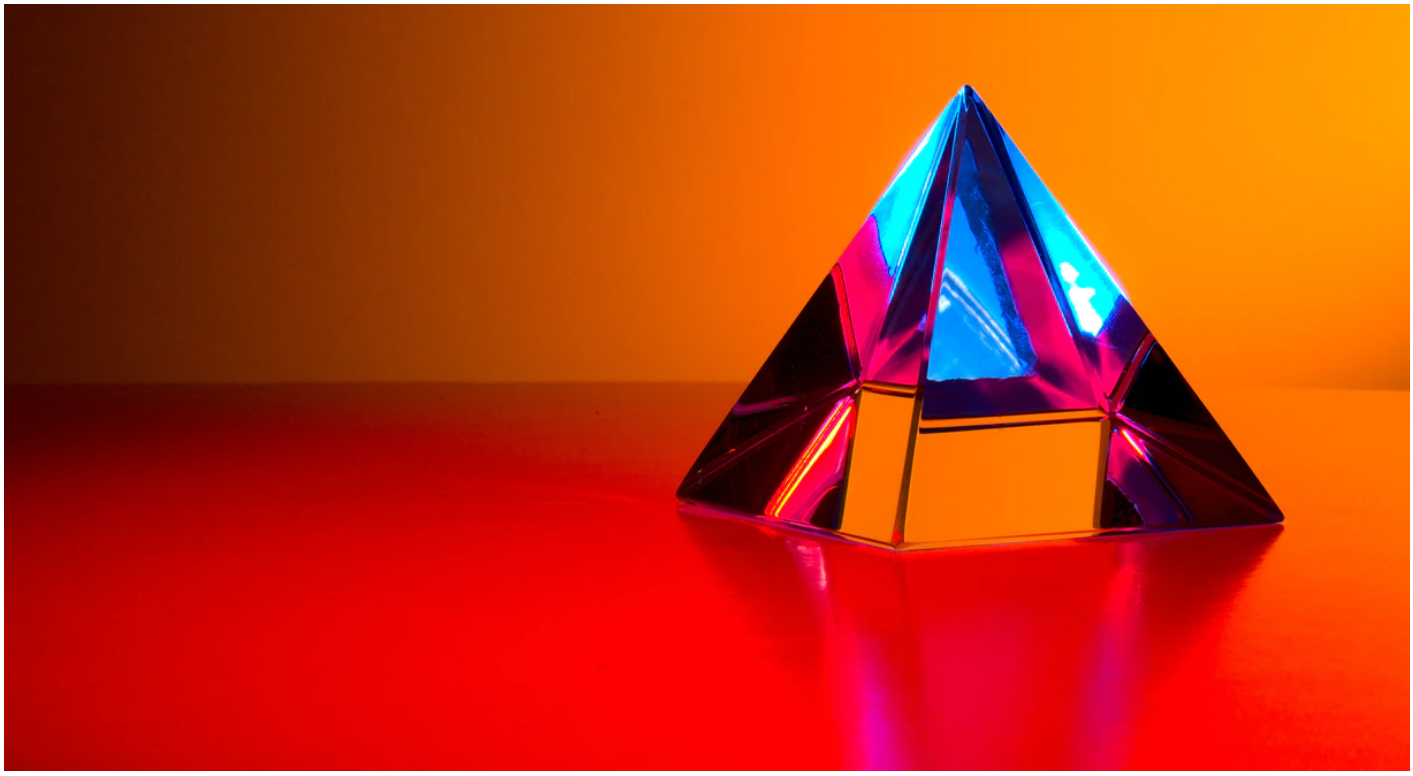
NYU TANDON SCHOOL OF ENGINEERING

Check my Vital Signs: A Security Assessment of NYU's Virtual Lab Platform



Team Vital Signs

CS-GY 6803: Information System Security and Management

Spring 2021

NYU TANDON SCHOOL OF ENGINEERING

Table of Contents

NYU TANDON SCHOOL OF ENGINEERING

Project Objective

To provide a comprehensive risk assessment of Vital (NYU's Virtual Lab) Network in identifying and addressing security gaps within the system.

Mission Statement

Our mission is to identify and correct 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. We hope to draw attention not only to the correctable security and policy gaps, but also the need to increase funding and staffing to better support such a crucial part of NYU's networking curricula.

Team Members

- Aparajita Sinha (as12554)
- Crystal Dennis (cmd9622)
- Geethanjali (Geetha) D (gd2148)
- Michael Duan (md2682)
- Zirui (Jimmy) Xu (zx1002)
- Tsung Lin (Jerry) Yang (ty2065)
- Kevin Zhang (kz519)
- Yiwei Zhang (yz7303)
- Zhong Zhang (zz2431)

NYU TANDON SCHOOL OF ENGINEERING

Information Security Stakeholders

Our team collated a diverse group of stakeholders for Vital in order to better estimate risk, ranging from developers to users. Stakeholders contacted for interviews are listed below in bold, with comments..

1. NYU Vital: the 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.
            - **Our interviews, dated March 5th, 2021 and April 5th, 2021, were focused on the hardware, software, and staffing for Vital.**
2. 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
3. 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
4. Department of Computer Science and Engineering:
    - Main point-of-contact: **Guido Gerig**, gerig@nyu.edu
        - Professor Guido Gerig, Department Chair and Institute Professor of Computer Science and Engineering
            - **Reached out to Professor Gerig on March 18th, 2021. Redirected to Professor Reddington.**
    - Alternate Contacts:
        - Nasir Memon, Vice Dean for Academics and Student Affairs, memon@nyu.edu
        - Torsten Suel, Director of Undergraduate Programs, torsten.suel@nyu.edu
        - Yi-Jen Chiang, Director of the MS Program, chiang@nyu.edu
5. Students and Professors: the customers of Vital
    - Our team will attempt to interview all professors whose courses involve using Vital, in this semester and prior semesters.
    - Spring 2021
        - CS-GY 6823 Network Security
            - **Damon McCoy** Associate Professor mccoy@nyu.edu
                - **Our interview, dated March 26th, 202, was focused on the user experience and curricular impact of Vital.**
            - **Phillip Mak** Adjunct Professor pmak@nyu.edu
                - **Reached out to Professor Mak on March 28th, 2021. Redirected to Professor Reddington.**
        - CS-GY 6573 Penetration Testing and Vulnerability Analysis
            - Mantej Rajpal Adjunct Professor
            - Pete Klabe Adjunct Professor pete.klabe@nyu.edu

Discovery

Information Security Policies and Procedures

NYU has a rigorous information security and management policy in place that governs the majority of its assets. This is laid out in their document "Policy on Compliance with Cybersecurity Requirements of NYU," and sequestered under the New York State Department of Financial Services. As such, they are responsible for protecting confidentiality, integrity, and availability of the NYU community at large. This includes the different undergraduate and graduate schools (e.g. NYU College of Arts and Sciences, NYU Tandon), their portal campuses and study away locations (e.g. NYU Shanghai, NYU Abu Dhabi), and any and all infrastructure carrying the NYU name (e.g. physical academic buildings, NYU software, NYU merchandise). NYU units charged with carrying out this policy include the Faculty Housing Office, the Office of General Counsel, and the Office of the Controller (all prospective stakeholders in the eyes of this report).

In compliance with NY State Law, NYU and its assets are required to conduct penetration testing, vulnerability testing, trail auditing, and data disposal regularly in order to determine security gaps and areas in need of remediation. In the process of securing data, NYU will need to implement least privileges, third-party application controls, security training for faculty and staff, and a thorough business continuity plan in the case of crisis or natural disasters.

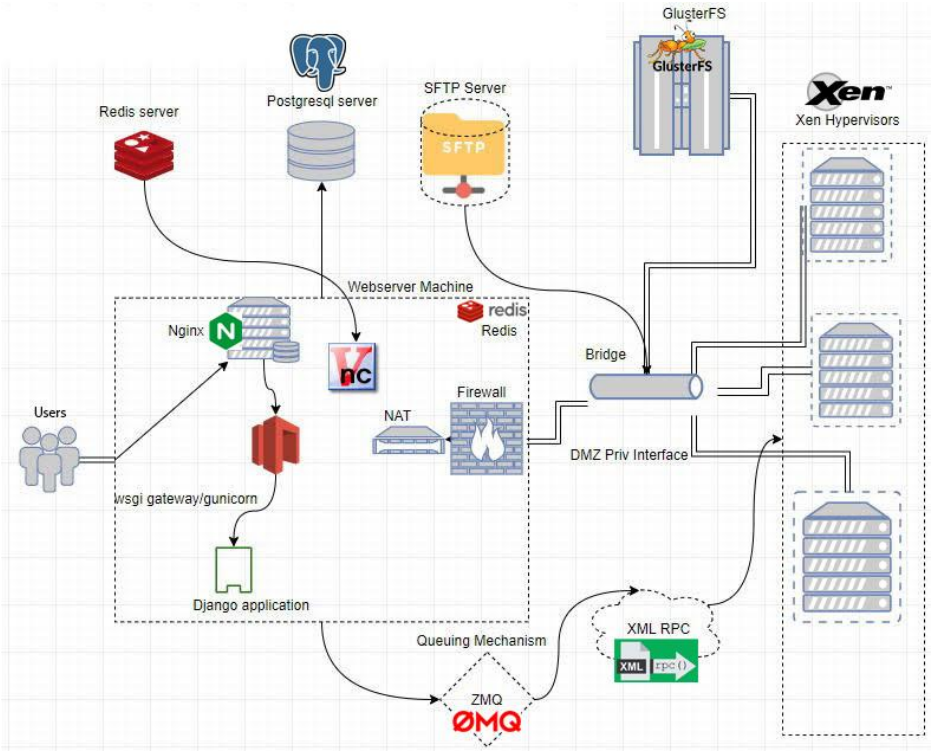
As a part of NYU infrastructure (specifically organized under NYU Tandon School of Engineering), Vital is required to abide by the NYU Policy on Compliance, and respectively the NYS Department of Financial Services. Current public records of Vital's compliance with NYU policy is limited, as the site itself has not conducted any form of penetration test or vulnerability analysis (this report being the first). Vital does conduct a timed flush of its student registry every semester, deleting all user accounts for Vital, while only preserving those with administrator privileges. Students are required to re-register for Vital and input newly populated course codes in order to authenticate their status as students. This policy is thorough in monitoring user population and preventing unauthorized access; however, more thorough enforcement of tenants of the NYU policy is required.

