Check my Vital Signs

Information Systems Security and Management
CS-GY 6803

Our Team

Crystal Dennis
Yiwei Zhang
Michael Duan
Aparajita (Appy) Sinha
Kevin Zhang
Tsung Lin (Jerry) Yang
Zirui (Jimmy) Xu
Geethanjali (Geetha) D
Zhong Zhang

Table of Contents

Objective and Mission Statement

Project Objective

Risk assessment of Vital (NYU's Virtual Lab) Network to identify and address the security gaps within the system.

Mission Statement

A comprehensive analysis of critical security faults present within NYU's Vital virtual machine cloud. Vital's network is used by a collective of students, professors, and faculty researchers as both a teaching and research tool. The Vital network has previously faced issues arising from Availability faults, causing outages for project use and coverage gaps within student curricula.

Stakeholders Overview

NYU Vital: Developing and maintaining group of Vital

- Main point-of-contact: Thomas B. Reddington, tbr226@nyu.edu
- Professor Thomas Reddington is the designer and developer of Vital, also the leader of the current Vital team.

OGC (Office of General Counsel): legal services department of NYU

- Main point-of-contact: Aisha Oliver-Staley, aisha.oliver-staley@nyu.edu
- Aisha Oliver-Staley is the Senior Vice President and head of OGO

Office of the Controller: Finance Representative

- Main point-of-contact: Kerri Tricarico, kerri.tricarico@nyu.edu
- Kerri Tricarico, Senior Associate VP of Financial Operations and University Controller

Department of Computer Science and Engineering:

- Main point-of-contact: Guido Gerig, gerig@nyu.edu
- Guido Gerig, Department Chair and Institute Professor of Computer Science and Engineering

Students and Professors: the customers of Vital

- Damon McCoy (Associate Professor)
- Mantej Rajpal (Adjunct Professor)
- Pete Klabe (Adjunct Professor)

Vital Architecture

Key Components (in terms of security):

Nginx (HTTP web server)

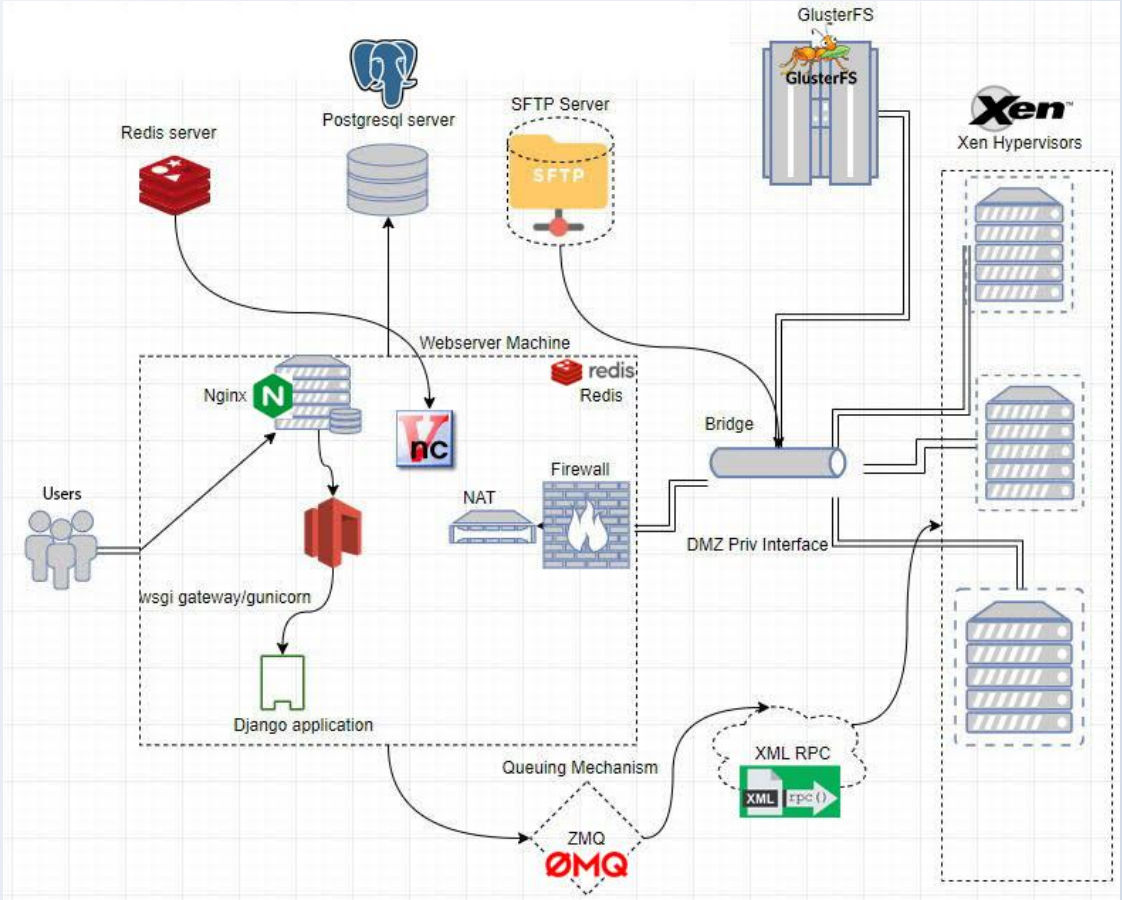
Django (Python web framework)

