Vulnerability Assessment & Penetration Testing

By

Md. Minhajul Islam Showkhin
183-35-382

A document submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Software Engineering

Department of Software Engineering

DAFFODIL INTERNATIONAL UNIVERSITY

Summer – 2022

APPROVAL

This thesis titled on "**Vulnerability Assessment & Penetration Testing**", submitted by **Md. Minhajul Islam Showkhin (ID: 183-35-382)** 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

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

Khalid Been Badruzzaman Biplob
Lecturer (Senior)
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

External Examiner

Md. Tanvir Quader
Senior Software Engineer
Technology Team
a2i Programme

DECLARATION

I hereby certify that I completed my internship under the guidance of Mr. SK. Fazlee Rabby, Lecturer, Software Engineering Department, and Daffodil International University. I hereby further swear that neither this internship nor any portion of this internship has been offered as credit toward a degree elsewhere.

Supervised by:

Mr. SK. Fazlee Rabby
Lecturer
Department of Software Engineering
Daffodil International University

Submitted by:

showkhin

Md. Minhajul Islam Showkhin
ID: 183-35-382
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

First, let me begin by expressing our sincere gratitude and appreciation to Almighty God, who by His divine favor enabled me to successfully finish the final year internship.

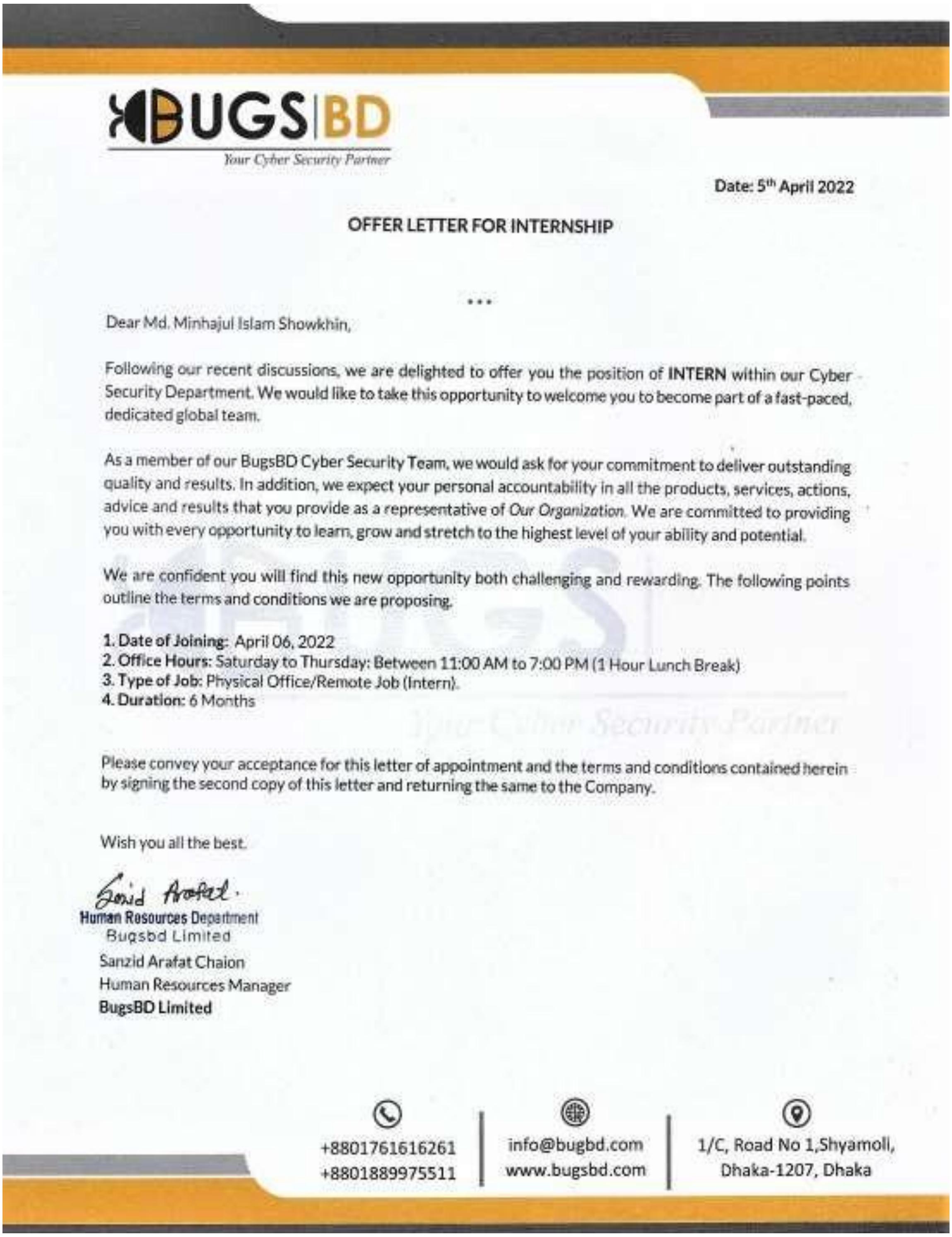
I would want to express my sincere gratitude and deep debt of gratitude to Mr. SK. Fazlee Rabby, lecturer at the Daffodil International University in Dhaka's department of software engineering. My supervisor chose to supervise this internship because of his extensive knowledge and enthusiasm in the subject of "Software Engineering." This internship was made possible by his never-ending patience, academic guidance, constant encouragement, frequent and vigorous supervision, and constructive criticism, invaluable advice, reading numerous subpar drafts and fixing them at all stages.

I would like to express our heartiest gratitude to **Dr. Imran Mahmud (Associate Professor & Head In-Charge), Mr. Md. Maruf Hassan (Associate Professor)** Department of Software Engineering, for their kind help to finish my internship and also to other faculty member and the staff of Software Engineering department of Daffodil International University.

I want to thank every one of our classmates at Daffodil International University who participated in this discussion while also attending class.

Last but not least, I must express my gratitude for my parents' unwavering support and patience.

APPOINTMENT LETTER



BUGS|BD
Your Cyber Security Partner

Date: 5th April 2022

OFFER LETTER FOR INTERNSHIP

Dear Md. Minhajul Islam Showkhin,

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 06, 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.

Human Resources Department
Bugsbd Limited

Sanzid 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

CHAPTER 1: INTRODUCTION

1.1 Background

I'm Md. Minhajul Islam Showkhin, a student in the software engineering department at Daffodil International University. I work with Microsoft SQL Server, React, JavaScript and penetration testing. I've been an intern at Bugsbd Limited for the last six months. It is a cyber-security organization. As a penetration tester, I identify weaknesses in websites and report them to the appropriate authorities. I'm interested in VAPT and want to start a career in Bangladesh as a cyber-security expert.

1.2 Motivation

I am interested in the cyber security so this internship is most benefited for me. I am learn from here much more things which is helping to me motivated about the cyber security specialist. Cyber security is an important thing for this digital word. Every single day we are compete with cyber-attack by others. I am work in the intern as penetration tester for findings vulnerability in the website and ensure that attacker never to steal the users data from website. In the beside I am work in network penetration testing for identify the loop whole in the system which is help to attacker trace the packet and modify the data and again send it to the user.

1.3 Objectives

The ultimate and most important purpose of cyber security is to keep data from being stolen or compromised. To do so, I'll look at three key cyber security objectives.

- Maintain the confidentiality data
- Preserve the integrity of data
- Promote the availability of data for authorized users

All security programs are founded on these objectives for confidentiality, integrity, and availability. The security model intended to direct information security practices within the walls of an organization or business.

1.4 Scope

The cyber security industry offers a wide range of job options. Information security analyst, chief information security officer, security architect, and security engineer are examples of potential careers. The administration of businesses and organizations, credit intermediation and associated activities, scientific and technological consulting services, and computer systems design are the most common industries that hire cyber security specialists.