Communications Plans for Data Leak

Based on New York General Business Law 899-aa and State Technology Law 208, if more than 5,000 New York State residents must be notified, breached entities must also notify consumer reporting agencies. Moreover, if there is any potential security incident that may place either high or moderate risk data at risk of unauthorized access, the NYU IT Global Office of Information Security must be notified.

Vital Architecture (based on GitHub and Professor Reddington Interview)

Based on analysis of the GitHub repository, as well as scheduled interviews with Professor Reddington, we were able to identify key components of Vital's architecture. The web code utilizes Django (a Python web framework) while the site runs on an Nginx web server. This is part of the web portion of Vital where bugs regarding user access and management of VMs can occur.



The virtual machines run on XEN Hypervisors, which are type-1 virtual machines. The VMs also use ZMQ for asynchronous messaging with sockets. These are part of the VM mechanism and are areas where potential issues regarding VM availability and port sharing with increased user load can occur.

SFTP is used for secure file transfer for students to upload and download files from an external network. This can increase risk when students introduce outside files, if not properly contained within VMs. GlusterFS is a network-attached file storage system, where VM data is stored. This is potentially where issues regarding file storage and bleedover between user storage can occur. Ansible is a provisioning tool that allows professors to deploy established configurations based upon the needs of certain courses.[1]

Vital consists of two systems (along with a few distributions used by other professors for research purposes): the production version (used by around 500-700 students), and the development version (currently not working, used to experiment with new code). Vital systems need to be run on a server - there is a potential to run it offline among a combination of different devices (One running XEN, one running QEMU, and one running a virtual machine). Each Vital login does not run on a distinct VM, but on a QCOW (QEMU Copy On Write) file, which delays storage allocation until necessary, from the QEMU virtual hosted machine service. This allows the administrator to limit the access of the users, and can suppress update notifications and remove certain accesses.

[1] Source: **Vital User Guide**

IAM Maturity Evaluation Calculator

We have decided to use the IAM Maturity Evaluation calculator for Vital. The IAM Maturity Evaluation calculator stands for Identity and Access Management Maturity Evaluation calculator. The IAM Maturity Calculator is typically used for evaluating an enterprise or company's Identity and access management. We chose this for our evaluation because there are various important benefits of Identity and Access Management. Additionally, we chose the IAM Maturity Evaluation because of the increased security levels you can achieve with Identity and Access Management and its strategic benefits to Vital. In this section, we will conduct an identity management maturity assessment on Vital.

Q1. Do you know where your identities are stored in comparison to your accounts?(Actual Score:4 Target Score:3)

We will be rating this measurement by levels as below:

1. No central Identity store. Accounts all locally hosted. No formal documentation in place.
2. Central ID store for users, but not servers. No formal process for move/add/change/delete.
3. Central ID store in place with formal, auditable process.
4. Full integration of all critical devices into a common ID store. Exception process in place
5. Full integration of all critical devices into a common ID store. Exceptions less than 1% of monthly workload.

By the information we get from the interview with Professor Thomas Reddington, we know that by the end of every semester they flush out all the registered students' accounts for the next group. Therefore, we can make a conclusion that they have Central IDs stored in place with a formal, auditable process. Finally, since they gathered all machines into the same place at 370 Jay st. so it actually gets through the level 4. At least but not least, since they still have other maintenance to deal with so we can not rate it with 5.

Q2. Do you have an end-to-end understanding of how users authenticate to workstations,network devices, applications, or non-windows servers?
(Actual Score:3 Target Score:3)

We will be rating this measurement by levels as below:

1. There is no formal policy governing authentication processes.
2. Default user authentication to a standard directory. No standard practices for servers and network devices.
3. Formal requirements exist and are documented.
4. Machine-to-machine(M2M) service accounts are formally managed
5. Formal requirements exist are supported via modern infrastructure solutions(SSO/TACAS)

Based on the experiences of our team members who have had the experience with vital in other courses. We can conclude that it is a virtual system which has a website for the interface and there is a authentication mechanism which requires our username for identification and the password for authentication. By these experiences and the information we got from the interview with Professor Thomas Reddington, we can rate it with level 3.

Q3. Is your Identity/Account Management process well defined, repeatable, and automated?(Actual Score:5 Target Score:3)

We will be rating this measurement by levels as below:

1. No process exists. All work is ad-hoc.
2. Standard practices exist, but not formally documented or auditable.
3. Formal processes exist, are documented, and evidence of adherence can be provided
4. Formal processes exist, are auditable and have annual attestation campaigns.
5. Fully auditable and validated process with an exception rate under 1%.

By the interview with Professor Thomas Reddington. We get the information that at the very beginning of Vital, the Identity/Account Management process had been all set and still remain the same policies until now. Therefore, we can score it with 5 with no doubt.

Q4. Does your identity management process activate with changes to the HRIS platform?(Actual Score:1 Target Score:3)

We will be rating this measurement by levels as below:

1. No integration between the HRIS platform and the Identity store.
2. Manual/batch upload of data from HRIS to ID Store.
3. Connection between HRIS and ID store for Joiners/Leavers with basic birthrights.
4. Full permission integration of Joiners/movers/leavers.
5. Automated validation/attestation campaigns for all associated HRIS changes.

From the interview with Professor Thomas Reddington. We noticed there is no Human Resource Department in the Vital team, so they do not have an HRIS platform.

Q5. Do you have an attestation process in place to identity and resolve accounts with unnecessary access rights?(Actual Score:1 Target Score:3)

We will be rating this measurement by levels as below:

1. There is no formal attestation process in place.
2. Informal attestations occur for critical systems
3. A manual attestation campaign occurs annually for selected systems
4. Formal, automated attestations occur for critical and financial systems on a regular basis.
5. Automated attestations occur for critical/Financial systems whenever a user or role change occurs.

By the information we get from the interview with Professor Thomas Reddington. We are aware that this is a current vulnerability which he and vital team are working on and will address with it in the near future. Therefore, we can only rate it with the score of 1.

Q6. Are the majority of rights granted to users derived from predefined birthright roles rather than exceptions?(Actual Score:2 Target Score:3)

We will be rating this measurement by levels as below:

1. Birthright roles are not in use.
2. Birthright roles are used for basic directory access only.
3. Birthright roles are used for all fundamental access for every employee.
4. Birthright roles exist for each business line, providing more than 50% of normal access requirements.

Based on the experience by our team members who have had the experience with Vital. They provide us that each account is made for each one of us and it is only for basic directory access. Therefore, we rate it with the score of 2.

Q7. Do you regularly test the validity of identity and user controls in all of your environments?(Actual Score:5 Target Score:3)

We will be rating this measurement by levels as below:

1. Identity/user controls are not reviewed as a practice
2. Identity/user controls are spot-checked during access control audits.
3. Identity/user controls on critical hosts are manually reviewed on an annual basis.
4. Identity/user controls for all hosts are reviewed annually
5. Identity/user controls are validated automatically on an ongoing, continual basis.

From the interview we had with Professor Thomas, we are aware that every semester Vital runs a flush of its student registry, and deletes all student access to Vital. This means that vital did test the validity of identity and user controls environments regularly. In addition, since it has happened once a semester, we can give 5 points to it.

Q8. Do you have a privileged accounts strategy which protects authoritative accounts against abuse or takeover and creates an auditable trail of activities?
(Actual Score:4 Target Score:3)

We will be rating this measurement by levels as below:

1. Privileged accounts are shared, not monitored and have no special handling.
2. Privileged accounts are managed through a central repository.
3. Privileged accounts are required to have multi-factor authentication.
4. Privileged accounts use one-time passwords via a centralized Privileged Access solution which tracks access requests.
5. Privileged accounts are centralized, have full keystroke logging, use one-time passwords and are actively monitored for use.

Vital does have a privileged accounts strategy that protects authoritative accounts against abuse or takeover. Although it doesn't create an auditable trail of activities, the privileged accounts do use one-time passwords via a centralized privileged access solution. Hence we will give Vital a rating of 4.

