



**Daffodil**  
*International*  
**University**

## **INTERNSHIP REPORT**

**Vulnerability Assessment and Penetration Testing at**

**BugsBD Limited**

### **SUBMITTED BY**

**Md. Naimur Rahman**

**191-35-439**

**Department of Software Engineering**

**Daffodil International University**

### **SUPERVISED BY**

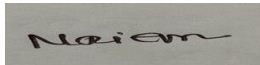
**Syeda Sumbul Hossain**

**Senior Lecturer**

**Department of Software Engineering**

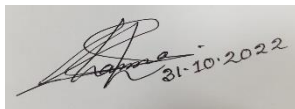
## Declaration

I am Md. Naimur Rahman, ID:191-35-439, student of DIU- Daffodil International University. I am declaring that I have completed the internship in Penetration testing at BugsBD Ltd under the supervision of Syeda Sumbul Hossain, Department of software Engineering. A penetration test, also known as a pen test, is a simulated cyber-attack against our computer system to check for exploitable vulnerabilities. I am also declaring that this report has not been submitted previously for any other purpose, or reward by anyone rather than me.



-----  
Md: Naimur Rahman  
Student ID: 191-35-439  
Department of Software Engineering  
Faculty of Science & Information Technology  
Daffodil International University

### Supervised By:



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

## **Acknowledgment**

In the name of ALLAH, who created me. I want to thank my supervisor Syeda Sumbul Hossain Lecturer, Department of Software Engineering, who was my supervisor. I am extremely grateful to her for her expert, sincere, and valuable guidance to me. Dr. Imran Mahmud, Professor, and Head of the Software Engineering Department has been a consistent source of support for me.

I'd like to show my thankfulness to those who contributed to my internship by making valuable suggestions. I am really grateful and glad to have this opportunity to express my gratitude and deep appreciation to our esteemed faculty members of the Department of Software Engineering.

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

# Offer Letter



Date: 31<sup>th</sup> March 2022

## OFFER LETTER FOR INTERNSHIP

Dear Md. Naimur Rahman,

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 02, 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.

*Sanzid Arafat*  
Human Resources Department  
Bugsbd Limited  
Sanzid Arafat Chaion  
Human Resources Manager  
BugsBD Limited

+8801761616261  
+8801889975511

info@bugbd.com  
www.bugbd.com

1/C, Road No 1, Shy  
Dhaka-1207, Dh

## Contents

Declaration .....	i
Acknowledgment .....	ii
Offer Letter .....	iii
CHAPTER 1 .....	1
1.1: INTRODUCTION: .....	1
1.2 Rational: .....	1
1.3 Background: .....	1
1.4 Testing methods: .....	2
1.5 Scope: .....	2
1.6 The main objective: .....	3
2.1 About: .....	4
2.2 Vision and Mission: .....	4
2.3 Location: .....	5
2.4 SERVICES: .....	5
2.5 SOLUTIONS: .....	5
2.6 Clients: .....	6
2.7 Values: .....	6
2.8 summary: .....	6
CHAPTER 3: COMPANY CULTURE .....	7
3.1 BugsBD Ltd Dept. list .....	7
<b>3.1.1 Cyber Security:</b> .....	7
3.2 Services of BugsBD Ltd. ....	7
<b>3.2.1 Red Team Assessments</b> .....	7
<b>3.2.1.1 overview</b> .....	7
<b>3.2.1.2 case study</b> .....	7
<b>3.2.1.3 Problem statement</b> .....	8
<b>3.2.1.4 Solutions</b> .....	8
<b>3.2.1.5 Benefits</b> .....	9
3.2.2 Vulnerability Assessment .....	9
<b>3.2.2.1 Overview</b> .....	9
<b>3.2.2.2 Case study</b> .....	9
<b>3.2.2.3 Problem statements</b> .....	10
<b>3.2.2.4 Solutions</b> .....	10
<b>3.2.2.5 Benefits</b> .....	11

3.2.3 Penetration Testing Services .....	11
<b>3.2.3.1 Overview</b> .....	11
<b>3.2.3.2 Case study</b> .....	11
<b>3.2.3.3 Problem statements</b> .....	12
<b>3.2.3.4 Solutions</b> .....	12
<b>3.2.3.5 Benefits</b> .....	13
3.2.4 Mobile Security .....	13
<b>3.2.4.1 Overview</b> .....	13
<b>3.2.4.2 Case study</b> .....	13
<b>3.2.4.3 Problem statements</b> .....	13
<b>3.2.4.4 Solutions</b> .....	14
<b>3.2.4.5 Benefits</b> .....	14
3.2.5 Source Code Review .....	14
<b>3.2.5.1 Overview</b> .....	14
<b>3.2.5.2 Case study</b> .....	14
<b>3.2.5.3 Problem statements</b> .....	14
<b>3.2.5.4 Solutions</b> .....	15
<b>3.2.5.5 Benefits</b> .....	15
3.2.6 Network Security .....	15
<b>3.2.6.1 overview</b> .....	15
<b>3.2.6.2 Case study</b> .....	15
<b>3.2.6.3 Problem statements</b> .....	16
<b>3.2.6.4 Solutions</b> .....	16
<b>3.2.6.5 Benefits</b> .....	16
3.3 Cyber Security Solutions for organizations .....	16
3.4 Internee Life Cycle .....	17
<b>3.4.1 Professional Environment</b> .....	17
3.5 First Day at Office .....	17
3.6 Other Relevant Activities .....	17
CHAPTER 4: TECHNOLOGY EMPLOYING .....	18
4.1 Fundamental Technologies: .....	18
<b>4.1.1 Supportive Technologies:</b> .....	18
4.2 Technology in use: .....	18
CHAPTER 5: PROJECT EXERTION .....	19
5.1 Project Name: .....	19

