INTERNSHIP PROJECT FINAL REPORT

Intern: Mahedi Hasan Raju
Id: 183-35-380
Institution: Daffodil International University
Dept. in Software Engineering
Company: BugsBD Limited
City: Shaymoli, Dhaka
Duration: April 2 - September 7 (6 months)
Tutors: T R Nayan Chief Technology Officer
Supervisor: Syeda Sumbul Hossain, Senior Lecturer

Your Cyber Security Partner

October 29, 2022

Approval

APPROVAL (Room- 603)

This internship titled "**Internship in Penetration Testing**", submitted by **Mahedi Hasan Raju (ID: 183-35-380)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Chairman

Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information
Technology Daffodil International University

Internal Examiner 1

Kaushik Sarker
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Dr. Md. Fazla Elahe
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

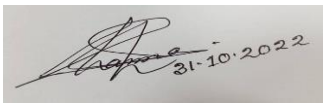
Mohammad Abu Yousuf, PhD.
Professor
Institute of Information Technology
Jahangirnagar University

Declaration

I am Mahedi Hasan Raju 183-35-380, a student of Software Engineering, at Daffodil International University, hereby declare that the report entitled BugsBD Limited is an original work done by me under the supervision of Syeda Sumbul Hossain, Senior Lecturer of the Department of Software Engineering of Daffodil International University.

Name : Mahedi Hasan Raju
ID No: 183-35-380
Batch No: 27
Major: Cyber Security
Department of Software Engineering
Daffodil International University

Supervised By:



Syeda Sumbul Hossain
Lecturer(Senior Scale)
Department of Software Engineering
Daffodil International University

Acknowledgment

I had a fantastic chance to learn and advance my career during my internship at BugsBD Limited. As a result, I view myself as a really fortunate person who was given the chance to participate in it. I am also appreciative of the opportunity to interact with so many lovely people and experts who guided me during my internship.

In light of the foregoing, I would like to take this opportunity to express my sincere gratitude and particular thanks to the MD of BugsBD Limited, who, despite being incredibly busy with other obligations, took the time to listen to me, give me advice, and keep me on the right track while also allowing me to complete my project at their prestigious organization and extending during the training.

I would like to extend my sincere gratitude to T R Nayan, Chief Technology Officer, for contributing to helpful decisions, providing necessary advice and guidance, and setting up all facilities to make life easier. I want to express my gratitude for his contribution right now.

I would like to express my sincere appreciation and best wishes to Mr. Shahriar Siddique, Jr. Cyber Security Specialist, Mr. Nowsher Ali Shovon, Jr. Cyber Security Specialist, and Mr. Fahim Ahmed, CEH, CISA, Chief Business Development Officer for their thoughtful and priceless guidance, which was extremely helpful for my study both theoretically and practically.

I perceive this opportunity as a big milestone in my career development. I will strive to use gained skills and knowledge in the best possible way, and I will continue to work on their improvement, in order to attain desired career objectives. Hope to continue cooperation with all of you in the future.

Sincerely,

Mahedi Hasan Raju 183-35-380

BugsBD Limited

Abstract

This document describes the work I have done as part of my six-month internship at BugsBD Limited in Vulnerability Assessment. The first task of this internship was the found vulnerability, targeted toward security auditors of IoT devices. The second task was to participate in different penetration tests along with the company's consultants. This report presents the result of my work on both of these tasks, specifically, details about the architecture and implementation of the tool, and my contribution to different penetration tests.

Keywords: Vulnerability Assessment, Source Code Audit, Hardware audit, Penetration testing, Compliance test, Software development.

.

TABLE OF CONTENTS

CHAPTER 1:

Introduction :

The internship program provides a great opportunity for students to relate their theoretical knowledge with practical, industry-oriented knowledge. Moreover, if the internship program is within the bachelor's program and the students have to return to the academic institution after completing it, the knowledge they have gained during the internship program helps them make more sound academic results. Daffodil International University(DIU) provides this opportunity to its students. I am very lucky that I am a student of DIU and I was sent to BugsBD Limited to perform my internship. I joined there as an intern on April 4, 2022. Now nearing the end of the internship I must admit that it was really a wonderful journey.

Motivation :

The main reason for doing an Internship:-

- To Get experience in industry work.
- Have the opportunity to learn and watch From professionals.
- To enhance my testing knowledge in more depth.
- Gain the ability to put new things into practice.
- Gather abilities for facing real-life problems.
- To communicate.
- Build confidence.

Objective :

The objectives of a student participating in an internship:

- Testing web application security.
- Monitoring inbound security data.
- Responding to minor security events.
- Escalating events as needed.
- Assessing network security for vulnerabilities.
- Disassembling and debugging malicious software.
- Researching threats.
- Assisting with penetration testing.

