



BAHIR DAR UNIVERSITY

BAHIR DAR INSTITUTE OF TECHNOLOGY

FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING

COMPUTER ENGINEERING DEPARTMENT

HOSTING COMPANY: INFORMATION NETWORK SECURITY

ADMINISTRATION (INSA)

INTERNSHIP REPORT

DURATION: JUN 17- AUG 30 / 2024 GC

PREPARED BY: ADONAY MUSSIE --- 1307562

YETSEDAW GETNET---1306131

MENTOR: MR. TINBIT ADMASU

COMPANY SUPERVISOR: MR. TILAHUN EJIGU (PHD)

SUBMITTED DATE: 04/11/2024 GC

BAHIRDAR, ETHIOPIA

DECLARATION

We are a 4th year Computer Engineering student that we have undertaken our internship experience in Information Network Security Administration (INSA) for two and half months (Jun 17- Aug 30) under the guidance of Mr. Tilahun Ejigu (director of cyber Audit and Evaluation) and Mr. Tinbit (Academic advisor).

We clarify that our work is original and compiled according to the internship report writing guideline given by the institute.

-----	-----	-----
Name of Student	Date	Signature

-----	-----	-----
Name of Student	Date	Signature

As a mentor, I clarify that the internship prepared by the student is original work and compiled according to the guideline provided by the Institute office.

-----	-----	-----
Name of the Mentor	Date	Signature

ACKNOWLEDGMENT

We would like to express our deepest gratitude to the Information Network Security Administration (INSA) for providing us with the opportunity to complete our internship and for the valuable experiences gained throughout the duration of the program.

We extend our heartfelt thanks to our supervisor, Mr.Tilahun and the other mentors that guided us through this internship, for their consistent guidance, support, and insightful feedback, which played an essential role in the successful completion of our tasks. Their mentorship and encouragement allowed us to enhance both our technical and professional skills, especially in the areas of web development and cyber security.

We are also grateful to our mentor, Mr.Tinbit, for his advice and assistance throughout this internship. Our sincere appreciation goes to our fellow interns and team members at INSA, who contributed to a collaborative and motivating work environment. Their willingness to share knowledge and work together on challenging tasks made the experience both enjoyable and enriching.

Lastly, we would like to thank Bahirdar Institute of Technology, particularly Computer Engineering department, for organizing this internship opportunity. The skills and experiences gained during this internship have been invaluable to my personal and professional development.

EXECUTIVE SUMMARY

This report provides an overview of the internship experience at the Information Network Security Administration (INSA), where we undertook the role of a web developer and security tester. The internship, lasting for two and half months, focused on the development of a secure website using the Laravel framework and conducting penetration testing on both the developed website and additional assigned websites.

The primary objective of the internship was to enhance the administration's digital security by building a robust and secure web application while identifying and mitigating security vulnerabilities through penetration testing. Throughout the internship, we applied theoretical knowledge gained from our web development and computer security coursework to real-world tasks, focusing on both web development and cyber security.

Key responsibilities included designing and developing the website's front-end and back-end, integrating a database, and performing security assessments. Penetration testing revealed several vulnerabilities, and detailed reports were created, providing actionable recommendations for securing the web applications.

This internship allowed us to develop essential skills in web development, cyber security, and while enhancing our ability to work both independently and in a team. The challenges encountered, such as balancing development and security tasks, strengthened our technical abilities and time management skills.

The internship provided a valuable opportunity to apply academic knowledge in a professional setting, offering insights into both web development and web security. The experience significantly contributed to our personal and professional growth, reinforcing our interest in pursuing a career in secure software development and cyber security.

This report consists of five chapters. First chapter gives overview of INSA, about its Background and Structure. Second chapter discusses the task we have been performing at INSA. The Third chapter includes all about our internship project. The fourth chapter describes what benefits we gained from internship program such as theoretical, practical team playing skill, inter personal skill and leadership skills. The last chapter contains conclusions and recommendation.

Contents

DECLARATION	ii
ACKNOWLEDGMENT.....	iii
EXECUTIVE SUMMARY	iv
LIST OF FIGURE.....	vii
LIST OF TABLE	vii
ACRONYMS	viii
CHAPTER ONE	10
1. Historical Background of INSA.....	10
1.1 Brief History	10
1.2 Vision, Mission, Objectives And Core Value Of INSA	11
1.2.1 Vision.....	11
1.2.2 Mission.....	11
1.2.3 Objective Of Insa	11
1.2.4 Core Value	11
1.3 Main Products or Services of INSA.....	12
1.4 Its Main Customers or End Users of Its Product or Service	13
1.5 Organizational Work Flows of INSA Cyber Audit And Evaluation	15
CHAPTER TWO	16
2. Over All Internship Experience	16
2.1 Objective of The Internship	16
2.2 How We Did Get In To The Company	16
2.3 The Section of The Insa We Have Been Working.....	17
2.4 The Work Flow In The Section Looks Like	17
2.5 The Task And Work Piece We Have Executed In The Section.....	18
2.5.1 The task we have executed in the section	18
2.5.2 Work piece we have been executing.....	21
2.6 Procedures We Have Been Using While Performing Our Work Tasks.....	28
2.7 How Good We Have Been In Performing Our Work Tasks.....	29
2.8 The Challenges We Have Been Facing While Performing Our Work Tasks	29
2.9 The Measures We Have Taken In Order To Overcome Our Work Tasks	30
CHAPTER THREE	31
3. Benefit We Gained From Internship.....	31
3.1 What We Gained In Terms Of Improving Our Practical Skills	31

3.2 In Terms Of Upgrading Theoretical Knowledge	32
3.3 In Terms Of Improving Interpersonal Communication Skills	33
3.4 In Terms Of Improving Team Playing Skills.....	33
3.5 In Terms Of Improving Leadership Skills	35
3.6 In Terms Of Understanding About Work Ethics Related Issues	35
3.7 In Terms Of Entrepreneurship Skills	36
CHAPTER FOUR.....	37
4. Internship Projects	37
4.1 Project On Web Development	37
4.1.1 Project Title.....	37
4.1.2 Introduction.....	37
4.1.3 Summary of the Project.....	37
4.1.4 Problem Statement	38
4.1.5 Objective	38
4.1.6 Scope Of The Project	38
4.1.7 Contribution Of The Project	39
4.1.8 Methodology	39
4.1.9 Result	40
4.1.10 Conclusion	42
4.2 Project On Penetration Testing	43
4.2.1 Vulnerability Analysis On Task Management System	43
4.2.2 Testing Mutillidae	49
4.2.3 Local Hosted Web Server http://172.21.35.221/EARS/ Security Audit Report	51
CHAPTER FIVE	59
5. Conclusion and Recommendation	59
5.1 Conclusion	59
5.2 Recommendation	59
5.2.1 Recommendation For The Company	59
5.2.2 Recommendation For The Faculty.....	60
5.2.3 Recommendation For Industrial Linkage.....	60
References:.....	61

LIST OF FIGURE

Fig 1.1 INSA Headquarter	10
Fig 1.2 Work Flow of INSA's Cyber Audit and Evaluation	15
Fig 2.1 VS code.....	22
Fig 2.2 Figma Work Space	22
Fig 2.3 GitHub	23
Fig 2.4 Oracle Virtual Box.....	23
Fig 2.5 Kali Linux Operating System	24
Fig 2.6 Nmap	24
Fig 2.7 Burp Suit.....	25
Fig 2.8 Metasploitable 2	25
Fig 2.9 Enum4linux	26
Fig 2.10 Hydra	26
Fig 2.11 Nikto	27
Fig 2.12 SqlMap.....	27
Fig 2.13 Fuff	28
Fig 3.1 Google Meet Screenshot.....	34
Fig 4.1 Expert Login Page	40
Fig 4.2 Admin Login page	40
Fig 4.3 Create New Task Page.....	40
Fig 4.4 Create New User Page.....	40
Fig 4.5 View Users Page.....	41
Fig 4.6 Profile Page.....	41
Fig 4.7 Assigned Task Page.....	41
Fig 4.8 Notification Page	41
Fig 4.9 Laravel Session Cookie Persistence Post-Logout.....	46
Fig 4.10 Database Query Exposure.....	47
Fig 4.11 Mitigation Code for IDOR.....	47
Fig 4.12 Session Cache on Admin Dashboard.....	54
Fig 4.13 Broken Authentication on organizations/create page	55
Fig 4.14 Broken Authentication on organizations/search page	55
Fig 4.15 Broken Authentication on roles page	56
Fig 4.16 Broken Authentication on offices/create page.....	56
Fig 4.17 Clear text Login Credentials on Login Page.....	57

LIST OF TABLE

Table 4.1 Summary Of Findings	44
-------------------------------------	----

Table 4.2 Laravel Session Cookie Persistence Post-Logout Vulnerability Finding	46
Table 4.3 Database Query Exposure Vulnerability Finding	47
Table 4.4 IDOR Finding	47
Table 4.5 Summary of Findings.....	49
Table 4.6 Summary of Finding	52
Table 4.7 Session Cache Vulnerability Finding.....	54
Table 4.8 Broken Authentication Vulnerability Finding	56
Table 4.9 Clear text Login Credentials Vulnerability Finding	57

ACRONYMS

App	Application
-----	-------------

CSRF	Cross Site Request Forgery
Enum	Enumeration
FFUF	Fuzz Faster U Fool
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDOR	Insecure Direct Object Reference
INSA	Information Network Security Administration
IP	Internet Protocol
JS	Java Script
Nmap	Network Mapper
MOU	Memorandum of Understanding
OWASP	Open Web Application Security Project
RBAC	Role Based Access Control
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UAT	User Acceptance Testing
VS	Visual Studio
XSS	Cross-Site Scripting

CHAPTER ONE

1. Historical Background of INSA

1.1 Brief History

Information Network Security Administration (INSA) is established for the first time in the year 2006 by Council of Ministers Regulation No.130/2006 with an objective to defend our country's information and information infrastructure from attack, and protecting our national interest. However, as it was necessary to amend the administration's power and functions to prevent cybercrimes that become gradually complex and to protect our national interest, its establishment regulation was amended by Council of Ministers Regulation No.250/2011 and recently re-amended by Proclamation No.808/2013.

INSA plays a role in surveillance and internet censorship in close cooperation with Ethio telecom and other government agencies. As of 2014, INSA had the technical ability to listen to live mobile phone calls, while Ethio telecom did not. In 2013, INSA employees had access to the email and other passwords of users of Woredanet (funded by the World Bank and the African Development Bank), Schoolnet (funded by the World Bank and the United Nations Development Programme), and Agrinet.