5.2Project Name: VAPT .....	23
5.3 Project name: .....	26
CHAPTER 6: EXPERIENCE AND ACHIEVEMENTS .....	30
6.1: Acquired Knowledge .....	30
6.2: Overcome Problems and Difficulties.....	30
6.3: Implications to University’s Internship Program .....	30
6.4: Soft skill.....	30
6.5: Achievement .....	31
6.6: Dependence.....	31
CHAPTER 7: CONCLUSIONS And RECOMMENDATIONS.....	32
7.1 Summary .....	32
7.2 Recommendations for Future Actions .....	32
<b>7.2.1 Organization</b> .....	32
<b>7.2.2 University</b> .....	32
<b>7.2.3 Professional</b> .....	33
REFERENCES .....	34

# CHAPTER 1

## **1.1: INTRODUCTION:**

I interned as a Penetration tester at BugsBD Ltd, Internships as part of my Undergraduate degree of Bachelor of Science in Software Engineering at Daffodil International University (DIU). I am interested in Vulnerability Testing, and my internship in Penetration testing gave me the opportunity to work at BugsBD Ltd, on which this report is based.

## **1.2 Rational:**

Internship helps to build up confidence, etiquette, and habits which contribute to success. Internships can offer a variety of benefits. Internships provide students with much learning experiences and possibilities as they begin their careers. I want to emphasize the value of my theoretical knowledge as well as my practical experience and indeed it helped me to earn more practical experience.

## **1.3 Background:**

A penetration test, sometimes referred to as a pen test or ethical hacking, is an authorized simulated cyberattack that is conducted to evaluate the security of a computer system.

To grasp the distinction, compare this to a vulnerability analysis. Bug avoidance, decreased development costs, and improved performance are just a few benefits of testing. Make a plan for handling testing. Pen testing involves breaking into multiple application systems to look for security flaws like unsensitized inputs that are susceptible to code injection attacks. The information gained from the penetration test may be used to strengthen our WAF security protocols and address vulnerabilities that were discovered.



It consists of following stages:

- . Planning and reconnaissance
- . Scanning
- . Gaining Access
- . Maintaining access
- . Analysis

#### **1.4 Testing methods:**

- . External testing
- . Internal testing
- . Blind testing
- . Double-blind testing
- . Targeted testing

#### **1.5 Scope:**

Application, user, network, device, account, and other assets that should be examined to meet the organization's goals are referred to as the "scope" of a penetration test. When the scope is limited due to constraints on time, money, or improperly stated objectives, issues arise. On the other side, problems can also result from overscoring, which frequently results in high costs or an unbalanced influence on operations. Organizations should collaborate with their penetration testers to establish goals and purposes before beginning the process in order to define the scope properly. The comprehensive list of everything a penetration testing team will investigate or has agreed not to examine in penetration is known as the penetration testing scope. There is never just one factor or aspect that makes up penetration scope. The total of an engagement's scope includes.

## **1.6 The main objective:**

A penetration test, commonly referred to as a pen test, simulates a cyber-attack on our computer system to look for weaknesses that might be exploited. Penetration testing is frequently used to supplement a web application firewall in the context of web application security. The most crucial phase of a penetration test is reconnaissance. It is there that we learn more about the target. The more knowledge we have about the target, the simpler it will be for us to try to obtain access, therefore reconnaissance is crucial. Penetration testing's objective is to identify security flaws that might be used by attackers.

## **CHAPTER 2: COMPANY OVERVIEW**

### **2.1 About:**

In Bangladesh, BugsBD is not only the top provider of cyber security services, but also a pioneer in bringing about reforms in the field. Instead, then employing conventional techniques, BugsBD has always prioritized the development of novel concepts. In order to maintain security operations in a unique manner, BugsBD's working technique is constantly distinct from others.

### **2.2 Vision and Mission:**

We assist countries, governments, and companies all around the world with cybercrime defense, risk reduction in the connected world, regulatory compliance, and operational transformation. Our goal is to become a global leader in the fields of data protection, user behavior analytics, and employee monitoring. Our mission is to create a safe online environment based on our cutting-edge technology and reliable service. We deploy integrated cyber-security and cyber-defense systems that counter sophisticated attacks, reducing the vulnerability of the digital environment and enhancing security. Our top objective is to develop better customer relationships. We provide customers with superior security goods and services that go above and beyond their expectations. We provide first-rate training that can help any firm maintain high standards of performance.

### **2.3 Location:**

Shyamoli,1/C (level 5), Road no: 01, Dhaka 1207.

### **2.4 SERVICES:**

1. cyber security Services
- 2.cyber security Solutions
- 3.Cyber Security Consulting Services
- 4.cyber security company
- 5.information security services

### **2.5 SOLUTIONS:**

1. SIEM & Security Operation Center (SOC)
- 2.Privileged Access Management (PAM)
3. Vulnerability Assessment
- 4.Penetration Testing
5. Security Compliance Service
- 6.Endpoint Security & Protection
- 7.IT Security Consultancy

## 2.6 Clients:



## 2.7 Values:

Scalable cyber security solutions are offered to clients by BugsBD using its broad knowledge, strong technical skills, and top-notch support services. Our accomplishment of 1000+ international clients demonstrate our expertise and dedication to provide our clients top-notch digital services and solutions. providing scalable IT solutions to clients.

## 2.8 summary:

A software development and security service provider in Bangladesh is called Bugsgbd. It started in 2015 and has since offered the greatest solutions all around the world. A strong group of experts working tirelessly to position themselves as one of the leading organizations.

## **CHAPTER 3: COMPANY CULTURE**

### **3.1 BugsBD Ltd Dept. list**

#### **3.1.1 Cyber Security:**

Usually In this dept worked any type of cyber security problem

### **3.2 Services of BugsBD Ltd.**

#### **3.2.1 Red Team Assessments**

##### **3.2.1.1 overview**

A red team evaluation is a purpose-driven examination of a company's ability to protect its security in real time. Therefore, a red team assessment may be thought of as a white-hat hacker group or individual simulating an intrusion attempt on a company without really disrupting its regular business operations. An allotted length of time will be given to the attacker to do their test. They will take every precaution at this time to look for any type of system vulnerabilities that may provide them access to the organization's private data.

