Aryan School of Engineering

Department of Information and Technology

AFFILIATED TO: PURBANCHAL UNIVERSITY

Minor Project Proposal on:

HACKER4ME

[Code No: BIT279CO]

By

Jeet Bahadur Rana- Roll No: 15

Pratik Shrestha- Roll No: 22

Sajan Rai- Roll No: 23

Seazone Joshi- Roll No:27

Kathmandu, Nepal

2020

Aryan School of Engineering

Department of Information and Technology

AFFILIATED TO: PURBANCHAL UNIVERSITY

HACKER4ME

[Code No: BIT279CO]

PROJECT PROPOSAL SUBMITTED TO THE DEPARTMENT OF INFORMATION TECHNOLOGY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE BACHELOR OF INFORMATION TECHNOLOGY

By

Jeet Bahadur Rana Roll No: 15

Pratik Shrestha- Roll No:22

Sajan Rai- Roll No: 23

Seazone Joshi- Roll No:27

Kathmandu, Nepal

Jan 2020

PURBANCHAL UNIVERSITY

Aryan school of Engineering

Department of Information and Technology

Aryan College of Engineering

Department of Information Technology

Affiliated To: Purbanchal University

CERTIFICATE

The undersigned certify that they have read and recommended to the Department of Information Technology, a minor project work entitled "HACKER4ME" submitted by Jeet Bahadur Rana (15) Pratik Shrestha (22) Sajan Rai (23) and Seazon Joshi(27) in partial fulfillment of the requirements for the degree of Bachelor of IT.

(Project Coordinate)	(Head of Department)
Department of Electronics and	Department of Electronics and
Computer Engineering.	Computer Engineering.
Aryan School of Engineering	Aryan School of Engineering

ACKNOWLEDGEMENT

We would like to extend our heartiest thanks with a deep sense of gratitude and respect to all those who provides me immense help and guidance during my training period. We have been greatly benefited from their regular critical reviews and inspiration throughout my work.

We would also like to thank my project supervisor **Mr.Amit Shrestha** for his unfailing cooperation and sparing his valuable time to assist us in our work for preparing proposal of the project.

We would like to express our sincere thanks to our Head of Department **Er. Nisha Karki** and our internal guide **Mr. Amit Shrestha,** who gave us an opportunity to undertake such a great challenging and innovative work. We are grateful to them for their guidance, encouragement, understanding and insightful support in the development process.

Last but not the least we would like to mention here that we greatly indebted to each and everybody who has been associated with our project at any stage but whose name does not find a place in this acknowledgement.

ABSTRACT

HACKER4ME is developed as a bug bounty platform. A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.HACKER4ME allows you to connect with the brightest and most experienced hackers and penetration testers on the globe. Engage them in your program and experience true out-of-the-box security. Track down the vulnerabilities that classic pen-testing methods would never uncover. Have our community of researchers, hackers and pentesters assess the security of all your digital assets. Make reporting, managing and fixing vulnerabilities a true walk in the park. Our platform comes with a measurable built-in process to follow up on all your vulnerability reports. Get access to security researchers across the globe and benefit from their knowledge. Hacker4me community is at your constant disposal, allowing you to hand pick your researchers and validate their findings. Hackers and security experts here is your chance to earn rewards for every bug you track down and submit. Work whenever you want to, wherever you want to. Get ranked for every bug reported. Join our vibrant community and earn the top spot in our ranking. Get inspired by the work of others and embrace the opportunity to collaborate.

List of Figure

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet of things". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.

A penetration test, colloquially known as a pen test, pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed. The process typically identifies the target systems and a particular goal, then reviews available information and undertakes various means to attain that goal. A penetration test target may be a white box (which provides background and system information) or black box (which provides only basic or no information except the company name). A gray box penetration test is a combination of the two (where limited knowledge of the target is shared with the auditor). A penetration test can help determine whether a system is vulnerable to attack if the defenses were sufficient, and which defenses (if any) the test defeated.

HACKER4YOU provides platform for both business and individuals to maintain their security standards. Individual, security experts, pentesters and researchers can use our platform to participate in various bug bounty programs where as various business can put their system to test.