In 2021, INSA shifted to new headquarters in a building constructed near Wello Sefer at a cost of Br 2.1 billion. The new building is shared by the Ministry of Peace, Artificial Intelligence Center, and Financial Intelligence Center.



Fig 1.1 INSA Headquarter

1.2 Vision, Mission, Objectives And Core Value Of INSA

1.2.1 Vision

To realize national capability that ensures information superiority.

1.2.2 Mission

- To build National Cyber Power capable of protecting the national interest.
- To provide technical intelligence pertaining to national interest so as to support decisions and actions of the government.
- To build data and computing capacity so as to ensure the transformation of the national high-tech and security industry.

1.2.3 Objective Of Insa

1.2.3.1 General Objective

The Information Network Security Administration (INSA) of Ethiopia has the general objective of safeguarding Ethiopia's national interests in cyberspace.

1.2.3.2 Specific Objective

- Defending against cyberattacks on government institutions and critical infrastructure
- Developing and implementing cybersecurity policies and standards
- Cooperating with international partners on cybercrime prevention

1.2.4 Core Value

In fulfilling its mission and achieving its vision the Administration will uphold, promote and be guided by the following core values:

- **Resilience:** INSA emphasizes being prepared to withstand cyberattacks and disruptions, and to bounce back quickly to continue its mission.
- **Making Difference:** The commitment to have a positive impact on Ethiopia's cyber security landscape. INSA strives to actively improve the nation's defenses against cyber threats and contribute to a more secure digital environment.
- **Integrity:** The unwavering commitment to honesty, ethical conduct, and transparency. INSA emphasizes acting with trust and accountability in all its endeavors.

- Respect for the people: Recognizing the rights and needs of Ethiopian citizens in the digital age. INSA aims to balance security measures with respect for privacy and individual freedoms.
- Respect for the law: Operating within the legal framework of Ethiopia. INSA ensures its actions comply with national legislation and upholds the rule of law.

1.3 Main Products or Services of INSA

INSA of Ethiopia plays a crucial role in national cybersecurity, with a broad range of products and services designed to protect and strengthen Ethiopia's digital infrastructure. As the country's primary administration for cybersecurity, INSA's offerings encompass various fields, including threat intelligence, secure digital communications, cybersecurity training, and research and development.

In addition to monitoring, INSA provides cybersecurity consultation services to government agencies and private companies. Through these services, the administration helps organizations evaluate their security postures, identify vulnerabilities, and implement best practices for secure digital operations. INSA's consultation services are crucial for organizations handling sensitive data, such as financial institutions and government bodies, ensuring that their systems meet the highest standards of security.

INSA also develops secure communication tools for the Ethiopian government, aimed at facilitating confidential and encrypted exchanges among officials. Given the increasing reliance on digital communication, these tools ensure that sensitive information remains secure and is protected from unauthorized access or leaks.

Moreover, INSA is engaged in research and development (R&D), focusing on creating indigenous cybersecurity solutions tailored to Ethiopia's specific security needs. This includes the development of local cybersecurity software, protocols, and tools. By fostering in-house innovation, INSA reduces dependence on foreign technologies and builds local expertise, ensuring that Ethiopia can independently secure its digital ecosystem.

INSA is heavily involved in cybersecurity education and training. The administration offers training programs for various stakeholders, from IT professionals to students, aimed at building a skilled workforce capable of protecting Ethiopia's cyber environment.

Through partnerships with universities and specialized training institutes, INSA enhances the country's capacity to manage cyber risks and respond effectively to incidents.

1.4 Its Main Customers or End Users of Its Product or Service

The Information Network Security Administration (INSA) of Ethiopia serves a diverse range of customers and end users, reflecting its commitment to safeguarding the nation's digital landscape. INSA's primary client includes government entities, private sector organizations, educational institutions, and international partners. Each of these groups benefits from INSA's comprehensive cybersecurity products and services tailored to their unique needs and challenges.

Government Entities

As the leading authority on cybersecurity in Ethiopia, INSA's foremost customers are government agencies at all levels, including federal, regional, and local governments. These entities rely on INSA for threat intelligence, secure communication tools, and cybersecurity training. Given the sensitive nature of government operations and the critical data they handle, INSA's services are vital for protecting national security and ensuring the integrity of government functions. INSA also collaborates with various ministries, providing them with essential cybersecurity protocols and support during incidents.

Private Sector Organizations

The private sector forms another significant customer base for INSA, particularly businesses that handle sensitive customer data or operate in sectors like finance, telecommunications, and healthcare. These organizations turn to INSA for cybersecurity consultation, vulnerability assessments, and incident response services. As the threat landscape evolves, private sector companies recognize the importance of robust cybersecurity measures to protect their assets, maintain customer trust, and comply with regulatory requirements. INSA assists these organizations in implementing best practices, thereby enhancing their overall security posture.

Educational Institutions

Educational institutions, including universities and vocational training centers, are key end users of INSA's services. Through training programs and workshops, INSA aims to cultivate a skilled workforce capable of addressing the challenges posed by cyber threats. These institutions benefit from INSA's expertise in curriculum development and access to resources that equip students with the necessary skills for careers in cybersecurity. By fostering partnerships with academic institutions, INSA not only supports education but also strengthens the overall cybersecurity ecosystem in Ethiopia.

International Partners

INSA also engages with international partners, including other governments and international organizations, to enhance collaborative efforts in cybersecurity. These partnerships often involve knowledge sharing, joint training initiatives, and participation in international cybersecurity forums. Through these collaborations, INSA expands its reach and access to best practices, enabling it to better serve its domestic customers. This international engagement is crucial for keeping up with global cybersecurity trends and challenges, thereby enhancing Ethiopia's standing in the international cybersecurity community.

General Public

Finally, the general public is an indirect but essential end user of INSA's services. By securing critical infrastructures and services, INSA helps create a safer online environment for citizens. Public awareness campaigns and educational initiatives aimed at promoting safe online practices further empower individuals to protect themselves from cyber threats.

1.5 Organizational Work Flows of INSA Cyber Audit And Evaluation

Cyber-Security Audit-Evaluation and Accreditation Work Flow

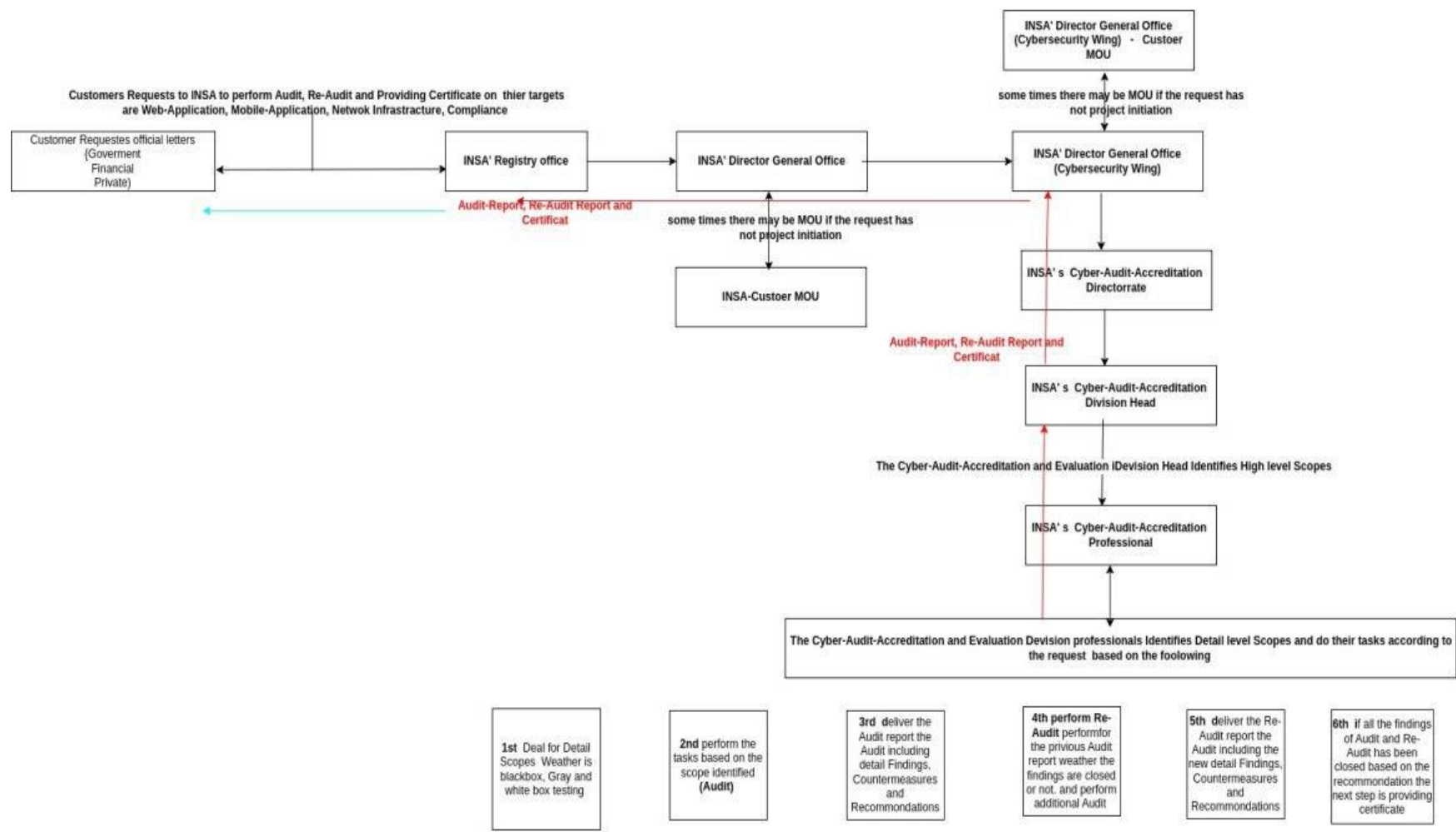


Fig 1.2 Work Flow of INSA's Cyber Audit and Evaluation

CHAPTER TWO

2. Over All Internship Experience

2.1 Objective of The Internship

The objective of internship is to provide student operational environments which formulate and focus on their career objectives. It also to connects students with potential employers and provides opportunities to explore the variety of career objectives that are often available within in the hosting company. Such opportunities also help students relate theories and knowledge acquired in the academic year with the skills and attitudes found in the company and develop idea appreciate businesses area and provide experience that many employers value.