##### **3.2.1.2 case study**

The team decides on several sorts of cyberattacks they believe are essential to expose the weaknesses and vulnerabilities after thoroughly examining all the material. However, this process is carried out in a more planned manner by adhering to a certain list that they will use to carry out the assaults. Once penetration testing has begun, the useless tests are gradually removed.

I.E-mail & Telephone-based social engineering

ii. Exploitation tactics

### **3.2.1.3 Problem statement**

Red team assessment is often a test of real-time, multi-vector attack detection and reaction time in which a group impersonates a cyber attacker and attempts to breach the security perimeter. However, it is exceedingly challenging to provide these services to a particular firm. It is extremely likely that the network we use now will be insecure in the near future since cybersecurity threats are always changing.

1. Digital assets
2. Physical assets
3. Technical process
4. Operational process
5. Identify potential critical risk in time

### **3.2.1.4 Solutions**

The attackers target large corporations in an effort to identify their weak areas in the system and exploit them. Red team assessments are beneficial to businesses because they may set up a simulation in which a white hat hacker can inform them of the weaknesses in their network or system. Red team evaluation offers the answer that will benefit every firm.

1. A real-world perspective of threat actor.
2. An integrated view of security control.
3. Analyze and evaluate security incident response capabilities.

### **3.2.1.5 Benefits**

This entire method mostly aids in learning whether the organization's system has any form of backdoor via which it may be infiltrated. Below are some advantages that the organization receives from this exam.

- 1.A comprehensive attack drill by simulating a hacker group.
- 2.Identify potential serious risk in time.
- 3.Protect business and customer.
- 4.Risk classification scheme.

## **3.2.2 Vulnerability Assessment**

### **3.2.2.1 Overview**

Vulnerability testing and vulnerability assessment are two related terms. In order to reduce the likelihood of a threat or hazard, this sort of software testing is carried out to evaluate the security risks in the software system. Vulnerabilities are errors or weak points in the internal controls, design, implementation, or security measures of any system. It frequently leads to a breach of the system's security policy.

### **3.2.2.2 Case study**

The corporate environment is unsafe due to system weaknesses, which leaves it vulnerable to hackers. Cyberattacks are among the most significant dangers to the firm, after overregulation and terrorism, according to the PwC Global Investor Survey conducted in 2018. Due to the system's weakness, there are numerous cases of assaults. Some of these include phishing, shadow IT, cryptocurrency mining, malware, poorly managed cloud servers, etc. There are very few businesses that do not experience dangers as a result of vulnerability.



### **3.2.2.3 Problem statements**

We need to be aware of any weaknesses while managing a firm. Data is our company's most valuable asset, and we cannot risk losing it. We never want our data to fall into the wrong hands due to a vulnerability. Our data leaks might also result in illegal access, compromised operations, and a threat to people's financial security. What then are the risks we face when we strive to become great entrepreneurs?

Some mentionable ones are here-

- 1.Hackers and Other Cybercriminals
- 2.Inadequate Data Backup
- 3.Unsecured Endpoints
- 4.Human Error
- 5.Cloud Storage Apps
- 6.Third-Party Apps

### **3.2.2.4 Solutions**

The greatest remedy for issues that are now plaguing your system is vulnerability assessment. The finest vulnerability assessment tool can identify the different kinds of system problems. The solution must adhere to a prescribed process in order to get the best results. The remedy employs a unique process to deliver excellent outcomes. The process is shown here.

- 1.Vulnerability identification
- 2.Vulnerability analysis
- 3.Risk assessment
- 4.Remediation

### **3.2.2.5 Benefits**

You've already calculated the damage that vulnerability can do to any firm. Having a vulnerability assessment solution in your system is therefore a sensible choice. This has enormous positive effects. Here are some of them for your consideration.

Determines the level of risk associated with internal systems and sensitive data. After finding current holes, prevents future assaults by providing full remedies. System updates and security updates become more effective

## **3.2.3 Penetration Testing Services**

### **3.2.3.1 Overview**

Penetration testing is a form of safety procedure where a cyber security professional looks for and attempts to attack weaknesses in a certain computer technique. The goal of the simulated attack is to identify any vulnerable spots in a procedure shield before the attackers secure and exploit them. Pencil assessments of vulnerabilities are a crucial component. The variety of penetration testing services offered by bugsgbd includes the following:

1. Services for network penetration testing
- Services for Web Application Penetration Testing
3. Services for Mobile Application Penetration Testing

### **3.2.3.2 Case study**

Any intrusion into your system is implied by the phrase "penetration." This makes it possible to mimic any form of assault on software or the complete IT infrastructure. These days, highly skilled hackers are capable of adopting a wide range of strategies to pose dangers to your system. Finding ways to endanger the system using the vulnerability is the goal of penetration testing, which comes after the vulnerability assessment.

### **3.2.3.3 Problem statements**

Operating systems, networking equipment, and software applications all have flaws. Some issues directly connected to the pen test include the DDOS assault, phishing, and ransomware. Your losses will be substantial due to your deficiencies. You cannot predict how you will be attacked or what procedures to take because the security system is not that developed without a pen test. It's similar to leaving your front door open. Some threats that occur without the pen test are:

1. Web Application Attacks
2. Network Attacks
3. Memory-based attacks
4. Wi-Fi attacks

### **3.2.3.4 Solutions**

The pen test can resolve any issue described above. You are safer the better the pen test is. The ideal pen test adheres to a few suitable steps. To do the pen test correctly and keep you secure, there are a few basic procedures. The actions are

1. Reconnaissance
2. Scanning
3. Exploitation
4. Post exploitation and analysis
5. Report

### **3.2.3.5 Benefits**

There are several advantages to using Bugsbd.Ltd penetration testing service. It is up to us to fully safeguard our systems. Some advantages of this include

1. Explores existing weaknesses in your system.
2. Shows the risks and difficulty in exploitation level.
3. Detects attacks and respond adequately on time.
4. Examines your cyber-defense capability.
5. Acts like a business continuity audit.

