



Daffodil
International
University

Internship Report

Vulnerability Assessment and Penetration Testing at
BugsBD Limited

SUPERVISED BY

Syeda Sumbul Hossain
Lecturer
Dept. of Software Engineering
Daffodil International University

SUBMITTED BY

Mohammad Jobaer Khan
ID: 191-35-437
Dept. of Software Engineering
Daffodil International University

APPROVAL

This Internship titled on “Vulnerability Assessment and Penetration Testing”, submitted by **Mohammad Jobaer Khan (ID: 191-35-437)** 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



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

Chairman



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

Internal Examiner 1



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

Internal Examiner 2



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

External Examiner

Declaration

I am **Mohammad Jobaer Khan**, ID:191-35-437, student of Daffodil International University. I am declaring that I have completed the internship in **Vulnerability Assessment and Penetration Testing at BugsBD Limited** under the supervision of **Syeda Sumbul Hossain**, Department Of Software Engineering. The VA/PT Specialist of BugsBD Limited has been prepared for the partial fulfillment of Practicum of Bachelor Software Engineering. Additionally, I am stating that I did not produce or submit this report prior for any other reason, incentive, or presentation by someone other than myself. Additionally, it is affirmed that none of the information from numerous websites and sources included in this research is plagiarized.

Jobaer Khan

Mohammad Jobaer Khan

ID: 191-35-437

Batch 27

Department Of Software Engineering
Daffodil International University

Supervised By:

Syeda Sumbul Hossain
31.10.2022

Syeda Sumbul Hossain

Lecturer (Senior)

Department Of Software Engineering
Daffodil International University

Acknowledgement

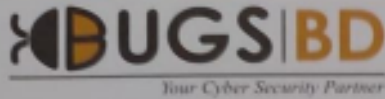
In the name of the most forgiving and gracious ALLAH.

My supervisor, Syeda Sumbul Hossain, a lecturer in the department of software engineering, deserves my gratitude. She provided me with competent advice, for which I am incredibly thankful and genuine, priceless advice and support for me. Professor and Department Head of Software Engineering Dr. Imran Mahmud holds a dependable source of encouragement for me

I'd want to express my gratitude to those that supported my internship by making useful suggestions. I'm quite appreciative and delighted to have this chance to convey my gratitude and heartfelt thanks to the distinguished faculty members of the software engineering department.

Finally, I'd like to thank my parents, who have always been a source of inspiration for me. Without their help I would not have reached to where I am now .

Offer Letter



Date: 6th April 2022

OFFER LETTER FOR INTERNSHIP

Dear Mohammad Jobaer Khan,

Following our recent discussions, we are delighted to offer you the position of **INTERN** within our Cyber Security Department. We would like to take this opportunity to welcome you to become part of a fast-paced, dedicated global team.

As a member of our BugsBD Cyber Security Team, we would ask for your commitment to deliver outstanding quality and results. In addition, we expect your personal accountability in all the products, services, actions, advice and results that you provide as a representative of Our Organization. We are committed to providing you with every opportunity to learn, grow and stretch to the highest level of your ability and potential.

We are confident you will find this new opportunity both challenging and rewarding. The following points outline the terms and conditions we are proposing.

1. Date of Joining: April 07, 2022
2. Office Hours: Saturday to Thursday: Between 11:00 AM to 7:00 PM (1 Hour Lunch Break)
3. Type of Job: Physical Office/Remote Job (Intern).
4. Duration: 6 Months

Please convey your acceptance for this letter of appointment and the terms and conditions contained herein by signing the second copy of this letter and returning the same to the Company.

Wish you all the best.

Sanid Arafat
Human Resources Department
Bugsbd Limited
Sanid Arafat Chaion
Human Resources Manager
BugsBD Limited



+8801761616261
+8801889975511



info@bugbd.com
www.bugsbd.com



1/C, Road No 1, Shyamoli,
Dhaka-1207, Dhaka

Table Of Contents

Approval.....	I
Declaration.....	II
Acknowledgement	III
Offer Letter	IV
Table Of Content.....	V
CHAPTER-1	1
1.1: INTRODUCTION:.....	1
1.2 Rational:.....	1
1.3 Background:.....	1
1.4 Scope:.....	2
1.5 The main objective:.....	3
CHAPTER-2 Company Overview	4
2.1 About My Company.....	4
2.2 Vision and Mission.....	4
2.3 Company Location	4
2.4 SERVICES:.....	5
2.5 Clients:.....	5
2.6 Company Summary.....	6
CHAPTER-3 Technology Employing.....	7
3.1 Technology	7
3.2 Technology Use	7
CHAPTER-4 Project Exertion.....	8
4.1 Confidentiality	8
4.2 Assessment Summary	8
4.3 Purpose	8
4.4 Scope	9
4.5 Summary of Finding	9
4.6 Visual Summary	10
4.7 Anti CSRF Tokens.....	10
4.7.1 Description	10
4.7.2 Impact.....	11
4.7.3 Step of Reproduce	11
4.7.4 Proof of Concept	11
4.7.5 URL: view-source.....	11
4.7.6 Method.....	11
4.7.7 Evidence.....	11
4.8 Clickjacking: X-Frame-Options header	12
4.8.1 Description.....	12