SFTP (secure file transfer protocol)

GlusterFS (scalable network file storage)

Xen Hypervisor (type-1 virtual machine)

ZMQ (asynchronous messaging with sockets)

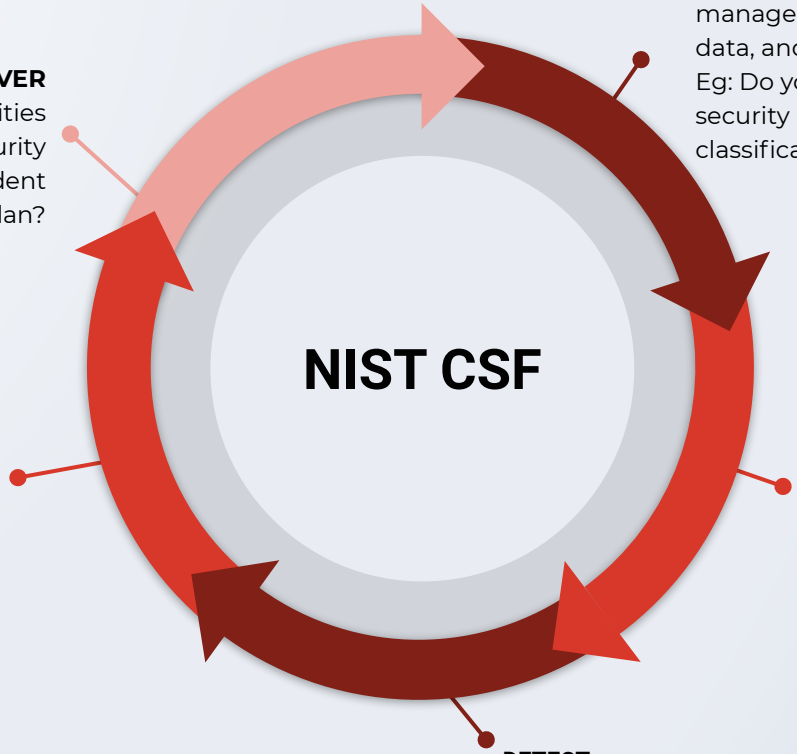


NIST Questionnaire

Our team conducted preliminary risk assessment using NIST CSF checklist categories

IDENTIFY
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Eg: Do you have a well-defined information security policy, data usage policy and data classification policy?

RECOVER
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Eg: Do you have a documented Incident Response plan?



PROTECT
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Eg: Do you use any Identity Access Management tool for your application?