Q9. Does your program monitor for permission changes on existing accounts as well as the creation of new accounts?(Actual Score:3 Target Score:3)

We will be rating this measurement by levels as below:

1. No monitoring of account maintenance is performed.
2. Monthly batch reporting of new/closed accounts is performed.
3. Daily reporting of new/closed accounts is performed.
4. Daily reporting of all account maintenance activated is performed.
5. Real-time notification of account.

By the information we get from the interview with Professor Thomas Reddington: "Every semester Vital runs a flush of its student registry, and deletes all student access to Vital. All students in the next semester need to re register for Vital, using their name and emails (to create an account) and then an accompanying course code." By such, we can rate it with a score of 3. Furthermore, there is no evidence that they have the daily report of all account maintenance nor real-time notifications. Therefore, we can give it a 3 for no doubt.

Q10. Are you actively monitoring user access activities for signs of abuse or takeover?(Actual Score:4 Target Score:3)

We will be rating this measurement by levels as below:

1. No user access monitoring is in place.
2. Batch activity reporting is performed regularly.
3. Real-time invalid login monitoring is in place.
4. All suspicious user activity(failed logins, foreign country, outside normal hours, etc) is monitored.
5. User behavior risk modeling is performed for all users and escalated as necessary.

By the information we get from the interview with Professor Thomas Reddington:"Vital script prevents users from receiving security or distribution updates for the VMs or their images, as this could cause issues with students running administrative functions, etc". By such, we can conclude that the vital team is keep working on this issue to make sure that the identification is not compromised. Therefore, we can rate it with a score of 4.

Q11. Do you have a process in place to identify, track, and verify third-party users and contractors?(Actual Score:1 Target Score:3)

We will be rating this measurement by levels as below:

1. No central repository exists.
2. Contractors are maintained in the corporate directory and treated the same as employees.
3. Contractors are stored in the corporate directory, but have limited, reduced access.
4. Contractors are in a special user class/org unit in the directory which facilitates special real-time monitoring.
5. Full integration with procurement/HR for contract management and automated onboarding/offboarding of contractors.

From the interview with Professor Thomas, we had been told that sometimes vital third-party users(other schools students) outside of NYU and they are not treated the same as employees but students as well. Plus, Vital is completely created by Professor Thomas and his team which recruited members from NYU graduate students from the CSE department, so there are no contractors. In conclusion, they have not built the environments to integrate with contractors nor third-party users.

Q12. Does your identity program encourage integration between your authentication infrastructure and external providers via open standards or leading CASB services? (Actual Score:1 Target Score:3)

We will be rating this measurement by levels as below:

1. There is no integration between internal user access and cloud/*aaS services.
2. Manual/automated synchronized directories which allow for basic authentication actions.
3. Basic federated authentication between predetermined trusted partners.
4. Federated functionality exists for basic user authentication via open standards(REST, OAuth, OpenID).
5. Fully integrated federated connectivity supporting roles, SoD rules, and fine grained access controls.

By the observation of our team members and the information we get from the interview with professor Thomas Reddington. We can make sure that there is no such integration hence we will rate it with a score of 1.

Q13. Do you maintain an inventory of application and machine-to-machine(M2M) credentials and manage them under a standard process?(Actual Score:3 Target Score:3)

We will be rating this measurement by levels as below:

1. App/M2M accounts/passwords are hardcoded, not monitored and have no special handling.
2. App/M2M passwords satisfy a higher level of password strength.
3. App/M2M accounts have minimum functional requirements and passwords are changed on a regular basis.
4. App/M2M account activity is monitored real-time for out-of-normal usage patterns.
5. App/M2M accounts use one-time passwords via integration with a centralized Privileged Access solution which tracks access.

Vital does maintain an inventory of application and machine-to-machine credentials. But the App/M2M account activity isn't monitored real-time for out-of-normal usage patterns. Vital's App/M2M accounts only have minimum functional requirements and passwords that are changed on a regular basis. Hence, we'll give Vital a rating of 3

Q14. Do you correlate logical access attempts to recent physical locations; alerting on discrepancies in both directions?(Actual Score:2 Target Score:3)

We will be rating this measurement by levels as below:

1. No physical/logical correlation is supported.
2. Real-time alerting exists, but no blocking
3. Access locations are permitted/denied via network controls.
4. Time-of-day/Location controls exist at a user level.
5. real-time geolocation/timestamping risk modeling determines access levels.

From the information we get from the interview with professor Thomas Reddington: "Previously servers were located in Metrotech, but now the server itself is a box located in 370 Jay St. NYU IT machine room. Any physical security issues will need to be related to 370 Jay St. 2017 - dealt with a lot of physical problems because the system itself was located in the basement of Metrotech, rain and lack of air conditioning would cause.

Current issues are that since the "server box" is located in an NYU IT governed space, Professor Reddington (the developer) does not have easy access to the hardware. He has limited access and needs to call an IT person to open it for him (if he needs access). The Server itself is located in the Machine Room in the group floor of 370 Jay St. It's a server rack with a few boxes (Professor Reddington mentioned it may be difficult to get a student to examine, but could take some pictures for us)." By such, we can conclude that the physical devices are gathered in a place and it has its own logical access in both directions. Therefore, we will rate it with a score of 2.

Q15. Are you able to make risk-based access decisions, in real time for critical infrastructure, and require additional authentication if the risk is too great?(Actual Score:4 Target score:3)

We will be rating this measurement by levels as below:

1. There is no correlation between user, access request, and risk level in determining access rights
2. Hardcoded controls exist (time of day, country code, IP address) for specific environments
3. Correlation exists at a monitoring control to alert for suspicious activity
4. Correlation exists at a blocking level for basic permit/deny decisions
5. Fully adaptive correlation exists allowing additional authentication requirements based on specific risk associated with user, resource, or access request

Vital is able to make risk-based access decisions in real time for critical infrastructure. However it doesn't require additional authentication if the risk is too high. Vital's correlation exists at a blocking level for basic permit/deny decisions but it lacks fully adaptive correlation which allows additional authentication requirements based on specific risk associated with user, resource, or access request. Hence, we will give Vital a rating of 4.

Site Visit

Virtual Interviews

1) Professor Thomas Reddington - Risk Manager

On March 5th, 2021, our group conducted an interview with Professor Thomas Reddington, a Senior Faculty Member and Industry Professor within the Computer Science and Engineering (CSE) Department at NYU Tandon School of Engineering.

Professor Reddington worked for around thirty years at Bell Laboratories before joining NYU Polytechnic University (the former name) in 2007, building a treasure trove of experience in computer networking and security - an area he specializes in to this day as an educator. When Professor Reddington joined the university, he took on the task of modernizing the Vital platform. In the last ten years, he has served as the sole designer, developer, and owner of Vital. Professor Reddingotn rewrote the source code of the product and repurposed the original product to be used in a variety of courses.

Employing a small team of two or three Graduate Assistants (GA) from current Masters' students within the CSE Department, Professor Reddington continues to innovate and expand the scope of the Vital project. The GAs handle maintenance tasks and assist in development and design; however, due to relatively quick turnover of students (due to the prevalence of short two-year MS programs), sustainable support is interrupted by bringing new students up to speed.

Professor Reddington has previously raised issues regarding Vital, most notably its physical server location as well as departmental support for upkeep and development of the software. Previously, servers were located in Metrotech, where the machine itself suffered from a range of environmental issues. Chief among these issues include lack of access to air conditioning and flooding of rain water, both causing server outages. Currently, the server itself is a box located in the 370 Jay St. NYU IT machine room. Any physical security issues will be related to the 370 Jay St. building (further expanded upon in the Site Visit - Physical Security Questionnaire section).

As part of access management and privilege restriction, Professor Reddington elaborated that every semester Vital runs a flush of its student registry, and deletes all student access to Vital. Students in the following semester need to re-register for Vital, using their name and emails (to create an account). Courses distribute an accompanying course code, which serves as a secondary verification of access (Vital is restricted to individuals who use it in a course). If logs are not flushed (which occurred after NYU's Summer 2020 semester due to manpower constraints), the amount of users who can access Vital surpasses the processing power/availability of the software itself - causing crashes and downtime. Misconfigurations, as highlighted by Professor Reddington, form the basis of most security faults, and Vital was in no way immune to this.

Finally, Professor Reddington indicated that several critical areas were currently in need of revitalization. The Github provides a public-facing repository where individuals can see some of the inner workings of the software; however, not all elements are uploaded and the Github resources are

several years out of date. As a documentation methodology, this will need to be updated. Additionally, Professor Reddington clued our team into the fact that major parts of Vital were currently being Dockerized and will eventually be run in independent sandbox environments. This, hopefully, will reduce strain on the existing program, and allow more active users and further flexibility to implement more taxing functionality to the teaching tool.

On April 5th, 2021 we conducted a second interview with Professor Reddington, utilizing some of the questions from the NIST Questionnaire. We were hoping to gather some additional information regarding the internal workings of Vital, as well as the variety of courses that utilize Vital. He was able to provide us with the below information, as well as a login access code for NYU Vital (for the currently empty Penetration Testing course):

Professors Teaching Courses Utilizing Vital
Jeffrey Epstein - 3 courses - 1) Programming 2) Parallel Distributions 3) Computer Architecture
Gustavo Sandoval - 2 courses - 1) Computer Architecture 2) Operating Systems
Professor Damon McCoy - 1 course - 1) Networking
Professor Justin Cappos - 1 course - 1) Networking
Professor Philip Mak - 1 course - 1) Networking

Typical Virtual Machines Allocated Per Course
Networking - Multiple Virtual Machines
Operating Systems - 1 Virtual Machine
Programming - 1 Virtual Machine
Computer Architecture - 1 Virtual Machine
Parallel Distribution Systems - 4 Virtual Machines

In addition, Professor Reddington indicated that it was difficult to fully track empty courses, as well as the level of use per class. Namely, the virtual machine allocations are theoretical as there are times when demand is high for a particular course (usually around key assignment deadlines), which require shifting of priorities.