CHAPTER 2: COMPANY OVERVIEW

2.1 About

The business was established in 2015. Both the company's income and its workforce have increased fast and strategically. We now employ more than 35 people. We are entirely distributed, much like our program, which is one of our most distinguishing characteristics. We served both domestic and international clients. We work when it is most convenient for us because we are dispersed across six different countries and several different time zones. More than 80 projects have been completed successfully by Bugsbd Limited during the past six years. We served both domestic and international clients [7].

Bangladeshi cyber-security firm Bugsbd Limited. Founded in 2015, they currently employ more than fifty people. A specialist IT Security Company in Bangladesh focuses exclusively on information and cyber security.

Utilize our leading IT Audit & Consultancy Service, VAPT tools, and Security Incident Event Management (SIEM), Privileged Account Management (PAM), Endpoint Protection, Email Security & Encryption, AI driven Cyber Security Immune System, Secure Web Gateway, and Network Threat Protection solutions to stay safe.

2.1.1 Mission & Vision

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 transform data protection, user behavior analytics, and employee monitoring into global leaders in these fields. Our mission is to create a safe online environment based on our cutting-edge technology and reliable service.

Our goal is to establish a solid reputation as a company that offers high-quality, trustworthy solutions and services in the ICT sector [3]. Our task is to create and/or deploy premium IT products and services to improve the business operations of its clients. We wish to increase our customers' customers' business growth. Our goal is to surpass your expectations and establish a relationship with you that will last forever and benefit both of us.

Bugsbd mission includes:

- Offering top-notch software development services, Professional consultation and development outsourcing to enhance the operations of our customers
- Simplifying and securing information access Enterprise Business
- Increasing business-to-business communication and data sharing
- Offering our clients value for their money
- Offering our staff opportunity for advancement and meaningful work.

Vision

In deploying combined cyber-security and cyber-defense systems that counter modern threats, we lessen the vulnerability of the digital environment and help to increase security. Our top goal is improving customer interactions. We provide superior security products and solutions that go above and beyond client requirements. We provide amazing training services and work with top-tier personnel to maintain high work standards in any firm. We hope to be recognized as a major worldwide technological pioneer by conquering the difficulties of cyber security [3]. Bugsbd is a major provider of IT consulting services and the deployment of industry-leading business solutions to esteemed local and foreign clients.

Our mission is to provide high-quality goods and services at competitive prices in order to achieve 100% customer satisfaction. We also work to establish ourselves as a leader in technology-based business solutions that can demand an unwavering reaction from the niche that we are targeting. Additionally, we have specialist knowledge in developing bespoke software, and we provide our business clients specific goods, IT services, and completely unique end-to-end solutions.

2.1.2 History

The majority of firms anticipate additional funding in 2019 to expand their security teams as cyber security threats continue to rise in complexity and number. How does a business evaluate a successful applicant when it comes to hiring the proper talent? According to a recent survey, interpersonal and soft skills are among the most important factors to take into account when hiring and staffing. Many people think that a single personality type is necessary for a cyber-security team, but in reality, a team is stronger when its members have a variety of features [3]. A business can benefit from creativity and improved problem-solving abilities brought about by different skill sets that complement one another.

2.1.3 Location

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

2.2 Services & Solutions

Our Services:

- Red Team Assessments
- Vulnerability Assessment
- Penetration Testing
- Mobile Security
- Source Code Audit
- Network
- Security

Our Solutions:

- SIEM & Security Operation Center
- Privileged Access Management
- Vulnerability Assessment
- Penetration Testing
- Security Compliance Service
- Endpoint Security & Protection
- IT Security Consultancy

They provide cyber security services and solutions, including SIEM, PAM, VAPT, endpoint & email security, DLP & compliance, vulnerability assessment, and penetration testing.

2.3 Clients

টালিখাতা
SureCash
a2i
প্রথম আলো
Prothom Alo
ekpay
Konnect
জমি
GRS
দপ্তর
শিক্ষক বাতায়ন
মুক্তপাঠ
ই-চালান
ইমাম বাতায়ন
নথি
আইডিয়া ব্যাংক
Daffodil University
SDG Tracker
Bangladesh's Development Mirror
ALTEX COATINGS LTD
LeadSearch
Qvafy
qvazon

2.4 Summery

Bugsbd is a software development and security service provider company in Bangladesh. It incepted in 2015, all the way, it provided best solutions worldwide. A robust team with highly trained professionals working relentlessly to become one of the well- established organizations.

CHAPTER 3: COMPANY CULTURE

3.1 Department

In the Bugsbd limited have some department mainly there are six department which are

- Red Team Assessment
- Vulnerability Assessment
- Penetration Testing
- Mobile Security
- Source Code Audit
- Network Security

Red Team Assessment
Real-time simulated attacks may be used to test your security, and incident response skills can help you safeguard your digital environment.

Vulnerability Assessment
The process of identifying, evaluating, and rating vulnerabilities in computer systems is known as vulnerability analysis or vulnerability assessment.

Penetration Testing
An approved simulated attacks on a computer system is called a penetration test, or pen test, and it is carried out to assess the security.

Mobile Security
For mobile penetration testing, this technique helps to increase repeatability and transparency.

Source Code Audit
Examining an application's source code is the process of looking for mistakes that were missed during the early stages of development.

Network Security

With today's quickest, most reliable cyber-attack defense, you can safeguard networks, data, and people.

3.2 Working Environments and Protocols

The majority of cyber security workdays follow the standard 9 to 5 schedule that we see in many professions. Despite this, cybercriminals don't exactly take a break after work. Due to the possibility of an after-hours security breach, many of these computer professionals may also need to be available on weekends or during the evenings.

3.2.1 Rules and Regulation

Many businesses still see cyber security as purely an IT issue. This impression is untrue in every way. Cyber disasters affect several organizational sectors when they occur locations when prompt response is required. The departments listed below must have developed protocols in place to deal with any potential cyber-attack. To increase cyber security, their involvement is necessary prior to prevention, during response, and after conclusions a cyber-incident. Our staff are the first line of defense in cyber security. Everyone is responsible for it, from top executives to a receptionist working at the front desk [9].

The following values should be highlighted in order to develop a cyber-security culture inside the company Awareness The emphasis will be on ignorant users who can damage your network by visiting malicious websites, responding to phishing emails, postponing software updates and data backups, leaving their log-in credentials in unsecured locations, or even disclosing sensitive information over the phone when subjected to social engineering. Employees need to be taught to recognize these varied dangers and respond appropriately.

3.2.2 Motto of the Organization

In 2019, the majority of firms plan to allocate more funds to expanding their security teams due to the complexity and quantity of cyber security threats. How does a business evaluate a successful applicant when it comes to hiring the proper talent? According to a recent survey, interpersonal and soft skills are among the most important factors to take into account when hiring and staffing. Many people think that a single personality type is necessary for an information security team, but in reality, a team is stronger when its members have a variety of features [8]. Diverse skill sets that work well together can help an organization innovate and improve its problem-solving abilities.

3.2.3 Handling Clients

Providing customers with visibility into a company's data security capabilities helps build trust in its efforts to manage their data with integrity. The financial services industry, and the banking sector, in particular, has been heavily regulated from a cyber-security perspective. As a result, many companies in the sector have made aligning their capabilities and putting in place solid governance structures a top priority in order to comply with legal obligations, lessen legal scrutiny, and control the reputational risk that goes along with them. Due to the rapid speed of technology advancement, companies should change their views of cyber security from merely a 'tick box' exercise to a strategic instrument that may help them further their business goals and gain the confidence of their customers if they are to be genuinely successful. The messaging to build an awareness of cyber security within the organization comes from the top. Board members should participate in regular tabletop exercises to inform the board on their duties and responsibilities to address cyber security threats in order to enable the board to support senior leadership to drive cyber security results. This would help them better understand the potential effects of a cyber-attack on their company. To encourage boards to challenge their technology, business, and cyber security leadership teams to enable risk-based prioritization, communication, and decision making rather than compliance-based prioritization, key questions should be provided to them as they receive formal cyber security programmed updates. Following that, the next learning curve will be for board members to gain experience in understanding the implications of the answers they receive. A board member's good reaction

May support financing decisions, prioritize projects, and provide the proper executive attention since board members frequently get crucial input from cyber security specialists.