2.2 How We Did Get In To The Company

Gaining an internship at the INSA was a challenging yet rewarding journey that required determination, persistence, and strategic planning. Given INSA's prestigious reputation as a leading organization in cybersecurity, we recognized that gaining acceptance would not be easy. However, our passion for cybersecurity and our desire to acquire the skills and knowledge necessary for a successful career drove us to pursue this opportunity. We got lucky to gain this chance, which we deeply appreciate.

The first step in our journey was conducting thorough research about INSA, its mission, and its key areas of focus. Understanding the administration's role in protecting Ethiopia's digital infrastructure helped us tailor our application to align with its objectives. We realized that INSA offers a unique environment where we could gain hands-on experience in penetration testing and ethical hacking areas that we are particularly passionate about. This knowledge fueled our motivation to apply, as we believed that an internship at INSA would provide us with invaluable insights into the cybersecurity field.

Next, we focused on building a strong application. We updated our resume to highlight our relevant skills, including our experience with penetration testing, knowledge of cybersecurity principles, and familiarity with various tools and technologies used in the field.

This process allowed us to concentrate on ensuring our qualifications were clearly presented, demonstrating our commitment to learning and our understanding of the challenges faced by cybersecurity professionals in Ethiopia.

With determination and a well-prepared application, we submitted our materials and eagerly awaited a response. After a period of anticipation, we received the exciting news that we had been accepted into the internship program. This achievement not only validated our efforts but also marked the beginning of a transformative journey in our pursuit of a career in cybersecurity at INSA.

2.3 The Section of The Insa We Have Been Working

Since INSA is the digital military force of our country, it has plenty of department sections. During our internship period we have been working on INSA's Cyber Audit and Evaluation division. Cyber Audit and Evaluation have the responsibility to perform different cyber security based evaluations according to the INSA's standard and provide an audit and re-audit report to customers who want to check their web-app, mobile-app, systems, and other IT infrastructures.

2.4 The Work Flow In The Section Looks Like

The work flow in INSA cyber audit and evaluation division, if some customers whether it be private or governmental came and want to ask a request to this division to perform an overall cyber security test they have to write a letter and provide their target (web-app, mobile-app, systems) with its specification for INSA general office. Then the general office gives this job to the cyber audit and evaluation division with official letter. The cyber audit and evaluation division director distribute the target to the professional who participate on this INSA's division. The cybersecurity professionals perform different security evaluation on the target and provide an audit and re-audit report to their department director. Finally the department director will present the report to the INSA's general director with a great honor and reliable work. The general director provides the report and all the mitigation steps to the customers. We have conduct our internship work based on this work flow and we perform as cyber security professionals.

2.5 The Task And Work Piece We Have Executed In The Section

2.5.1 The task we have executed in the section

In this cyber audit and evaluation division, we were working as a team member in cybersecurity professionals, and web developer. At the beginning of our internship program the INSA's human resource officer Mr. Melese gave us an orientation and introduced us with the company's policies, procedures, and security protocols. Then our mentor and the cyber audit and evaluation director Mr. Tilahun (phd) gave us general orientation and a road map to our entire internship period. Our mentor told us to begin our internship from web development and then to proceed with security work. Some of the daily tasks we have executed in the section are as follows.

2.5.1.1 Web development using Laravel

During the first phase of our internship period we have developed a task management system by using Laravel as backend and React.js as a frontend. This task management system idea was provided by our mentor to mitigate his task management problem in his office when he distributes tasks to his professional workers. We developed a task management system with in a group and we finished our job on three weeks with full functionalities. A brief review of the task management system stated as follows:

- It has two roles the admin and the expert(user)
- Admin is the only one that can add new experts to the system and the experts can login. Both have session control. The home page is the dashboard for experts but if not logged in and have an expired token (session) make him go back to the login page of user admin have a separate dashboard at /admin which will also redirect to an admin login page if not logged in or have a proper session token.
- In the dashboard of an expert can see the tasks that are assigned to, can search a specific task from the list and can click on and see the details of the specific task. In there he can only right comment on the tasks and also if he wants to notify the admin that the task is done he can check the finished button and the admin will be notified.

- The tasks option reveals all the tasks and also has a search bar on top to search for a specific task and also the users both the admin and the experts can sort the tasks by the attributes they have. There is also add new task button on top that will reveal a form to create new tasks. The admin can get into and see the details of a task by clicking on the task and can comment like the experts. In the task details the admin can edit specific info of the task, delete the whole task, see the notification sent by the experts that say they finished and also approve if it is finished which changes the status of the task from in progress to finished or sent back that will leave the status to in progress.
- The expert option show all the experts available in here he can also search experts, there is an add new expert button the reveal a form to add new expert and can click on an expert to see his details and which tasks he is assigned on, and also can edit the details of the expert, and also delete the user.
- The last option is the settings where the admin can edit his own credentials.

After completing the development and testing phases, we successfully deployed the task management system on a local server with the IP address 172.20.74.19. This deployment has provided significant benefits to the division, streamlining the process of task allocation, tracking, and control across all teams. This task management system provides numerous benefits that streamline workflows and improve team efficiency. It enables clear task organization by allowing users to set priorities, deadlines, and track progress, which helps ensure tasks are completed on time and in order of importance. The system enhances team collaboration with integrated communication tools that allow updates, feedback, and direct messaging within the platform, reducing the need for scattered communication channels. With centralized tracking, team leaders can monitor resource use, identify bottlenecks, and adjust assignments as necessary to optimize productivity. Real-time reporting and analytics offer insights into individual and team performance, empowering managers to make data-driven decisions. Additionally, this task management system increase accountability by making task progress visible to all stakeholders, fostering a sense of responsibility

2.5.1.2 Penetration Testing

In the second phase of our internship, we shifted focus to cybersecurity, starting with the “Certified Ethical Hacking” course led by Dale Meredith. This video course encompasses 16 chapters and it’s above 50 hours long, provided comprehensive training in ethical hacking methodologies, including vulnerability assessment, exploitation techniques, and penetration testing. Following this basic training, we practiced on "Mutillidae," a deliberately vulnerable web application hosted on Metasploitable, with Burp Suite as our primary tool. Burp Suite is widely used in the cybersecurity community to intercept and manipulate web requests, test for vulnerabilities, and assess security controls. This hands-on experience solidified our understanding of key cybersecurity concepts, preparing us for real-world testing environments. To perform these activities we have to learn a new operating system Kali Linux which is a famous operating system favorite to ethical hacking before all we learn basic commands of kali linux.

With our foundational knowledge established, we returned to the task management system we had developed in Phase 1 to test it further for vulnerabilities. During this stage, we discovered an IDOR vulnerability, which could have potentially allowed unauthorized access to user data within the system. According to OWASP, IDOR vulnerabilities fall under broken access controls and can be exploited when an application fails to validate the legitimacy of requests made by users for sensitive data. We successfully mitigated this issue by implementing additional authorization checks on user data access requests, thus securing the system from unauthorized access attempts. This experience underscored the importance of proactive security measures and strengthened our understanding of secure coding practices.

Then our mentor, Mr. Tilahun (phd), assigned us the task of assessing the security of an internal application, the Ethiopian Federal Ethics and Anti-Corruption Commission’s (EARS) web system, hosted at 172.21.35.221/EARS. During this assessment, we identified multiple critical vulnerabilities, including broken authentication, session cache issues, and transmission of login credentials in clear text. Broken authentication is vulnerability where an attacker could gain unauthorized access due to weak or improperly implemented authentication mechanisms. Session caching issues can lead to session hijacking if session tokens are stored insecurely, and the transmission of credentials in plain text exposes users to the risk of credential theft,

especially over unsecured networks. We documented these findings comprehensively in an audit report submitted to Mr. Tilahun, including recommendations for enforcing secure authentication methods, ensuring proper session handling, and encrypting login credentials to prevent data interception, and we calculate the risk according to INSA's risk calculation standard.

In the final stage of our internship, we conducted a penetration test on a web application belonging to the Ethiopian Federal Judicial Administration Council Secretariat (<https://fjacs.dov.et/>). Our testing followed the OWASP standards, a globally recognized framework for web security testing. The OWASP framework outlines various aspects of web application security, emphasizing testing for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and broken authentication, among others. By adhering to these standards, we ensured that our testing was thorough, covering a wide range of potential vulnerabilities. This phase of our internship provided invaluable experience in both applying structured testing methodologies and handling the challenges of real-world penetration testing. But this project hasn't completed yet, we have done this since the last week of our internship period and currently we are trying to test this website and contact our internship mentor.

2.5.2 Work piece we have been executing

Some of the tools which we used in our internship period are:

- VS Code
- Figma
- GiHhub
- Virtual Box
- Kali Linux
- Nmap
- Burp Suit
- Metasploitable
- Enum4linux
- Hydra
- Nikto
- SQLMap
- Fuff

VS Code

Visual Studio Code is a widely-used source-code editor developed by Microsoft, designed for building and debugging modern web and cloud applications. Known for its flexibility, VS Code supports syntax highlighting, IntelliSense, and debugging for a variety of languages like JavaScript, Python, and more.

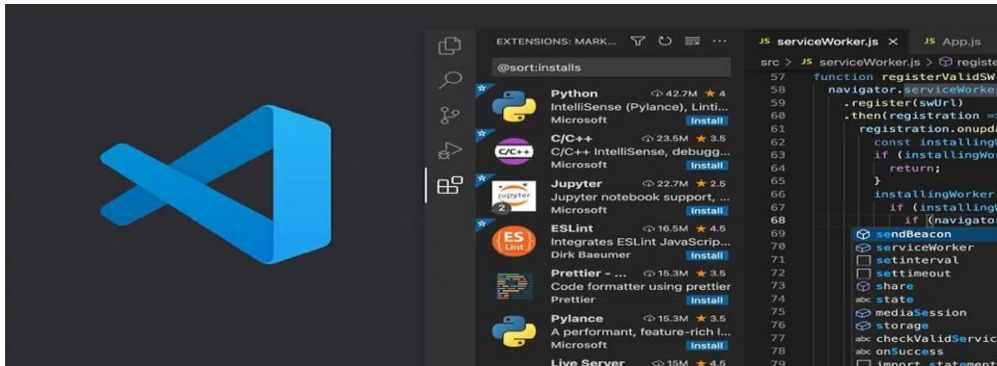


Fig 2.1 VS code

Figma

Figma is a powerful design tool, particularly popular in UI/UX design for its collaborative nature. This cloud-based platform enables designers to create, share, and iterate on designs in real-time, making it ideal for team projects. With features like vector editing, prototyping, and developer handoff, Figma facilitates the entire design process, from wireframing to final designs. Its ability to create interactive prototypes is especially useful for web and app development, as it allows stakeholders to visualize the user experience before development.