As stated previously, there are a total of three levels of users: Developer, Faculty, and Students, which are mapped to the Production and Development Vital instances respectively. Faculty and Student accesses are relatively the same, offering minimal access and limited read/write abilities. Developers comprise of GAs and Professor Reddington who maintain sudo (root) access to all instances of Vital. A fourth access level previously existed: Author. This access would allow professors to serve as an admin for their own classes, allowing them to write their own assignments and programs within the platform to match their tailored curricula. However, these accounts were minimized as demand is high and professors mainly wish for uninterrupted service to Vital. As such, Vital development is wholly under Professor Reddington.

In regards to security architecture, Vital only utilizes two-factor authentication. This occurs when new users register an account - they will need access to their email. This works off a nonce/token-base

approach and usually is paired with the users' NYU Net ID email address. A secondary authentication occurs when the user has successfully created an account - a course code is required to register an account and establish access to the virtual machine/QEMU instances. Although this does provide some degree of security, it does not necessitate a link with a specific NYU account.
However, this does deviate from normal NYU policy, in which most NYU services require a multi-device authentication through the Duo authentication application. This is done through the Shibboleth web portal, and provides an extra layer of validation and security for the user and the system. A potential add-on to Vital's security would be to include the same Shibboleth multi-factor authentication; however, this would also make Vital more appetizing as a target for lateral attacks in order to gather more information on other NYU technological assets.

As part of continued event monitoring, Professor Reddingto was able to share with us that Vital has experienced availability issues (like previous semesters) due to the system having greater than 100 simultaneous connections on each VM. The issues are once again clustered around due dates for courses, as many NYU students are looking to complete their assignments last minute. This has reached a peak of 400 simultaneous connections, which is far higher than available bandwidth. Professor Reddington also indicated that Vital was not designed to have a clean shut-down process. When Vital is restarted, individual student accounts can try and log in while fixes are being completed. This slows down the system and process of patching, and creates additional issues.

For event logging, Vital utilizes standard Linux-based logging of interfaces. Every time a VM is turned on, a log is printed into the database; however, this is not a serious concern by Vital. As availability is the key goal, logging does not provide much help - in fact it uses valuable bandwidth that can be utilized by the virtual machines. Vital currently exists as buggy software where many NIST checklist issues are not main priorities. It will experience one "fire" or serious issue each semester that is usually unrelated to hardware.

In terms of certificates, Vital utilizes roll-over digital certificates that are mostly self-signed. As in other cases, if these certificates are affected or beaten, there is not much damage to the overall system as private/damaging information is relatively sparse for Vital. A potential vulnerability is the SSH access to the server; if an attacker were able to access the Vital server houses, this attacker may be able to identify other individuals in the network .They would be able to see who is logged on and be able to SSH access their accounts. In this vein, an attacker could obtain the name, email address, Vital password, and netID of an individual user within Vital. Obtaining this password may not be more effective than a brute force dictionary attack on NYU Home (Shibboleth). However, there is the case that lateral attacks using known information (for example if NYU email or password are the same as those utilized on the main NYU netID accounts) to access more protected NYU services. As a rule, Vital passwords conventions follow ISO 27001 / ISO 27002 requirements, utilizing multiple letters/numbers/special characters. However, no prompt or check exists to indicate students should not utilize their main account passwords.

Finally, it is interesting to note that Vital does not have an individual business continuity plan. Instead, it relies on policies laid out by NYU's overall compliance and risk (included in the

aforementioned information security policy section in this paper). Professor Redignton did note that it might be good to let Vital fail in the case of a crisis, as it would bring attention to a gap in technology currently present in the NYU networking curriculum. He also highlighted that this approach may be possible to replicate utilizing AWS, but AWS does have a significant oversight in that it does not allow series of multiple virtual machines (thus decreasing potential population served by Vital).

As a reach goal, Professor Reddington is attempting to gather a strong team and funds to dockerize the servers of Vital. This would consist of organizing current services into multiple web servers, creating a post-risk database, and moving the current centralized data environment into a docker container. Additionally, the current process of debugging involves logging on to individual student accounts to identify and replicate errors. This process is slow and requires manual logging of each students' passwords - stored in a password receptacle in clear text. Professor Reddington has indicated that although a secure solution would be to convert stored passwords to ciphertext, it would hamper debugging. Passwords themselves are not highly sensitive data, unless students utilize the same password for Vital as they use for their main NYU accounts (which is very common).

2) Professor Damon McCoy - Principal User

On March 26th we conducted an interview with Professor Damon McCoy, a current Associate Professor of Computer Science and Engineering at NYU Tandon School of Engineering. He currently teaches as a Network Security Professor, focusing on measuring security and privacy of technological systems while also exploring intersections such as socio-economic impacts (i.e. cyber-physical systems, anonymous communication, censorship evasion).

Professor McCoy has been using Vital for about 6 years in his course curriculum, and generally believes that Vital has had a positive impact on students. Vital is effective as a tool for his classes in terms of providing an isolated system of virtual machines for students to work on labs. Students do not have to install or configure VMs on their own computers; additionally, any unintended bugs or systems are sequestered within Vital.

However, he also mentioned that there are some weaknesses in its usage and configuration. Certain bugs can cause students to lose their files from storage (especially when restarting or reimaging VMs), or in some cases, bleed over between different student accounts. Finally, availability failures due to DNS errors and SSH faults have caused Vital to crash in the past. This is exacerbated by the fact that many students often try to access the service at the same time before assignments are due. Students sometimes also forget to turn off the VMs after using them, which causes a hang up of resources.

Professor McCoy has not been provided with any business continuity plan or an incident response plan. When problems arise, it is usually more of a best effort, try to be flexible, type of situation. Some semesters have been bad, this semester has been fine. (Note: on the Mon/Tue following the interview, Vital experienced runtime and availability issues, potentially due to many students working on a network security lab that was due on Wed). Last semester, Vital experienced hardware failures,

resulting in the destruction of work as a hard reset and re-image of the whole system had to occur. Availability can sometimes be shaky over the course of a semester.

In terms of comparing Vital to other similar technologies, there are some websites and third-party services that provide vulnerable web applications specifically for the purposes of security testing. Additionally, there is the option of providing students with VMs to run on their own computers, but this can involve the issue of whether all students are able to run VMs on their own.

Only NYU is currently using this system, and one suggestion from Professor McCoy is that if Vital was transformed or replaced with a more open-source system with collaboration with other universities, it may be more manageable to develop and maintain. This would also allow for sharing of labs between university professors. One possible resource to look at are the SEED Labs developed at Syracuse University.

3) Christopher Ng - NYU IT and Senior Lab Instructor

Christopher Ng is a Senior Lab Administrator for NYU IT, and is the direct contact for NYU IT's support for the Vital platform. He has a networking and Linux background, and has been working at NYU IT for around two years. His responsibilities regarding Vital include coverage of a number of computer science labs onsite within 370 Jay St. and Roger's Hall (namely the server room Vital sits in, as well as Professor Hadimioglu's various research laboratories). Specifically, he covers the technical aspects of Linux maintenance and patching, and OS upgrades for a wide variety of labs and projects. These resources (Linux and otherwise) serve both faculty members and students (usually in the form of a professor-sponsored project).

When inheriting Vital's coverage, Chris inquired as to what his role and responsibilities would be regarding Vital's upkeep. Professor Reddington indicated that the only requirements he had for Vital were physical access to the Vital server and data center, a sustainable source of power, and lighting/AC for the server. NYU Vital's physical infrastructure is only available to NYU IT, Professor Reddignton, and Vital GAs. It is protected by two RFID card readers (external to the room, and behind an internal chain gate within the room). The server is also monitored 24/7 by a series of cameras, both within the building and within the server room. NYU Facilities and Management (NYU FCM) governs the actual access and power within the building (and the room respectively) and is the direct contact for any queries. Hani Basilious and Oswaldo Hernandez serve as the heads of NYU IT and direct contact for any issue escalation. Together, they also are notified if the temperature of any of the server rooms reaches unsafe levels (whether this is due to hardware installed in the room or a close relationship with NYU FCM is unknown). It is important to note, the server room is slated to physically move to the 7th floor of 370 Jay St. in June 2021. So far, Professor Reddington has not yet visited the physical location; however two of his GAs have stopped by for routine maintenance. This included replacing a bad hard drive a few months ago that displayed an error light. Chris had noticed this faulty hard drive while doing routine server searches and notified Professor Reddington of the defective hardware.