CHAPTER - 2 :

Company Overview :

The company was founded in 2015. The company has grown quickly and strategically, in both revenue and staff. There are 25 employees working right now in the company. In 2018 Bugsbd(https://bugsbd.com/over-view) Limited achieved one of the best service-providing companies. Bugsbd Limited, the goal is simply to make organizations better at building complex business systems. They design, sell and support software used by system architects, developers, and operations teams worldwide.

Company Service :

Now we can see my company Services -

1. Vulnerability Assessment
2. Penetration Testing
3. Security Audit
4. Network Security
5. Web application Security
6. Red Team Assessments
7. Mobile Security
8. Source Code Audit
9. API Security

Motivation :

The main reason for doing an Internship:-

- To Get experience in industry work.
- Have the opportunity to learn and watch From professionals.
- To enhance my testing knowledge in more depth.
- Gain the ability to put new things into practice.
- Gather abilities for facing real-life problems.
- To communicate.
- Build confidence.

Company Mission :

We help nations, governments, and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulations and transform their operations. Our mission is to make a significant change in the area of Data Protection, User Behaviour Analytics, and Employee Monitoring and become a worldwide leader. Based on our innovative solutions and trusted service, we want to make a secure cyber world.

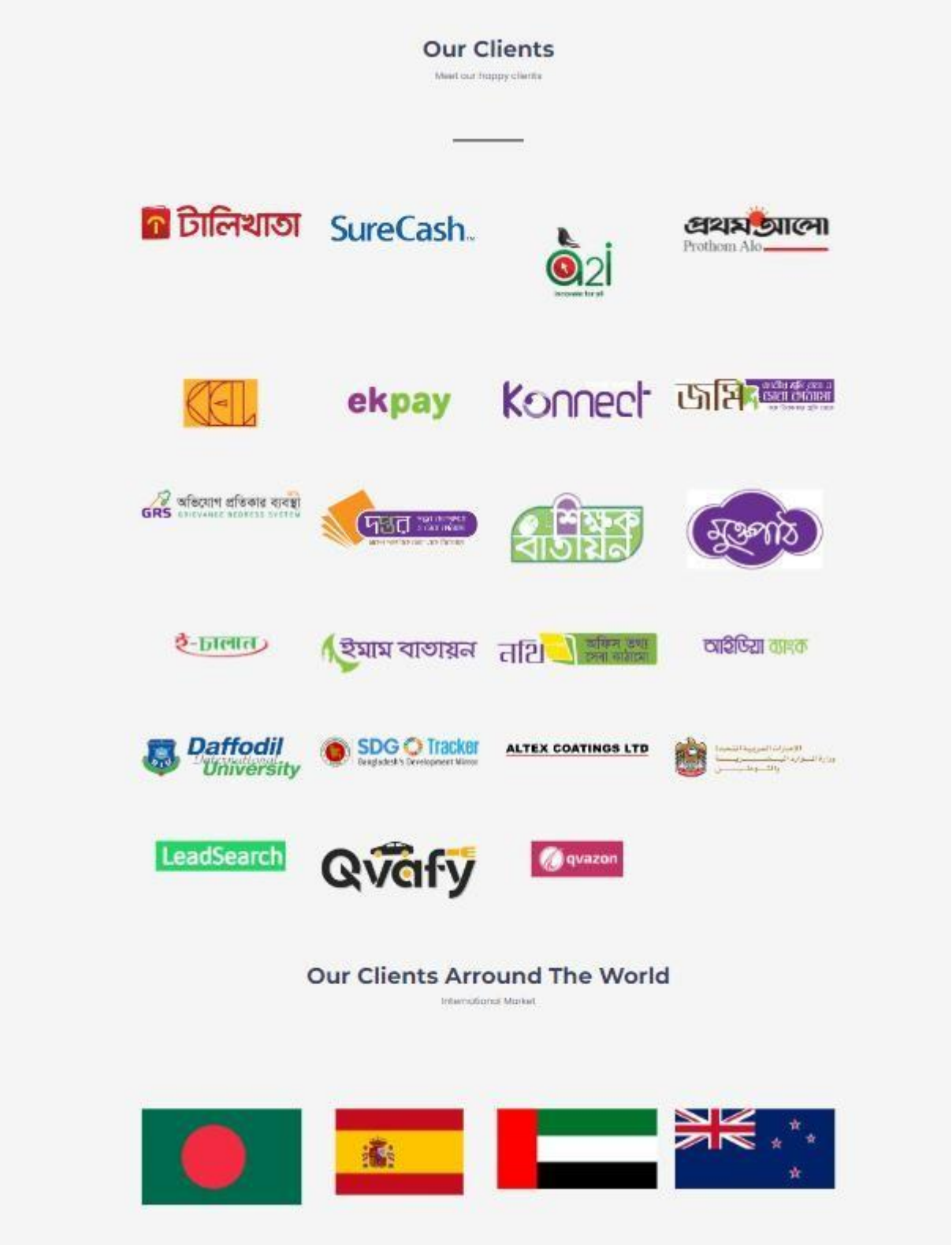
Company Vision :