Fig 2.2 Figma Work Space

GitHub

GitHub is a web-based platform for version control, utilizing Git, where developers can collaborate on projects, track changes, and manage code versions in repositories. It supports project documentation, issue tracking, and code reviews, making it ideal for both open-source and private development projects. GitHub also offers powerful integrations with other development tools, CI/CD pipelines, and cloud services, streamlining the workflow from development to deployment.



Fig 2.3 GitHub

Virtual Box

Oracle's VirtualBox is a cross-platform virtualization tool that allows users to create and manage multiple virtual machines (VMs) on a single physical host. This tool enables developers and cybersecurity professionals to simulate various environments and test configurations without affecting the host system. VirtualBox supports numerous guest operating systems, making it a valuable asset for testing, software development, and isolated security testing within contained environments.



Fig 2.4 Oracle Virtual Box

Kali Linux

Kali Linux is a Debian-derived Linux distribution specifically designed for penetration testing and cybersecurity. Known for its comprehensive collection of pre-installed security tools, including Nmap, Burp Suite, and Metasploit, it allows security professionals to conduct tasks such as vulnerability scanning, digital forensics, and intrusion detection. Its customizability and support for ARM architectures make it versatile for various hardware setups and security assessments.



Fig 2.5 Kali Linux Operating System

Nmap

Network Mapper (Nmap) is an open-source tool used to discover hosts and services on a computer network. Known for its versatility, Nmap performs port scanning, OS detection, version detection, and host discovery, making it essential for network administrators and security analysts. Its scripting engine enables customization and automation of tasks, allowing users to perform comprehensive assessments of network security.



Fig 2.6 Nmap

Burp Suit

Burp Suite is an integrated platform for performing security testing of web applications. It includes a range of tools for mapping and analyzing attack surfaces, as well as identifying and exploiting vulnerabilities. Burp Suite's ability to intercept HTTP requests and responses, combined with its extensive extension options, makes it a powerful tool for identifying issues like cross-site scripting (XSS), SQL injection, and session-related vulnerabilities.



Fig 2.7 Burp Suit

Metasploitable

Metasploitable is a purposefully vulnerable virtual machine created for security training purposes. Often used with the Metasploit framework, it enables students and professionals to practice identifying and exploiting common vulnerabilities in a controlled environment. This platform is ideal for testing attack techniques and validating security tools in a safe and educational setting.



Fig 2.8 Metasploitable 2

Enum4linux

Enum4linux is a command-line tool for gathering information from Windows and Samba systems. It is particularly useful for identifying network shares, usernames, group memberships, and operating system versions in Windows environments. In cybersecurity, Enum4linux is frequently used to assess network security and identify weak points in permissions and configurations.



Fig 2.9 Enum4linux

Hydra

Hydra is a fast password-cracking tool used to perform brute-force and dictionary attacks across a range of protocols, including SSH, FTP, and HTTP. With its flexible configuration options, Hydra allows penetration testers to target multiple authentication protocols, making it valuable for assessing password security and testing for weak authentication mechanisms within networks.



Fig 2.10 Hydra

Nikto

Nikto is a web server scanner that detects a wide range of vulnerabilities, misconfigurations, and outdated software on web servers. By scanning web applications, Nikto identifies issues like open directories, insecure HTTP methods, and server configuration weaknesses, providing valuable insights for web application security assessments.



Fig 2.11 Nikto

SQLMap

SQLMap is an automated tool for detecting and exploiting SQL injection vulnerabilities in databases. With a robust range of features, SQLMap supports database fingerprinting, retrieving database data, and even accessing the underlying operating system, making it an invaluable tool in web application security testing.

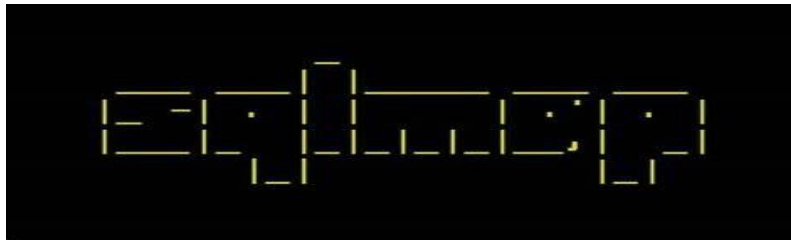


Fig 2.12 SqlMap

Fuff

FFUF (Fuzz Faster U Fool) is a command-line web fuzzer that automates the discovery of hidden files, directories, and parameters on web servers. Useful for web application testing, FFUF is customizable and allows security testers to identify unintended exposure of sensitive files or parameters, which can lead to vulnerabilities within the application.



Fig 2.13 Fuff

2.6 Procedures We Have Been Using While Performing Our Work Tasks

Throughout our internship at INSA, we implemented structured procedures to effectively accomplish our tasks, which enhanced our consistency, accuracy, and learning in the work environment. Each project began with a detailed planning phase, where tasks were broken down into manageable steps with a timeline for completion. This initial stage helped us identify potential challenges and set clear objectives, especially with new tools and concepts. Since many tasks required learning new tools, we prioritized research, consulting online resources, reviewing materials from our mentor, and seeking guidance from experienced INSA professionals. This constant research was essential as we worked with complex tools like Burp Suite, Nmap, and VirtualBox.

At the end of each project, we performed thorough testing and verification of our work to ensure accuracy and functionality. We double-checked configurations and re-tested changes to confirm they had the intended effect without introducing new issues. After completing each task, we reviewed our results and processes to identify areas for improvement, incorporating lessons learned into future tasks. This giving us a strong foundation in cybersecurity and application development during our internship at INSA.

2.7 How Good We Have Been In Performing Our Work Tasks

We believe we did great at performing all the task that we have been assigned to do and the reason behind that is we were fast learners and adaptive to the technologies. We were introduced to many new concepts and managed to master all of them within this internship period. We believe we have added prominent value to the startup we worked for and also done a good work for our host INSA. It is not enough if only us witnessed our work so we have asked the same question both staff members and our mentor Mr.Tilahun(phd) about how well we performed our task and they give good feedback and suggestion to improve our skill.

2.8 The Challenges We Have Been Facing While Performing Our Work Tasks

Throughout our internship at INSA, we encountered several challenges that tested our resilience and adaptability. These obstacles stemmed from the nature of the projects we worked on, our foundational knowledge, and the demands of the cybersecurity field. However, these challenges also provided invaluable learning experiences that ultimately strengthened our skills and understanding.

One of our primary challenges was Laravel's unfamiliar structure and syntax required extra time to study documentation and test its features.

Moving from theory to real-world cybersecurity projects demanded critical thinking and adaptability beyond our coursework.

Our limited experience with tools like Kali Linux presented a learning curve. We invested time in mastering this OS, which enhanced our understanding of ethical hacking and practical cybersecurity skills.

The consistent work schedule challenged us to manage our time effectively and maintain productivity.

2.9 The Measures We Have Taken In Order To Overcome Our Work Tasks

Facing a range of challenges during our internship at INSA required us to develop strategies to adapt and progress effectively. Through proactive learning, seeking guidance, and utilizing our resources, we were able to navigate obstacles and continue to grow in our roles. Here are some of the key measures we took to overcome the challenges in our work tasks:

First, we actively explored online resources to build our knowledge and skills in the frameworks and tools we encountered. Laravel, which was new to us, required substantial . By accessing online tutorials, forums, and documentation, we were able to gain a basic understanding of how Laravel functions, which ultimately improved our efficiency in project work. Additionally, the internet served as a valuable resource for all our learning needs, allowing us to expand our understanding of cybersecurity concepts and tools at our own pace.

Our mentor also played an important role in supporting our progress. Recognizing our interest in cybersecurity, they provided us with relevant materials that clarified the essential concepts and gave us a structured foundation in the field. These materials significantly improved our understanding, particularly in areas where we were unfamiliar, such as penetration testing and ethical hacking methodologies.

Motivation was another critical factor in overcoming our tasks. Our curiosity and desire to learn more about cybersecurity drove us to dedicate extra time to understanding complex topics. This motivation not only kept us engaged but also helped us push through difficulties. As we learned more about cybersecurity, we became increasingly invested in our work, which positively impacted our performance and growth.

More, we reached out to professional workers at INSA whenever we encountered challenges beyond our understanding. Consulting experienced professionals was invaluable, as it provided us with immediate guidance and insights that were often difficult to find elsewhere. This approach also helped us develop problem-solving skills by exposing us to practical advice and real-world techniques.

CHAPTER THREE

3. Benefit We Gained From Internship

Our internship at the Information Network Security Administration (INSA) was a big learning experience, giving us real-world practice in cybersecurity and helping us grow in both technical skills and personal abilities. This report explains the main benefits we gained in several areas, including practical and theoretical knowledge, communication, teamwork, and professional ethics. We hope to show how much this internship has impacted our journey as cybersecurity learners.

3.1 What We Gained In Terms Of Improving Our Practical Skills

During our internship at INSA, we gained valuable hands-on experience with tools that are essential in cybersecurity. We used tools like Kali Linux, Burp Suite, Nmap, and Hydra to conduct tasks like vulnerability checks, penetration tests, and network scans. Working with these tools gave us a better understanding of how to protect networks and data knowledge we could only learn by actually doing the work.

Handling real projects showed us the kinds of challenges professionals face every day. For instance, while identifying system vulnerabilities, we applied techniques like network scanning and brute-force testing. This hands-on work helped us build troubleshooting and problem-solving skills, which are critical for tackling cybersecurity tasks.

Some practical skills we gained with tools:

- Kali Linux → For penetration testing and vulnerability assessments
- Nmap → Used for network discovery and security auditing
- Burp Suite → Assisted in web application security testing
- Hydra → Enabled us to perform brute-force testing

Real-World Problem Solving:

- Troubleshooting → Resolved issues independently in practical scenarios
- Problem Analysis → Applied critical thinking to solve network vulnerabilities
- Report writing → Writing audit and re-audit report according to INSA's standard

Application of Theory to Practice:

- Network Scanning → Practiced theoretical knowledge through live network scans
- Vulnerability Identification → Identified security gaps using practical tools

Skill Development in Cybersecurity:

- Tool Familiarization → Enhanced knowledge of widely-used cybersecurity tools
- Confidence Building → Gained confidence through hands-on application

Practical Knowledge in Development:

- Laravel → Gained experience in web development using Laravel
- VS Code → Enhanced coding skills using Visual Studio Code for development
- GitHub → Learned version control and collaboration through GitHub
- React js → Gained experience in front end web development using react js library

3.2 In Terms Of Upgrading Theoretical Knowledge

Alongside practical skills, we also deepened our theoretical knowledge in cybersecurity and software development. We kept learning about cybersecurity basics, risk management, and network security protocols, giving us a strong foundation we could apply directly in our tasks at INSA.