3.3 Comparative Analysis of Office Culture

Workplace cultures have evolved to categorically classify all cyber security-related problems as "Not My Problems." Every level of the workplace exhibits this approach, employing numerous defenses, ranging from management to entry-level jobs. Cyber security training must become more personalized and interactive if cyber security is to advance as a career in the twenty-first century. Do I dare speak the tired click we must instill compassion in our cyber security professional's .Almost all authors who write on this subject take the time to mention that humans are any network's biggest security problem. However, I'd say that when it comes to user education and training, just about 99% of organizations perform the bare minimum.

3.3.1 Mixed up with Office Culture

The objective of the contemporary workplace must be to combine the older generation's cautious approach to new technology with the young generation's openness to trying new things. This will allow for the development of a setting that is more prone to embracing new technology while also being more cognizant of its weaknesses and dangers. But even doing so won't be sufficient. It is the responsibility of the cyber security expert to demonstrate how it may be incorporated into the everyday life of the organization's members at all levels after a work environment has been prepared to grasp the relevance of cyber security in this current era of the Internet of Things. Bringing these ideas to the management team entails getting them to adopt these behaviors into their daily life as well.

3.3.2 Escalating Motivation & Capability

Recognizing this, many organizations are adopting purposeful leadership in an effort to help employees connect their views to organizational goals and comprehend how their individual contributions affect the company's ability to influence society as a whole. Additionally, in the age of employee activism, more employees are expecting their companies to take a position on contentious social topics and are requesting greater corporate accountability for issues relating to fairness, diversity, and inclusion as well as other issues they care about. Organizations should be aware of how this may effect employee motivation and loyalty as silence on a problem can be a strong statement in and of itself. Lack of motivation is not the cause of low engagement. What separates an engaged person from a disengaged person is not their level of motivation, but rather the caliber of their drive. The daily transition to optimal motivation, when employees' work is linked, integrated, or intrinsic, is the key to long-term engagement.

Just as important as engagement at work is engagement in relationships. The leader's participation in interpersonal relationships is a critical and distinguishing aspect of employee engagement. The relationships a leader maintains with coworkers, employees, stakeholders, and clients are diverse. Relational engagement is a leader's level of drive, zeal, and involvement when collaborating with others. Engagement is increased via career growth. Numerous studies have indicated that firms with high levels of employee motivation, happiness, and retention exhibited distinct talent management strategies than those with low levels of engagement. Processes for developing talent were key differentiators.

3.4 Internee Life Cycle

It goes without saying that networking plays a significant role in success in any sector. Who you know may frequently make the difference between finding work fast and spending a lot of time applying to jobs. Through internships, individuals may network with industry experts who frequently have their own connections. Having these relationships will be very helpful while looking for work. Finally, it's not unusual for a business to extend a full-time offer following a paid internship (or occasionally an unpaid internship). When a company needs to fill a position, it frequently looks at its intern pool. This is due to the fact that the businesses have already made financial investments in their interns. Employing people who have previously proven they can suit the role makes the most sense into the organization's culture and workforce. Internships are beneficial in just about any industry, and cyber security is no different.

3.4.1 Getting Started

On April 6, 2022, I begin my internship at Bugsbd Limited. It's a six-month internship, and throughout that time I've increased my expertise and learnt a lot from this place. Professionals with training and expertise in cyber security are in great demand. One approach to provide recent graduates in cyber security the experience they need to enter the field right away is through internships. There are many various things to think about when it comes to cyber security, including whether an internship with a private corporation or the government makes the most sense. A private firm is considerably more likely to pay for an internship, as was already noted in this article. However, acquiring a degree in government is necessary for students who want to work for the government full-time.

The best internship would be in government. Finding an internship in the specific field of cyber security one want to pursue a career in might be significantly more advantageous than just searching for broad internships using keywords like "cyber security intern" or "information security intern."

3.4.2 Recruiting Policies

While working on a temporary basis with Bugsbd Limited, you can have access to trade secrets and confidential or sensitive company information. By accepting this offer, you acknowledge that Bugsbd Limited must maintain the confidentiality of this information and that you will not use it for your personal gain or divulge it to anybody else. Additionally, you agree to return any company-issued items like furniture and office supplies as well as any data and paperwork the firm owns as soon as your internship is finished. I shall start working for the firm after accepting all of the requirements in the aforementioned appointment offer for the post of intern.

- Be it clearly understood and agreed that as a full-time intern remote job employee.
- Your duty hours must be specific to your assignment and are subject to modification at the Management's sole discretion for convenience and work-related reasons. You

can resign within 7 days of start working depending your interest.

- You are in charge of completing the tasks that have been delegated to you to the full satisfaction of the Management. You cannot switch job before confirming.
- Before quitting your work or changing jobs, you should give at least two months' notice.
- You will perform your obligations on time and consistently, and you won't skip work without the management's prior approval.
- The Management shall have the authority to terminate your employment at any time and for any cause by providing you with one week's notice in lieu of such termination.

CHAPTER 4: TECHNOLOGY EMPLOYING

Malware, phishing, man-in-the-middle, and denial-of-service attacks are among the most frequent risks to organizations today, according to technology company Cisco. The IT sector is vulnerable to hackers due to a mix of fast digital transformation and a skills shortage in cyber-security. Particularly smaller businesses frequently struggle to combat cyber threats. The few security experts that exist frequently accept jobs with bigger enterprises, leaving smaller businesses with insufficient knowledge. Given the state of the sector right now, it doesn't appear that the lack of cyber security professionals will be addressed anytime soon. Because of the growing demand for cyber security professionals, there are far more open opportunities than qualified candidates.

Companies must approach the problem from all angles, taking into account their staff, workflows, and available technology. Businesses need to make the most of their current resources rather than depending on one specialist to handle all cyber security issues.

CHAPTER 5: PROJECT EXERTION

This test presents the results of the "Grey Box" penetration testing for Infrastructure. To make it simpler to resolve the security concerns that have been discovered, the recommendations presented in this report are categorized. This document formally certifies the most recent Infrastructure Penetration Testing [6]. Data collected throughout the engagement is rated in relation to "best in class" security standard standards. We believe that the assertions made in this paper provide a trustworthy assessment of Infrastructure. We strongly suggest reading the sections on the Summary of Business Risks and High-Level Recommendations for a fuller understanding of risks and discovered security issues.

Grading Criteria

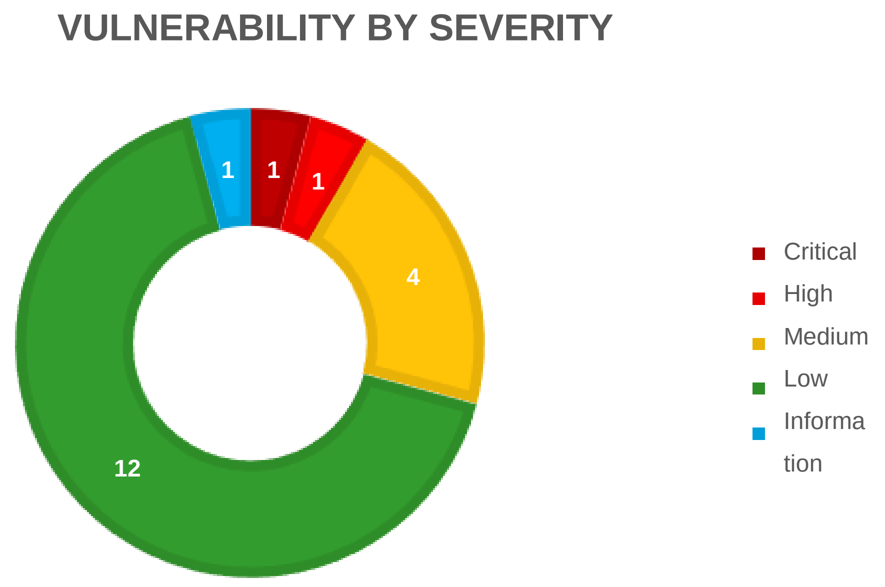
Grade	Security	Criteria
A	**Excellent**	Standards for "Industry Best Practice" security are exceeded. Only a few low-risk abnormalities were observed, and the overall posture was deemed to be excellent.
B	**Good**	The security complies with recognized "Industry Best Practice" requirements. Only a few flaws with a medium or low risk were observed, making the overall posture robust.
C	**Fair**	Some enterprise areas are protected from security risks by current solutions. To bring the discussed areas up to "Industry Best Practice" standards, moderate adjustments are needed.
D	**Poor**	There are serious security flaws. The issues raised should be given immediate attention in order to address the exposures found. To raise standards to "Industry Best Practice" levels, significant adjustments are needed.
F	**Inadequate**	There are serious security flaws. Almost all of the security controls studied had flaws, if not all of them. Enhancing security calls for inadequate.