## **3.2.4 Mobile Security**

### **3.2.4.1 Overview**

In order to protect mobile device apps from cybercrime such as virus, hacking, and other illegal manipulation, mobile app security is the measure and method of doing so. Technology tools must be used in conjunction with individual reactions and organizational procedures to accomplish mobile app security.

### **3.2.4.2 Case study**

According to our analysis, many businesses lack enough infrastructure to ensure the security of mobile applications. Many employees lack the necessary education on the dangers of mobile apps. They are unable to actively identify the malicious programs. They seriously damage your system by downloading malicious programs. Additionally, the programs are frequently acquired from unreliable sites.

### **3.2.4.3 Problem statements**

Malware or illegal rogue apps downloaded by a device user might undermine a mobile application. Actually, neither of them has been launched. They, therefore, run a significant risk of falling victim to an online scam.

#### **3.2.4.4 Solutions**

You may get the finest solution to your mobile application security issues on Bugsbd. We concentrate on upholding the highest standards while rendering the service.

#### **3.2.4.5 Benefits**

There are many benefits like as

1. Increase Flexibility.
2. Improve Productivity.
3. Increase Security Awareness.

### **3.2.5 Source Code Review**

#### **3.2.5.1 Overview**

An investigation of an application's source code's security vulnerabilities is known as source code security analysis. The tester examines an application's code line by line using a code analyzer. The pentester tries manually to close any vulnerabilities detected after installing the analyzer in the environment.

#### **3.2.5.2 Case study**

The tool is crucial for businesses. Many of them have experienced severe dangers as a result of not using this instrument. As a result of increasing dangers from not employing the tool, their system was under assault. They left their systems vulnerable to assault by neglecting the correct keyboard navigation, screen reader accessibility, flexibility for internationalization, and nice, non-JavaScript behavior.

#### **3.2.5.3 Problem statements**

Lack of sufficient source code review results in a number of issues. Encryption mistakes, SQL injection, XSS flaws, buffer overflows, and race situations are four of the main vulnerabilities. Weak encryption methods and powerful encryption algorithms with poor implementation are both part of the first issue.

#### 3.2.5.4 Solutions

The source code review is constructed with a few primary objectives in mind to produce the best results possible. It is they-

1. Improves code quality
2. Identifying defects
3. Learning and Knowledge sharing
4. Increase a sense of mutual responsibility
5. Better solutions

#### 3.2.5.5 Benefits

The advantages listed below will result from our use of source code review as a tool:

1. In this, each team member simultaneously serves as a teacher and a student. They all share complementary approaches, business regulations, design patterns, framework characteristics, and best practices.
2. Source code review facilitates and lowers the cost of problem discovery.
3. It is advisable to confirm the functionality. This tool checks technical and commercial requirements to perform this task.

### 3.2.6 Network Security

#### 3.2.6.1 overview

Any action taken to maintain the integrity and usefulness of our network and data is considered network security. Both hardware and software technologies are included. Numerous risks are marked by this service. Our network is vulnerable to threats or attacks coming from anywhere. They are prevented from entering or spreading throughout our network via network security. Access to the network is controlled by effective network security.

#### 3.2.6.2 Case study

The network is essential to the development of our industry. Any network issues might do major harm to our business. Numerous examples of network problems exist. Malware, social engineering attacks, improperly configured firewalls and operating systems, and exploits targeted at the Windows Subsystem for Linux are just a few of them.

### **3.2.6.3 Problem statements**

The network is a vast area with both beneficial and detrimental impacts. The good effects of business may be disseminated. However, the issues that prevent you from growing significantly are plainly undesirable. Trojans, worms, and viruses are the network's difficulties.

### **3.2.6.4 Solutions**

Any network needs to address all of the aforementioned issues. So, when connected to the network, you had best practice prevention. Because Bugsbd provides the highest network security, you can rely on us. We take a few simple precautions to guard against network security assaults. It also provides us with a sneak preview of the technologies we employ to enhance network security. Those are-

1. Network Monitoring Tools.
2. Web Vulnerability Scanning Tools.
3. Packet Sniffers and Password Auditing Tools.
4. Network Defense Wireless Tools.
5. Network Intrusion & Detection.

### **3.2.6.5 Benefits**

You will reap the greatest rewards if you can efficiently combat the challenges that are emerging in your network since they have the potential to seriously hurt you. You'll have a fantastic helping hand defending your network thanks to our network security services. Some advantages of using our service are-

1. Increased Profits
2. Client Confidence
3. Disaster Recovery

## **3.3 Cyber Security Solutions for organizations**

1. Endpoint Security
2. File Integrity Monitor
3. Network monitoring System
4. DNS Security
5. DDOS & Application Protection

### **3.4 Internee Life Cycle**

Since an internship provides actual work experience, it is comparable to a job. We may develop our excellent manners, regulations, understanding of the worth of time, and all other qualities that are crucial in our line of work. such as-

#### **3.4.1 Professional Environment**

a polished workplace with highly competent, courteous, responsible, and mature individuals working toward a single objective.

### **3.5 First Day at Office**

The first day of the office was really exciting. Meeting new people, new place, new environment overall it was a different feeling.

### **3.6 Other Relevant Activities**

Actually, I was placed on the cyber security team as part of a week-long rotation program that was established to provide me a better understanding of the department. I had the option to sit with each of the other teams throughout this rotation period. This helped me understand how each department assists the one that deals with cyber security. I also gained knowledge of the team's functionality, processes, and systems.