Our mentor and other professionals provided us with helpful materials on topics like secure coding, network setups, and web application security. Learning this theory helped us make better decisions when using security tools, so we understood why each security rule and protocol mattered. Combining theory with hands-on practice helped us learn faster and more thoroughly.

Additionally, there were a block chain professional in our office and he is willingly to teach us some basics about block chain and crypto currency. For two day he gave us a lecture for a couple of hours. On this block chain and crypto currency lecture we gather much basic theoretical knowledge. By this opportunity we want to thank Mr. Abel for his willingly and his amazing lectures.

3.3 In Terms Of Improving Interpersonal Communication Skills

One of the best parts of our internship was improving our communication skills. We worked closely with coworkers on group projects, which required regular discussions and teamwork. Whether we were talking about project ideas or sharing updates, these interactions helped us learn to explain technical things more clearly and to listen to feedback.

We also built strong connections with INSA's professionals and mentors, which allowed us to discuss cybersecurity topics more deeply during lunch breaks or other informal times. These talks not only increased our knowledge but also built friendships with people we still talk to even though we aren't in the same office now. These communication skills will help us in both professional and personal growth.

So, in terms of inter personal communication we improve to explain what we have in our mind to others and the program helped us to do so. Also, to develop:

- sharing ideas and knowledge
- Respect co-workers and people
- Improves Handling information
- It brings social interaction to the organization employees
- Improve to build up self confidence
- It improves our speaking and listening skills

3.4 In Terms Of Improving Team Playing Skills

Our experience working on teams at INSA taught us how important collaboration is. Each project meant working with people who had different skills and perspectives. We learned how to bring our skills together and help each other in areas where we had less experience, creating an environment where everyone could learn and succeed together.

Working in a team also taught us the importance of clear communication, sharing tasks, and solving problems together. These teamwork skills are very useful, especially in cybersecurity, where collaboration is often needed to solve complex issues.

During our team work we use different tools like Google meet to online meeting, figma for designing the web development task and git hub to push and pull repositories.

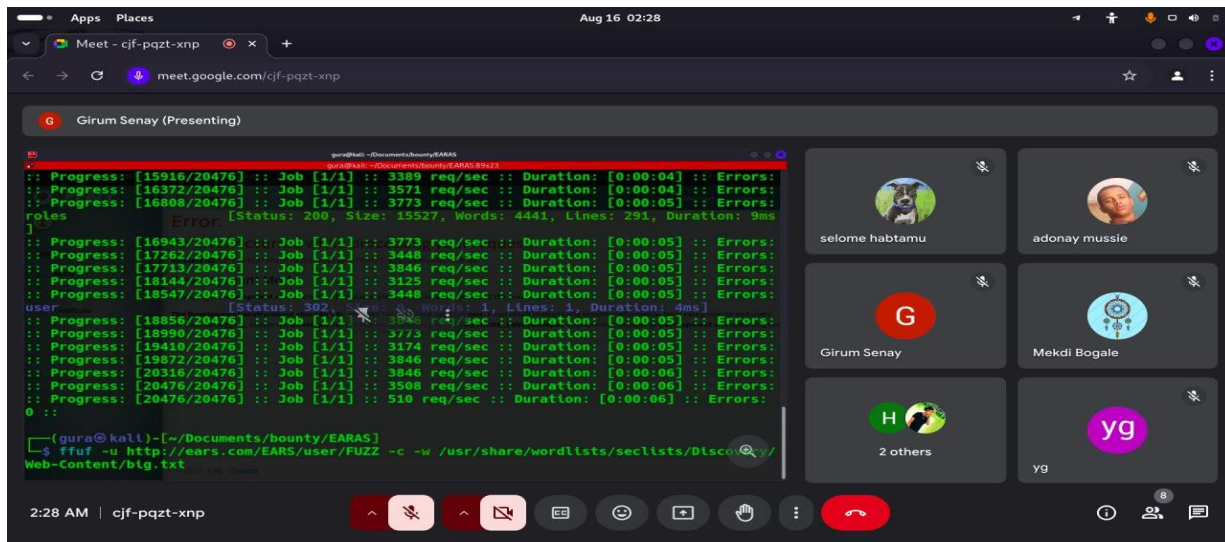


Fig 3.1 Google Meet Screenshot

We have learned from internship period that team works leads us being successful and productive.

- To do works with group of teams.
- Increase the speed of activities
- Ability of problem identification for solving problems
- Selecting the most appropriate method to solve the existing problem
- Generating or forwarding flexible permissions to solve the problems raised
- A good decision maker

3.5 In Terms Of Improving Leadership Skills

The internship gave us chances to grow our leadership skills, especially when we needed to take initiative. Sometimes, we had to lead a part of a project, lead team discussions, or organize tasks. Through these experiences, we learned how to balance being responsible with supporting our teammates.

Leading also meant making decisions that impacted the project and the team. We learned to:

- Manage risks
- Handle resources
- listen the idea of any employee
- Be a problem solver
- Resist problems
- Be Transparency
- Be Accountable for your duty
- Be Punctual
- Be Responsible
- Create self-motivation and workers' motivation
- Be a communicable person with everyone with a great Smile

This experience prepared us to take on more leadership roles in the future.

3.6 In Terms Of Understanding About Work Ethics Related Issues

The internship at INSA taught us the importance of work ethics, which are essential for building trust and professionalism in any organization. We were committed to completing tasks given by our mentor, meeting deadlines, and negotiating priorities to reach project goals.

- Punctuality,
- Professionalism, and
- Discipline were key parts of the work culture at INSA, which we aimed to follow.

Our supervisor emphasized values like transparency, honesty, and dedication, which helped us internalize these qualities and build a strong work ethic. Practicing these values contributed to our growth and helped us build a professional relationship with our colleagues, reflecting positively on our work. We have seen that in our internship period a strong work ethic is vital to a company achieving its goals. We have known important things about work ethics like: -

- Co-operation
- Honesty
- Obedience to relatives, user and our instructor
- Sense of responsibility
- Having willing to do some task
- Confidentiality
- Respect the rules and the regulations
- Discipline
- Act in the public interest
- Commitment
- Sense of teamwork

3.7 In Terms Of Entrepreneurship Skills

While working on projects, we started to understand what it means to think like an entrepreneur. This involved looking at problems from different perspectives, identifying risks, and coming up with creative solutions. We were encouraged to think independently and find new approaches, which helped us apply entrepreneurial thinking to cybersecurity tasks.

These experiences taught us about practical aspects of entrepreneurship, like managing resources, making plans, and staying resilient. By taking ownership of our tasks and working independently, we developed skills that will be useful not only in cybersecurity but also in potential business ventures.

CHAPTER FOUR

4. Internship Projects

During our internship at INSA, we complete five projects in total: one focused on web development and four dedicated to penetration testing.

4.1 Project On Web Development

4.1.1 Project Title

Task Management System Using Laravel

4.1.2 Introduction

During our internship at the Information Network Security **Administration** (INSA), our team was tasked with developing a task management system using Laravel. The primary goal of the project was to create a platform that would streamline task assignment, tracking, and completion, optimizing daily workflows **for efficient team management**.

The system was designed with scalability and user-friendliness in mind, utilizing Laravel, a robust PHP-based framework for web application development. Through Laravel's capabilities, we built a solution tailored to meet task management needs, incorporating features to support clear tracking, assignment delegation, and timely completion of tasks across teams.

4.1.3 Summary of the Project

The task management system developed during our internship at the Information Network Security Agency (INSA) aimed to streamline and optimize task organization and completion processes within team environments. Built using the Laravel framework, the system provides a centralized platform for creating, assigning, monitoring, and completing tasks. Key functionalities include task assignment, priority setting, deadline management, and progress tracking, all geared toward enhancing productivity and transparency.

The development process followed a structured approach, beginning with requirement gathering and progressing through stages of development, testing, and refinement. The system's design prioritizes an intuitive user interface to facilitate ease of use, ensuring that users can efficiently navigate the platform with minimal training. The completed task management system is a functional, efficient tool capable of enhancing workflow management and productivity for teams at INSA.

4.1.4 Problem Statement

At INSA(mainly in cyber audit and evaluation division) , effective task management was hold up by reliance on Excel spreadsheets for assigning and tracking tasks, which, while functional, presented significant limitations in real-time updates, collaboration, and progress visibility. This approach led to inefficiencies such as missed deadlines, difficulty in monitoring task completion, and limited transparency, which impacted both team members and leadership. Team leads found it challenging to allocate resources and ensure accountability, while team members struggled to prioritize tasks and track their progress in alignment with project goals.

4.1.5 Objective

4.1.5.1 General Objective

To develop a centralized task management system using Laravel.

4.1.5.2 Specific Objective

- To replace the existing Excel-based task management process with a user-friendly, web-based platform for streamlined task assignment and monitoring.
- To enable real-time progress tracking and updates for both team leads and team members, enhancing accountability and transparency.
- To improve team collaboration by creating a shared environment where all task-related information is easily accessible and up-to-date.
- To increase productivity by providing tools for setting task priorities, deadlines, and status updates, allowing for efficient resource allocation and workload management.

4.1.6 Scope Of The Project

The scope of this project involves creating a web-based task management system to replace the current Excel-based process. This system will support only the English language and it is functional only in INSA.

4.1.7 Contribution Of The Project

This project contributes to the organization by enhancing efficiency through a user-friendly web-based task management system that replaces the current Excel process. It improves accountability with real-time tracking, facilitates collaboration by providing a shared space for team members to access task information, and allows for better resource management through tools for setting priorities and deadlines. The system is designed to be low-cost and supports only the English language, making it a practical solution that meets the organization's needs while ensuring scalability for future enhancements. Overall, the project aims to boost productivity and streamline task management processes.