1.2 PROBLEM OF STATEMENT

In computers and computer networks an attack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyberattack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent. A cyberattack can be employed by sovereign states, individuals, groups, society or organizations, and it may originate from an anonymous source. A cyberattack may steal, alter, or destroy a specified target by hacking into a susceptible system. Cyberattacks can range from installing spyware on a personal computer to attempting to destroy the infrastructure of entire nations. Legal experts are seeking to limit the use of the term to incidents causing physical damage, distinguishing it from the more routine data breaches and broader hacking activities. Cyberattacks have become increasingly sophisticated and dangerous. Any development project in an organization takes place in rapid pace, codebase are pushed out rapidly and performing security audits traditionally aren’t effective in present context. Unorthodox, out of the box ,individual group of pentesters and hackers are much more efficient in finding flaws and bugs in a system

1.3 SCOPE

Hacker4ME can be used by individual hackers, pentesters, security experts and individuals to participate in various bug bounty programs to earn cash prize and improve their ranking where as business can enlist their system for test and announce attractive incentive to lure multiple hackers to find vulnerabities and bugs in their system. Multiple hackers can contribute their skills set and since it is no cure no pay system only the hacker that find flaws gets the reward.

1.4 PROJECT FEATURES

Features of this project are as follows:

- Simple, minimalistic and effective interface.
- A no cure, no pay approach to vulnerability.
- Ranking and incentives.
- Community of researchers, hackers and pentesters.
- Detailed POC of vulnerability reports.

1.5 OBJECTIVE

The main objective of our project is:

- To create secured cyber ecosystem by maintaining availability, integrity and confidentiality.

1.6 SYSTEM REQUIREMENT

1.6.1 Software Requirement (while developing)

- Windows 10 or Linux
- Programming languages: Html, CSS, JavaScript, PHP
- Framework: Laravel
- Text editor: Sublime Text/VS Code

1.6.2 Hardware Requirement (while developing)

The following is a list of computer hardware specifications that are suggested by the developer as the minimum requirements for a computer to efficiently run the system.

- Processor: Pentium IV or higher
- Memory: 2 GB minimum
- Hard drive: 40 GB free space
- 1024 * 768 Resolution Color Monitor

CHAPTER 2:LITERATURE REVIEW

2.1 BACKGROUND

A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. Today mainstream usage of "hacker" mostly refers to computer criminals, due to the mass media usage of the word since the 1980s. This includes what hacker slang calls "script kiddies", people breaking into computers using programs written by others, with very little knowledge about the way they work. This usage has become so predominant that the general public is largely unaware that different meanings exist.[1]

A bug bounty program is a deal offered by many websites, organizations and software developers by which individuals can receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.These programs allow the developers to discover and resolve bugs before the general public is aware of them, preventing incidents of widespread abuse. Bug bounty programs have been implemented by a large number of organizations,.[2] .

Since the late 1980s cyberattacks have evolved several times to use innovations in information technology as vectors for committing cybercrimes. In recent years, the scale and robustness of cyberattacks has increased rapidly, as observed by the World Economic Forum in its 2018 report: "Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents."[3].In May 2000, the Internet Engineering Task Force defined attack in RFC 2828 as:[4] An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

CNSS Instruction No. 4009 dated 26 April 2010 by Committee on National Security Systems of the United States of America[5] defines an attack as: "Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or

destroy information system resources or the information itself. The increasing dependency of modern society on information and computers networks (both in private and public sectors, including the military)[6] has led to new terms like cyber attack and cyberwarfare."

Hunter & Ready initiated the first known bug bounty program in 1983 for their Versatile Real-Time Executive operating system. Anyone who found and reported a bug would receive a Volkswagen Beetle (a.k.a. Bug) in return.[7] A little over a decade later in 1995, Jarrett Ridlinghafer, a technical support engineer at Netscape Communications Corporation coined the phrase 'Bugs Bounty'. Netscape encouraged its employees to push themselves and do whatever it takes to get the job done. Ridlinghafer recognized that Netscape had many enthusiasts and evangelists for their products, some of whom to him seemed even fanatical, particularly for the Mosaic/Netscape/Mozilla browser. He started to investigate the phenomenon in more detail and discovered that many of Netscape's enthusiasts were actually software engineers who were fixing the product's bugs on their own and publishing the fixes or workarounds

Figure 1: A Facebook "White Hat" debit card, given to researchers who report security bugs.

A vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An exploitable

vulnerability is one for which at least one working attack or "exploit" exists.[8] Vulnerabilities are often hunted or exploited with the aid of automated tools or manually using customized scripts. To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of these categories below:

- Backdoor
- Denial-of –service attack
- Direct-access attack
- Eavesdropping
- Phishing
- Social Engineering
- Spoofing

Serious financial damage has been caused by security breaches, but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."[9] Security breaches continue to cost businesses billions of dollars but a survey revealed that 66% of security staffs do not believe senior leadership takes cyber precautions as a strategic priority. However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic Gordon-Loeb Model analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the expected value of the loss resulting from a cyber/information security breach).[10]

CHAPTER 3:METHODOLOGY

3.1 FEASIBILITY STUDY

Early studies have been made on this, as it is a rising topic. Some research have been done before setting goals or objectives for the project and initializing the project. It has been known from the research that there had been earlier attempts for creating such products and there are some products that meets certain portion of the public and market demands. But from deep research we have come to know that there has not been any kind of complete product relating to this topic so we decided to have an attempt on creating more facilitated and complete product in comparison to the earlier products that already exist in the market.

Thus, after long term research and discussion among the group members we have decided to make a proposal for the project defining the researches and objectives we have set for the project.

There are three tests of Feasibility Study:-

- Operational
- Technical
- Economical /financial

3.1.1 Operational Feasibility

This test of feasibility asks if the system will work when it is developed and installed. This feasibility observes the all operations like finding products, gathering information, getting supports & software & more.

3.1.2 Technical Feasibility

This involves the technological consideration like available technology to run the purposed system. The system has been created with the most common technology available. Hence the system is technically feasible.

3.1.3 Economical Feasibility

Cost of the system will be affordable for the user. As it is a simple product financial consideration was not a big deal for our project.