We reduce the vulnerability of the digital environment by implementing combined cyber-security and cyber-defense systems that neutralize advanced threats, thereby contributing to the improvement of security. Greater customer relationships are our first priority. We deliver high-quality security products and solutions that exceed customer expectations. To maintain great work standards in any organization, we offer outstanding training services and engage high-quality professionals. By overcoming the challenges of cyber security, we want to see ourselves as global technology innovators.

Location :

1/C (5th floor) Road# 1, Shyamoli
8801889975511
info@bugsbd.com

Client :


Our Clients
Meet our happy clients
টালিখাতা
SureCash
a2i
প্রথম আলো
Prothom Alo
ekpay
Konnect
জমি
GRS
অভিযোগ প্রতিকার ব্যবস্থা
GRIEVANCE REDRESS SYSTEM
দপ্তর
শিক্ষক বাতায়ন
মুক্তপাঠ
ই-চালান
ইমাম বাতায়ন
নথি
আইডিয়া ব্যাংক
Daffodil International University
SDG Tracker
ALTEX COATINGS LTD
LeadSearch
Qvafy
qvazon
Our Clients Arround The World
International Market

CHAPTER 3: COMPANY CULTURE AND CARRYING OUT

Department/Section Overview

I am working here as a VAPT Engineer. Now I am reviewing VAPT. Both the security services of vulnerability assessment and penetration testing (VAPT) concentrate on finding weaknesses in the network, server, and system infrastructure. Both services have diverse purposes and are used to accomplish various but complementary objectives.
The following deliverables are what a Vulnerability Assessment & Penetration Testing (VAPT) operation should provide in ideal circumstances:

- Executive Report:
  A high-level summary of the activities, issues found risk categories and actions.
- Technical Report :
  A comprehensive report outlining each issue found, including step-by-step POCs, code examples, configuration examples, and reference links for further information.
- Real-Time Online Dashboard:
  This is an online gateway that enables your teams to track repairs and closure status, monitor the audit process in real time, and act quickly on high-risk issues.

Working Team :

I performed both solitary and collaborative work. Three people made up my group. I belong to the group PROTECT VIRUS. In any firm, teamwork is crucial. Strong coordination among security personnel can be helpful in many ways. Building a culture of trust among our employees, in particular, increases the likelihood that they will help one another to accomplish the shared objective. Additionally, it makes team communication more effective.

Working Environments & Protocols:

Although I find it beneficial to sometimes get together with my coworkers during the month, I prefer a setting where I can do the majority of my job on my own. I work alone a lot as a Cyber Security Specialist before returning to my team to make adjustments. The ideal working environment for me is a place where I can develop my program alone before it is shared. I found the working environment in my office to my liking.

Plans, guidelines, activities, and precautions are used in cyber security procedures to guarantee your business is protected from any potential breaches, attacks, or incidents. Since it protects against data theft and deletion, cybersecurity is essential. This includes sensitive information, personally identifiable information (PII), protected health information (PHI), personal data, data belonging to intellectual property, and information systems used by the government and businesses.

Rules & Regulations :

First of all, the organization demands that all workers act professionally and respectfully. The main goal of the business is to draw clients by having staff that behaves admirably. Employees must also wear a face mask when working in the workplace. They have an obligation to maintain a safe and hygienic workplace.
Employees are also responsible for safeguarding property used for business reasons. Any official machinery, such as a computer, printer, scanner, camera, etc., that is damaged will be their responsibility. Only official uses are permitted for company-issued equipment.

Every employee must secure papers since our organization is aware of the need to retain records. Without adequate justification, the office will not accept any argument. As a result, staff should keep official documentation for future use.
Employees are not permitted to consume alcohol while at work, according to the business. Additionally, no employee shall use any official machinery or drive any corporate cars while intoxicated. While neither encouraging nor discouraging you from drinking alcohol, our company does advise against doing so while you are working.

Meals should be consumed by workers during breaks. Employees are urged to make the most of their break time because the company won't provide them with more time for meals. Our organization is diligent in upholding the moral standards of its employees. Employees that engage in corruption and bribery will be fired by the firm without their knowledge.

Motto of the Organisation :

"Your Cyber Security Partner" is the motto of our Company.