5.1 Assumption & Consumption

Consultants undertook the discovery process to gather more information about the target and search for information leakage issues. With the help of this information, we conducted the majority of our manual testing, which comprised input validation tests, impersonation authentication and authorization tests, and session state management tests. This penetration testing tries to draw attention to security issues by using environmental defects that could allow for the acquisition of unauthorized access and/or the recovery of sensitive data [5]. The weaknesses identified during the review were used to produce recommendations and mitigation steps intended to enhance the overall security posture.

5.1.1 Result Overview

The test found a few bugs that could cause problems with resource availability, user session hijacking, the leakage of private information, and broken confidentiality and integrity. Security testing procedures have discovered known vulnerabilities in a number of components. Despite the fact that the discovered vulnerabilities cannot be employed in an actual attack, the threat they offer to the company could be quite detrimental.



The results of manual security testing conducted by security professionals are shown below

Security	Critical	High	Medium	Low	Informational
Issues	1	1	4	12	1

Severity scoring:

- Critical - Immediate risk to crucial company operations.
- High - Immediate danger to crucial business procedures.
- Moderate - Partially threatened or indirect threat to critical business processes.
- Low - There is no immediate threat. A vulnerability might be used to exploit another vulnerability.
- Informative - While this discovery does not point to a vulnerability, it does include a comment on implementation issues and design faults that could have long-term consequences.

5.1.2 Summary of business risks

Issues of high severity pose a direct danger to the company since they can be user session can be stolen using an XSS attack, giving the attacker complete control over the user's account. Due to the application's vulnerability, which is utilized by clients of the organization, client data would be exposed. If this weakness is exploited effectively, the organization may suffer severe reputational and financial losses. Issues with a medium or low severity may develop.

Attacks on communication networks result in the disclosure and modification of private information, undermining the accuracy and confidentiality of sent information. Information about system components that is leaked and might be used by attackers to conduct further damaging actions assaults on system components with a number of obsolete and unpatched publicly known vulnerabilities. The passwords of existing users may be brute-forced using their email addresses and usernames. They may easily enter their session after taking advantage of high level risks because the session token is the same for each login. It is simple to use blackmail, intimidation, or social engineering when sending emails from an open SMTP server. These strategies have the potential to impede corporate operations, result in the theft of credentials or combined with further attacks. Combining a few issues can help assaults be realized more successfully. Informational severity problems don't pose a direct danger, but they may be utilized by an attacker to acquire knowledge that will be helpful to them.

5.1.3 High-Level Recommendations

Given all the problems that have been identified, we strongly advise that us:

After considering all the issues that have been discovered, evaluate the IT/Security program as it exists today and in the future. A project should be given a security engineer to undertake SAST and DAST security testing evaluations as well as identify best practices for safe SDLC. Architecture for applications. Use a web application firewall solution to detect any malicious operations. Logs should be routinely examined for anomalies in order to spot odd behavior and fraudulent transactions. This task ought to be given to a security operations engineer. Implement patch management procedures for users' and developers' endpoints as well as the whole IT infrastructure [4]. Patch systems and environments in production and development often with the most recent updates and security patches. Each appropriate set OWASP Top 10 Security Threats

All set of applicable SANS 25 Security Threats

Criteria Label	Status
SQL Injection	Meets criteria
Authentication failure	Fails criteria
Exposed Sensitive Data	Fails criteria
External Entities in XML	Meets criteria

Ineffective Access Control	Meets criteria
Security configuration error	Fails criteria
Cross-Site Scripting (XSS)	Fails criteria

5.1.5 Methodology

Base our penetration testing methodology on the following standards and guidelines:

- Execution Standard for Penetration Testing
- 2017 Top 10 Application Security Risks as listed by OWASP
- Testing Guide for OWASP
- SANS: Running an Organization Penetration Test
- Methodology for Open Source Security Testing

An industry project for web application security is called Open Web Application Security Project (OWASP). The ten most frequent attacks that are successful against web applications have been determined by OWASP. The OWASP Top 10 is made up of these.
Application penetration testing covers all of the OWASP Top 10 topics and more. The penetration tester attempts to remotely exploit the OWASP Top 10 vulnerabilities. The table below shows the issues that OWASP has identified in its most recent Top 10 and the application's progress in addressing them.

5.2.1 Finding Details

Reflected Cross Site Scripting in multiple pages

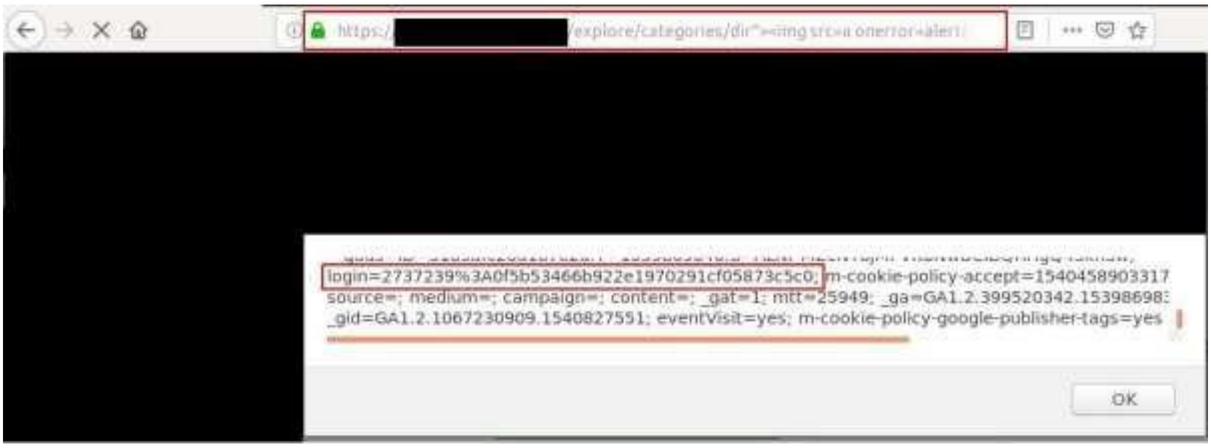
SEVERITY: High

ISSUE DESCRIPTIN:

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. A malicious script can be sent to an unwary user by an attacker via XSS [3]. The end user's browser will run the script regardless of the fact that it shouldn't be trusted. The malicious script is able to access any cookies, session tokens, or other sensitive data stored by the browser and used with that site since it believes the script is from a reliable source. These programs have the ability to completely change HTML.