In terms of non-physical access, Chris has access to administrative credentials for both the production and development instances of Vital (that is, the student and research/development sectors). Additionally, around when Chris joined NYU IT, the Vital server was moved from 6 Metrotech to Room 243 of 370 Jay St. This was due to both administrative and facilities reasons (outside the purview of Professor Reddington and NYU IT), as well as the fact that Vital had suffered availability gaps during a particularly warm summer (the server had overheated). A separate team of NYU IT is also responsible for anomalous monitoring of ping, memory, and load. This is not specific to NYU Vital, but for the overall NYU network. Nagios is used liberally to monitor any potential network load in the case of a DDoS attack. In the past, many students and faculty members have reached out to NYU IT help desk for support; however, NYU IT is not currently equipped to provide technical support specifically for the Vital platform. In response, Professor Reddington included a banner to the top of the Vital Page, indicating that any queries or support questions should be directed towards the Vital support email.

From a network standpoint, NYU Vital employs a series of three public servers and two private switches. All of these are located on the NYU network, with a combination of different port configurations. Professor Reddington's two private switches piggyback off of servers with a public IP interface. By default, every port is usually closed (fail-safe defaults), and a request must be filed with NYU IT for each port opened. For example, for VItal's Development instance, a request was sent to request that all ports are open. Typically, however, most NYU services do not have all ports open.

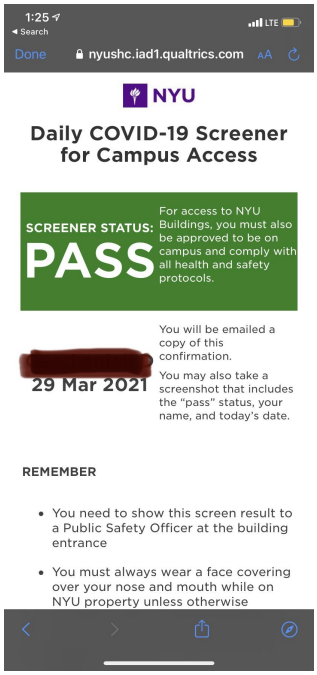
1) VLAB_Vital_Production - IP: 128.238.77.21 - connected to internal poly switch (NYU Tandon)
    a) Ports Open:
        i) TCP 80 - HTTP
        ii) TCP 443 - HTTPS
        iii) TCP 5900-65000 - RFB, VNC (VM infrastructure and GUI)
2) VLAB_Vital_Development - IP: 128.238.77.20
    a) All Ports Are Open
3) Poly_Dev - IP: 128.238.77.09
    a) Ports Open:
        i) TCP 22 - SSH
        ii) TCP 80 - HTTP
        iii) TCP 443 - HTTPS

Physical Security Questionnaire

As part of our security assessment, we conducted a thorough physical security analysis on the building that contains the Vital server, located at 370 Jay Street, Brooklyn, NY 11201. Previously a building housing the NYC MTA department and serving as a transit hub for Brooklyn-bound trains, NYU purchased the building and is currently in the process of redeveloping the multi-use structure for educational purposes. The various floors of the building have been divided among different departments within NYU Tandon, with notably the Computer Science and Engineering departments taking residence on the 7th floor. Additionally, many courses have already been moved into the building as it contains one of the largest lecture halls, located on the fourth floor.

Before heading in for the inspection, we categorized our goals for the inspection into 5 different divisions. The following is a list of what our top priorities were regarding the building in their individual area of concern and what we have found:

- **Access Management:** Which areas of the building are considered sensitive? Do students/faculty/building staff have access to those areas? Who determines the access privileges and how are they managed (e.g. RFID scans, physically locked doors, private elevators).
    - In order to access any building in NYU, students and staff need an NYU ID. Guests are required to swap their ID and be escorted by a NYU student or staff to gain access to the building. However during events, access to buildings is more liberal and guests can walk into the buildings after exchanging an ID without the need for an NYU staff/student escort. In the midst of the pandemic, building access has become more rigid. Anyone accessing the NYU buildings has to take a covid test and show their covid screening results.



Despite these rigid measures to enter the building itself, we found that accessing certain rooms and unauthorized areas, such as the boiler room, within the building to be easy. There were cameras everywhere but students, staff or guests could easily slip into some unauthorized areas and cause severe damage to the property if they wanted to. Furthermore, since the building at 370 Jay Street was under construction, it opened further avenues of access. Key areas such as server rooms and classrooms were still properly secure though.

- **Physical Barriers of Entry**: Are there several possible areas of ingress and egress? How are these locations secured from visitors or unauthorized individuals? Does the fact that the building is under construction affect access management? Is it possible to tailgate? Can someone gain access by signing in under a false name, or falsifying a department to go see?
    - In the building that hosts Vital, 370 Jay Street, we found that there was only one main entrance through which NYU students, staff and guests can enter. This entrance is protected by barricades that only allows access when a valid NYU ID is tapped. With the pandemic in place, another layer of security has been added and any person entering the building has to show the security at the front desk their health screening results, before tapping for access through the RFID gates of the building.

There was also a back entrance for the construction crew that was working on the building. We managed to find this entrance while snooping around the building. There were no guards or barricades that would prevent students or staff from entering this area, making it an easy target.

- **Wireless security:** Are Wifi Endpoints and SSID present and are they secured against on-site attacks? Who has access to these Wifi hotspots and are they protected by enterprise security?
    - Several wifi networks were available for both guests and NYU members. They were all secured with WPA2 or stronger protection, and required a signed certificate. The following are a list of wireless networks that we identified in the location:
        - Nyu
        - Nyu-legacy
        - Nyuguest
        - Nyuguest-legacy

- **Safe Disposal of Assets**: Are external disposal methods secure? Is there a third-party company that processes the destruction of sensitive information through paper shredding, etc. (e.g. Iron Mountain). Are other non-document forms of media destroyed as well?
    - During our physical investigation we could not learn much about disposal methods being used. However, based on interviews that we conducted with the IT in charge of the server room and some research, we found that documents are shredded and destroyed as per the following policy (Link). “NYU's two preferred destruction service providers are USA Shred and Shred It.” (under “Destruction Services”).

- **Penetration Tests**: Are there public records of a history of penetration tests? Are there any records or documents that exist that cover access management? As the location has shared access to public transit (Jay St. Metro station below) are there any possible entry points from that station that exist?
    - As mentioned above, there is only one main entrance to 370 Jay Street. As for criminal records on the property, based on NYU acquiring the property in 2017 and on NYU’s crime log, there have been no major break ins or criminal logs on trespassing, so the building itself has been crime free for the past 3 years. However, there have been incidents of trespassing in the past few years.

NIST Checklist Questionnaire

Our team conducted a preliminary risk assessment using the following steps. These steps namely address the five core NIST-CSF Categories: *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*.

1. **Initial Data Request:** This will encompass our initial interview questions that we will review with the Vital System's team and relevant stakeholders. We have included a few questions below, for reference. A detailed list of questions can be found at this link.
    - Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
        - *Ex: Do you have a well-defined information security policy, data usage policy and data classification policy?*
    - Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
        - *Ex: Do you use any Identity Access Management tool for your application?*
    - Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
        - *Ex: Have you performed a CIA risk assessment for your application?*
    - Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
        - *Ex: What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data like student information?*
    - Recover: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
        - *Ex: Do you have a documented Incident Response plan?*

2. **First-level Review:** Review the responses and identify the gaps: Based on the information received, we will perform our internal assessment and identify any gaps that exist.
    a. The first-level included collecting asset lists. It is pertinent to identify the two types of available resources:
        i. Devices, processes and applications that are charged with safeguarding;
        ii. Defensive tools deployed to be first-responders

    For our first-level review, we were able to connect with multiple stakeholders to get an understanding of how Vital is designed and how it protects its users' data. We also conducted physical site visits to review the data center which hosts Vital.

3. **Remediation Plan:** Get their inputs on compensating controls for their identified gaps or a mitigation plan for their gaps
    a. Any risk management plan must have the following:
        i. Understanding of the risk
        ii. Deploying an additional layer of security - compensating control
        iii. Have a remediation plan in place

    For example, in one of our assessments, we identified a vulnerability that weak cryptographic algorithms are implemented. For this vulnerability, we performed our analysis and assigned it a risk score to have an understanding of the underlying risks to loss, compromise or

manipulation of data. Based on our analysis, we have also prepared a list of recommendations for the said vulnerability.

4. **Recommendations:** Provide our recommendations for addressing the security concerns. An important aspect of risk management is having a well-defined remediation plan based on the recommendations provided during any risk assessment. This report also provides a comprehensive list of recommendations for cyber risk strategy implementation.

Lightweight Penetration Testing

SecurityScorecard™

SecurityScorecard™ is a security ratings service that uses an easy-to-understand A-F grading system to rate companies on their overall security as well as across 10 major risk factors.

A company with a C, D, or F rating is 5.4 times more likely to suffer a consequential breach versus A or B-rated companies. Certain risk factors, such as application security and patching cadence, are even more indicative of the likelihood of breach. An F versus an A in these factors may translate into a tenfold increase in the likelihood of a data breach or successful attack.

Factors

SecurityScorecard™ grades the system based on the factors shown below:

- **Network Security**: Detect insecure network settings
- **DNS Health**: Detecting DNS insecure configurations and vulnerabilities
- **Patching Cadence**: Out of date company assets which may contain vulnerabilities or risks
- **Endpoint Security**: Measuring security level of employee workstations
- **IP Reputation**: Detecting suspicious activity, such as malware or spam, within your company network
- **Application Security**: Detecting common website application vulnerabilities
- **Cubit Score**: Proprietary algorithms checking for implementation of common security best practices
- **Hacker Chatter**: Monitoring hacker sites for chatter about your company
- **Information Leak**: Potentially confidential company information which may have been inadvertently leaked
- **Social Engineering**: Measuring company awareness to a social engineering or phishing attack

Results of Vital

Our team used the SecurityScorecard™ Report report of Vital on April 23th as the most updated report and extracted our result from the captured security issues. The major (high severity) security issues were detected in Application Security and Network Security while a low severity issue was detected in DNS Health.