4.8.2 Impect.....	12
4.8.3 Proof of Concept.....	12
4.8.4 URL	13
4.8.5 Method.....	13
4.8.6 Evidence.....	13
4.9 Error-based SQL Injection.....	13
4.9.1 Vulnerability Description.....	13
4.9.2 Impact.....	13
4.9.3 Proof of concepts.....	13
4.9.4 URL.....	14
4.9.5 Method.....	14
4.10 Cross site scripting(XSS).....	15
4.10.1 Vulnerability Description.....	15
4.10.2 Impect.....	15
4.10.3 Proof of Concept	15
4.10.4 URL.....	16
4.10.5 URL	16
4.10.6 Method.....	16
4.10.7 Evidence.....	16
4.10.8 Technical Findings.....	16
4.11 Conclusion.....	17
Chapter-5 Conclusion And Recommendation.....	18
5.1 Summay.....	18
5.2 Suggestions for Further Action.....	18
5.3 Organization.....	18
5.4 University	19
5.5 Professional.....	19

Chapter 1

Introduction

1.1 Introduction

I interned as a VA/PT specialist at BugsBD Limited Internships as part of my Undergraduate Degree of Bsc in Software Engineering at Daffodil International University. In my internship period I worked especially in web penetration testing and my internship in web penetration testing gave me the opportunity to work at BugsBD Limited, on which this report is based.

1.2 Rational

Internships aid in developing professionalism, manners, and habits necessary for success in the workplace. Internships come with a number of advantages and can be used for undergraduate applied/technical elective credit. Students can gain valuable career-launching opportunities and learning experiences through internships. Because I want to highlight the importance of both my theoretical knowledge and my actual experience, I'm apprehensive to start my report. This gave me the opportunity to think differently and gave me a deeper knowledge of the concepts I learned in theory class.

1.3 Background

During a vulnerability assessment, the security weaknesses of an information system are methodically investigated. It assesses the seriousness of any known faults, evaluates whether the system is susceptible to them, and, if required, recommends remedies or mitigation measures.

Examples of threats that Vulnerability Assessment can stop include:

- 1)Code injection attack include SQL injection, XSS and others.
- 2)Privileges are increased as a result of insufficient authentication techniques.
- 3)Software with insecure default settings, such as admin passwords that are simple to figure out.

Steps of Vulnerability Assesment:

1. Assets discovery.
2. Prioritisation.
3. Vulnerability scanning.
4. Results analysis & Remediation.
5. Continuous Security.

1.4 Scope

VAPT (Vulnerability Assessment and Penetration Testing) services assist in assessing the current state of security, pinpointing specific faults, and recommending a corrective action plan to protect the system. VAPT tests the strength of your IT systems and security procedures in relation to potential internal and external threats. IT systems are put through a variety of simulated scenarios that potential hackers may use to access your information through a combination of automated and manual examinations. Based on the results, a thorough risk assessment report is provided, along with the steps needed to reduce the risk. By addressing these security flaws, you may be sure that you are being secured to the fullest extent possible. To guarantee that the discovered vulnerabilities have been fixed, revalidation can be done.

1.5 The main objective

A vulnerability assessment's objective is to compile a list of the network's security concerns and use that list as a road map for addressing those issues. By performing routine evaluations and fixing any security problems, a network's baseline security is supplied. Users and administrators can have peace of mind knowing that possible attackers won't be able to take advantage of vulnerabilities on their network.

Chapter 2

Company Overview

2.1 About My Company

In addition to being Bangladesh's top provider of cyber security services, BugsBD is also credited with being the first to introduce innovations to the industry. Instead of using conventional techniques to create a secure environment, BugsBD has always prioritized new approaches. The manner that BugsBD operates is constantly unique compared to other methods, allowing for customized security operations maintenance. If you really want to protect the cyber security of your business, the decision is ultimately up to you in this situation.