Comparative Analysis of Office Culture :

Comparative analysis is a technique used to contrast similar objects with one another in order to discover their similarities and differences.

Even while each organization's corporate culture is distinct, all company cultures share a number of common components:

- Goals and principles
- Management and employee relationships
- Recognition of the workforce
- Evolution of the profession
- Culture and aesthetics

Internee Life Cycle

Getting Started

I started working at BugsBD Limited Company on 2nd April.

Recruiting Policies

Our organization has a basic hiring procedure that may be modified depending on the demands of a post. Our typical procedure entails:

- Resume review
- Mobile Screening
- Assignment
- Interview

Depending on the position they are filling, hiring managers may decide to add or eliminate steps. For instance, they may incorporate the subsequent selection processes:

- Assessment centers
- Group interview
- Competency/Knowledge or other selection tests
- Referrals Evaluation

Evaluation of Referrals Typically, the interview and resume screening phases are required.

First Day at Office

I received a call one day from the company's HR director informing me that I had been employed and would begin working there the following Sunday. I was overjoyed and delighted to obtain the position. I started the office by doing my portion of the preparation and arrived 30 minutes early.

CHAPTER 4: TECHNOLOGY EMPLOYING

Fundamental Technologies

"The Four Fundamentals of Personal Cybersecurity" is a strategy that applies to both people and employees in the business.

- Protect our electronic papers and data.
- Our device.
- Our connection.
- Our email.
- Our email correspondence.

Cybersecurity Technologies :

- Behavioral Analytics.
- Blockchain.
- Cloud Encryption.
- Context-Aware Security.
- Defensive Artificial Intelligence (AI).
- Extended Detection and Response (XDR).
- Manufacturer Usage Description (MUD).
- Zero Trust.

Technology in use:

Acunetix

A fully automated tool that scans all kinds of websites for more than 4500 vulnerabilities. Additionally, it offers fundamental remedial advice and proof-of-concept HTTP requests.

BurpSuite

A computer program that includes several instruments helpful in web application testing. It includes a proxy server that enables the tester to see and change the requests and responses that the browser sends and receives, as well as an intruder tool that can conduct brute-force and fuzzing attacks, a crawler that maps the website, a repeater that can be used to manually resend modified versions of requests, among many other tools.

Nessus

A network security scanner that can identify more than 45,000 vulnerabilities and has access to more than 100,000 plugins to expand its functions.

Nmap

A device for host and service discovery within a network that also can check for security holes.

Sqlmap

A strong, automated tool for detecting and exploiting SQL injections that work with a large number of databases and injection types.

Wireshark

A program that is used to continuously record and analyze all trac passing sent or received on a particular interface.

CHAPTER 5: PROJECT EXERTION

: Training/ Domain Knowledge Sharing

A job-related learning experience known as an internship tie to a student's academic field or career interests by offering relevant, practical labor. An internship gives students the chance to learn new skills, increase their career alternatives, and explore those options.

I learn a lot about my skills, as well as my advantages and disadvantages. This could come in the form of wise counsel from peers or superiors. It's a once-in-a-lifetime opportunity that I may not have as a working adult.

When I worked with BugsBD Limited, I had the chance to put the knowledge and skills I had previously learned via my schooling to use. I was able to apply these abilities to my regular employment, which helped me appreciate and value them more deeply.
For instance, I was given the responsibility of doing some vulnerability assessments while assisting the Advertising Campaigns team. I utilized a few tools to arrange my research and describe my method to achieve this.

Project Name: Vulnerability Assessment (VA)

A vulnerability assessment has to be done on any website. Also while doing this project I was given a website. I was given this website www.rapiditydx.com. I did it manually and generated a report and explained it to the client.

Vulnerability Assessment Report:

After manually working I found 4 vulnerabilities in this website, I have divided these vulnerabilities into 3 parts Low, medium, and High.

Assessment Summary:

Here assessment summary of the www.rapiditydx.com website:

Phase	Description	High	Medium	Low	Total
1	Absence of Anti_CSRF Tokens	0	5	0	5
2.	Missing Anti-clicking Header	0	3	0	3
3.	Secure Pages Include Mixed Content(Include Scripts)	0	1	0	1
4.	Cross-Domain JavaScript Source File Inclusion	0	0	6	6

Proof of concept :

Now we will discuss a vulnerability found on this website. The name of the vulnerability is Anti CSRF Token.
Anti-CSRF tokens are related pairs of tokens that are distributed to users to validate their requests and stop attackers from issuing requests through the victim. Each token has a distinct, hidden value that is unpredictable and impossible for a third party to deduce.
A user is given a pair of cryptographically related tokens known as an anti-CSRF token to verify his requests. For instance, when a user requests a page with a form from a web server, the server generates two cryptographically associated tokens and sends them together with the response to the user.