4.1.8 Methodology

- **Requirements Gathering:** Collaborated with our mentor to collect all necessary requirements, ensuring the system aligns with organizational needs.
- **Design Drafting:** Worked as a group to create user interface using Figma, illustrating the intended look and functionality of the application.
- **Learning Technologies:** Engaged in hands-on learning of Laravel and React, focusing on the frameworks necessary for building the system through coding sessions and tutorials.
- **Development:** Built the core functionalities of the task management system using Laravel for the backend and React for the frontend.
- **Testing:** Conducted various testing methods, including unit testing and user acceptance testing (UAT), to ensure the system operates as intended and meets user expectations.
- **Deployment:** Deployed the application on a suitable server, making it accessible to all intended users while conducting final checks for functionality.

4.1.9 Result

Login credential

As we describe on the above, the task management system have two actors the admin and the experts, (professionals). Both the admins and experts can login to their account in the login page according to their role.

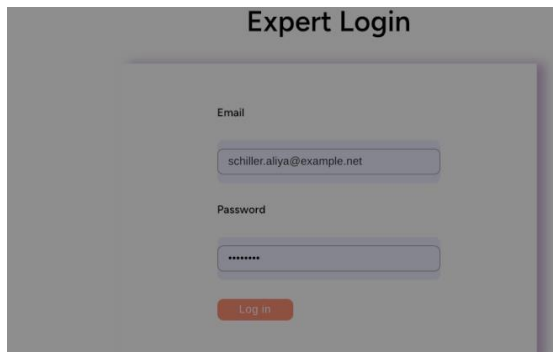
The image shows a login form titled "Expert Login". It has a light gray background with a white form area. The form contains two input fields: "Email" with the value "schiller.aliya@example.net" and "Password" with masked characters "*****". Below the password field is a red "Log in" button.

Fig 4.1 Expert Login Page

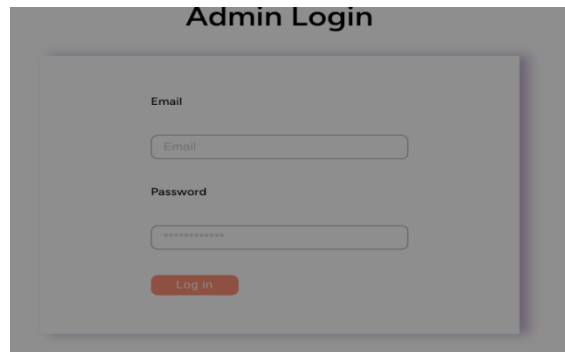
The image shows a login form titled "Admin Login". It has a light gray background with a white form area. The form contains two input fields: "Email" and "Password" (masked with "*****"). Below the password field is a red "Log in" button.

Fig 4.2 Admin Login page

Roles of Admin

- Create tasks
- Create users
- Read comments
- Delete tasks and users
- See and change profiles
- Send notifications

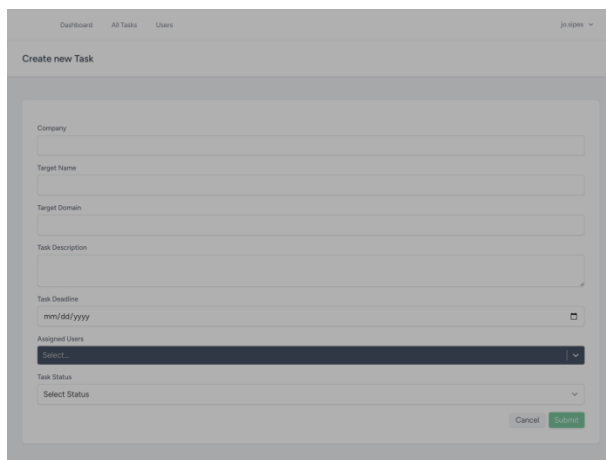
The image shows a form titled "Create new Task". It has a light gray background with a white form area. The form contains several input fields: "Company", "Target Name", "Target Domain", "Task Description", "Task Deadline" (with a date picker showing "mm/dd/yyyy"), "Assigned Users" (with a dropdown menu showing "Select..."), and "Task Status" (with a dropdown menu showing "Select Status"). At the bottom right are "Cancel" and "Save" buttons.

Fig 4.3 Create New Task Page

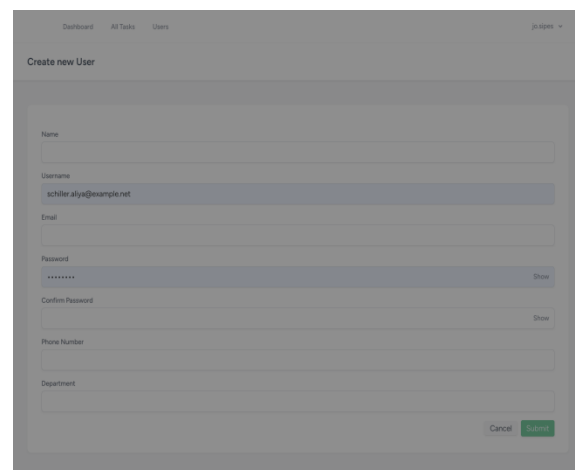
The image shows a form titled "Create new User". It has a light gray background with a white form area. The form contains several input fields: "Name", "Username" (with the value "schiller.aliya@example.net"), "Email", "Password" (masked with "*****" and a "Show" button), "Confirm Password" (masked with "*****" and a "Show" button), "Phone Number", and "Department". At the bottom right are "Cancel" and "Save" buttons.

Fig 4.4 Create New User Page

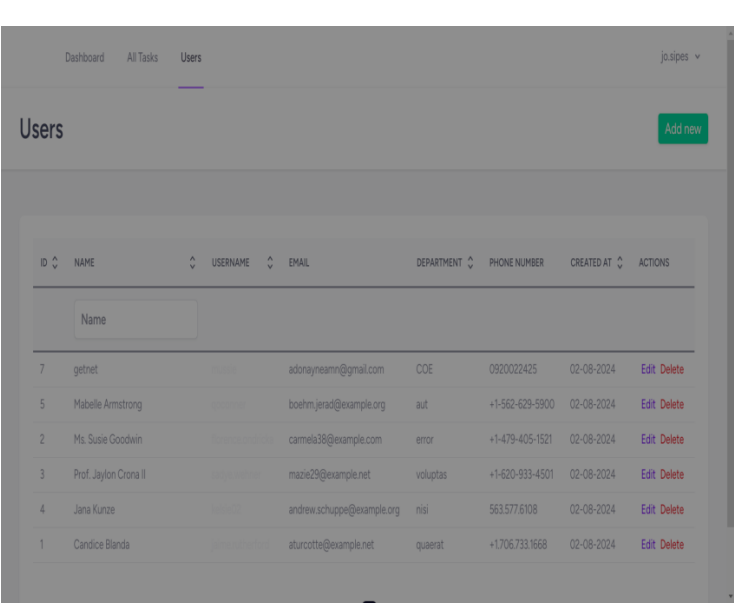


Fig 4.5 View Users Page

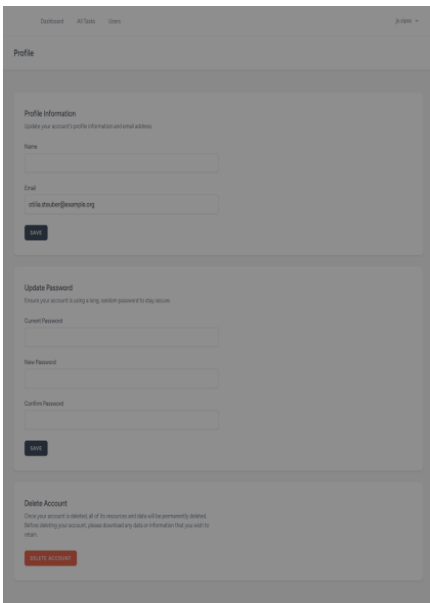


Fig 4.6 Profile Page

Roles of expert

- See assigned tasks
- Write the progress
- Read notifications
- Write comments

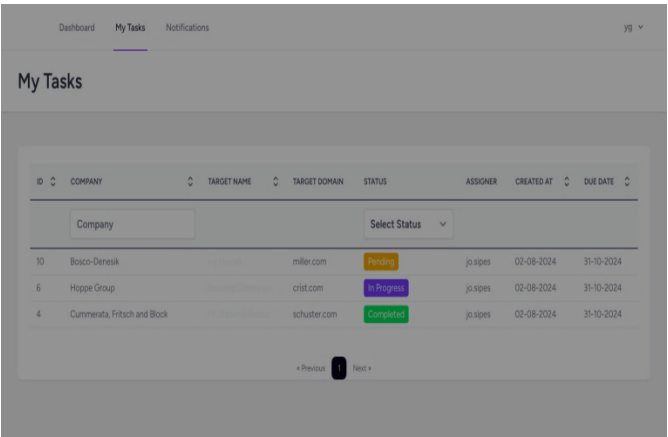


Fig 4.7 Assigned Task Page

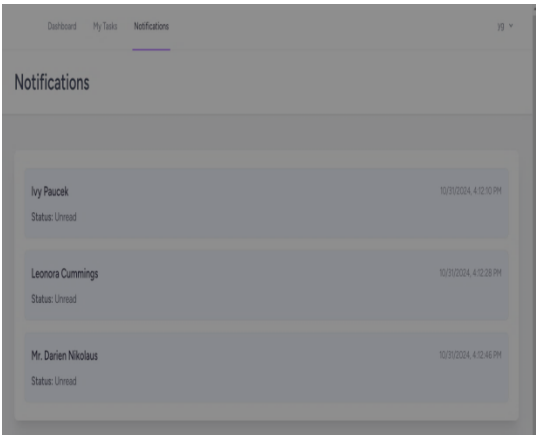


Fig 4.8 Notification Page

4.1.10 Conclusion

The development of the web-based task management system represents a significant advancement in the way our organization manages tasks and collaborates as a team. By transitioning from an Excel-based approach to a user-friendly web application, we have enhanced efficiency, accountability, and communication among team members. The project has successfully met its objectives of providing real-time tracking, improved resource management, and fostering a collaborative environment.

Through a structured methodology that involved gathering requirements, collaborative design, learning essential technologies, and thorough testing, we have created a solution tailored to the specific needs of the organization. The low-cost nature of this project, coupled with its focus on English language support, ensures it is both practical and accessible for all users.

As we move forward, continuous feedback will be vital in refining the system and implementing further improvements. This project not only equips our team with the tools needed to succeed but also lays the groundwork for future developments in task management practices within the organization.