3.2 BEHAVIOUR MODELING

3.2.1 FLOW CHART

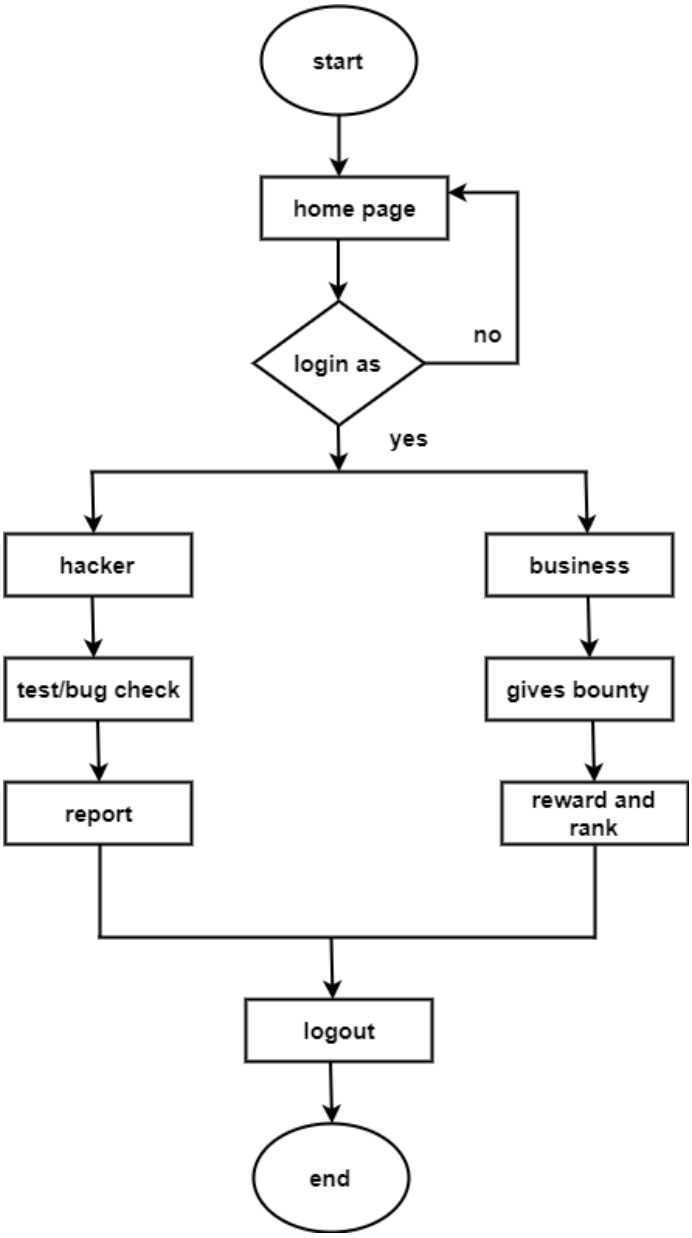

Figure 2:FLOW CHART

3.2.2 ER DIAGRAM DIAGRAM

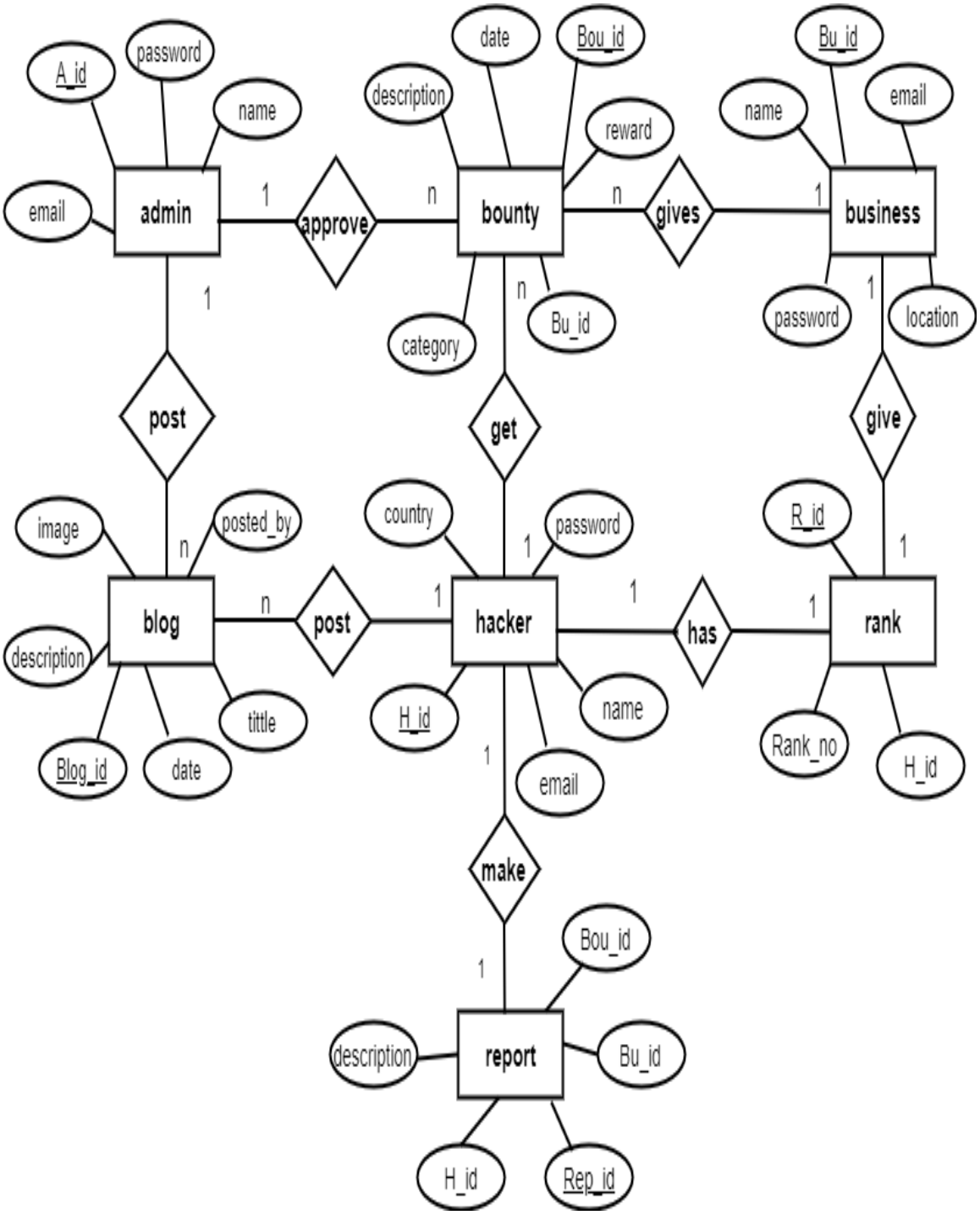

Figure 3:ER DIAGRAM

3.2.3 USE CASE DIAGRAM

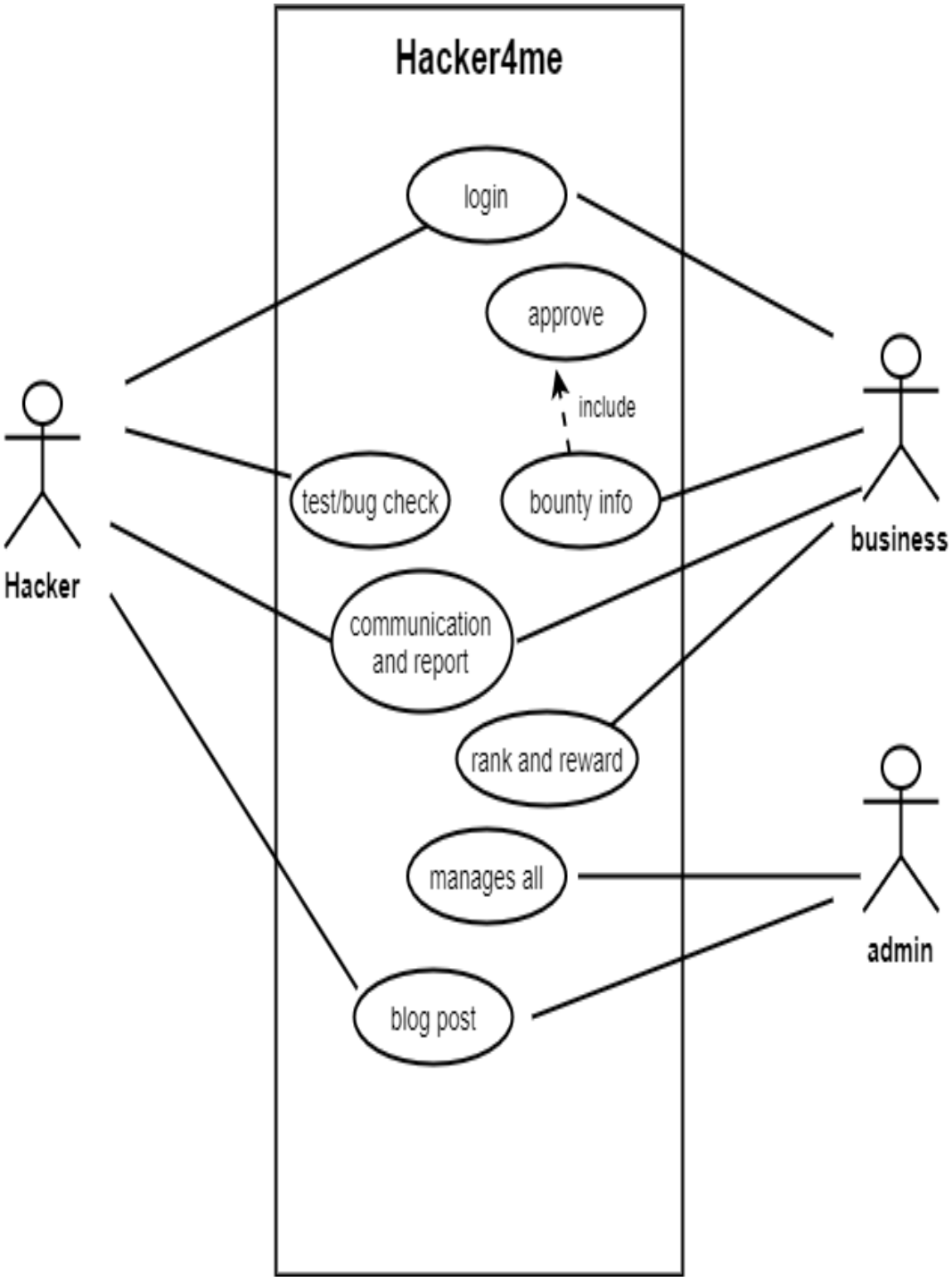