Proof of Concept:
URL: https://portal.rapiditydx.com/web/molgenics/booking/booking_form.php
Method: GET
Evidence: <form id="main_form" action="./paypal.php" method="post" enctype="multipart/form-data" >

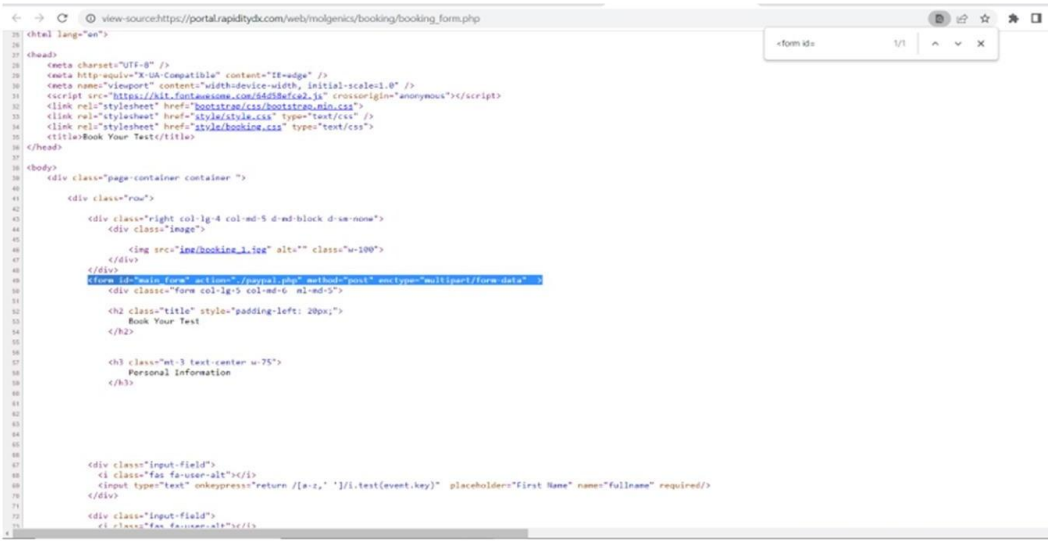


Figure: 1

Now we can see the blue marked code in the picture this code is Vulnerable.

: Solution/Prevention

In the absence of Anti- CSRF tokens, a Cross-Site Request Forgery attack may occur, resulting in the execution of a specific application action as another logged-in user, such as stealing their account by changing their email and password, or silently adding a new admin user account when executed from the administrator account.
Using anti-CSRF tokens is the most efficient way to prevent CSRF. All forms that permit users to change any state should have these tokens added by the developer. The web application should then verify that the right token is present before processing an operation.

Challenges

Because they resemble a trusted user's request for information very closely, CSRF attacks are also exceedingly challenging to identify. Since the last time the list was compiled, CSRF attacks have fallen from the fifth spot to the eighth most common and dangerous Web application vulnerability.

: Completion & Delivery

I was given 3 days to complete this project. Alhamdulillah, I can complete it and deliver it within 3 days. I am happy to finish this project on time and so is our client.

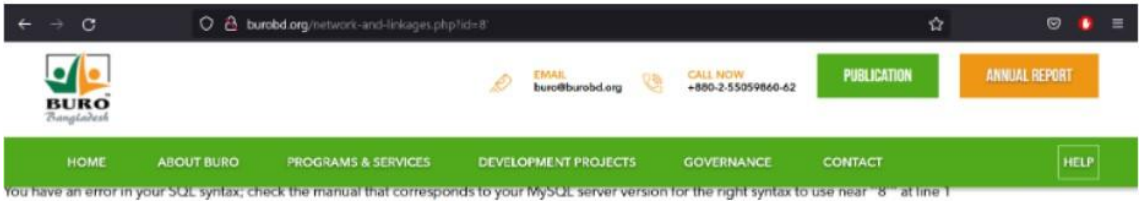
: SQL Injection Attack

SQL injection, often known as SQLI, is a common attack technique that uses malicious SQL code to obtain data that was not intended to be displayed by backend databases.