4.2 Project On Penetration Testing

4.2.1 Vulnerability Analysis On Task Management System

4.2.1.1 Introduction

As part of our internship project, we developed a task management system using Laravel and React, designed to streamline task assignments, progress tracking, and collaboration within teams. To ensure the system's reliability, security, and usability, we conducted thorough testing across various aspects of the application. This testing phase aimed to identify potential issues, improve functionality, and enhance the system's resilience against security threats.

Throughout the process, we uncovered different issues, including areas where the system's performance and security could be strengthened. This report provides an overview of the testing methodology, findings, and recommendations for improving the task management system to ensure it meets both functional and security standards.

4.2.1.2 Executive Summary

We have performed vulnerability assessment and penetration testing on the task management system which was built by us on the development phase and deployed on local server by IP address 172.20.74.19/website. We have conducted the security assessment in a manner that simulated malicious actors engaged in an attack against of the 172.20.74.19/ website by using different security vulnerability technical tools and best practices and measured the overall security status of the 172.20.74.19/

This report contains the details of the vulnerability assessment and penetration testing result along with suggested remedial solutions. The result shows that the application has different vulnerabilities that can expose the 172.20.74.19/ website to different threats.

4.2.1.3 Summary Of Findings

Types of Vulnerabilities	Level of Risks			
	HIGH	MEDIUM	LOW	TOTAL
Database Query Exposure	✓			
Laravel Session Cookie Persistence Post-Logout		✓		
IDOR	✓			
TOTAL	2	1	0	3

Table 4.1 Summary Of Findings

4.2.1.4 Objective

4.2.1.5.1 General Objective

The main objective is to identify potential security vulnerabilities and provide technical, managerial, physical and human related recommendations to remediate them.

4.2.1.5.2 Specific Objective

- To identify and analyze potential security vulnerabilities in the task management system web app
- To assess the application's performance and reliability under different conditions
- To enhance the application's overall security and compliance by testing for weaknesses that could be exploited

4.2.1.5 Scope Of The Project

The scope of this security audit is the portal of 172.20.74.19/ (the task management system)

4.2.1.6 Applied Methodology

To conduct the penetration testing, we used many methodologies. Some methodologies used to test the application are mentioned below:

- Following up Application security checklist
- Following up OWASP testing guide
- Application security testing tools

4.2.1.7 Detailed Security Audit Findings

The following tables show the details of the vulnerabilities identified during the security assessment process.

No	1
Vulnerability Name	Laravel Session Cookie Persistence Post-Logout
Target	http://172.20.74.19/admin
Vulnerability Description	The session cookie associated with Laravel users remains in the browser even after logging out. This persistence may allow an attacker to hijack the session by using the still-active session cookie, leading to unauthorized access.
Risk Level	Medium
Impact	An attacker could potentially gain access to a user's account after logout, leading to unauthorized actions, data theft, or other malicious activities within the application.
Countermeasure	Ensure the session cookie is securely invalidated and removed from the browser upon logout. Implement additional measures like setting a short expiration time for session cookies and utilizing secure and HttpOnly flags to enhance session security.

Evidence:

The screenshot shows a web browser at the URL `172.20.74.19/login`. The page has a logo at the top and a form titled "Expert Login" with fields for "Email" and "Password". Below the form, the Chrome DevTools console is open, showing the "Storage" tab. It lists two cookies:

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Partition	Cross S.	Priority
XSRF-TOKEN	eyJpdi6mo40TR2VpOW5SczYURyZmH5Sz0akE9...	172.20...	/	2024-0...	352			Lax			Medium
laravel_session	eyJpdi6mZmH5Sz0akE9...	172.20...	/	2024-0...	357	✓		Lax			Medium

Fig 4.9 Laravel Session Cookie Persistence Post-Logout

Table 4.2 Laravel Session Cookie Persistence Post-Logout Vulnerability Finding

No	2
Vulnerability Name	Database Query Exposure
Target	<u>http://172.20.74.19/admin/task/{id}</u>
Vulnerability Description	Unsecured database queries within the application may expose sensitive information, including SQL injection points. These exposed queries can be exploited by attackers to manipulate or extract critical data from the database.
Risk Level	High
Impact	Exposure of database queries can lead to severe consequences, including data breaches, unauthorized data manipulation, and full compromise of the database integrity.
Countermeasure	Implement parameterized queries and prepared statements to prevent SQL injection attacks. Regularly audit the codebase to identify and secure any exposed database queries and enforce strict access controls to the database.

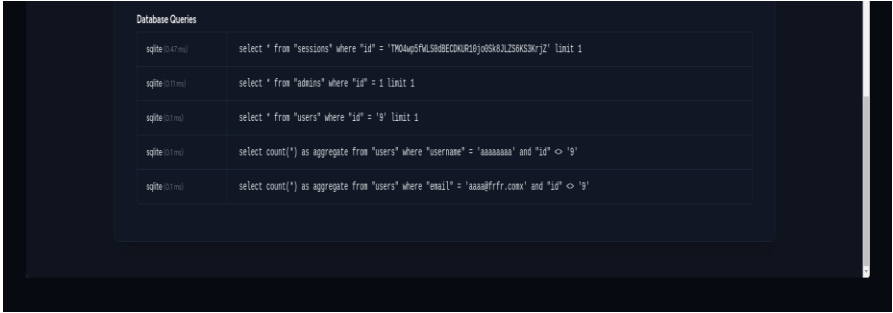
Evidence:	 <p style="text-align: center;">Fig 4.10 Database Query Exposure</p>
-----------	---

Table 4.3 Database Query Exposure Vulnerability Finding


No	3
Vulnerability Name	IDOR
Target	http://172.20.74.19/admin/task_delate
Vulnerability Description	IDOR vulnerability occurs when an application directly references an internal object, like a database record, based on user input, without properly verifying that the user is authorized to access it.
Risk Level	High
Impact	It can allow unauthorized access to sensitive data or system functionality, leading to privacy breaches or unauthorized actions. Due to its nature, IDOR vulnerabilities are difficult to detect with automated tools and require robust access control checks at the application level to mitigate.
Countermeasures	<p>This can be patched by integrating 1 line to check the creator of those object's in the retrieval Controllers of each object</p>  <p style="text-align: center;">Fig 4.11 Mitigation Code for IDOR</p>

Table 4.4 IDOR Finding

4.2.1.8 Risk Calculation

Throughout the document, each risk calculated has been listed in a table 4.1 as a finding and categorized as a High-Risk, Medium-Risk, or Low-Risk. INSA used the following Risk calculation formula to calculate the risks.

$$\text{Risk} = \text{Likelihood} * \text{impact}$$

High risk: - these findings identify conditions that could directly result in the compromise of the web application. These include getting access to the website by resetting user accounts of different user levels i.e. normal user up to administrator user level. This will allow an attacker to perform tasks on administrator user level.

Medium risk: - these findings identify conditions that do not immediately or directly result in the compromise but do provide a capability to gain control on the web application. These includes the session cookie does not expire after the users click on log out. These will allow attackers to login and perform tasks using the cookie once they steal it from legitimate user.

Low risk: - these findings identify conditions that provide information that could be used in combination with other information to gain insight into how to compromise the web application. These include vulnerabilities like information disclosure and displaying server banners.

4.2.1.9 Conclusion

After we perform a penetration test on the task management system which built by us, we conclude that our website needs some improvement. Then we list out each vulnerability and perform a mitigation stage activities and re deploy the system again.

4.2.2 Testing Mutillidae

4.2.2.1 Introduction

Mutillidae application, a deliberately vulnerable web application designed for practicing and testing various web security techniques. This application was selected for its wide range of vulnerabilities, which allowed us to develop hands-on experience in identifying and exploiting weaknesses commonly found in real-world web applications.

4.2.2.2 Executive Summary

This report provides an overview of our security testing efforts on the Mutillidae application. Mutillidae, known for its intentionally insecure structure, allowed us to apply penetration testing techniques in a controlled environment. Our objectives included identifying exploitable vulnerabilities, testing our access to sensitive areas, and verifying whether security flaws could lead to unauthorized data access or modifications. Despite the application's vulnerabilities, we successfully gained access to various sections of the site, demonstrating the potential security risks in web applications without adequate protection.

4.2.2.3 Summary Of Findings

Types of Vulnerabilities	Level of Risks			
	HIGH	MEDIUM	LOW	TOTAL
XSS	✓			
Sql Injection	✓			
CSRF	✓			
TOTAL	3		0	3

Table 4.5 Summary of Findings

4.2.2.4 Objective

4.2.2.3.1 General Objective

To gain practical skills in penetration testing by identifying and exploiting vulnerabilities in the Mutillidae application.

4.2.2.3.1 Specific Objective

- Identify and analyze common web vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) within the Mutillidae application.
- Test access control mechanisms to determine if unauthorized access to restricted areas or data is possible.
- Assess the application's response to various attack vectors, simulating potential real-world hacking scenarios.
- Develop a comprehensive understanding of how vulnerabilities impact an application's security and outline strategies to mitigate such risks.

4.2.2.5 Scope Of The Project

Identify and document vulnerabilities within Mutillidae, including SQL injection, XSS, CSRF, and broken access controls.

4.2.2.6 Result

Our testing on the Mutillidae application yielded notable results. Despite the application's intentional vulnerabilities, we successfully accessed various parts of the site that should have been restricted. These findings emphasize the risks associated with insecure web applications and underscore the importance of implementing strong access controls, validating inputs, and mitigating common vulnerabilities like SQL injection and XSS. Our results demonstrate how unprotected applications can expose sensitive information, highlighting the need for stringent security measures to prevent unauthorized access.

4.2.2.7 Conclusion

Testing the Mutillidae web application provided an invaluable learning experience in identifying, analyzing, and exploiting common web vulnerabilities. As a deliberately vulnerable web application, Mutillidae was an ideal environment to practice penetration testing techniques without the constraints or risks of testing live systems. Throughout this testing phase, we were able to explore and exploit vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and authentication flaws.

4.2.3 Local Hosted Web Server <http://172.21.35.221/EARS/> Security Audit Report

4.2.3.1 Introduction

This report details the testing of a web application, known as EARS, which was developed and submitted to INSA by the Ethiopian Federal Ethics and Anticorruption Commission. The primary purpose of this application is to register and manage the wealth and assets of high ranking government officials, ensuring transparency and accountability within the public sector.