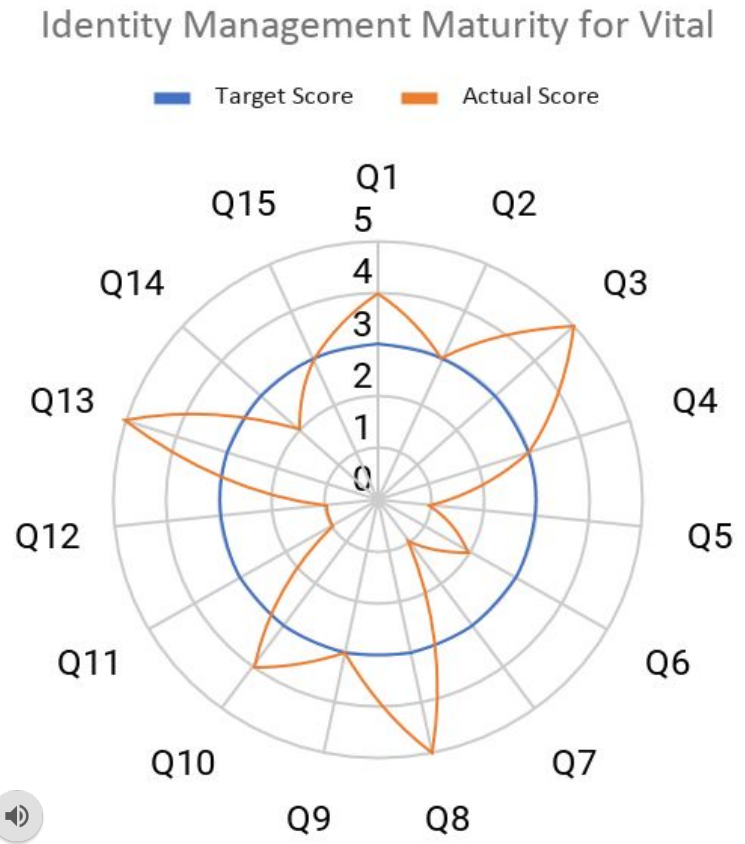
RESPOND
Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Eg: What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like student information

DETECT
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Eg: Have you performed a CIA risk assessment for your application?

Stakeholder Interviews

- **Risk Manager: Professor Thomas Reddington - Professor of Network Engineering**
  - Principal in charge of architecture, maintenance, upkeep, and staffing
  - Difficulty with providing availability access to stakeholders
- **On-site Cyber Security: Christopher Thomas Ng - Senior Lab Administrator**
  - TBD - interview scheduled Friday 4/16
- **On-Site Physical Security: Captain Ronnie West**
  - TBD
- **Educator and Client of Vital: Professor Damon McCoy - Professor of Network Engineering**
  - One of many faculty members who maintain Vital as a critical teaching tool in their curriculum

IAM Maturity Evaluation



- Identity and Access Management Maturity Evaluation calculator
- The tool evaluates an enterprise or corporate institution's Identity and access management.
- The IAM Maturity Evaluation provides increased security levels as it is a comprehensive guide on:
  - Degree of compliance required
  - Risk factors associated with the application/service
- It consists of three major elements:
  - A directory or identity repository of the personal data the systems
  - Tools for logging and monitoring to ensure integrity and audit requirements.
  - Mechanism for enforcing the industry best practices

Identity Management Maturity Assessment of Vital (Sample)

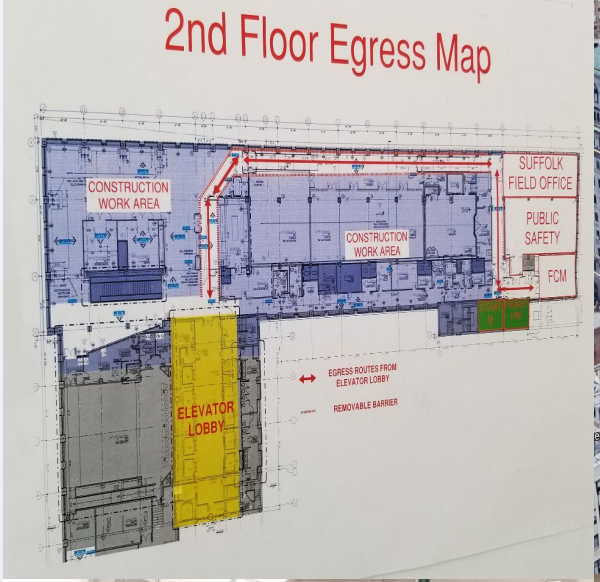
		Actual Score	Target Score	Measurement Levels
1	Do you know where your identities are stored in comparison to your accounts?(Actual Score:4 Target Score:3)	4	3	• No central Identity store. Accounts all locally hosted. No formal documentation in place. • Central ID store for users, but not servers. No formal process for move/add/change/delete. • Central ID store in place with formal, auditable process. • Full integration of all critical devices into a common ID • Full integration of all critical devices into a common ID store. Exceptions less than 1% of monthly workload.
2	Do you have an end-to-end understanding of how users authenticate to workstations,network devices, applications, or non-windows servers?	3	3	• We will be rating this measurement by levels as below: • There is no formal policy governing authentication processes. • Default user authentication to a standard directory. No standard practices for servers and network devices. • Formal requirements exist and are documented. • Machine-to-machine(M2M) service accounts are formally managed • Formal requirements exist are supported via modern infrastructure solutions(SSO/TACAS)
3	Is your Identity/Account Management process well defined, repeatable, and automated?	5	3	• No process exists. All work is ad-hoc. • Standard practices exist, but not formally documented or auditable. • Formal processes exist, are documented, and evidence of adherence can be provided • Formal processes exist, are auditable and have annual attestation campaigns. • Fully auditable and validated process with an exception rate under 1%.
4	Do you have an attestation process in place to identity and resolve accounts with unnecessary access rights?	1	3	• There is no formal attestation process in place. • Informal attestations occur for critical systems • A manual attestation campaign occurs annually for selected systems • Formal, automated attestations occur for critical and financial systems on a regular basis. • Automated attestations occur for critical/Financial systems whenever a user or role change occurs.