5.2.2 Vulnerability

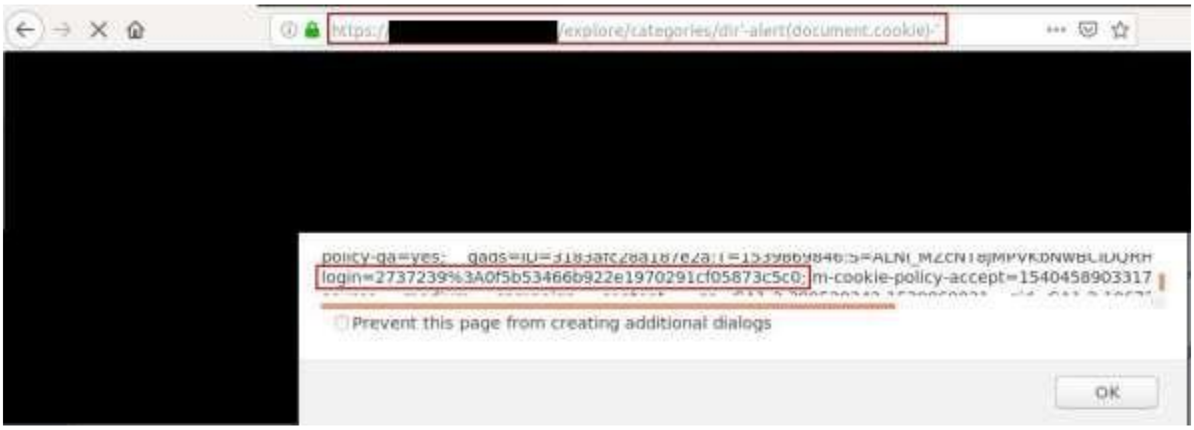
A URL can be used by the attacker to send JavaScript code directly to HTML code that will be executed.



https:/[redacted]/explore/categories/dir"><img src=a onerror=alert(

[redacted]

```
login=2737239%3A0f5b53466b922e1970291cf05873c5c0; m-cookie-policy-accept=1540458903317
source=; medium=; campaign=; content=; _gat=1; mtt=25949; _ga=GA1.2.399520342.15398698:
_gid=GA1.2.1067230909.1540827551; eventVisit=yes; m-cookie-policy-google-publisher-tags=yes
```

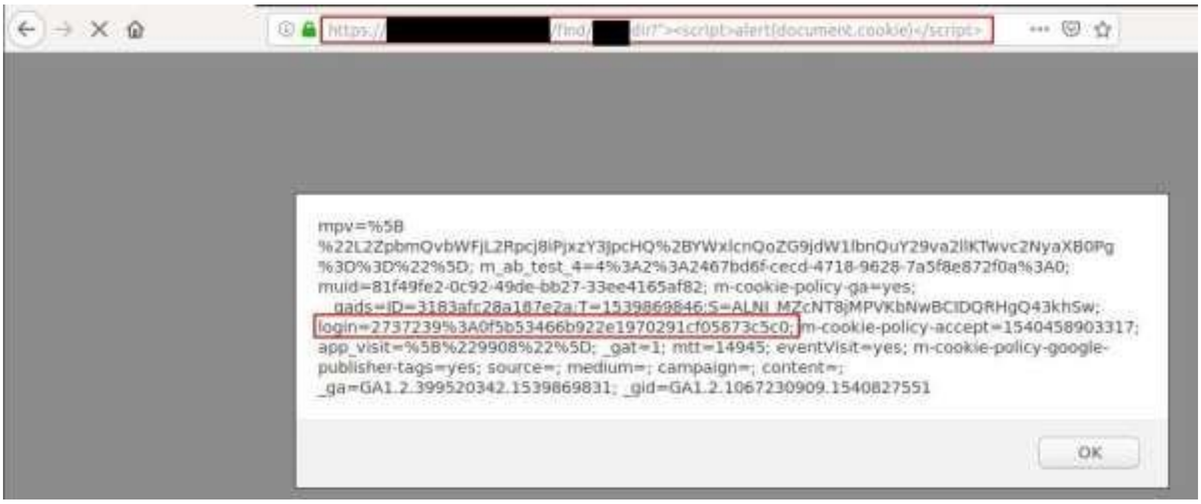


https:/[redacted]/explore/categories/dir'-alert(document.cookie)-'

[redacted]

```
policy-ga=yes; __gads=ID=3183afc28a187e2a:T=1539869846:S=ALNI_MZCNT8jMPVKDNWBLIDQRH
login=2737239%3A0f5b53466b922e1970291cf05873c5c0; m-cookie-policy-accept=1540458903317
```

☐ Prevent this page from creating additional dialogs



```
https://[redacted]/find/[redacted]dir?"><script>alert(document.cookie)</script>
```

```
mpv=%5B
%22L2ZpbmQvbWFjL2Rpcj8iPjxzY3JpcHQ%2BYWxlcnQoZG9jdW1lbnQuY29va2llKTwvc2NyaXB0Pg
%3D%3D%22%5D; m_ab_test_4=4%3A2%3A2467bd6f-cecd-4718-9628-7a5f8e872f0a%3A0;
muid=81f49fe2-0c92-49de-bb27-33ee4165af82; m-cookie-policy-ga=yes;
  gads=ID=3183afc28a187e2a:T=1539869846:S=ALNI_MZcNT8jMPVKbNwBCIDQRHgQ43khSw;
login=2737239%3A0f5b53466b922e1970291cf05873c5c0; m-cookie-policy-accept=1540458903317;
app_visit=%5B%229908%22%5D; _gat=1; mtt=14945; eventVisit=yes; m-cookie-policy-google-
publisher-tags=yes; source=; medium=; campaign=; content=;
_ga=GA1.2.399520342.1539869831; _gid=GA1.2.1067230909.1540827551
```

RECOMMENDATIONS:

Separating untrusted data from live browser content is necessary to prevent XSS. You may accomplish this by:

- Making use of frameworks like the most recent versions of Ruby on Rails and React JS that automatically escape XSS by design. Accurately manage the use cases that are not covered by the XSS protection provided by each framework by being aware of its restrictions.
- The vulnerabilities known as Reflected and Stored XSS may be fixed by escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL).

SMTP Server without authentication

SEVERITY:

Medium

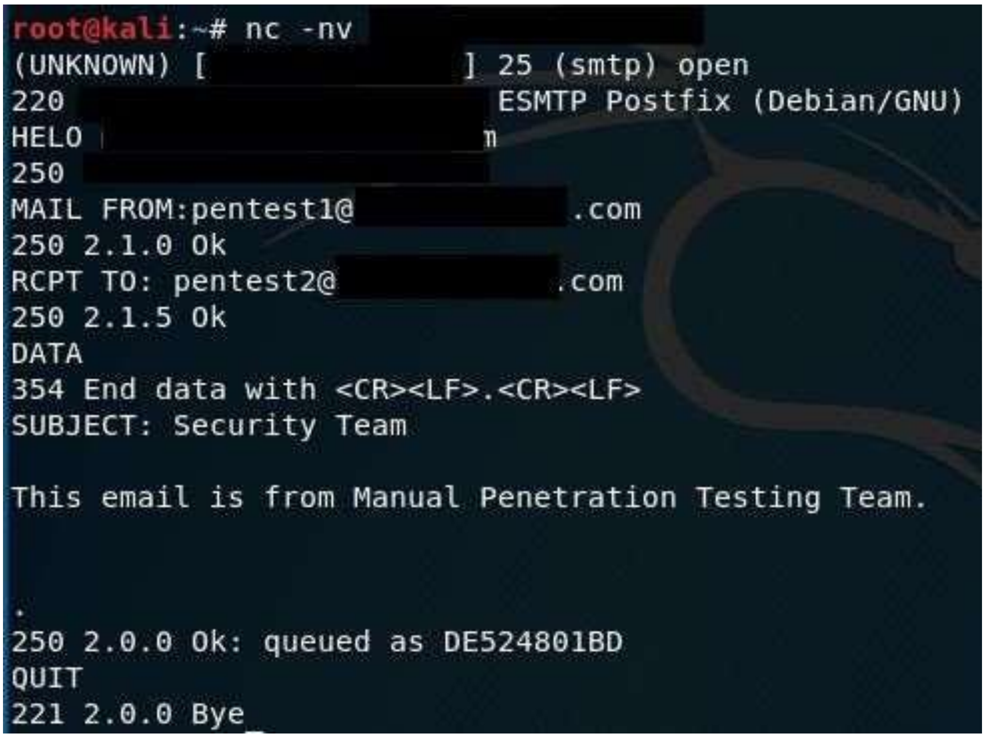
LOCATION:

SMTP client_ip:25

ISSUE DESCRIPTION:

An attacker might connect to the server's SMTP port and send emails to active email accounts from the following domains:

An attacker can use this flaw to perform social engineering attacks and send user’s phishing emails.



```
root@kali:~# nc -nv [redacted]
(UNKNOWN) [[redacted]] 25 (smtp) open
220 [redacted] ESMTP Postfix (Debian/GNU)
HELO [redacted]
250 [redacted]
MAIL FROM:pentest1@[redacted].com
250 2.1.0 Ok
RCPT TO: pentest2@[redacted].com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: Security Team

This email is from Manual Penetration Testing Team.


.
250 2.0.0 Ok: queued as DE524801BD
QUIT
221 2.0.0 Bye
```

RECOMMENDATIONS:

Implement access control and authentication. To transmit mail from the server, for instance, SMTP authentication requires users to enter a username and password. As few individuals as possible should have access to your servers, so make sure it is only granted when necessary.