## CHAPTER 4: TECHNOLOGY EMPLOYING

The usage of cyber security and its advantages will be covered in the chapter that follows.

### 4.1 Fundamental 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 several automated technologies, 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 vulnerabilities as well as how to manually find them.

#### 4.1.1 Supportive Technologies:

It stands for Remote Support: Tools and programs that link patients with caregivers directly, such as telnet and ssh (for networking)

### 4.2 Technology in use:

Usually there are mainly one type technology

1. automatic tools

**Automatic tools:** There are many types of automatic tools, like as

1. Burp suite
2. Nessus
3. Acunetix
4. Nmap

There have another one and this is *manually* and manually meaning here find out vulnerability manually.

## CHAPTER 5: PROJECT EXERTION

### 5.1 Project Name: Black Box vulnerability assessment

#### 1. Vulnerability name: TLS 1.0 enabled

URL: [REDACTED]

**Description:** It is an attack that uses cipher block chaining (CBC) mode encryption to take advantage of a flaw in the Transport-Layer Security (TLS) 1.0 and earlier SSL protocols. Attackers are able to steal authentication tokens as well as collect and decrypt HTTPS client-server connections.

**The impact of this vulnerability:** This issue may be used by an attacker to launch man-in-the-middle attacks to decrypt client-to-affected service connections.

**Method:** Get ()

**Impact:** High

#### Proof of concept:

```
→ sstlsca https://bridgit.care
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to [REDACTED]

Testing SSL server bridgit.care on

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    enabled
```

## 2.Vulnerability name: TLS 1.1 enabled

URL: [REDACTED]

**Description:** It is an attack that uses cipher block chaining (CBC) mode encryption to take advantage of a flaw in the Transport-Layer Security (TLS) 1.0 and earlier SSL protocols. Attackers are able to steal authentication tokens as well as collect and decrypt HTTPS client-server connections.

**The impact of this vulnerability:** This issue may be used by an attacker to launch man-in-the-middle attacks to decrypt client-to-affected service connections.

**Method:** Get ()

**Impact:** Medium

**Proof of concept:**

```
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to [REDACTED]

Testing SSL server bridgit.care

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

### 3.Vulnerability name: Missing SPF Records

URL: [REDACTED]

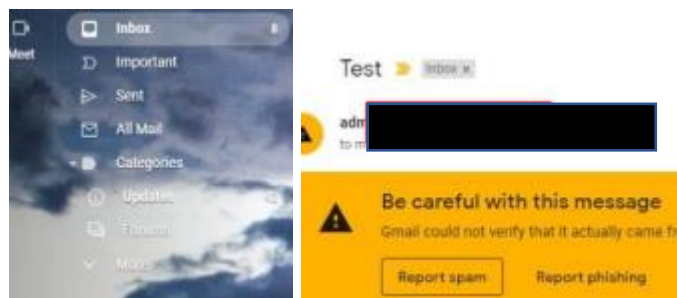
**Description:** The Domain Name Service (DNS) record known as an SPF record lets you specify which mail servers can send emails on your domain's behalf. An SPF record is used to stop spammers from using forged from addresses that are associated with your domain to send messages.

**The impact of this vulnerability:** SPF Records were formerly absent. Through any fake mailer, such as Emkei.cz, an attacker may spoof emails. An attacker can send emails under the alias "Support" and use social engineering to take control of a user account. Let's assume that despite the victim being aware of the phishing attacks, he still opens emails from legitimate domains. He is prone to being duped.

**Method:** POST ()

**Impact:** Medium

**Proof of concept:**



#### 4.Vulnerability name: Wordpress and Plugin Version Disclosure

URL: [REDACTED]

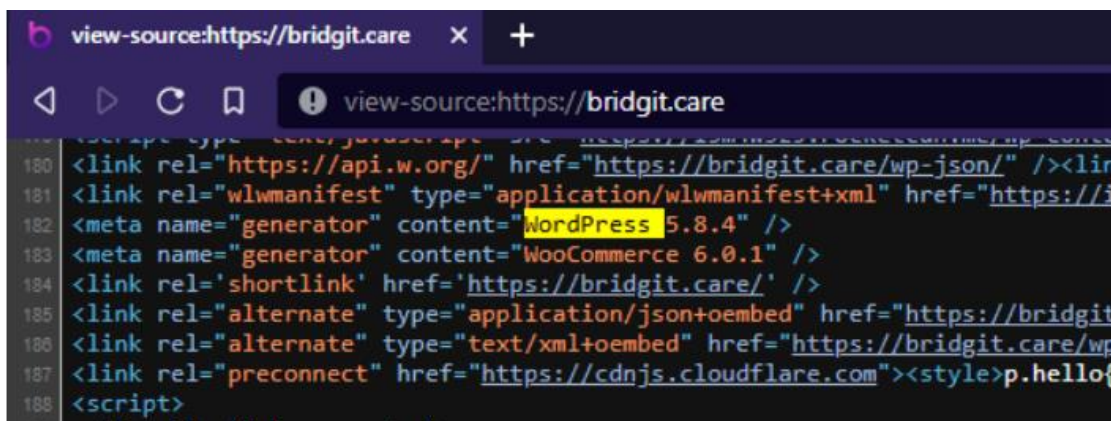
**Description:** I can see the wordpress version and the name and version of the plugins on this website when I open the view source.

**The impact of this vulnerability:** An attacker can quickly determine this version's vulnerability if they obtain it and start using plugins. And they have the ability to undermine the website.

**Method:** GET ()

**Impact:** Low

**Proof of concept:**



