities	**CRITICAL**	$288K in duplicate charges detected
5. Weak Authentication	**HIGH**	Administrative accounts at risk

Issue 1: System Files Publicly Accessible

Problem: Critical system files containing database passwords and security keys were accessible to anyone on the internet without any password or authentication.

Risk: Complete access to the visa database and all stored information.

Issue 2: Unrestricted File Upload

Problem: The system allows users to upload any type of file without proper validation, including malicious code.

Risk: Unauthorized individuals can gain complete control of the system.

Issue 3: Missing Access Controls

Problem: Visa records can be accessed by simply changing numbers in the web address - no authentication required.

Risk: Anyone can view any approved visa application.

Issue 4: Payment System Vulnerabilities

Problem: The payment system lacks proper validation, resulting in duplicate charges and potential fraud.

Financial Impact: Analysis shows $287,808 in duplicate payment charges affecting 1,519 customers.

Issue 5: Weak Authentication

Problem: Administrative accounts and system access lack strong security controls.

Risk: Unauthorized access to system management functions.

3. Data Accessibility Scope

The assessment determined that the following types of information were accessible without authorization:

Data Category	Approximate Volume	Sensitivity Level
Visa Applications	125,000+ records	**CRITICAL**
Passport Information	34,000+ records	**CRITICAL**
Email Addresses	27,000+ addresses	**HIGH**
Phone Numbers	123,000+ numbers	**HIGH**
Biometric Photos	20,000+ images	**CRITICAL**
Payment Transactions	12,400+ transactions	**CRITICAL**
Database Tables	73 tables	**CRITICAL**

International Impact

The visa system processes applications from 145 countries worldwide, including:

- International organization personnel (UN, NGOs)
- Foreign government officials
- Business travelers
- Humanitarian workers
- Diplomatic personnel

High-Value Targets Identified

⚠️ Sensitive Personnel Data Exposed

Email addresses and personal data of **167 high-profile individuals** from international organizations were accessible, including:

Organization	Email Count	Sample Email Addresses
United Nations	71 individuals	***@un.org, ***@unicef.org, ***@unops.org
UK Government (FCDO)	24 individuals	***@fcdo.gov.uk, ***@mod.uk
International NGOs	56 individuals	Various humanitarian organizations
German Development (GIZ)	16 individuals	Development cooperation personnel

Security Risk: These individuals' travel patterns, passport details, photos, and contact information were fully accessible. This creates significant operational security risks for international personnel working in Somalia.

4. Server Infrastructure Details

Hosting Location

Critical Finding: The Somalia eVisa system is hosted on servers physically located in the United States, not in Somalia.

Component	Details
Server IP Address	50.28.8.86
Physical Location	Tampa, Florida, United States
Hosting Provider	Liquid Web, L.L.C
Provider Location	Lansing, Michigan, USA
Server Type	Shared Hosting (cPanel/WHM)
Operating System	RedHat Enterprise Linux 9.6

Infrastructure Concerns

Data Sovereignty Issues:

- All Somalia citizen and visitor data is stored on US-based servers
- Subject to US jurisdiction and legal access requirements
- Shared hosting environment (multiple websites on same server)

- No apparent data residency controls

Technical Configuration

- **Web Server:** Apache with cPanel control panel
- **PHP Version:** 8.1.33
- **Database:** MariaDB 10.6.23
- **Framework:** CodeIgniter 4
- **CDN:** Cloudflare (provides some DDoS protection)

5. Payment System Findings

Financial Data

Payment Gateway: Mastercard Payment Gateway Services (MPGS)

Total Transactions Processed: 12,413

Total Revenue: $794,432

Standard Visa Fee: $64 USD

Critical Payment Issues Identified

Issue	Impact	Financial Risk
Duplicate Payment Processing	1,519 payment IDs charged multiple times	$287,808
No Payment Verification	System doesn't verify with Mastercard	High
Missing Fraud Detection	No monitoring for suspicious transactions	High
No Rate Limiting	608 rapid-fire transactions detected	Medium

Duplicate Payment Issue

Analysis identified 1,519 customers who were charged multiple times for the same visa application, totaling $287,808 in potential overcharges. This occurred due to lack of duplicate payment prevention in the system.