2.2 Vision and Mission:

We support nations, governments, and organizations all around the world with their efforts to protect themselves from cybercrime, reduce their risk in the connected world, follow laws, and modernize their operations. In the areas of user behavior analytics, data protection, and employee monitoring, our objective is to become a world leader. Based on our innovative goods and trustworthy service, we work to build a secure online environment.

By deploying combined cybersecurity and cyberdefense systems that counter modern threats, we lessen the vulnerability of digital environment and help to increase security. Our top priority is improving customer relations. We provide superior security products and solutions that go above and beyond client requirements.

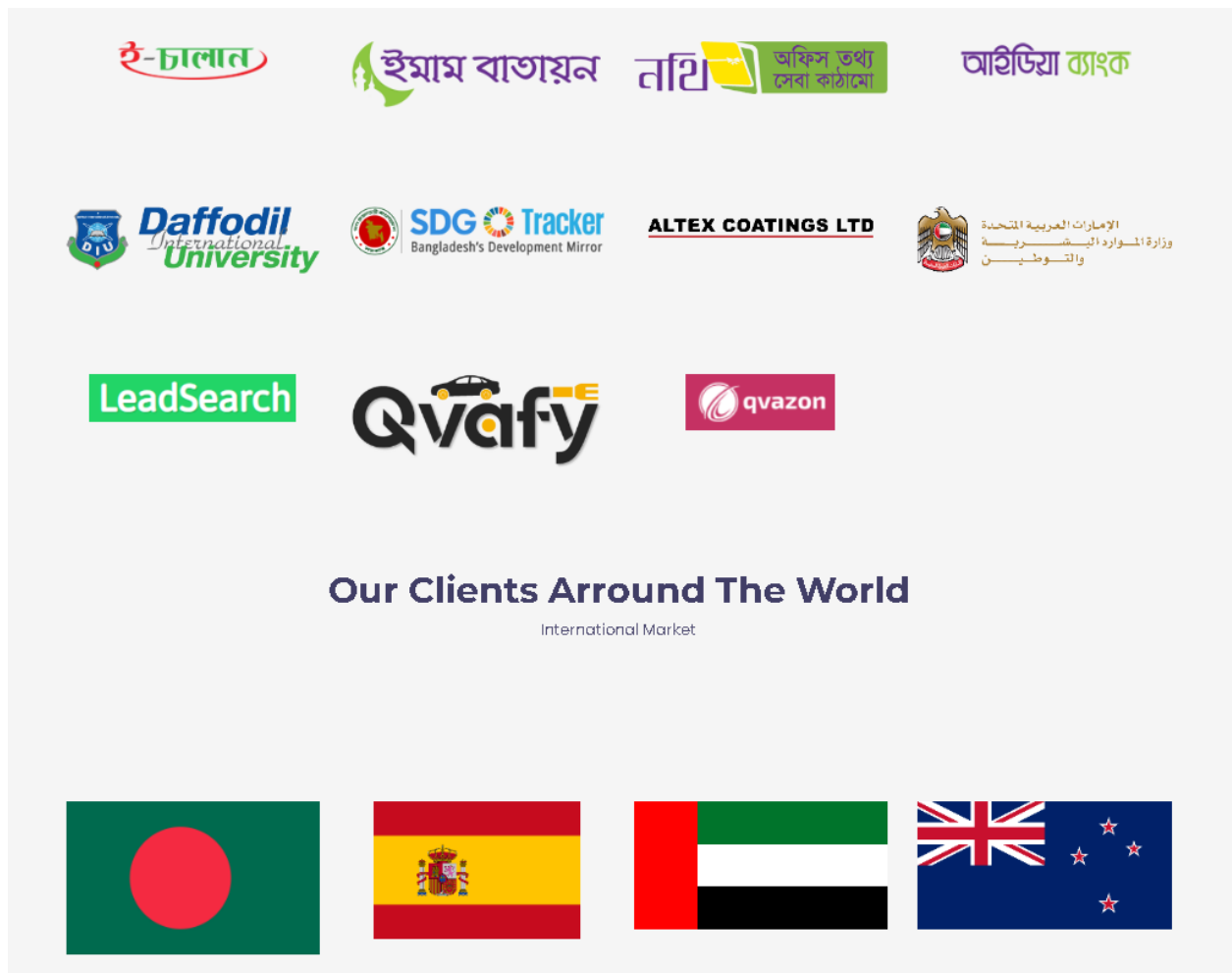
2.3 Company Location:

Shyamoli,1/C level 5, Road number: 1, Dhaka 1207,Bangladesh.