```
180 <link rel="https://api.w.org/" href="https://bridgit.care/wp-json/" /><lin
181 <link rel="wlwmanifest" type="application/wlwmanifest+xml" href="https://i
182 <meta name="generator" content="WordPress 5.8.4" />
183 <meta name="generator" content="WooCommerce 6.0.1" />
184 <link rel='shortlink' href='https://bridgit.care/' />
185 <link rel="alternate" type="application/json+oembed" href="https://bridgit
186 <link rel="alternate" type="text/xml+oembed" href="https://bridgit.care/wp
187 <link rel="preconnect" href="https://cdnjs.cloudflare.com"><style>p.hellof
188 <script>
```

## 5.2 Project Name: VAPT

### 1. Vulnerability name: Absence of Anti\_CSRF Tokens

URI: [REDACTED]

**Description:** An HTML submission form has no Anti-CSRF tokens. In a cross-site request forgery attack, a victim is made to submit an HTTP request to the target location without their knowledge or consent so that the attacker can act in place of the victim. The root reason is application functionality employing recurring, predictable URL/form operations. The attack's nature is that CSRF takes advantage of a user's confidence in a website.

**Impact:** A Cross-Site Request Forgery attack without Anti-CSRF tokens could lead to the execution of a particular 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.

#### Proof of Concept:

URL: [REDACTED]

Method: GET()

**Evidence:** `<form id="main_form" action="/.paypal.php" method="post" enctype="multipart/form-data" >`



```

<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <script src="https://kit.fontawesome.com/29392b9c02.js" crossorigin="anonymous"></script>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css" rel="stylesheet" />
    <link href="https://cdn.jsdelivr.net/npm/@fortawesome/fontawesome-free@5.15.2/css/all.min.css" rel="stylesheet" />
    <title>Bank Your Test</title>
  </head>
  <body class="page-container">
    <div class="row">
      <div class="right col-lg-8 col-md-9 col-sm-10">
        <div class="page">
          <div style="background-color: #f8d7da; padding: 5px; margin-bottom: 10px;>
            <div class="form col-lg-5 col-md-6 col-sm-12">
              <div class="text" style="padding-left: 10px;>
                Bank Your Test
              </div>
              <div class="text" style="padding-left: 10px;>
                Personal Information
              </div>
              <div class="input-field">
                <input type="text" value="" />
              </div>
              <div class="input-field">
                <input type="text" value="" />
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </body>
</html>

```

**Url:**



**Method:** GET()

**Evidence:** `<form id="main_form" action="/.paypal.php" method="post" enctype="multipart/form-data" >`

A screenshot of a web browser's developer tools showing the HTML source code of a page. The code is displayed in a light blue font on a white background. A blue highlight is visible over a line of code that appears to be a form element. The code includes various HTML tags such as <meta>, <script>, <div>, <img>, <table>, <input>, and <div class="form">. The highlighted line is: `<input type="text" value="" class="form" id="main_form" action="/.paypal.php" method="post" enctype="multipart/form-data" >`

**Prevention:** A Cross-Site Request Forgery attack without Anti-CSRF tokens may take place and cause the execution of a particular 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.

## 2. Vulnerability name: Cross-Domain JavaScript Source File Inclusion.

**Description:** The page contains one or more script files that originate from a different website.

**Impact:** A security warning against using JavaScript source files from another domain might affect a web application that employs one or more of those files. The victim's web application may be infected if a third party inserts and executes dangerous material, whether on purpose or by mistake.

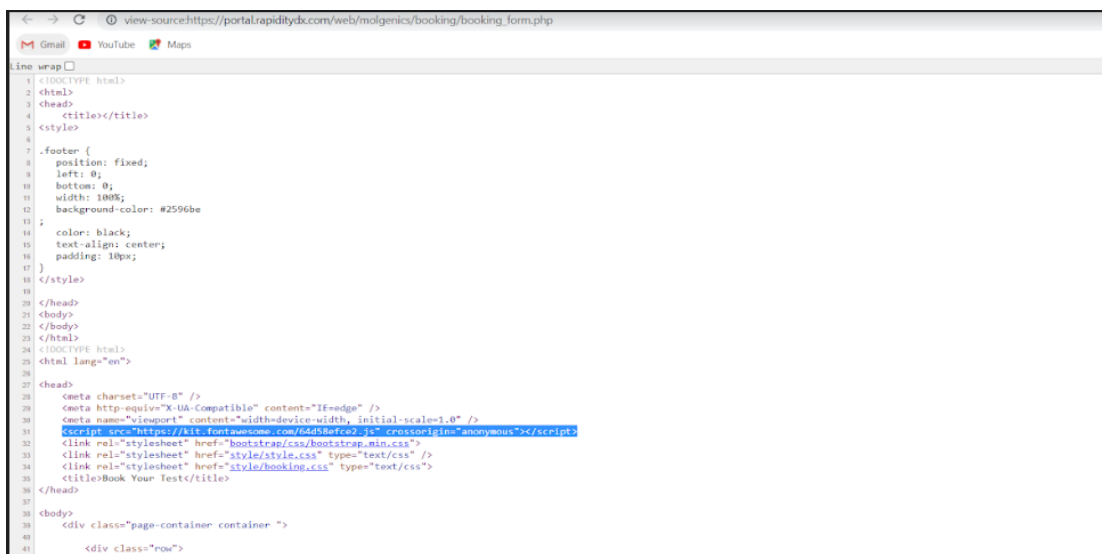
### Proof of Concept:

**URL:** [REDACTED]

**Method:** GET()

**Parameter:** https://kit.fontawesome.com/64d58efce2.js

**Evidence:** `<script src="https://kit.fontawesome.com/64d58efce2.js" crossorigin="anonymous"></script>`