Figure 4 :USE CASE DIAGRAGM

3.2.4 STATE DIAGRAM

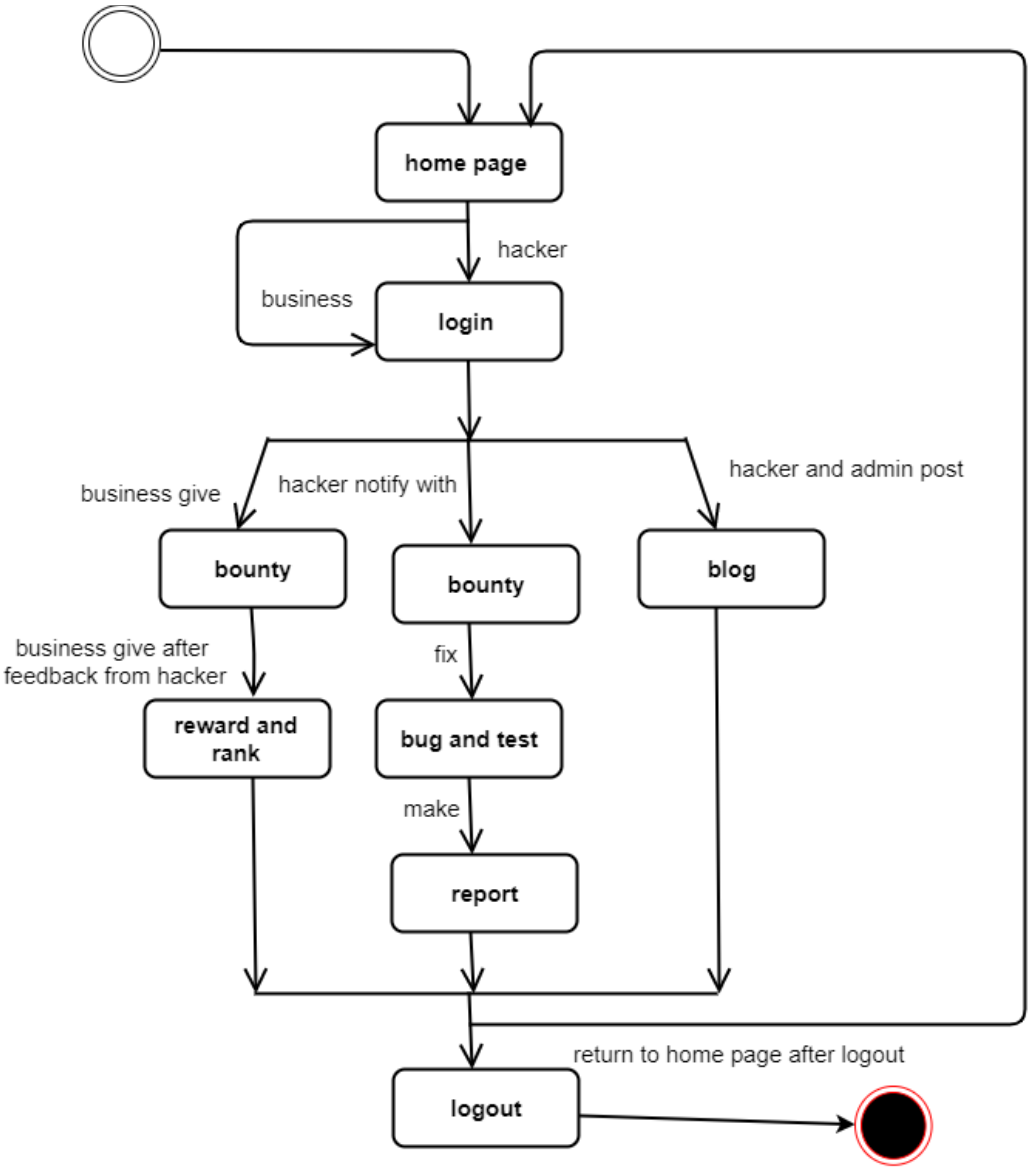

Figure 5:STATE DIAGRAM

3.3 COST ESTIMATION

These documents will provide the necessary data to feed into the budget line items. The accuracy of the budgets requires that attention be given both to individual expense per item. The budget goal, is to the extent possible, directly map the project expense to actual costs within 10 per-cent difference if there be any disparity.