Captured Security Issues

- Application Security:
    1. Issue Description: **Content Security Policy (CSP) Missing**
       Severity: High
       Findings: 11
    2. Issue Description: **Site does not enforce HTTPS**
       Severity: High
       Findings: 2
    3. Issue Description: **Insecure HTTPS Redirect Pattern**
       Severity: Medium
       Findings: 3
    4. Issue Description: **Website Does Not Implement HSTS Best Practices**
       Severity: Medium
       Findings: 30
    5. Issue Description: **Redirect Chain Contains HTTP**
       Severity: Medium
       Findings: 5
    6. Issues Description: Website does not implement X-Frame-Options Best Practices
       Severity: Low
       Findings: 11
    7. Issues Description: Website does not implement X-Content-Type-Options Best Practices
       Severity: Low
       Findings: 20
    8. Issues Description: Cookie Missing 'Secure' Attribute
       Severity: Low
       Findings: 1
    9. Issues Description: Website does not implement X-XSS-Protection Best Practices
       Severity: Low
       Findings: 20
- DNS Health:
    1. Issues Description: SPF Record Contains a Softfail
       Severity: Low
       Findings: 1

- Network Security:
    1. Issues Description: **SSL/TLS Service Supports Weak Protocol**
       Severity: High
       Findings: 1
    2. Issues Description: **Certificate Is Expired**
       Severity: Medium
       Findings: 3
    3. Issues Description: **Certificate Signed With Weak Algorithm**
       Severity: Medium
       Findings: 1
    4. Issues Description: **Certificate Is Self-Signed**
       Severity: Medium
       Findings: 1
    5. Issues Description: **TLS Service Supports Weak Cipher Suite**
       Severity: Medium
       Findings: 3
    6. Issues Description: Certificate Without Revocation Control
       Severity: Low
       Findings: 2

Manual Testing Results

Based on the scope of work, we performed a lightweight penetration testing against the Vital application. Penetration testing helps organizations to uncover and validate potential targets that can be exploited, determine if the target can be reasonably exploited and is worthy of being exploited, and then attempt to exploit the target and maintain control.

During the penetration assessment, we identified and validated several medium, low-level vulnerabilities that could negatively impact Vital. Further testing of social engineering attacks would be the next logical step for penetration testing outside the scope of work.

Key Findings

Classification	Vulnerability Description	Severity
Sensitive Data Exposure	*Weak cryptographic algorithms are implemented*	*Medium*
Security Misconfiguration	*Missing sufficient secure headers*	*Medium*
Security Misconfiguration	*Missing HSTS configuration*	*Medium*
Information Disclosure	*Server's version and sensitive directories are publicly accessible*	*Low*

Technical Details

Reconnaissance

During the reconnaissance phase, we focused on identifying the available public information and performing passive scanning against the testing network and application.

We ***utilized an initial DNS search*** by investigating the information base on the available domain vital.engineering.nyu.edu of the vital site. Using the tool 'dig' and 'nslookup', we were able to find the A records and a different domain record as vital.poly.edu. With the domain information, we were able to identify additional subdomains for the target site as trac.vital.poly.edu, and ensured there is no Zone Transfer vulnerability. Furthermore, we checked the whois records for the tested domains and found the information about the Registrant, and was able to find administrative contact, technical contact about the domain.

The next logical step is ***checking the host information*** based on the domain records. Using a couple of different modules with the 'recon-ng', we confirmed the host information for vital.poly.edu and trac.vital.poly.edu, and we did not find any further hosts related to the domain. With Censys, Shodan, and other public databases, we found the servers' potential latitude and longitude. We were expecting to identify some services and open ports on the server; however, the result indicated that information was not published to the public internet at this moment.

Understanding the network architecture could also be helpful in penetration testing. We searched vital.engineering.nyu.edu and vital.poly.edu, utilizing 30 hops max and 60 bytes packets. The packets passed through the dmzgwb-p2p-extgwc.net.nyu.edu, and there was no further information after it hit polypri-tmrborderrtr.net.nyu.edu. The hop did not acknowledge the packets within the expected timeout, or the packets hit the firewall and were blocked.

We moved on to ***investigating the web application***. We conducted a series of website fingerprint tests, including Wappalyzer and Whatweb (shown in figure x.y). We obtained the following information: the server is a Ubuntu server and hosting the web application with Nginx 1.14.0. The web application is programmed in Javascript, PHP, and Django. The implemented JQuery is under version 1.12.0, which is out of date. With 'wafwoof', it seems like the web application firewall is missing.

```
┌──(kali㉿kali)-[~]
└─$ whatweb https://vital.engineering.nyu.edu
https://vital.engineering.nyu.edu [302 Found] Country[UNITED STATES][US], HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubun
tu)], IP[128.238.77.21], RedirectLocation[/login/?next=/], X-Frame-Options[SAMEORIGIN], nginx[1.14.0]
https://vital.engineering.nyu.edu/login/?next=/ [200 OK] Cookies[csrftoken,sessionid], Country[UNITED STATES][US], Dj
ango, Email[vital@nyu.edu], HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)], HttpOnly[sessionid], IP[128.238.77.21],
JQuery[1.12.0], Mark-of-the-Web[http://engineering.nyu.edu/], PasswordField[password], Script[application/javascript,
text/javascript], Title[Vital - Virtual Lab], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], nginx[1.14.0]
```

(Figure x.y, WhatWeb fingerprinting)

Google Hacking is another excellent tool to identify information about a tested network and application. Since we identified the server is running on Ubuntu, and the web application is hosting with Nginx, we attempted to identify potential configuration files and sensitive information about the server and the application. The results returned as expected, in that we were not able to identify some critical information.

Scanning

During the scanning phase, we focus on actively scanning the server and start to single out possible vulnerabilities of the target.

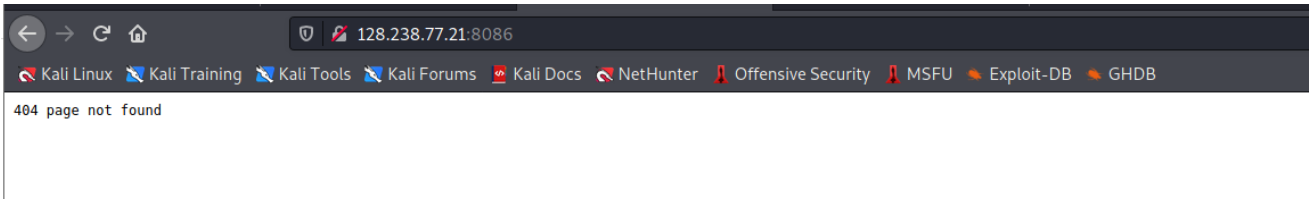
Certificates play an essential role in the Public Key Infrastructure; they help secure the data in transit and build trust. ***Understanding what certificates*** were implemented for the testing web application would be beneficial. Using 'sslyze', 'sslscan', and 'nmap script', we extracted the available TLS/SSL and ciphersuites. In January 2021, the NSA released a document to the public for eliminating obsolete transport layer security protocol configurations. Following the NSA's recommendations, we were able to identify some vulnerabilities in the web application. At this moment. The vital.engineering.nyu.edu is still accepting and preferring TLSv1.0 and TLS1.1, which are considered insecure protocols. There are a lot of insecure cipher suites, such as SHA1, and customized ecdh curves. We highly recommend reconfiguring the TLS/SSL protocol to remediate the potential vulnerabilities.

```
Nmap scan report for vital.engineering.nyu.edu (128.238.77.21)
Host is up (0.080s latency).
rDNS record for 128.238.77.21: vital.poly.edu

PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CCM_8 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CCM (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CCM_8 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CCM (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

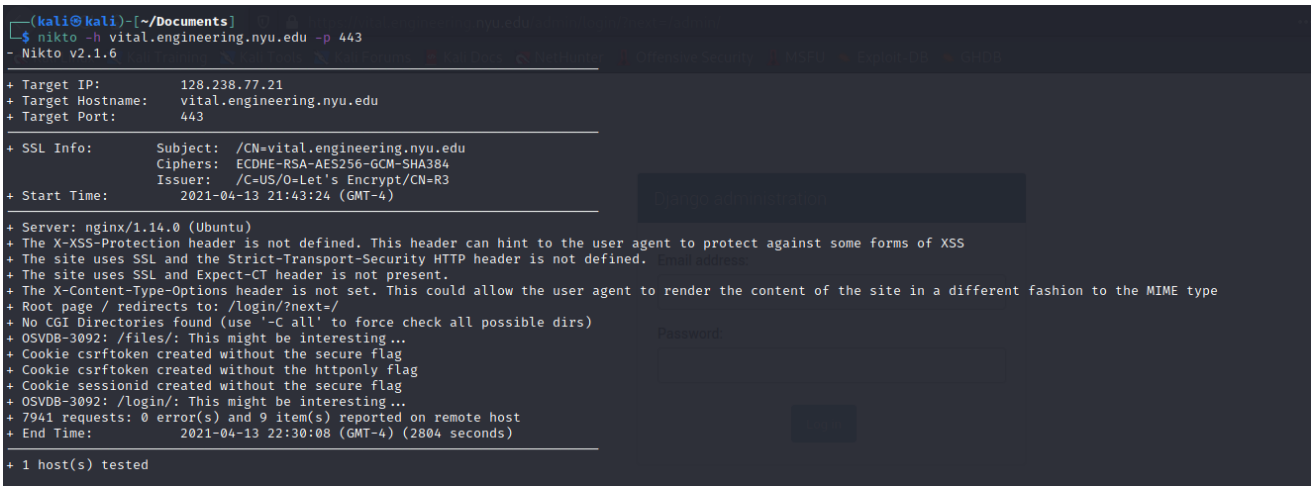
```
└─$ sslscan vital.engineering.nyu.edu
Version: 2.0.7-static
OpenSSL 1.1.1j-dev  xx XXX xxxx

