NYU Login Portal

Threat Model & Security Analysis

Sample Engineering Documentation

By: Michael Kazarian

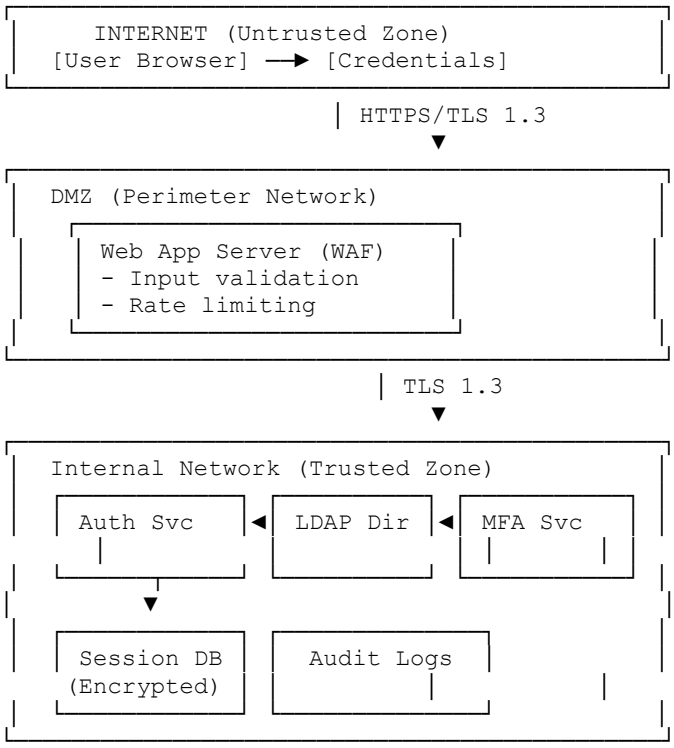
Document Version: 1.0
Date: February 3, 2026

Executive Summary

This document provides a comprehensive threat model for the NYU login portal, a critical authentication gateway serving over 60,000 students, faculty, and staff. The analysis identifies 18 potential distinct threat scenarios across six STRIDE categories, with particular focus on high-severity risks including credential theft, session hijacking, and authentication bypass attacks.

1. Data Flow Diagram (DFD)

DATA FLOW DIAGRAM - NYU LOGIN PORTAL



1.1 Trust Boundaries

1. 1. Internet to DMZ: External users accessing the login portal
2. 2. DMZ to Internal Network: Web application to backend services
3. 3. Internal Services: Authentication, directory, and session management

2. STRIDE Threat Analysis

Category	Threat	Impact	Potential Risk
Spoofing	Phishing attacks mimicking NYU login page	Credential theft	**Critical**
	Session token theft via wXSS	Session hijacking	**High**
	SAML assertion forgery	Unauthorized access	**High**
Tampering	SQL injection in auth queries	Data breach	**Critical**
	LDAP injection attacks	Directory compromise	**High**
Denial of Service	Credential stuffing attacks	Service unavailability	**High**
	DDoS attacks on login endpoint	System outage	**High**
Elevation of Privilege	Authentication bypass via parameter manipulation	Unauthorized access	**Critical**
	Weak password policy	Account compromise	**Medium**

3. Risk Register

ID	Risk	Potential Impact	Owner
R-001	Phishing attacks	Critical	Security Team
R-002	SQL injection	Critical	Dev Team
R-003	Auth bypass	Critical	Dev Team
R-004	DDoS attacks	High	Infrastructure

4. Operational Security Guide

4.1 Daily Operations

Monitoring & Alerting

- • Review SIEM dashboard for failed login spikes
- • Monitor WAF block rate (baseline: <2% of traffic)
- • Check SSL certificate expiry (30-day warning)
- • Verify MFA service uptime (99.9% SLA)

4.2 Incident Response

Level	Trigger	Response Time	Escalation
P1 - Critical	Service outage, data breach, auth bypass	15 minutes	CISO + VP IT
P2 - High	Suspected breach, repeated lockouts	1 hour	Security Manager
P3 - Medium	Performance degradation, unusual traffic	4 hours	On-call Engineer

Immediate Actions

4. 1. Isolate affected systems
5. 2. Capture system state (memory dump, network traffic)
6. 3. Preserve audit logs (copy to immutable storage)
7. 4. Initiate communication plan