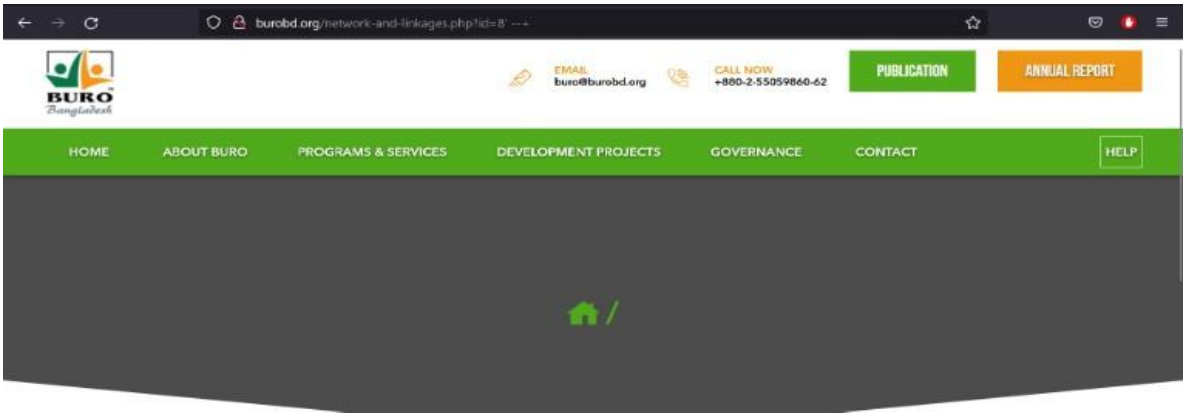
In this session, I learned how to perform SQL attacks and how to protect against SQL attacks. In the beginning, we will take the URL of a website and run a query on that website to find out where the vulnerability is. My Site Url: https://www.burobd.org/
Now we can step into SQL Injection Attack. we can use SQL query on this site and also see the URL.

Proof of concept :

Step 1 : check error

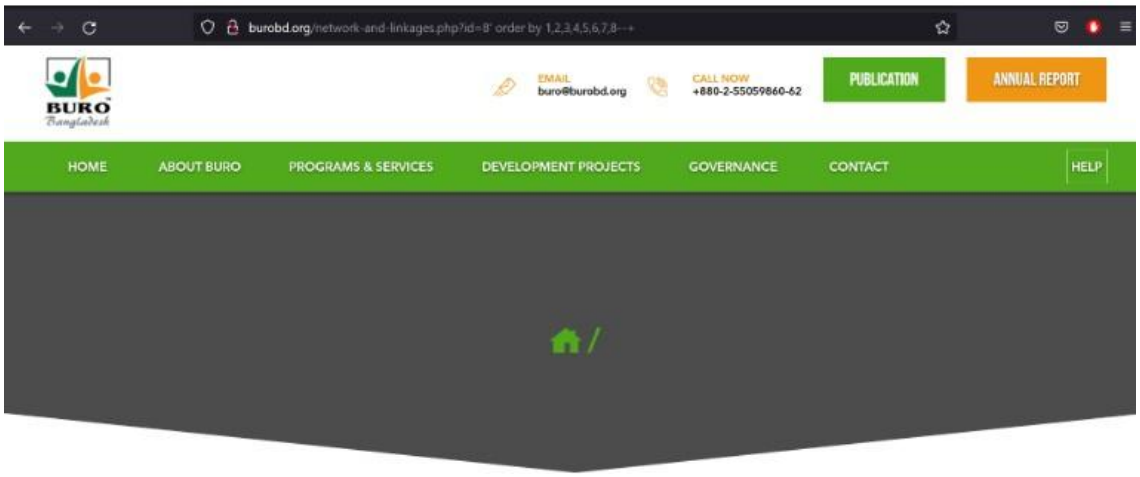


Step 2: error fixed



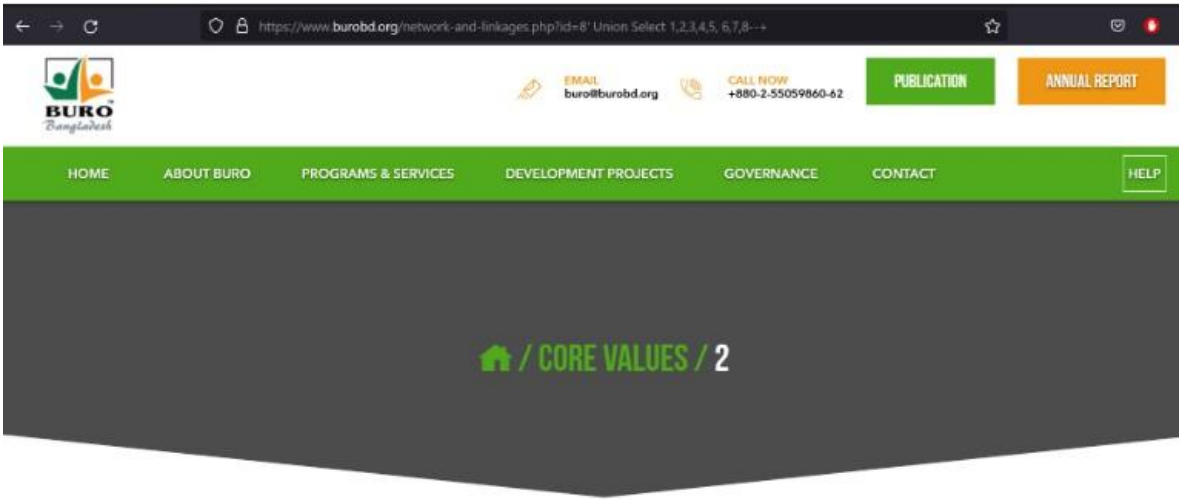
Step 3: find how many column in this website