```
view-source:https://portal.rapiditydx.com/web/molgenics/booking/booking_form.php
line wrap
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title></title>
5 <style>
6
7 .footer {
8   position: fixed;
9   left: 0;
10  bottom: 0;
11  width: 100%;
12  background-color: #2596be
13 ;
14  color: black;
15  text-align: center;
16  padding: 10px;
17 }
18 </style>
19
20 </head>
21 <body>
22 </body>
23 </html>
24 <!DOCTYPE html>
25 <html lang="en">
26
27 <head>
28   <meta charset="UTF-8" />
29   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
30   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
31   <script src="https://kit.fontawesome.com/64d58efce2.js" crossorigin="anonymous"></script>
32   <link rel="stylesheet" href="bootstrap/css/bootstrap.min.css">
33   <link rel="stylesheet" href="style/style.css" type="text/css" />
34   <link rel="stylesheet" href="style/booking.css" type="text/css">
35   <title>Book Your Test</title>
36 </head>
37
38 <body>
39   <div class="page-container container ">
40
41     <div class="row">
```



### 5.3 Project name: VAPT

#### 1. Vulnerability name: Local File Inclusion (LFI)

**Host:** [REDACTED]

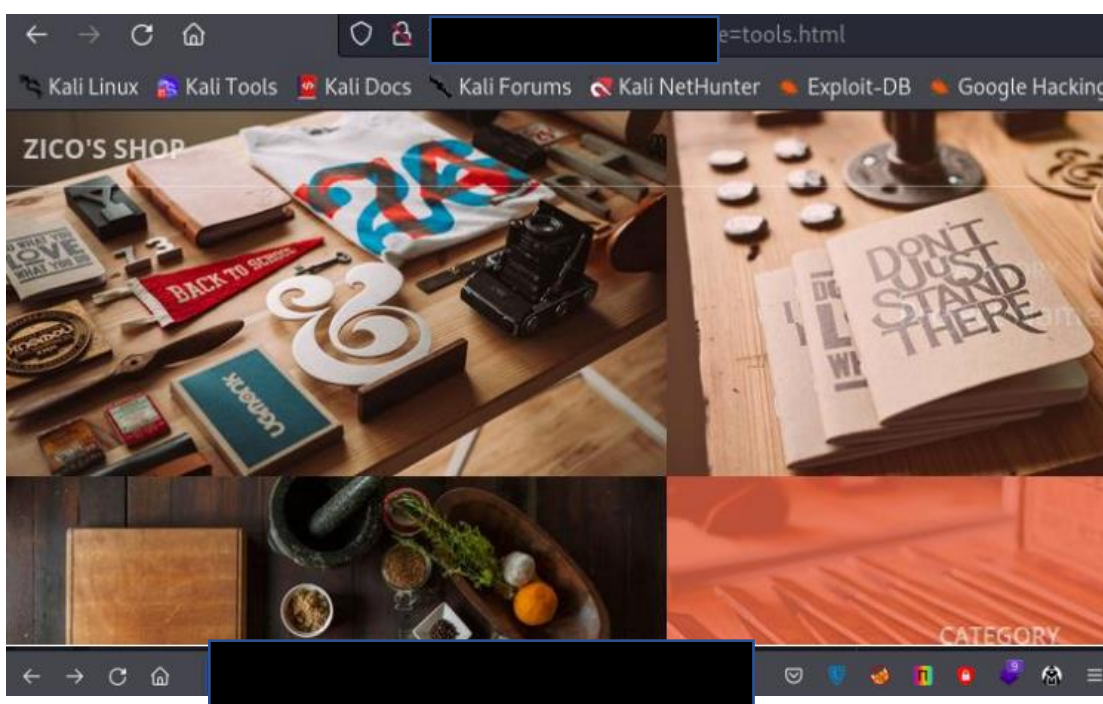
**Path:** view.php?page=../../../../etc/passwd

**Description:** By tricking the web application into executing or exposing files on the web server, an attacker can employ Local File Inclusion (LFI). Information exposure, remote code execution, or even cross-site scripting might result from an LFI attack (XSS). LFI often happens when a program requests the path to a file as input. A local file may be used in the include statement if the program regards this input as trustworthy. Remote File Inclusion and Local File Inclusion are extremely similar (RFI). The only files that an attacker utilizing LFI may add are local ones.

**Impact:** The /etc./password file, which provides a list of users on the server, is accessible to an attacker in the case above. The Directory Traversal vulnerability can also be used by attackers to get access to log files, source code, and other data.

**Impact:** CRITICAL

**Proof of concept:**



## 2. Vulnerability name: Exploiting PHP Lite Admin Remote Code Execution

Host: [REDACTED]

Path: [REDACTED]


Payload: <?php phpinfo()>

**Description:** Attacks such as remote code execution (RCE) provide an attacker the ability to remotely run malicious code on a computer.

**Impact:** A remote code execution (RCE) vulnerability can allow an attacker to execute malicious code or take complete control of a vulnerable system.

**Impact:** CRITICAL

**Proof of concept:**



```
#!/usr/bin/perl
use LWP::UserAgent;
my $url = "http://[REDACTED]";
my $ua = LWP::UserAgent->new;
my $resp = $ua->get($url);
my $body = $resp->content;
print $body;
```

```
PHP Version 5.6.40
PHP Language: PHP
PHP Architecture: Linux
PHP System: Linux
PHP Version: 5.6.40
PHP Build Date: Nov 19 2015 10:26:52
PHP Configuration File: /etc/php5/cli/php.ini
PHP Binary: /usr/bin/php
PHP Command Line Options:
PHP Environment:
PHP Variables:
```



#### 4.Vulnerability name: Development configuration files disclosed

**Host:** [REDACTED]

**Path:** /package.json

**Description:** A configuration file or files were discovered. These files could reveal private data that could enable a hostile person to plan more sophisticated assaults. The removal or restriction of access to certain kinds of files from production systems is advised.

**Impact:** These documents can contain private data. It is possible to conduct additional assaults using this information.

**Impact:** MEDIUM

#### Proof of concept:

---