> **Example Pattern:** Some payment IDs were charged 3-4 times instead of once, meaning customers paid $192-$256 instead of the standard $64 fee.

Revenue Analysis by Country

Top contributing countries to eVisa revenue (payment data analysis):

Rank	Region/Country Category	Percentage
1	East Africa Region	75%
2	Middle East	10%
3	Other Regions	15%

6. Recommended Immediate Actions

> ⚠️ **URGENT: These actions should be completed within 24-48 hours**

Priority 1: Remove Security Exposures (Within 24 Hours)

Action 1: Remove or restrict access to system configuration files

- Move sensitive files outside web-accessible directories
- Change all exposed passwords immediately
- Review and secure all system files

Action 2: Fix file upload security

- Implement strict file type validation
- Scan uploaded files for malicious content
- Store uploads in secure location

Action 3: Add access controls to visa records

- Require authentication to view visa applications
- Use non-predictable identifiers for records

- Implement proper authorization checks

Priority 2: Secure Payment System (Within 1 Week)

Action 4: Fix duplicate payment issue

- Implement payment ID uniqueness checks
- Add duplicate transaction prevention
- Review affected transactions for refunds

Action 5: Enable payment verification

- Verify all payments with Mastercard gateway
- Implement server-side amount validation
- Add fraud detection monitoring

Priority 3: Strengthen System Security (Within 2 Weeks)

Action	Purpose	Timeline
Reset all admin passwords	Prevent unauthorized access	Immediate
Enable security logging	Monitor for suspicious activity	1 week
Deploy web application firewall	Block malicious requests	2 weeks
Conduct full security audit	Identify any remaining issues	1 month

Action	Purpose	Timeline
Implement encryption	Protect sensitive data at rest	1 month

7. Long-Term Security Recommendations

System Security Improvements

- **Security Training:** Provide security awareness training for development and operations teams
- **Secure Development:** Implement secure coding practices and regular code reviews
- **Regular Testing:** Conduct periodic security assessments and penetration testing
- **Incident Response:** Develop and practice data breach response procedures
- **Compliance:** Align with international data protection standards

Infrastructure Upgrades

- **Modern Security Tools:** Deploy intrusion detection and prevention systems
- **Data Encryption:** Encrypt sensitive information in database and during transmission
- **Backup Systems:** Implement secure backup and disaster recovery
- **Network Segmentation:** Separate database and application servers
- **Access Management:** Implement role-based access controls

Payment System Enhancements

- **PCI Compliance:** Achieve Payment Card Industry security standards

- **Fraud Prevention:** Deploy automated fraud detection systems
- **Transaction Monitoring:** Real-time monitoring of payment activities
- **Alternative Methods:** Add secure mobile money and bank transfer options
- **Regular Reconciliation:** Automated payment reconciliation with gateway

8. Conclusion

> **Assessment Summary**
>
> This independent security assessment identified critical vulnerabilities in the Somalia eVisa system that require immediate attention. The issues discovered are fixable with proper security implementation and ongoing monitoring.

Key Points

1. **Critical Security Gaps:** The system currently has significant security vulnerabilities that allow unauthorized access to sensitive data.
2. **Data Protection:** Over 125,000 visa application records, including personal information from 145 countries, were accessible without proper authorization.
3. **Payment Issues:** The payment system lacks proper safeguards, resulting in $287,808 in duplicate charges and potential for fraud.
4. **Immediate Action Required:** Security improvements must be implemented urgently to protect citizen and visitor information.
5. **Achievable Solutions:** All identified issues can be resolved through standard security practices and proper system configuration.

Path Forward

The Federal Government of Somalia should:

- Form an emergency response team to address immediate security issues
- Engage qualified security professionals to implement recommended fixes
- Allocate resources for both immediate remediation and long-term security improvements

- Establish ongoing security monitoring and assessment programs
- Consider temporary system shutdown if immediate fixes cannot be implemented

> **Researcher Note:** This assessment was conducted independently by a Somali security researcher to help improve the security of government systems. All findings are reported in good faith to facilitate prompt security enhancements.