2.4 Company Services

1. Cyber Security Solution.
2. Cyber security Service.
3. Cyber Security Consulting.
4. Information Security Service.

2.5 Our Clients



The collage features the following logos:

- ই-চালান (E-Chalan)
- ইমাম বাতায়ন (Imam Baitan)
- নথি অফিস তথ্য সেবা কাঠামো (Nathi Office Information Service Framework)
- আগ্রিডিয়া ব্যাংক (Agridia Bank)
- Daffodil International University (DIU)
- SDG Tracker Bangladesh's Development Mirror
- ALTEX COATINGS LTD
- الإمارات العربية المتحدة وزارة الموارد البشرية والتوطين (UAE Ministry of Human Resources and Emiratisation)
- LeadSearch
- Qvafy
- qvazon

Our Clients Around The World
International Market

Flags representing international markets: Bangladesh, Spain, United Arab Emirates, and Australia.

2.6 Company Summery

Cybersecurity Services and Solution by BugsBD Limited with Vulnerability Assessment & Penetration Testing, Endpoint & Email Security, DLP & Compliance, SIEM, PAM, VAPT. To increase the value of your products and services, we provide straightforward and adaptable support packages. Company in Bangladesh with a primary focus on information and cyber security that specializes in IT security. Utilize our market-leading products and services, which include Security Incident Event Management (SIEM), Privileged Account Management (PAM), Endpoint Protection, Email Security & Encryption, AI-driven Cyber Security Immune System, Secure Web Gateway, Advanced Threat Protection (ATP), and Network Threat Protection, VAPT tools, and IT Audit & Consultancy Service, to stay safe.

CHAPTER 3

Technology Employing

3.1 Technologies

Fundamental technology is the combination of an understanding of how technology operates with theoretical concepts about how it has been or will be employed. We employ a variety of automatic tools, including the burp suite, Nessus, Acunetix, and Nmap. This autonomous tool is something we can learn about in fundamental technologies. We may learn about many types of vulnerability as well as how to manually find them.

3.2 Technology Use

Vulnerability scanners are useful tools that look for and report on any known flaws in the IT infrastructure of a company. An essential security technique that every organization may do is using a vulnerability scanner. By providing information about potential security flaws in the environment, these scans can provide an organization an indication of the security challenges they may be facing.

1. Burp suite
2. Nessus
3. Nmap
4. Acunetix
5. Open VAS

We also work in manually that means without the help of any tools.

CHAPTER 4

Project Exertion

4.1 Confidentiality

Information that belongs to Bugsbd Security and is confidential is contained in this document and [REDACTED] website. Before disseminating copies of this paper or its extracted contents, extreme caution should be taken. Our point of contact is authorized by Bugsbd security at [REDACTED] based on the website's data processing policy and procedures, to access and distribute this document as desired. It is recommended that this document be distributed only to those who have a legitimate need to know since it should be marked "CONFIDENTIAL."

4.2 Assessment Summary:

Here assessment summary of the [REDACTED] website:

Phase	Description	High	Medium	Low	Total
1	Anti-CSRF Tokens	0	1	0	1
2	Clickjacking: X-Frame-Options header	0	0	1	1
3	Error-based SQL Injection	1	0	0	1
4	Cross Site Scripting (XSS)	1	0	0	1

4.3 Purpose:

[REDACTED] has requested that bugsbd Security conduct a thorough security analysis of their website in order to test for vulnerabilities. At the time of the testing, this web-based interface was live, and we had access to a test/staging system. This report is being published to

reveal the complete outcomes of our testing efforts and to make recommendations when necessary. Some preliminary findings were provided under separate cover.

4.4 Scope:

This review's focus was on a single web application gateway with an Internet presence. The Internet-facing application needs a standard username and password to provide secure access.