ITEM	PRICE (Rs)	UNITS	TOTAL (Rs)
Backup device (Portable hard disk)	800	1	**800**
Modem	3,000	1	**3,000**
Antivirus software	3,000	1	**3,000**
Printing Costs	5 per page	Over 25 pages	**125**
Miscellaneous	-	-	**1,000**
Total	-	-	**7,225**

Figure 6:COST ESTIMATION

3.4 GANTT CHART

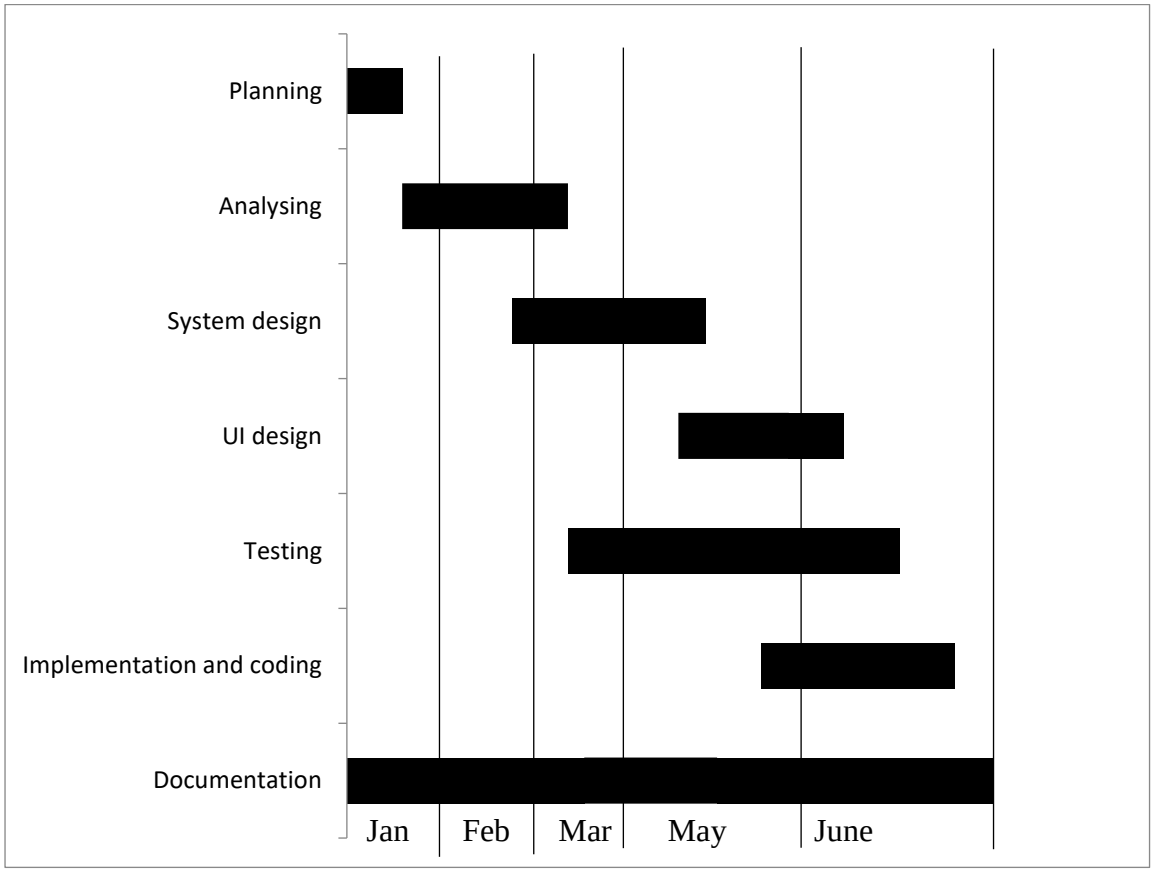

Figure 7-:GANTT CHART

CHAPTER 4:OUTPUT

4.1 SCREEN SHOTS

Expected screen shot.