- There have 8 column



Step 4: find vulnerable column

- Vulnerable column name 2

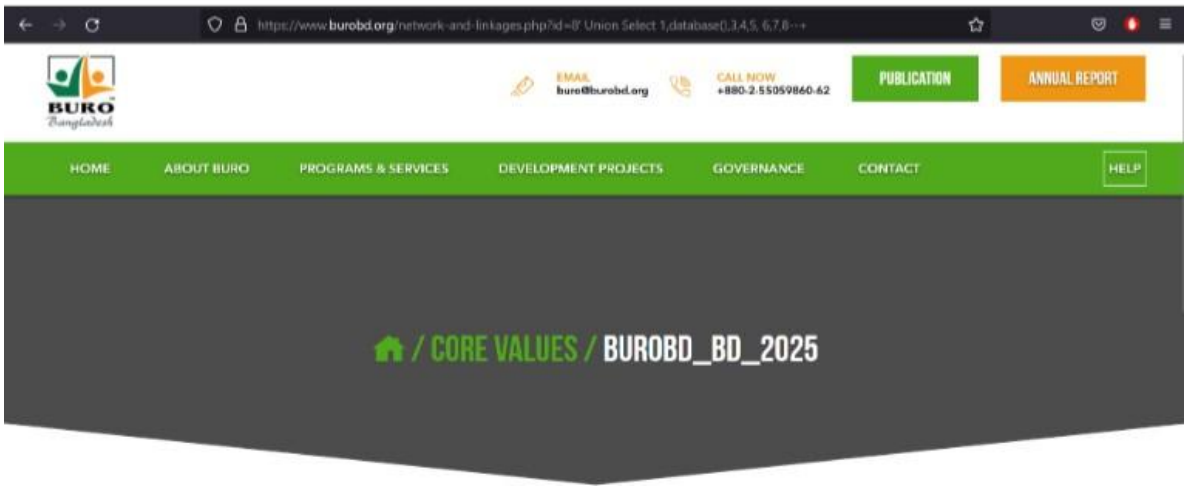


Step 5: vulnerable column database version check

- Version 5.651

Step 6: database name check

- Database name: BUROBD_BD_2025



: Solution/Prevention:

- Self-Imposed Attacks & Types of Detection.
- Check User Inputs.
- Limit special characters to clean up data.
- Enforce parameterization and prepared statements.
- Use the database's stored procedures.
- Manage patches and updates actively.
- Raise the physical or virtual firewalls.

Exploit :

- Modifying T SQL statements to return additional data.
- Modify stored procedures, functions, or other database schemas.
- Test for the existence of database or server objects, such as tables or users.
- Alter passwords or permissions.
- Access components outside of SQL Server, such as server or storage infrastructure.
- Delete, steal, alter, encrypt, or attempt to ransom data from within the database.
- Perform a denial-of-service attack on the database server by utilizing excessive resources.

: Completion & Delivery

I was given 2 days to complete this project. Alhamdulillah, I can complete it and deliver it within 2 days. I am happy to finish this project on time and so is our client. I learn new things in this project.

CHAPTER 6: EXPERIENCE AND ACHIEVEMENTS

Overcome Problems and Difficulties :

10 Ways to Overcome Challenges :

- Make A Plan. While I don't know what is going to happen in the future, I can always plan.
- Know I am Not Alone. Every person in this world has low points.
- Ask For Help.
- Feel My Feelings.
- Accept Support.
- Help Others.
- Think Big.
- Positive Mindset.
- Don’t Give Up.
- Work Smart, Not Hard.