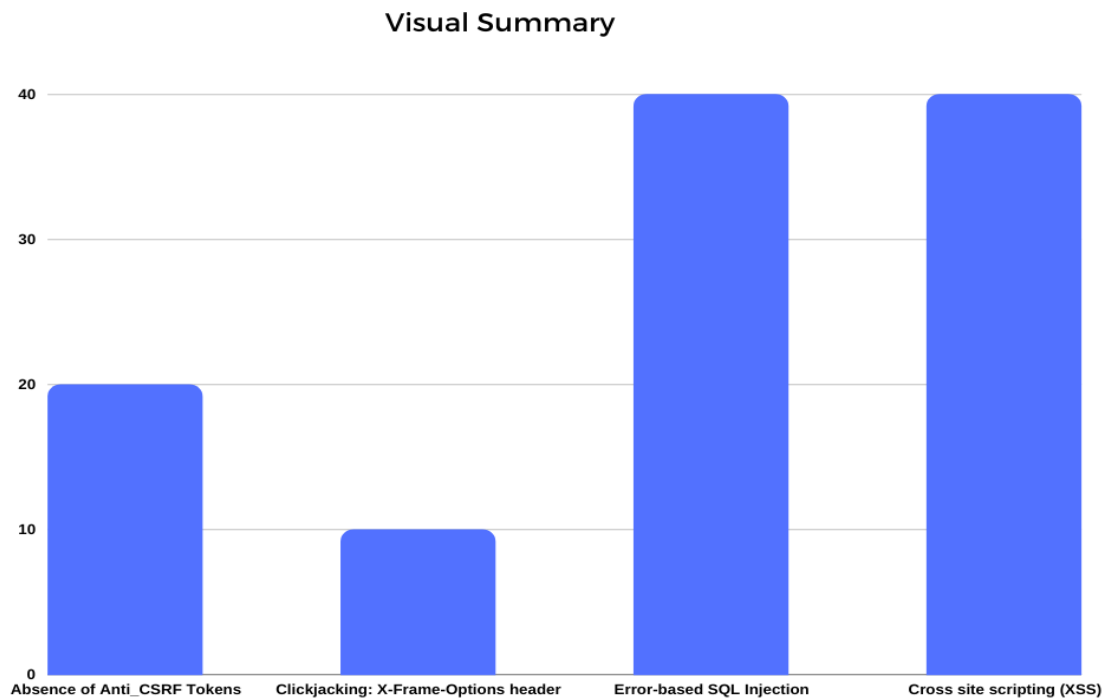
4.5 Summary of Finding:

In performing a detailed application penetration testing study against [REDACTED] application, security discovered that while there were a few cause for worry, the application as a whole was constructed using a strong security approach. We give succinct summaries of each testing category throughout this report and delve into greater detail when our results were unfavorable. A breakdown of the vulnerabilities found according to category and risk severity is shown in the table below. Following this table is a thorough breakdown of each category. A vulnerability marked as "Pending" in the table below has been reported.

Vulnerabilities with risk rating

ID	Vulnerability Title	Recommended Action	Risk category	CVSS
1	Anti-CSRF Tokens		Medium	4.3
2	Clickjacking: X-Frame-Options header		Low	3.7
3	Error based SQL Injection		High	7.3
4	Cross Site Scripting (XSS)	Make sure that all user supplied content is properly escaped.	High	7.8

4.6 Visual Summary:



4.7 Vulnerability Name: Anti CSRF Tokens.

Vulnerability Name	Risk Level
Anti CSRF Tokens	Medium

4.7.1 Description: we can not find Anti CSRF tokens in a HTML submission form.

Anti CSRF token as a pair of Cryptographically related tokens given to a user to validate his request. CSRF token can prevent CSRF attack by making it impossible for an attacker to construct a full valid HTTP request suitable for feeding to a victim user.

CSRF attacks work well when:

- * The victim is actively browsing the target website.

4.7.2 Impact: An attacker can launch a Cross-Site Request Forgery Attack by abusing the trust between the victim's browser and the webserver when a website sends a data request to another website on the victim's behalf along with the user's session cookie.

4.7.3 Step of Reproduce: Phase- Architecture and design.

Use a tested library or framework that either prevents this weakness from occurring or offers components that make it simpler to avoid this problem.

For example, use anti CSRF packages such as OWASP CSRF Guard.

4.7.4 Proof of Concept:

```
<button type="button" class="detail-modal-close detail-modal-close-small" data-bs-dismiss="modal" aria-label="Close" data-bbox="840 595 889 605">Close</button>
</div>
<div class="modal-body pt-2" data-bbox="141 615 889 712">
  <div class="contact-form-action" data-bbox="165 625 889 712">
    <small id="searchAlertModalTitle" class="mb-3 d-block"></small>
    <form id="createFavNameForm" method="POST" data-bbox="185 645 889 712">
      <div class="input-box" data-bbox="205 655 889 712">
        <div class="form-group" data-bbox="225 665 889 712">
          <input type="text" name="favName" required class="form-control" value="" placeholder="Favourite List" data-bbox="245 675 889 695"/>
          <br>
          <div class="btn-box pt-3" data-bbox="245 700 889 712">
```

4.7.5 URL: view-source: 

4.7.6 Method: GET

4.7.7 Evidence: <form id="createFavNameForm" method="POST"

4.8 Vulnerability Name: Clickjacking: X-Frame-Options Header

Vulnerability Name	Risk Level
Clickjacking: X-Frame-Options Header	Low

4.8.1 Description: Clickjacking (also known as User Interface redress attack, UI redress attack, or UI redressing) is a malicious technique used to trick a Web user into clicking on something other than what they think they are clicking on, potentially disclosing private information or taking control of their computer while they are clicking on what appear to be innocent web pages.