Connected to 128.238.77.21

Testing SSL server vital.engineering.nyu.edu on port 443 using SNI name vital.engineering.nyu.edu

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384    Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305   Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-CAMELLIA256-SHA384 Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-CAMELLIA128-SHA256 Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-CCM8
Accepted  TLSv1.2  256 bits  AES256-CCM
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-CCM8
Accepted  TLSv1.2  128 bits  AES128-CCM
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  128 bits  CAMELLIA128-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve 25519 DHE 253
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve 25519 DHE 253
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  128 bits  CAMELLIA128-SHA

  Server Key Exchange Group(s):
TLSv1.2  128 bits  secp256r1 (NIST P-256)
TLSv1.2  192 bits  secp384r1 (NIST P-384)
TLSv1.2  260 bits  secp521r1 (NIST P-521)
TLSv1.2  128 bits  x25519

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048
```

```
┌──(kali㉿kali)-[~/Documents]
└─$ nmap -sV -sC -p- vital.engineering.nyu.edu -Pn -oG nmap-vital
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 21:42 EDT
Nmap scan report for vital.engineering.nyu.edu (128.238.77.21)
Host is up (0.078s latency).
rDNS record for 128.238.77.21: vital.poly.edu
Not shown: 58977 closed ports, 6550 filtered ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Did not follow redirect to https://vital.engineering.nyu.edu/
443/tcp   open  ssl/http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
| http-title: Vital - Virtual Lab
|_Requested resource was /login/?next=/
| ssl-cert: Subject: commonName=vital.engineering.nyu.edu
| Subject Alternative Name: DNS:vital.engineering.nyu.edu
| Not valid before: 2021-02-12T19:48:58
|_Not valid after:  2021-05-13T19:48:58
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|_  http/1.1
8086/tcp  open  http        InfluxDB http admin 1.1.1
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
8088/tcp  open  radan-http?
42713/tcp open  caldav      Radicale calendar and contacts server (Python BaseHTTPServer)
|_http-title: Directory listing for /
42714/tcp open  caldav      Radicale calendar and contacts server (Python BaseHTTPServer)
|_http-title: Directory listing for /
42715/tcp open  caldav      Radicale calendar and contacts server (Python BaseHTTPServer)
|_http-title: Directory listing for /
59990/tcp open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6f:d7:ed:bd:e0:d5:ec:b5:57:b8:9e:56:bc:4c:a4:20 (RSA)
|   256 9d:2a:ff:29:4f:9d:46:ca:09:33:ff:cc:b8:e3:79:97 (ECDSA)
|_  256 6b:ea:1d:2f:ba:3f:38:e6:b7:03:bc:6e:60:cc:81:5b (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 238.32 seconds
```

To better understand the target, we performed a nmap scan against the server. We found a couple of open ports, such as 80, 443 ,8086, 8088, and 59990. Port 8086 indicates that there is an influx DB associated with this web application. Based on manual validation, we found no web portal to access this database; however, this may bind with the Vital Web Application for tracking and storing the data.

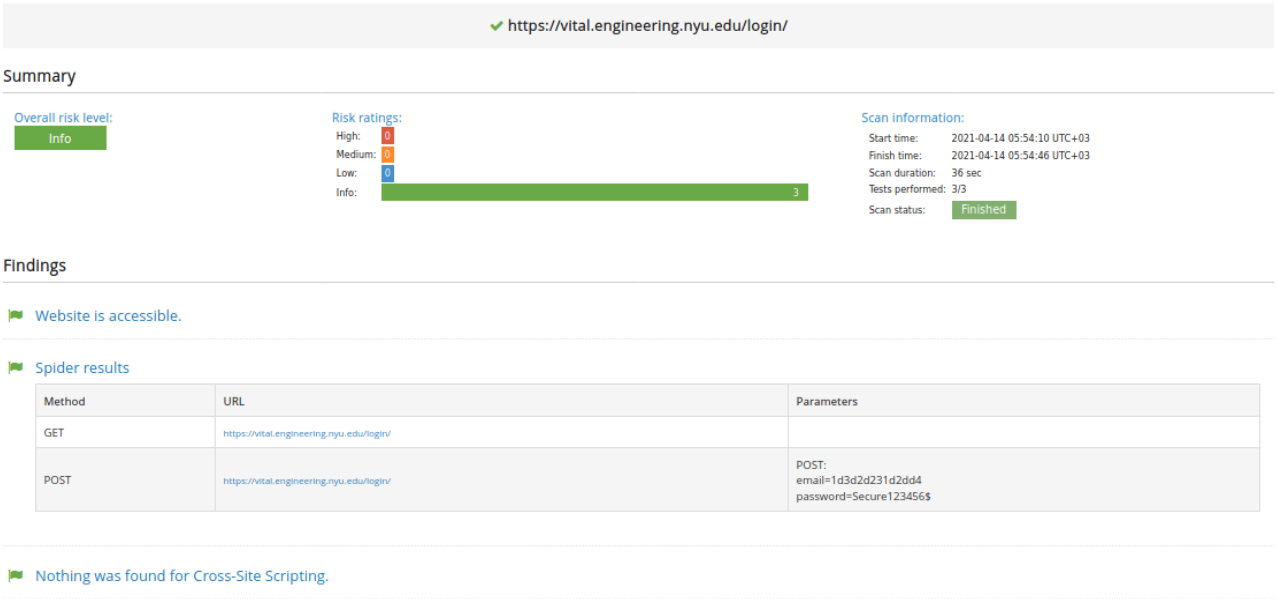


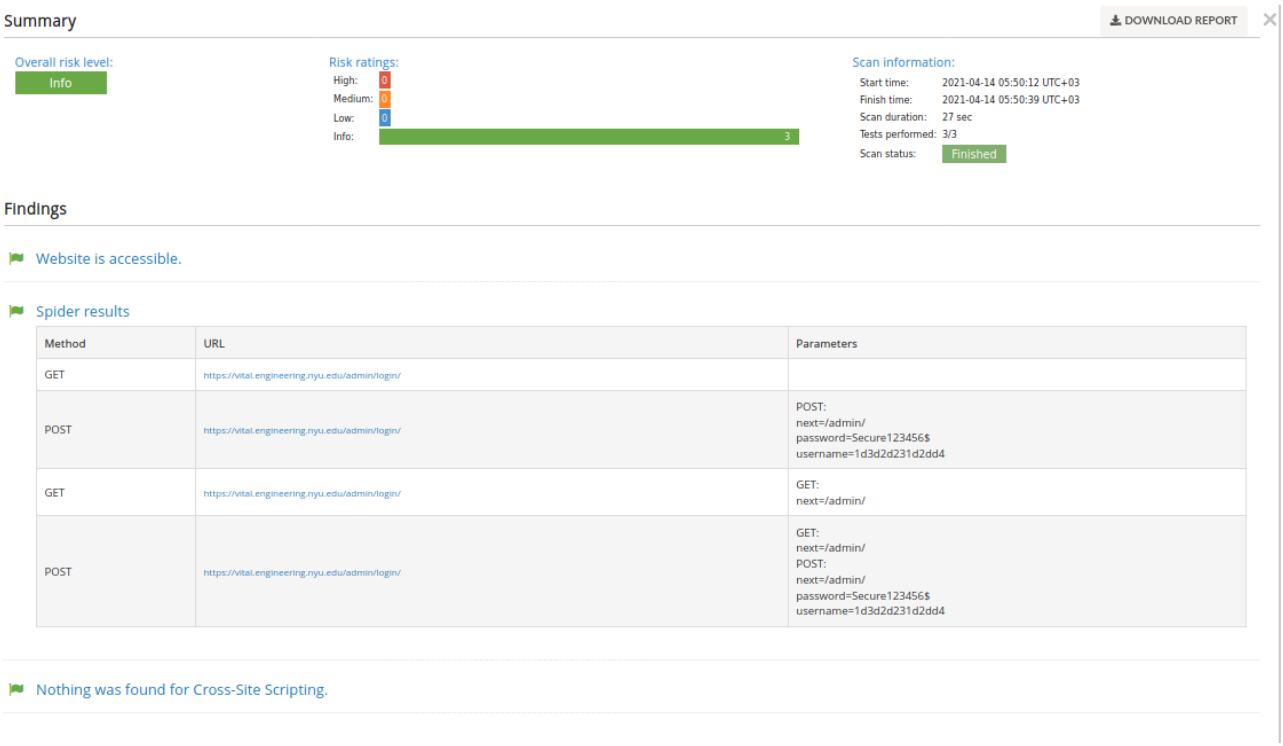
The next logical step is analyzing the web application. We utilized 'Nikto' and 'gobuster' to help us to understand the web application. We identified the web application hosted by Nginx (1.14.0) on an Ubuntu Linux OS based on the scan result. Moreover, we noticed the web application was missing sufficient secure headers. With 'gobuster', we can find out more directories in the application. The '/admin' portal and '/files' uploading portal are eye-catching. Moreover, we also identified another vhost that is configured within the same preliminary as 'gc._msdcs.vital.engineering.nyu.edu'.