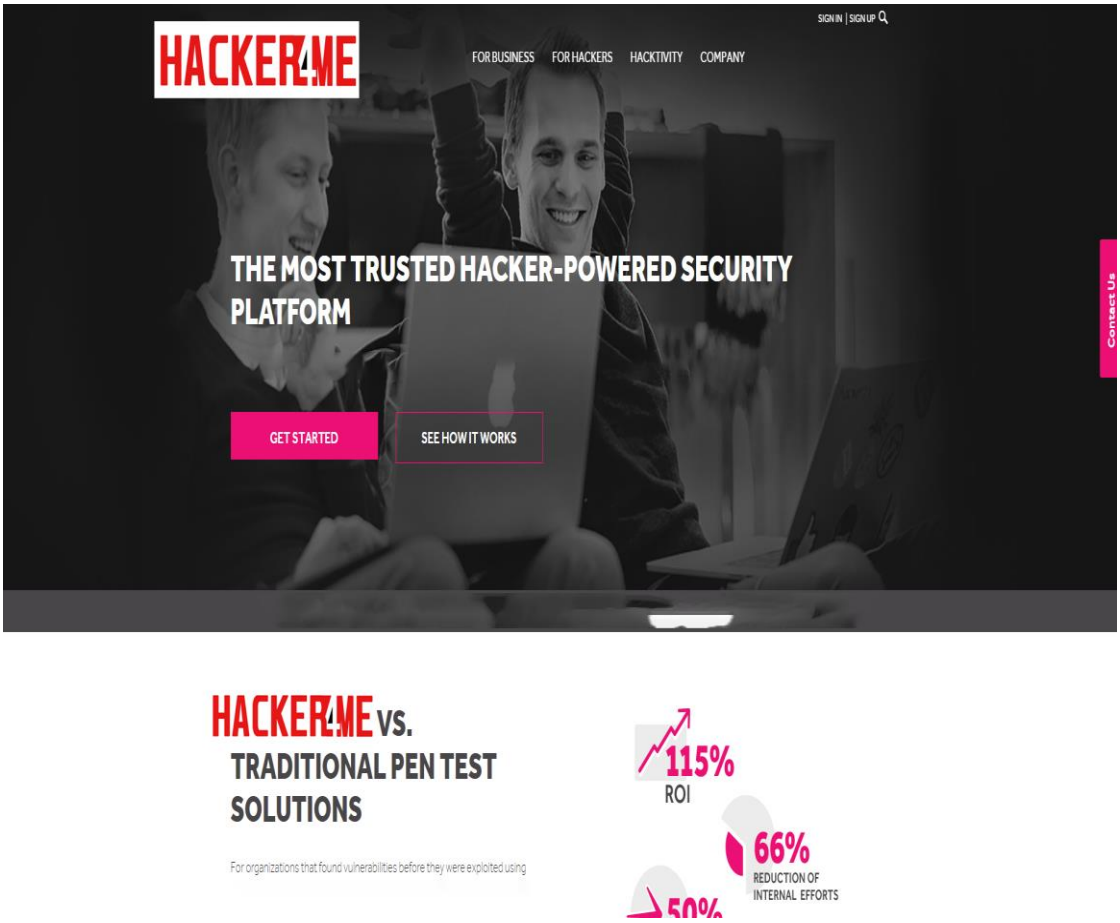

Figure 8:EXPECTED OUTPUT

CHAPTER 5:CONCLUSION

5.1 CONCLUSION

We have achieved a system that will aid in continually improve the security of current technologies and their product to minimize the impact of security vulnerabilities on users. We believe this project will empower individual hackers and security researchers while providing alternative solutions for traditional pentesting performed in organizations to strengthen their security needs. Overall our system will help create secured cyber ecosystem by maintaining availability, integrity and confidentiality.

REFRENCE

- [1] Yagoda, Ben. "A Short History of "Hack"". *The New Yorker*. Retrieved November 3, 2015.
- [2] "The Hacker-Powered Security Report - Who are Hackers and Why Do They Hack p. 23" (PDF). HackerOne. 2017. Retrieved 5 June 2018.
- [3] *World Economic Forum (2018). "The Global Risks Report 2018 13th Edition". World Economic Forum. Archived from the original (PDF) on 23 May 2018.*)
- [4] *Internet Security Glossary*. doi:10.17487/RFC2828. RFC 2828.
- [5] *Internet Security Glossary*. doi:10.17487/RFC2828. RFC 2828.
- [6] Cortada, James W. (4 December 2003). *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries*. USA: Oxford University Press. p. 512. ISBN 978-0-19-516588-3.
- [7] The first "bug" bounty program". Twitter. 8 July 2017. Retrieved 5 June 2018.
- [8] "Computer Security and Mobile Security Challenges". *researchgate.net*. 3 December 2015. Archived from the original on 12 October 2016. Retrieved 4 August 2016.
- [9] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.
- [10] Gordon, Lawrence; Loeb, Martin (November 2002). "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*. **5** (4): 438–457. doi:10.1145/581271.581274.