Password Brute Force

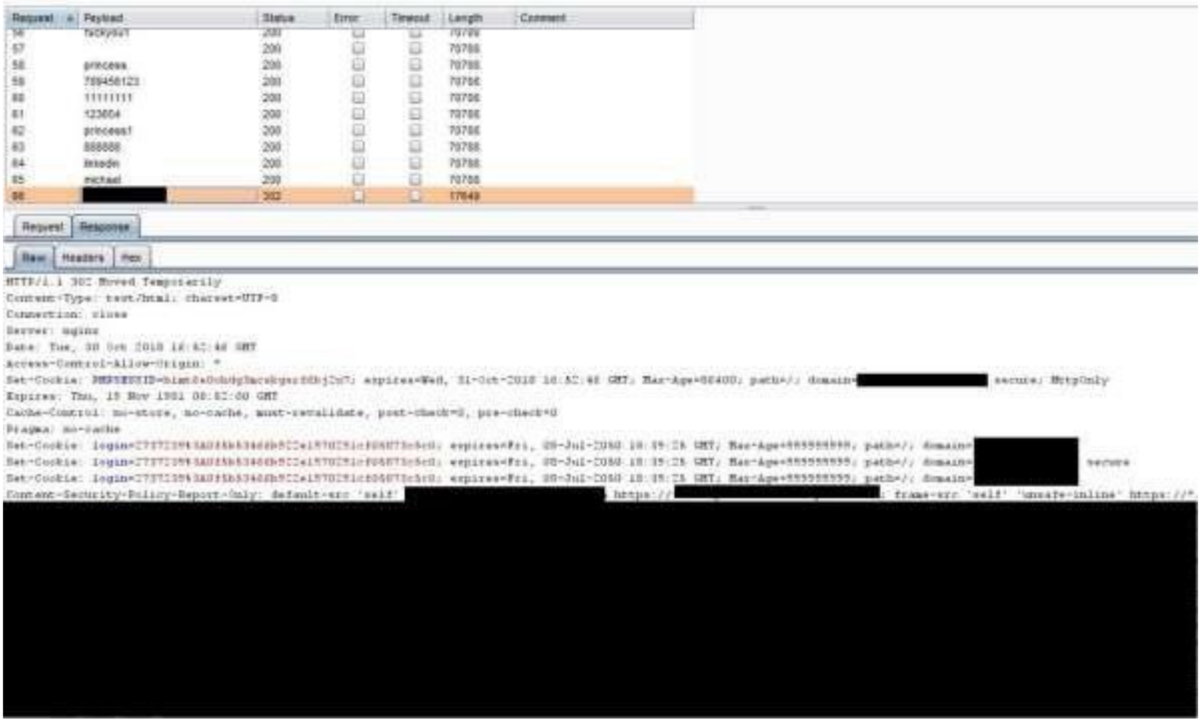
Allowed SEVERITY:

Medium LOCATION:

- https://clients.com/login
- https://services.com/signin
- https://services.com
- SSH clientip:22
- SSH clientip2:4118

ISSUE DESCRIPTION:

A brute force assault can take many various forms, but it often entails the attacker establishing specified values, sending those values in requests to a server, and then examining the server's response. An attacker may employ a dictionary attack with or without mutations or a typical brute-force assault using certain kinds of characters, such as alphanumeric, special, and case-sensitive characters, in order to maximize efficiency. The attacker can anticipate how long it will take to submit all selected predefined values by taking into account a specified technique, number of tries, efficiency of the system conducting the attack, and projected efficiency of the system being attacked.



Request	Payload	Status	Error	Timeout	Length	Comment
56	fuckyou1	200	☐	☐	70788	
57		200	☐	☐	70788	
58	princess	200	☐	☐	70788	
59	789456123	200	☐	☐	70788	
60	11111111	200	☐	☐	70788	
61	123654	200	☐	☐	70788	
62	princess1	200	☐	☐	70788	
63	888888	200	☐	☐	70788	
64	[illegible]	200	☐	☐	70788	
65	michael	200	☐	☐	70788	
66	[redacted]	302	☐	☐	17649	

```
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html; charset=UTF-8
Connection: close
Server: nginx
Date: Tue, 30 Oct 2018 16:52:48 GMT
Access-Control-Allow-Origin: *
Set-Cookie: PHPSESSID=[illegible]; expires=Wed, 31-Oct-2018 16:52:48 GMT; Max-Age=86400; path=/; domain=[redacted] secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: login=[illegible]; expires=Fri, 08-Jul-2050 18:35:26 GMT; Max-Age=999999999; path=/; domain=[redacted]
Set-Cookie: login=[illegible]; expires=Fri, 08-Jul-2050 18:35:26 GMT; Max-Age=999999999; path=/; domain=         secure
Set-Cookie: login=[illegible]; expires=Fri, 08-Jul-2050 18:35:26 GMT; Max-Age=999999999; path=/; domain=
Content-Security-Policy-Report-Only: default-src 'self' [redacted] https://[redacted]; frame-src 'self' 'unsafe-inline' https://*.
[redacted]
```

RECOMMENDATIONS:

There are several methods for stopping brute force attacks, including:

- Account locking procedures
- Increasing delays
- Use a challenge-response test to stop automated login submissions
- Locking off IP addresses.
- Information on how to stop this assault may be found

Insufficient session

expiration SEVERITY:

Medium LOCATION:

- https:// client.com

ISSUE DESCRIPTION:

After more than 50 hours without user activity, the session becomes active. Poorly implemented session management leads to insufficient session expiration vulnerability. Attackers may utilize this flaw, which can occur at the design and implementation levels, to obtain unauthorized access to the program.

Web developers have two options for managing sessions: use server tokens or create session IDs directly in the application. After the user hits the Log off button or after a certain amount of time, each session should be terminated called timeout. Unauthorized access may occur as a result of code flaws and server setup issues, which is unfortunate.

There are two different timeout kinds for when a session expires:

- Inactivity – This timeout is the period of inactivity before the session expires.
- Absolute – The entire amount of time a session may be active without re-authentication determines this timeout.

Certain attacks may be more likely to succeed if there is improper session expiry. The likelihood that an attacker would correctly guess a legitimate session ID rises with a long expiration period. More concurrent open sessions will be available at any given moment the longer the expiry period. The more sessions there are, the more probable it is that an attacker will pick one at random. A short session inactivity timeout does not assist if a token is utilized right away, but it does make it more difficult to capture the token while it is still active.

RECOMMENDATIONS:

This helps to keep the lifespan of a session ID as brief as possible and is required in a shared computing environment, where multiple people have unrestricted physical access to a computer. A Web application should invalidate a session after a predefined idle time has passed (a timeout) and give the user the ability to invalidate their own session (log out).

Additional details:

Https://www.owasp.org/index.php/SessionTimeout

Possible BEAST

vulnerability SEVERITY:

Low LOCATION:

- www.deals.client.com
- www.login.clien.com
- www.services.com
- www.services.com
- https://sservice-client.com
- https://wikiclient.com
- www.chatclient.com

ISSUE DESCRIPTIN:

In some configurations of Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, the SSL protocol encrypts data by using CBC mode with chained initialization vectors, allowing man-in-the-middle attackers to obtain plaintext HTTP headers via a block wise chosen-boundary attack (BCBA) on an HTTPS session, in combination with JavaScript code that uses the HTML5 Web Socket API, the Java Reconnect API

RECOMMENDATIONS:

Allow users to connect using TLS 1.1 or TLS 1.2, which are resistant to the BEAST attack, and disable TLS 1.0. Disabling TLS 1.0 increases overall security because it is currently regarded as unsafe.