This website may be vulnerable to a clickjacking attack since the server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN. Optional X-Frames A browser's ability to render a page inside of a frame or iframe can be controlled using the HTTP response header. By making sure that their material is not integrated into unreliable sites, websites can use this to protect themselves from clickjacking assaults.

4.8.2 Impact: The impact depends on affected Web Applications.

4.8.3 Proof of Concept:

The iframe element

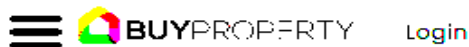


Figure: 1

4.8.4 URL: [REDACTED]

4.8.5 Method: GET

4.8.6 Evidence: <iframe src="https://www.w3schools.com" title="W3Schools Free Online Web Tutorials">
</iframe>

4.9 Vulnerability Name : Error-based SQL Injection

Vulnerability Name	Risk Level
Error-based SQL Injection	High

4.9.1 Vulnerability Description :

An in-band injection technique called error-based SQL injection enables threat actors to alter database data by taking advantage of error output from the database. It manipulates the database to produce an error that informs the actor of the database's structure.

4.9.2 Impact

The impact of this vulnerability:

A web application's authentication and permission controls can be disregarded by an attacker using SQL injection to access the full database's contents. In order to maintain data integrity, SQLi can also be used to add, alter, and delete records from databases. In the correct circumstances, an attacker can also utilize SQLi to run OS commands, which they can then use to further escalate their attack.

4.9.3 Proof of concepts:

Url: [REDACTED]

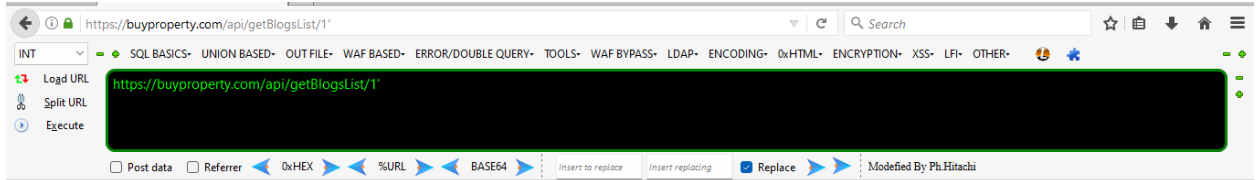


Figure: 2

4.9.4 URL: [REDACTED]

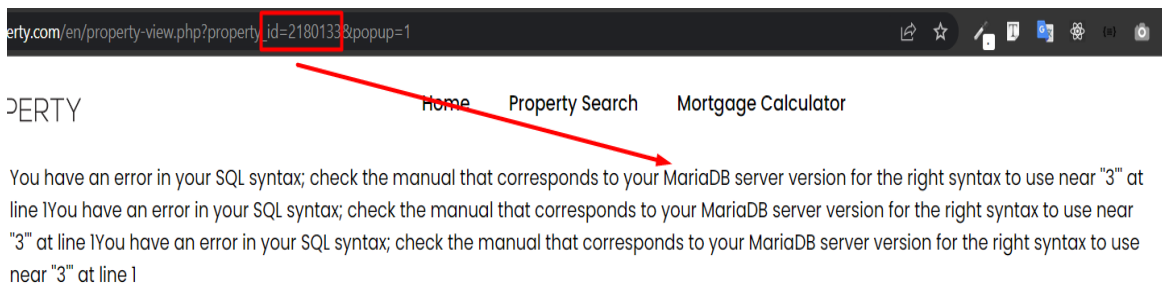


Figure: 3

4.9.5 Method: GET

4.10 Vulnerability Name: Cross site scripting(XSS)

Vulnerability Name	Risk Level
Cross site scripting (XSS)	High

4.10.1 Vulnerability Description : Malicious scripts are injected into otherwise trustworthy and innocent websites in Cross-Site Scripting (XSS) attacks. XSS attacks take place when an attacker sends malicious code, typically in the form of a browser side script, to a separate end user using an online application. These attacks can be successfully conducted everywhere a web application incorporates user input without verifying or encoding it into the output it produces.

4.10.2 Impact: Cross-site scripting assaults have dire repercussions. A susceptible application's code injection vulnerability allows for the installation of malware or the exfiltration of data. Through the use of session cookies, attackers can pretend to be authorized users and carry out any action permitted by the user account.