Working Practices :

Hackers always have to practice something so that they can start working as soon as it is necessary. One of them is :

1. Always update the software
2. Refrain from clicking on shady emails
3. Always update your hardware
4. Use a secure file-sharing solution.
5. Utilise anti-virus and anti-malware software to protect data.
6. Encrypt our connections using a VPN
7. Verify URLs before you click. 8. Be diligent with passwords.
9. Turn off Bluetooth when not in use 10. Turn on two-factor authentication
11. Get rid of the malware on our computers
12. Double-check that websites use HTTPS.
13. Don’t store important information in non-secure places
14. Scan external storage devices for viruses
15. Avoid using public networks
16. Avoid the secure enough mentality
17. Invest in security upgrades
18. Back up important data
19. Train employees
20. Use HTTPS on our website
21. Employ a White Hat hacker

Technological Enhancement

Security must be flexible to keep up with the current state of affairs, where cybercriminals pose an increasingly sophisticated danger. Fortunately, several recent technology advancements have enhanced the toolkit we have available to ensure we prevail over cyber attacks. The top five technological advancements that are now supporting cyber security initiatives the most are listed below.

- Blockchain
- Cloud Technology
- IoT Security
- AI and Machine Learning
- Application Security

Non-Technical Growth (Soft Skills)

We all possess non-technical talents, which are abilities unrelated to our particular line of work. These talents, often known as soft skills, are more closely related to our character traits and routines than to our technical competence. These abilities influence my interpersonal interactions and work output. Non-technical skills can increase productivity and provide a happy, productive workplace. Here are some soft skills that I am gain in my internship life :

- Communication
- Cooperation
- Adaptability
- Organisation
- Collaboration
- Creativity
- Time management
- Prioritisation
- Enthusiasm
- Emotional intelligence

Achievement:

Knowledge and experience obtained on the job are the main accomplishments I have made during my internship. I have a variety of transferable talents thanks to my previous employment. These include in-depth familiarity with source code audit and vulnerability find out.

CHAPTER 7:
: CONCLUSIONS AND RECOMMENDATIONS

Overall, this six-month internship met my expectations and was a worthwhile learning opportunity. It gave me the chance to learn about the daily life of a pentester and a software developer, and it also helped me expand my understanding of security and software development, especially low-level programming and hardware audits. Additionally, it allowed me to put the theoretical knowledge I had learned in both of my institutions to use, which perfectly complemented the goals of my double diploma and my professional aspirations. Since we used these abilities frequently and in meetings, this internship also helped me enhance my soft skills, like oral speaking, report writing, time management, and teamwork.

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

One of the most critical components of the quickly developing digital world is cyber security. It is essential to develop self-defense skills and impart those skills to others because the threats posed by it are difficult to ignore.

Limit the IP addresses from which the corporate network can be accessed to the geographic regions from which this should logically be possible.

Recommendations for Future Works :

The following areas have been recommended as a result of the deficiencies and restrictions of each of the three instruments and approaches created for the research study for further effort :

- The design for jigless assembly methodology.
- The assembly feature selection process to enable jigless assembly
- The Feature Library to facilitate jigless assembly

REFERENCES

1. https://www.studocu.com/in/document/visvesvaraya-technological-university/computer-organization/36-internship-report-shreesha-rao/23194886
2. https://www.academia.edu/40533515/Final_year_internship_report_Cyber security
3. www.indeed.com
4. www.google.com
5. https://bugsbd.com/
6. https://owasp.org/

Turnitin Originality Report

Processed on: 01-Nov-2022 15:16 +06
ID: 1941287089
Word Count: 4041
Submitted: 1

183-35-380 By Mahedi Hasan Raju

Similarity Index	Similarity by Source	
29%	Internet Sources:	18%
	Publications:	0%
	Student Papers:	24%

4% match (Internet from 25-Oct-2022)
https://bugsbd.com/over-view

3% match (Internet from 17-Jul-2020)
https://www.slideshare.net/JobayerAhmmed/internship-report-79185827

2% match (Internet from 11-May-2022)
https://www.coursehero.com/file/146681315/Credodocx/

2% match (Internet from 03-Mar-2022)
https://www.coursehero.com/file/84010072/Final-year-internship-report-Cybersecuripdf/

2% match (student papers from 20-May-2021)
Submitted to University of Northumbria at Newcastle on 2021-05-20

2% match (student papers from 09-Feb-2021)
Submitted to PSB Academy (ACP eSolutions) on 2021-02-09

1% match (student papers from 21-Jul-2022)
Submitted to RICS School of Built Environment, Amity University on 2022-07-21

1% match (student papers from 29-Aug-2022)
Submitted to City University on 2022-08-29

1% match (Internet from 26-Jan-2022)
https://ici2016.org/how-do-you-overcome-difficult-obstacles/

1% match (student papers from 24-Aug-2022)
Submitted to University of Dubai on 2022-08-24

1% match (Internet from 16-Oct-2022)
https://scanrepeat.com/web-security-knowledge-base/absence-of-anti-csrf-tokens

1% match (student papers from 10-Jul-2021)
Submitted to Baltimore City Community College on 2021-07-10

1% match (student papers from 30-Aug-2022)
Submitted to Crown Institute of Business and Technology on 2022-08-30