Additional Details:

www.acunetix.com/articles/tls-ssl-cipher-hardening

User and E-mail Enumeration

SEVERITY: Low

LOCATION:

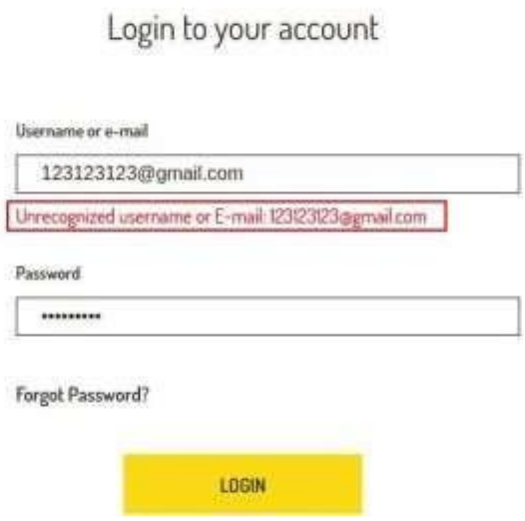
- www.services.com
- www.servicesclient.com

ISSUE DESCRIPTION:

A malicious actor can use brute force to either guess or validate the existence of valid users in a system, which is known as user enumeration. Even though it may be encountered in any system that requires user authentication, user enumeration is frequently a vulnerability in online applications. User enumeration frequently takes place on login pages and in Forgot Password sections of websites. We have discovered a user enumeration vulnerability that affects the Login and Forgot Password functions and that enables attackers to list current users.

PROOF OF VULNERABILITY:

User enumeration on the services.com login page



Login to your account

Username or e-mail

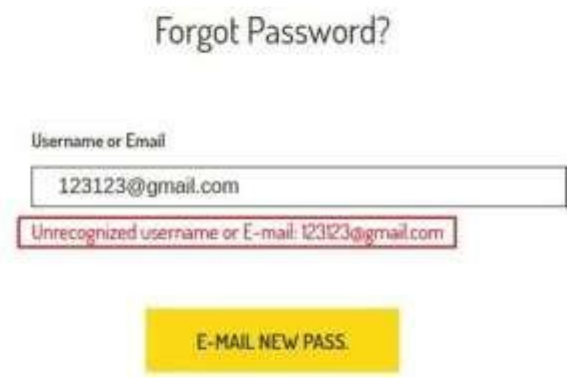
123123123@gmail.com

Unrecognized username or E-mail: 123123123@gmail.com

Password

•••••••••

User list on the servicesclient.com lost password page:



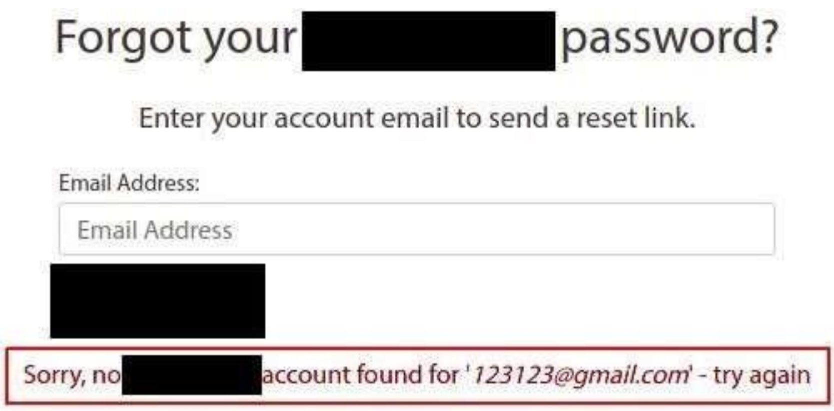
Forgot Password?

Username or Email

123123@gmail.com

Unrecognized username or E-mail: 123123@gmail.com

User enumeration found at forgot password page of service1.com



Forgot your [redacted] password?

Enter your account email to send a reset link.

Email Address:

Email Address

[redacted]

Sorry, no [redacted] account found for '*123123@gmail.com*' - try again

RECOMMENDATIONS:

Give more succinct replies to the functionality. Regardless of whether the login or email address is valid or not, the website should display the same generic message. A message that says something similar to "Further instructions have been sent to your email address." Please take into consideration utilizing the following link for further information:

https://blog.rightmove.com/about-user-enumeration/

Insecure Software Version

SEVERITY: Low

LOCATION:

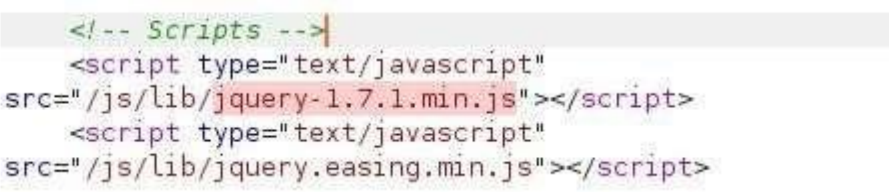
- https://services.com/
- https://servicesclient.com/bootstrap/js/bootstrap.min.js
- https://servicesdetails.com/jquery/jquery-2.2.4.min.js
- https://wikiclientdetails.com/download/contextbatch/batch.js

ISSUE DESCRIPTION:

Applying fixes and updating to a version of the program for which the vulnerability is patched is crucial when new software vulnerabilities are found. Since known vulnerabilities might be used by attackers, security updates ought to be applied as soon as they are made available.

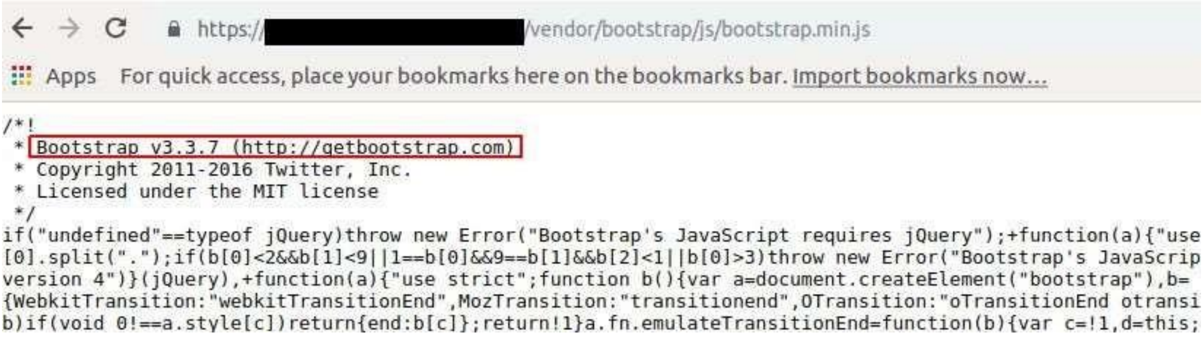
PROOF OF VULNERABILITY:

Vulnerable in scritp.js library which is serevicesclient.com:



```
    <!-- Scripts -->
    <script type="text/javascript"
src="/js/lib/jquery-1.7.1.min.js"></script>
    <script type="text/javascript"
src="/js/lib/jquery.easing.min.js"></script>
```

Vulnerable js lib in service3.com:



https://[redacted]/vendor/bootstrap/js/bootstrap.min.js

Apps
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

```
/*!
 * Bootstrap v3.3.7 (http://getbootstrap.com)
 * Copyright 2011-2016 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use
[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>3)throw new Error("Bootstrap's JavaScrip
version 4")}(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd otransi
b)if(void 0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var c=!1,d=this;
```

RECOMMENDATIONS:

Maintain software updates and replace any out-of-date software.