4.10.3 Proof of concepts: [REDACTED]

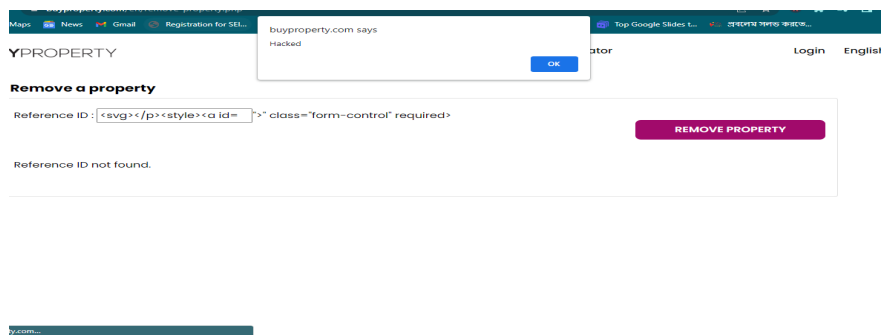


Figure: 4

4.10.4 URL: [REDACTED]

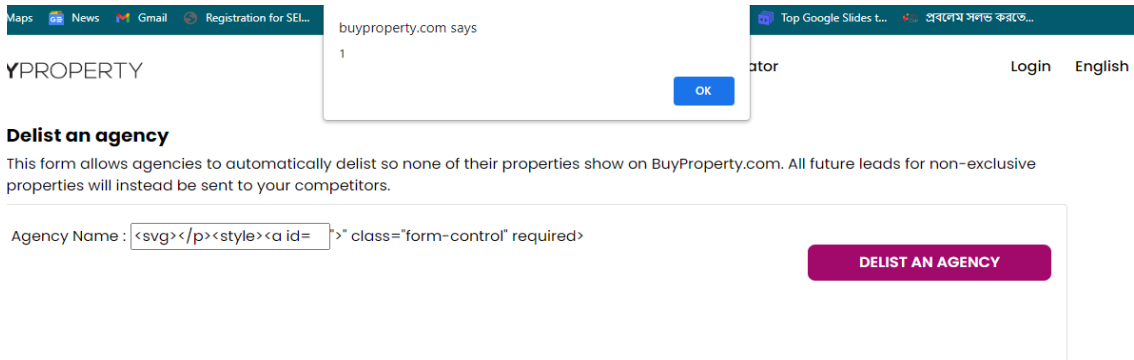


Figure: 5

4.10.5 URL:



4.10.6 Method:GET

4.10.7 Evidence: <svg></p><style><a id="</style>>

4.10.8 Technical Findings

Pentest advises Report URI to discuss each of the conclusions brought forth in this part. Each is given the following information:

Descriptive Vulnerability Title – The industry standard word is frequently used.

Background Information – Which briefly outlines the finding and is designed for an audience who have not encountered it before.

Details – This is completely suited to the target environment and contains evidence of the flaw's existence as well as the procedures needed to recreate it.

Risk Analysis – Contextual Information about the risk rating.

Recommendation – suggestions on how to handle the discovery. This will, whenever possible, suggest a specific fix for the issue. Some, though, might promote more conversation or provide suggestions for how to lessen the effect.

References – other web sites that might be read to completely comprehend a problem or that help with a solution.

Affected Item(s) – a statement describing the findings' effects. Depending on the situation, this will typically be a hostname, IP address, service, or an absolute or relative URI.

Based on the assessed risks, these have been listed in order of priority.

4.11 Conclusion:

A thorough way to find system vulnerabilities is vulnerability assessment. It offers advantages including financial loss protection, compliance with market authorities, customers, and shareholders, maintaining corporate image, and proactive risk removal. The preparation, administration, and analysis of tests are the three phases of the approach described in this work. Information collecting, vulnerability analysis, and vulnerability exploitation are the three processes in the testing phase. This step can be carried out manually. The testers should present the test results in a thorough format. The planning of remediation, which includes all essential remedial actions for the detected vulnerabilities, is one of the test analysis phase's most crucial components.

Chapter 5

Conclusion And Recommendation

5.1 Summary

A collection of methods, instruments, and processes together referred to as "cyber security" are used to protect computer systems, networks, and data from hacker attacks and unauthorized access. Cyber security's main objective is to safeguard all organizational resources against external and internal threats as well as disruptions caused by natural disasters.

Because organizational assets are made up of several distinct systems, an effective and efficient cyber security posture requires coordinated efforts across all of the organization's information systems.

5.2 Suggestions for Further Action

Students can gain practical experience in a field linked to their academics through internships. This opportunity for students to witness how their studies are put to use in the real world benefits them.