```
{
  "name": "creative",
  "title": "Creative",
  "version": "3.3.7+1",
  "homepage": "http://startbootstrap.com/template-overviews/creative",
  "author": "Start Bootstrap",
  "license": {
    "type": "MIT",
    "url": "https://github.com/BlackrockDigital/startbootstrap/blob/gh-pages/LICENSE"
  },
  "devDependencies": {
    "bootstrap": "^3.3.7",
    "browser-sync": "^2.13.0",
    "font-awesome": "^4.6.3",
    "gulp": "^3.9.1",
    "gulp-clean-css": "^2.0.10",
    "gulp-header": "^1.8.7",
    "gulp-less": "^3.1.0",
    "gulp-rename": "^1.2.2",
    "gulp-uglify": "^1.5.4",
    "jquery": "^1.11.3",
    "magnific-popup": "^1.1.0",
    "scrollreveal": "^3.1.4"
  },
  "repository": {
    "type": "git",
    "url": "https://github.com/BlackrockDigital/startbootstrap-creative.git"
  }
}
```

## **CHAPTER 6: EXPERIENCE AND ACHIEVEMENTS**

### **6.1: Acquired Knowledge**

I was completely unfamiliar with the surroundings when I began my internship at BugsBD Ltd. However, I was always eager to learn new things. As a newcomer, I had concerns about how penetration test would relate into the Cyber Security. But, day by day, I became accustomed to it and gained confidence. As a result, adjusting to this daily schedule was difficult and stressful for me.

### **6.2: Overcome Problems and Difficulties**

My goal as an intern was to find out if there was any weakness that was vulnerable. In this case, I tried a bug check to see if any other vulnerability were missing. I tried Come up with solutions for improvement. This was not always possibly Come up with a quick fix, but I had tried finding best solution.

### **6.3: Implications to University's Internship Program**

I want to thank the Faculty of Science & Information Technology for keeping internship credit in the graduate program's curriculum and providing me with the opportunity to sample the flavor of industry-oriented chores and the field of employment that interests me. I'm also grateful to DIU's Faculty of Science and Information Technology, as well as the Office of Placement and Alumni, for arranging an opportunity for me to choose an organization that interests me and complete an internship there.

### **6.4: Soft skill**

It also known as power skills, common skills or core skills, are skills applicable to all professions. My first experience of professional life came in the form of an internship, which helped me hone my personal skills. Truly I want to say that a strong sense of duty, and the ability to be imaginative, resourceful, open, and receptive to change have all evolved in me.

## **6.5: Achievement**

Depending on the alterations, humans may become immortal or common. I had a huge change in my situation. For some reason, I am really good at learning new things. Computer exposed me to a number of innovative tools and technologies for teamwork, which turned out to be a highly effective way to quickly understand a network. I had come to appreciate the importance of time by completing my internship. I had thought about how significant time in life is.

## **6.6: Dependence**

The concept of reliability carries a lot of weight. Many businesses fail to adhere to it. They do not want to assign their interns to work on their main projects. However, I believe it is crucial because by doing this, a fresher may experience the workplace. Many people lack a basic understanding of how to begin a project or how to get along with everyone. The internship, in my opinion, may provide you the best flavor. Even though internships only last a few weeks, we get to make choices that will affect the rest of our lives. Internships are occasionally offered for collaborative projects, and occasionally everyone is permitted to work alone. Each person can cooperate when working in a group, yet

## **CHAPTER 7: CONCLUSIONS And RECOMMENDATIONS**

### **7.1 Summary**

Cybersecurity is the practice of protecting systems, networks, and programs from third party attacks. These cyberattacks often try to gain access to, alter, or destroy sensitive data. Example extorting money from users or interrupting normal business processes. I think we all need to have at least a basic understanding of cyber security. Taking me as an example, I knew only theory before joining the internship but later realized the importance of cyber security.

### **7.2 Recommendations for Future Actions**

Internships provide students with a time of hands-on experience in a field related to them studies. Students benefit from this experience since it allows them to see how their studies are applied in the real workplace.

#### **7.2.1 Organization**

Before joining to BugsBD, I had no idea what is success. However, I am now fully aware of the situation. I will never forget the incredible support I received from my other team member at BugsBD. However, not everyone is as fortunate as I am. So, I strongly advise them that it is up to them to deal with the office environment and culture. There must be some sort of plan in place for office recreation. As part of my entertainment, I had a lot of fun playing Carrom, which always motivated me to work hard. Life is not bed of roses so we would have to grow our daily routine. As a result, everyone should take some time away from work to recharge their batteries.

#### **7.2.2 University**

An internship is a fantastic way for potential employees to obtain experience in a specific profession, determine if they are interested in a specific vocation, build a network of Internship Report. I am proud to be a DIU student because the internship course is part of the course curriculum. I want to express my gratitude to the Institute of Information Technology for giving me the opportunity to prepare for the professional fields. It has undoubtedly improved me practical abilities. Now I'm looking forward to taking on the world's forthcoming difficulties.

### **7.2.3 Professional**

Humans make mistakes, and mistakes are the only way to learn. Therefore, internships are a perfect platform for the next step in self-development. Many people take it as a para, I think this idea is wrong, because everything can be made easy if you have your own effort and desire. That is what I believe and Internships are also very useful to interns themselves as they offer the chance to find out what working for a particular company, or within a certain industry, are really like. There are some typical challenges that interns usually face such as - time management is a challenge. Whatever the issue, it is important to take the best knowledge from the internship.



## REFERENCES

1. [https://www.tutorialspoint.com/penetration\\_testing/penetration\\_testing\\_method.htm](https://www.tutorialspoint.com/penetration_testing/penetration_testing_method.htm)
2. <https://www.secureideas.com/knowledge/what-is-the-scope-of-a-penetration-test>
3. <https://bugsgbd.com/services/penetration-testing>