```
┌──(kali㉿kali)-[~/Documents]
└─$ gobuster vhost -u https://vital.engineering.nyu.edu -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          https://vital.engineering.nyu.edu
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/04/13 23:21:19 Starting gobuster in VHOST enumeration mode
===============================================================
Found: gc._msdcs.vital.engineering.nyu.edu (Status: 400) [Size: 26]

===============================================================
2021/04/13 23:22:00 Finished
===============================================================
```

For complete penetration testing, the next step is identifying and validating the potential issue, so the next step could be a manual test based on OWASP Top 10. However, based on the limited permissions we were granted for this project, we decided not to move on.





Summary

DOWNLOAD REPORT

Overall risk level:
Info

Risk ratings:
High: 0
Medium: 0
Low: 0
Info: 3

Scan information:
Start time: 2021-04-14 05:50:12 UTC+03
Finish time: 2021-04-14 05:50:39 UTC+03
Scan duration: 27 sec
Tests performed: 3/3
Scan status: Finished

Findings

Website is accessible.

Spider results

Method	URL	Parameters
GET	https://vital.engineering.nyu.edu/admin/login/	
POST	https://vital.engineering.nyu.edu/admin/login/	POST: next=/admin/ password=Secure123456$ username=1d3d2d231d2dd4
GET	https://vital.engineering.nyu.edu/admin/login/	GET: next=/admin/
POST	https://vital.engineering.nyu.edu/admin/login/	GET: next=/admin/ POST: next=/admin/ password=Secure123456$ username=1d3d2d231d2dd4

Nothing was found for Cross-Site Scripting.

Recommendations

Project Outcomes

Some general recommendations and findings from the Risk Assessment. The following are the anticipated outcomes of Risk Assessment of Vital (Virtual Lab):

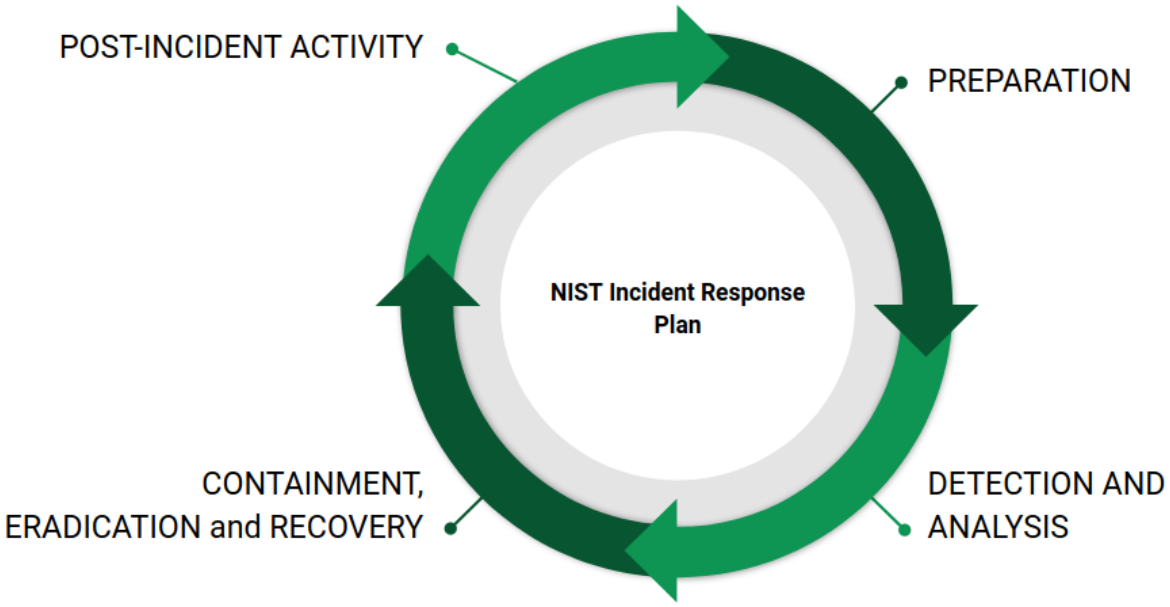
- Provide an analysis of possible threats (Physical and Virtual)
- Preventing injuries or illness (Physical risk assessment)
- Meeting legal requirements
- Creating awareness of security hazards and risks (Physical and Virtual)
- Create an accurate inventory of available assets
- Justifying the cost of managing risks
- Determining the budget to remediate risks

Architecture Recommendations

A few suggestions can be made based on the analysis of Vital's architecture, which will be based on improving the overall user experience. Many bugs in Vital seem to be associated with increased user load. The Nginx server and corresponding web framework should be reviewed for issues regarding user access and management of VMs. SFTP protocol and implementation should be checked for proper containment of outside files. In terms of data storage, where GlusterFS and other components are used, the implementation should be reviewed as this is potentially where issues regarding file bleed-over between users occur. The VM mechanism, including the XEN hypervisors and ZMQ, should be reviewed for bugs and also considered for increased scaling, because this is where issues regarding VM availability and port sharing with increased load can occur.

IT Governance Recommendations

Having a well-defined incident response plan is pertinent for first-responders in an event of a data security breach. For our report, we have relied and analysed the NIST Incident Response plan for Vital.



Prepare

Preparation is the key to rapid response. Compile asset lists and rank them based on the level of importance. Monitor their traffic patterns to create baselines for usage. Create a communication plan with guidance on who to contact, how, and when based on each incident type. Determine which security events, and at what thresholds, these events should be investigated. Then create an incident response plan for each type of incident. It can be improved through security event simulations, where you identify holes in your process.

Detection and Analysis

At this point in the process, a security incident has been identified. This is where we go into research mode. Gather everything we can on the incident. Then analyze it. Determine the entry point and the breadth of the breach. This process is made substantially easier and faster if you've got all your security tools filtering into a single location.

Containment, Eradication, and Recovery

NIST views the process of containment, eradication, and recovery as a singular step with multiple components. Containment aims to stop the bleeding. Here is where we patch the threat's entry point. Eradication aims to remove the threat. Recovery aims to get the system operational if it went down or simply back to business as usual if it didn't.

Post-Incident Activity

This step provides the opportunity to respond to future security events based on past experiences.

Virtual Interview Recommendations

As a takeaway from our interviews, Vital suffers a shortage of both funding to carry out additional security upgrades, and staff to conduct thorough reviews and to build on the existing product. Currently, Vital operates with availability as a priority; however it is not given the adequate resources to meet those requirements. From both the developer and user perspective, Vital will need a surge in improvement to meet the current needs of the networking curriculum at NYU. As NYU brings on more and more students in their Computer Science and Engineering department, so does the demand for Vital to perform as intended.

Additionally, NYU IT currently is offering limited support for the Vital platform; in the future, a role could be created in NYU IT in tandem with the CSE department to govern physical upgrades and monitoring of the Vital server. In this case, it would create a position for a subject matter expert and also reduce the potential strain on Professor Redington as the developer. This faces an initial cost by both the CSE department and NYU IT, but could evolve into a value-added situation regarding NYU Vital. Vital is a unique platform not offered by similar universities and, as indicated by Professor Reddington, has the potential (and track record) of being exported to other teaching institutions.

If given more time, we believe that we could interview other stakeholders and also see if Vital has indeed been a useful tool among NYU CSE Alumni (i.e. Cybersecurity, Cyber Fellows, Computer Science).

Physical Security Recommendations

Based on the results of the physical assessment, we recommend that NYU increase its security when it comes to guest access during events and construction crew access. Though it was evident that the server room itself was well protected, major areas like the boiler room were easily accessible to people who could enter the building. The impact of damage from these areas to other areas of the building could be severe. Trespassing was not an uncommon occurrence as well. Therefore, we recommend tighter restrictions when it comes to access to construction sites and areas that should be protected from unauthorized personnel.

Security Scorecard Recommendations

Based on the result of the security scorecard assessment, we recommend a few things to be implemented in the near future. For the network security perspective, we recommend that Vital should enhance their cipher suite and change the protocol to the latest one for TLS/SSL service. For the application security perspective, we recommend that Vital should enable CSP headers via their website configuration. These are the key points with high severity that need to be addressed not necessarily immediately, but very soon to keep the website secured.

Penetration Testing Recommendations

Based on the result from our limited manual testing, we validated the scan result from SecurityScorecard™. To enhance the security of the Vital web application, we highly recommend that the cryptographic protocols and cipher suites be managed regularly, implementing the secure

configurations to reduce the vulnerability from the browser side, and reducing the attacking surfaces.