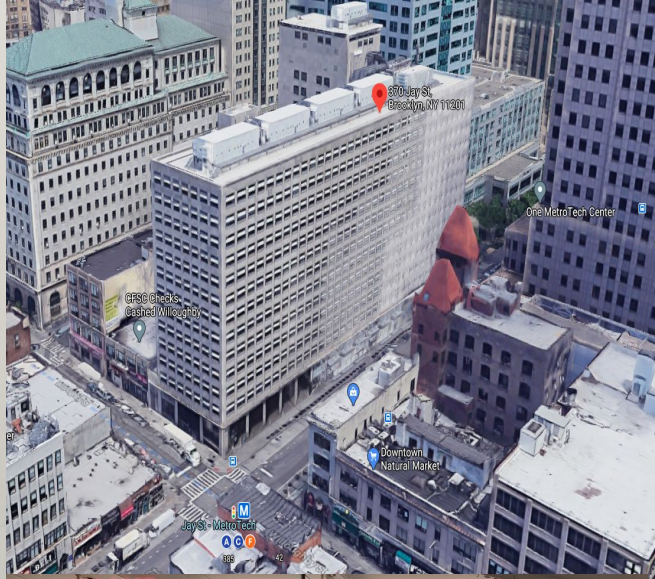
Physical Security Assessment

We have conducted a thorough physical security analysis on the building that contains the Vital server, 370 Jay Street; Brooklyn, NY; 11201.

Our top priorities regarding the building concern the following areas:

- Access Management
- Physical Barriers of Entry
- Wireless security
- Safe Disposal of Assets
- Penetration Tests





Security Scorecard

Custom Scorecard* Overview

Vital 2

52 Security Score

Partition of New York University 

Custom Scorecard*

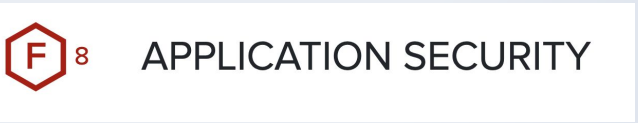
Factors

F	8	APPLICATION SECURITY	14 ISSUES	A 100	IP REPUTATION	0 ISSUES
A	100	CUBIT SCORE	0 ISSUES	A 100	INFORMATION LEAK	0 ISSUES
A	90	DNS HEALTH	1 ISSUE	F 0	NETWORK SECURITY	6 ISSUES
A	100	ENDPOINT SECURITY	0 ISSUES	A 100	PATCHING CADENCE	0 ISSUES
A	100	HACKER CHATTER	0 ISSUES	A 100	SOCIAL ENGINEERING	0 ISSUES

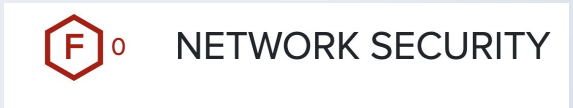
Security Scorecard

High Severity Factors:

- ### Application Security:
  1. Content Security Policy (CSP) Missing (11 findings)
  2. Site does not enforce HTTPS(2 findings)



- ### Network Security:
  1. SSL/TLS Service Supports Weak Protocol (1 finding)



Lightweight Penetration Testing

Objective

We conducted a lightweight penetration testing for the site vital.engineering.nyu.edu, which is a productive website with real customer data. Penetration Testing activities only includes reconnaissance and a limited scanning stage.