5.3 Organization

Before I started working at BugsBD, I had no concept of success. I'm fully aware of the situation now, though. I'll never forget the outstanding help I got from my fellow team member at BugsBD. Not everyone, though, is as lucky as I am. It is up to them to deal with the office environment and culture, I strongly advise them. There must be a recreation strategy in place for

the workplace. I had a lot of joy playing Carrom for entertainment, which always encouraged me to put in a lot of effort. We would need to expand our everyday routine because life is not always a bed of roses. Therefore, everyone needs to take a break from work so they can refuel.

5.4 University

A terrific approach for prospective employees to learn more about a certain career, assess their interest in that profession, and develop a network is through an internship. Because the internship course is a requirement for the course, I am happy to be a DIU student. I want to thank the Institute of Information Technology for giving me the chance to get ready for the working world. Without a doubt, it has helped me become more practical. I'm now eager to face the challenges the world will present.

5.5 Professional

Humans make mistakes, and the only way to learn is via mistakes. Internships are a great way to take your self-development to the next level. Many people see it as a paraphrase, but I believe this notion to be false because anything is possible with enough willpower and effort. That is what I think, and internships are also incredibly helpful to the interns themselves since they provide them the chance to learn more about what it's actually like to work for a specific business or in a particular sector of the economy. There are certain common difficulties that interns encounter, such as difficult time management. Take the best knowledge you can away from the internship, no matter the situation.

Turnitin Originality Report

Processed on: 01-Nov-2022 15:37 +06
 ID: 1941293931
 Word Count: 3674
 Submitted: 1

191-35-437 By Mohammad Jobaer
 Khan

Similarity Index

23%

Similarity by Source

Internet Sources: 14%
 Publications: 0%
 Student Papers: 13%

5% match (Internet from 26-Oct-2022)

<http://dspace.daffodilvarsity.edu.bd:8080/bitstream/handle/123456789/8586/181-35-329.pdf?isAllowed=y&sequence=1>

3% match (Internet from 21-Apr-2022)

<https://pentestreports.com/reports/Pentest-Limited/Report%20URI%20-%202020%20Penetration%20Test%20Report.pdf>

2% match (student papers from 04-Apr-2018)

Class: Article 2018
 Assignment: Journal Article
 Paper ID: [940943762](#)

2% match (Internet from 25-Oct-2022)

<https://bugshd.com/over-view>

2% match (student papers from 06-Sep-2022)

[Submitted to Republic of the Maldives on 2022-09-06](#)

1% match (student papers from 06-Oct-2022)

[Submitted to Asia Pacific University College of Technology and Innovation \(UCTI\) on 2022-10-06](#)

1% match (Internet from 04-Oct-2022)

<https://www.ijraset.com/files/serve.php?FID=170>

1% match (student papers from 21-Dec-2016)

[Submitted to RMIT University on 2016-12-21](#)

1% match (student papers from 02-Oct-2022)

[Submitted to uwe on 2022-10-02](#)

1% match (student papers from 04-Aug-2022)

[Submitted to Noroff University College on 2022-08-04](#)

1% match (Internet from 29-Nov-2020)

<https://www.synopsys.com/glossary/what-is-cyber-security.html#:~:text=The%20main%20purpose%20of%20cyber,caused%20due%20to%20natural%20disaster>

1% match (student papers from 11-Oct-2022)

[Submitted to San Jacinto College District on 2022-10-11](#)

1% match (student papers from 15-May-2020)

[Submitted to Leeds Metropolitan University on 2020-05-15](#)

1% match (student papers from 02-Aug-2021)

[Submitted to Mapúa University on 2021-08-02](#)

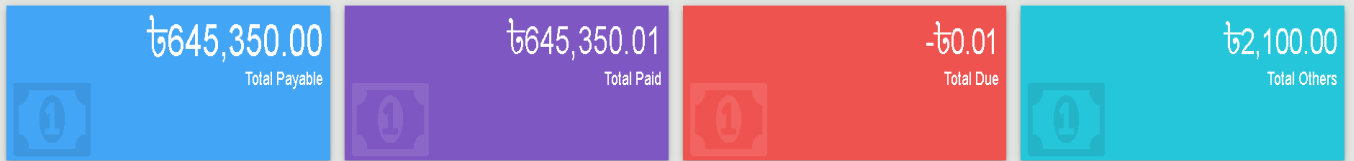
1% match (student papers from 14-Sep-2022)

[Submitted to TAFE NSW Higher Education on 2022-09-14](#)

< 1% match (student papers from 23-Sep-2022)



Student Dashboard



Payment Scheme

Daffodil International University