CHAPTER 6: EXPERIENCE AND ACHIEVEMENTS

6.1 Overcome Problems and Difficulties

I must provide your cyber security workforce with the most recent training and certifications to maintain their abilities up to date given the constantly shifting nature of the cyber threat scenario. Investment in training and reskilling programs benefits corporations as well as people since it increases employee retention. A well-trained, modern cyber security workforce is advantageous to companies. Additionally, these sponsored training courses and certifications would help non-cyber security personnel who are just starting out in the field advance in their positions. If workers feel their existing employers are interested in their skill development and give them opportunity for it, they will be less likely to look for other employment options.

6.2 Working Practices

Adapt the security laws. Businesses typically use outdated security methods that don't take best practices like zero trust architectures or contemporary cyber threats into consideration. Security policies are the foundation of enterprise security. Make careful to update your policies before changing your security protocols and educating your team about the new policies. Cyber-attacks typically employ compromised user accounts to get access to a company's internal resources. By demanding multi-factor authentication, which may be done by each user using a smart card with a PIN or a biometric, many cyber-attacks may be avoided. If your business cannot adopt multi-factor authentication, at the very least require users to use secure passwords that are impossible for attackers to guess.

Anyone with privileged access to systems and networks, such as system administrators and security professionals, has to authenticate. Raising employees' awareness of security. Too often, educating employees about security risks consists of listening to the same presentation for an hour every year and sending the odd email. It happens much too frequently that initiatives to raise security awareness are viewed as time wasters. To understand the importance of security and the necessity of everyone playing their part, the culture as a whole has to change. You might help your business change its culture about cyber security by taking a few minutes to explain to staff members why specific activities are required, asked, or not requested, in a particular way. Slowly, with each new generation, cultures change.

6.3 Technological Enhancement

Security must be flexible in order to keep up with the increasingly complex threat posed by cybercriminals. Thankfully, a number of recent technology advancements have enhanced the tools at our disposal to guarantee we prevail in the battle against cyber-attacks [1]. Here are the top five technology developments that are now bolstering cyber security efforts the most. Block chain is much more than simply a trendy term, and its significance goes far beyond the price of a single bit coin. Block chain is fundamentally a security mechanism. The digital ledger eliminates the usual dangers associated with disclosing data to other parties and enables safe information sharing and identity identification. This is why health care organizations like

Block chain is being tested by the NHS in the UK as a way to safeguard patient data and share it around institutions.

The cloud has been found to have limitations despite being useful. A single cloud account might be able to store an incredible number of various sorts of data, but doing so exposes users to obvious security issues. Fortunately, engineers have ensured that all data is substantially better protected against intrusions than previously, and as a result, cloud security has evolved significantly in recent years. Many businesses use cloud storage to handle customer data, from e-commerce sites like Shoplift to online gaming providers like Lotto land. Security is highly valued by these companies in order to protect customer financial information that customers may use to pay for products and services, such playing online lotteries. Businesses like those above use cloud services to store consumer personal data, therefore it only makes sense that they give data protection a top priority [1].

6.4 Non-Technical Growth (Soft Skills)

Technical proficiency is by no means the whole picture. Working in cyber security entails being proficient in a variety of soft skills, much like almost other tech-related industries. Again, depending on your role, the soft skills required for cyber security might differ slightly [2]. Several significant illustrations of adaptable abilities that might be useful for a career in cyber security are shown below.

Even subject matter specialists don't know everything there is to know. One of the most important work skills is the ability to quickly and accurately fill in the knowledge gaps. As an area that is always changing, cyber security necessitates vigilance to remain compliant and informed of new developments. Any person who enters the field must be dedicated to studying. New cyber security skills to keep pace with the change of technology [2]. That might mean learning an array of entirely new skills consistently throughout your career.

In any sector, having good communication skills is constantly in demand. Like the majority of IT employment, cyber security positions frequently entail teamwork, which frequently necessitates the possession of good communication skills. Additionally, you might need to communicate with those who lack your technical skills and explain the kinds of solutions that might be best suitable for any specific issue. Similar to verbal communication, technical writing is a talent that may be particularly useful for individuals working in the technologically advanced and linked world.

CHAPTER 7: CONCLUSIONS

Cybersecurity is one of the most important aspects of the quickly developing digital world. Because its dangers are hard to disprove, it is crucial to know how to counter them and teach others this skill. To learn more about cyber security and how to deal with hackers so you may save the day on digital platforms, enter our courses area. Organizations are under pressure to respond quickly to the continually increasing number of cyber security threats. Because attackers have been using an attack life cycle, organizations were forced to build a vulnerability management life cycle. The goal of vulnerability management's life cycle is to rapidly and successfully prevent the attackers' attempts. Regarding the susceptibility In this chapter, we've discussed the vulnerability management life cycle. An asset inventory, information flow management, risk and vulnerability have all been built.

REFERANCES

[1] 10 best Cyber Security Technology trends you must know. (n.d.). Retrieved November 5, 2022, from https://hkrtrainings.com/cyber-security-technologies

[2] Balaban -, B. D., Maguire -, J., Maguire -, J., Maguire -, J., Maguire -, J., & Maguire -, J. (2022, May 6). How To Check a Website for Vulnerabilities. eWEEK. https://www.eweek.com/enterprise-apps/how-to-check-a-website-for-vulnerabilities/

[3] Bugsbd Limited. (2016, January). bugsbd.com. https://bugsbd.com/

Explore Cybersecurity Degrees and Careers | CyberDegress.org. (2022, August 9). Explore Cybersecurity Degrees and Careers | CyberDegrees.org. https://www.cyberdegrees.org/

[4] GeeksforGeeks. (2021, November 20). Kali Linux - Vulnerability Analysis Tools. https://www.geeksforgeeks.org/kali-linux-vulnerability-analysis-tools/

[5] International Journal & Research Paper Publisher | IJRASET. (n.d.). Retrieved November 5, 2022, from https://www.ijraset.com/

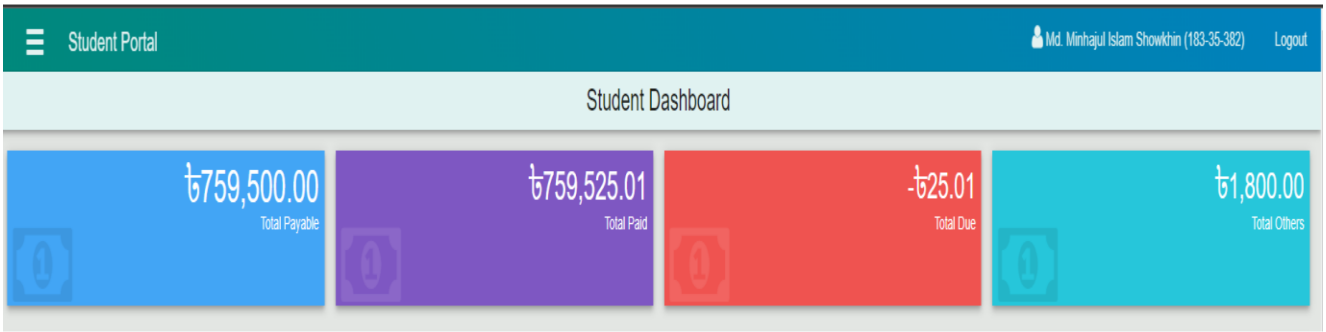
[6] OWASP Top Ten 2017 | 2017 Top 10 | OWASP Foundation. (n.d.). Retrieved November 5, 2022, from https://owasp.org/www-project-top-ten/2017/Top_10

[7] Scarfone, K. (2021, January 6). 10 cybersecurity best practices and tips for businesses. SearchSecurity. https://www.techtarget.com/searchsecurity/tip/10-cybersecurity-best-practices-and-tips-for-businesses

[8] Sengupta, S. (2022, August 18). How to Find Vulnerability in a Website. Crashtest Security. https://crashtest-security.com/how-to-find-vulnerabilities/

[9] vumetric. (n.d.). Retrieved November 5, 2022, from https://www.vumetric.com/company/methodologies/

ACCOUNT CLEARANCE



Student Dashboard

৳759,500.00
Total Payable

৳759,525.01
Total Paid

-৳25.01
Total Due

৳1,800.00
Total Others