Result

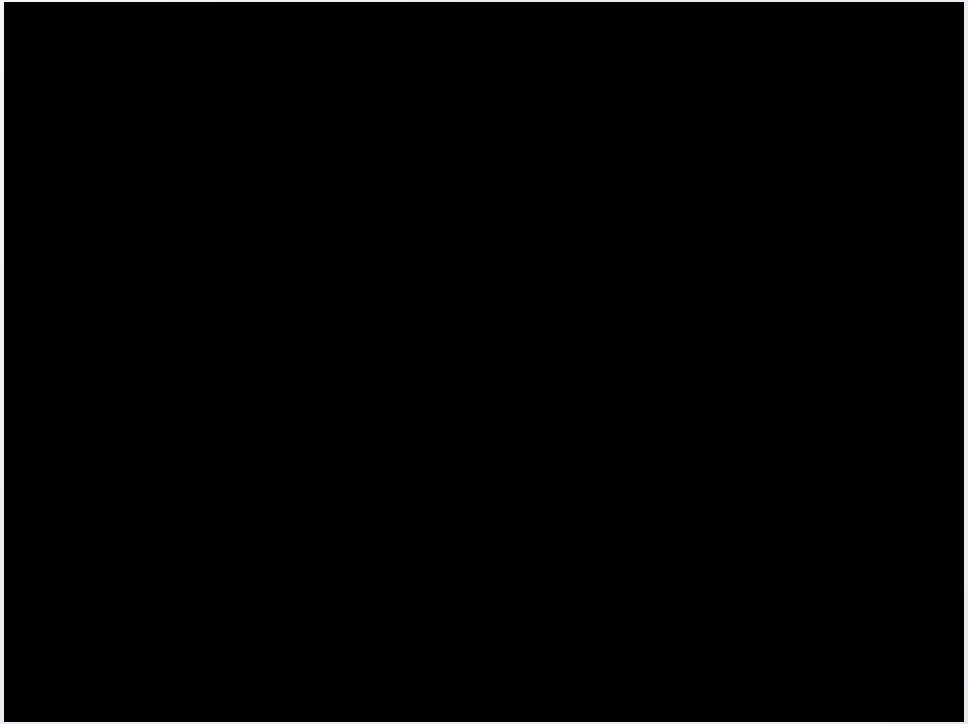
With the limited assessment, we determined the risk score of the vital web application was **Medium**. We identified weak ciphersuites, and some misconfigurations issues with the web application.

Recommendations

Based on the limited testing performed, we recommend the following:

- Managing the certificates in a regular basis
- Implementing secure configurations for all of the headers
- Implementing Http Strict Transport Security
- Reducing the attacking surfaces by removing the unused services and applications

Lightweight Penetration Testing – Process



Lightweight Penetration Testing – Detailed Findings

Classification	Vulnerability Description	Recommendation	Severity
Sensitive Data Exposure	Weak cryptographic algorithms are implemented.	Eliminating the use of the insecure TLS protocol configurations	Medium
Security Misconfiguration	Missing sufficient secure headers	Implementing sufficient secure headers	Medium
Security Misconfiguration	Missing HSTS configuration	Implementing HSTS	Medium
Information Disclosure	Server's version and Sensitive directories are public accessible	Reviewing the findings and making sufficient actions	Low

Analysis

Project Objective

Risk assessment of Vital (NYU's Virtual Lab) Network to identify and address the security gaps within the system.

We have met our objective.

Recommendations

- **Architecture**
  - Review bugs regarding user load and increase scaling
- **IT Governance**
  - Create well-defined incident response plan
- **Interviews**
  - Increase NYU support for Vital
- **Physical Security**
  - Augment security regarding guests, construction, and key building areas
- **SecurityScorecard™**
  - Enhance cipher suites and implement latest TLS/SSL
- **Penetration Testing**
  - Regularly update cryptography and secure configurations

Thank you for your prompt attention!

Questions, Comments, Concerns?
“netID”@nyu.edu