Given the significance of this application in promoting ethical governance, INSA was tasked with conducting thorough testing to identify vulnerabilities and ensure the system's integrity and security. Our team was entrusted with this responsibility, and we approached the testing process with diligence and a commitment to uncovering any potential issues that could compromise the application's effectiveness.

This report outlines our methodology, findings, and risk calculation from the testing process, highlighting our efforts to enhance the security and reliability of the EARS application for its intended use.

4.2.3.2 Executive Summary

We have performed vulnerability assessment and penetration testing on the 172.21.35.221/EARS/ website. We have conducted the security assessment in a manner that simulated malicious actors engaged in an attack against of the 172.21.35.221/EARS/ website by using different security vulnerability technical tools and best practices and measured the overall security status of the 172.21.35.221/EARS/. This report contains the details of the vulnerability assessment and penetration testing result along with suggested remedial solutions. The result shows that the application has different vulnerabilities that can expose the 172.21.35.221/EARS/ website to different threats. These security vulnerabilities can be categorized as follows:

- Poor usage of security Policy,
- Poor security control,
- Poor usage of authentication setup.

Therefore, 172.21.35.221/EARS/ should give a serious attention and be committed to manage the security vulnerabilities listed here in the report. Otherwise, the organization may be exposed to different damages. Please note that the solutions recommended here can serve as a starting point to remediate the security weaknesses. Nevertheless, that does not replace researching further by the administrators to provide a better solution.

4.2.3.3 Summary Of Findings

Types of Vulnerabilities	Level of Risks			
	HIGH	MEDIUM	LOW	TOTAL
Session Cache	✓			
Broken Authentication		✓		
Clear text Login Credentials		✓		
TOTAL	1	2	0	3

Table 4.6 Summary of Finding

4.2.3.4 Objective

4.2.3.3.1 General Objective

To identify potential security vulnerabilities and provide technical, managerial, physical and human related recommendations to remediate them.

4.2.3.3.2 Specific Objective

- To identify and analyze potential security vulnerabilities in the EARS application
- To assess the application's performance and reliability under different conditions
- To enhance the application's overall security and compliance by testing for weaknesses that could be exploited
- To support the Ethiopian Federal Ethics and Anticorruption Commission's objectives

4.2.3.5 Scope Of The Project

The scope of this security audit is the portal of 172.21.35.221/EARS/.

4.2.3.6 Applied Methodology

To conduct the penetration testing, we used many methodologies. Some methodologies used to test the application are mentioned below:

- Following up Application security checklist
- Following up OWASP testing guide
- Application security testing tools

4.2.3.7 Detailed Security Audit Findings

The following tables show the details of the vulnerabilities identified during the security assessment process.

No	1
Vulnerability Name	Session Cache
Target	http://172.21.32.221/EARS
Vulnerability Description	When a user logs out of a website, but can still view the previous pages by using the browser's back button, potentially regaining access to sensitive data until the page is refreshed. This issue is related to how browsers cache pages and can be mitigated by properly configuring cache headers on sensitive pages.
Risk Level	Medium
Impact	Attackers could exploit this vulnerability if they gain physical access to a user's device and navigate to a sensitive page using the back button. Users who have logged out can still view previously accessed pages, potentially accessing sensitive information.
Countermeasure	Ensure that sessions expire after a short period of inactivity, and any interaction with the site after logging out should redirect the user to the login page.
Evidence:	

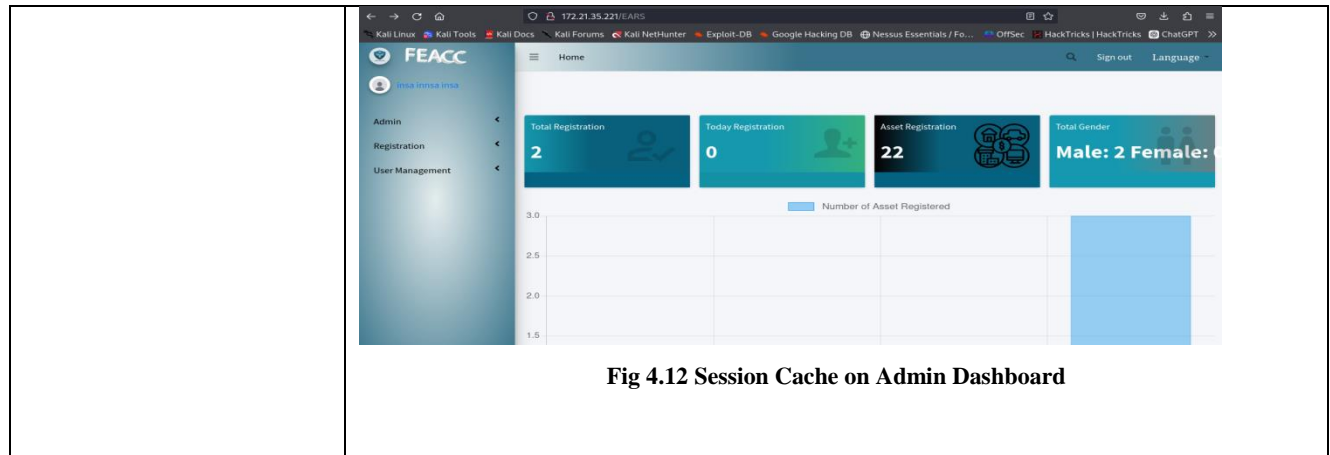


Fig 4.12 Session Cache on Admin Dashboard

Table 4.7 Session Cache Vulnerability Finding

No	2
Vulnerability Name	Broken Authentication
Target	http://172.21.35.221/EARS/organizations/create http://172.21.35.221/EARS/organizations/search http://172.21.35.221/EARS/offices/create http://172.21.35.221/EARS/roles
Vulnerability Description	Broken Authentication occurs when an application's authentication mechanisms fail to properly verify users' identities, leading to unauthorized access to sensitive functionalities or data.
Risk Level	High
Impact	An attacker can access certain sub directories or interact with forms without logging in, and can add any organization.
Countermeasure	Ensure that all directories and forms are protected by proper authentication and authorization checks. Implement RBAC to ensure that only authorized users can access and interact with sensitive resources. Log all access to sub directories and form submissions, and monitor for suspicious activity

Evidence:

The screenshot shows a web browser at the URL 172.21.35.221/EARS/organizations/create. The page has a sidebar with a 'Registration' link and a main content area with a form. The form contains the following fields:

- Category Type: A dropdown menu with 'Ministry' selected.
- Category ID: A dropdown menu with 'None' selected.
- Organization Code: A text input field.
- Organization Name: A text input field with a red asterisk indicating a required field.
- Category Description: A text input field.

At the bottom of the form, there are two buttons: 'Create' and 'Back to List'.

Fig 4.13 Broken Authentication on organizations/create page

The screenshot shows a web browser at the URL 172.21.35.221/EARS/organizations/search. The page has a sidebar with a 'Registration' link and a main content area with a search interface and a table of organizations.

Search Interface:

- Selection By: A dropdown menu with 'All' selected.
- Selection String: A text input field.
- Filter: A blue button.

Table of Organizations:

Category ID	Organization Code	Organization Name	Category Type	Category Description	
INSA	Auth01	INSA	Administration	etc	Edit
Org	Auth01	Org	Administration	etc	Edit
asdasdasdd	%3b%00 Nullbyte	asdasdasdd	Ministry	asdasdasdasd	Edit
gura	4331	gura	Ministry	affd	Edit

Fig 4.14 Broken Authentication on organizations/search page

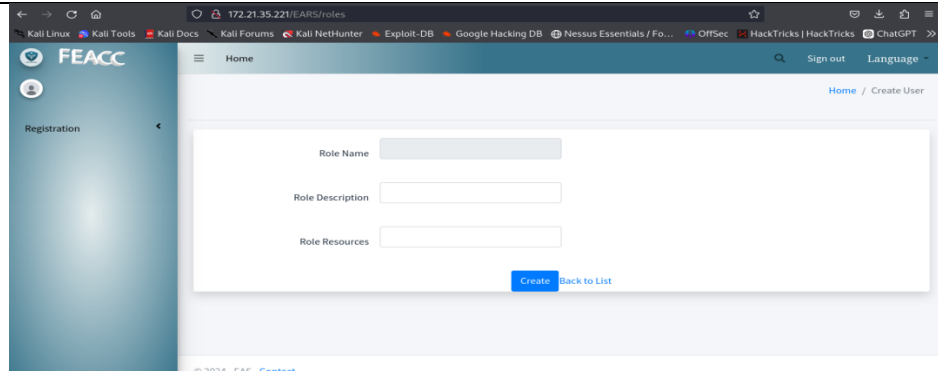


Fig 4.15 Broken Authentication on roles page

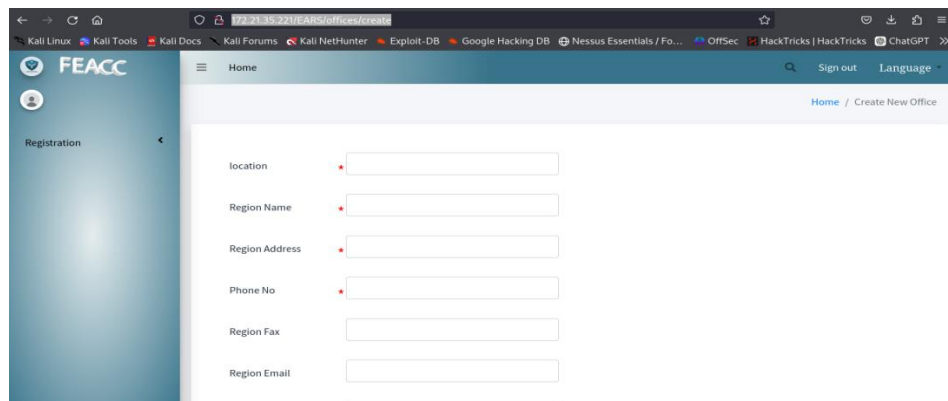


Fig 4.16 Broken Authentication on offices/create page

Table 4.8 Broken Authentication Vulnerability Finding

No	3
Vulnerability Name	Clear text Login Credentials
Target	http://172.21.35.221/EARS/Login/Login
Vulnerability Description	Username and passwords are transmitted over the network without proper encryption. If login credentials are intercepted by Burp Suite or similar tools, it typically means that the data is being sent in plaintext or using weak encryption protocols.
Risk Level	High
Impact	Attackers can intercept and manipulate the data being transmitted, potentially leading to further exploitation. Exposure of login credentials can lead to a broader data breach, affecting the confidentiality and integrity of the application.

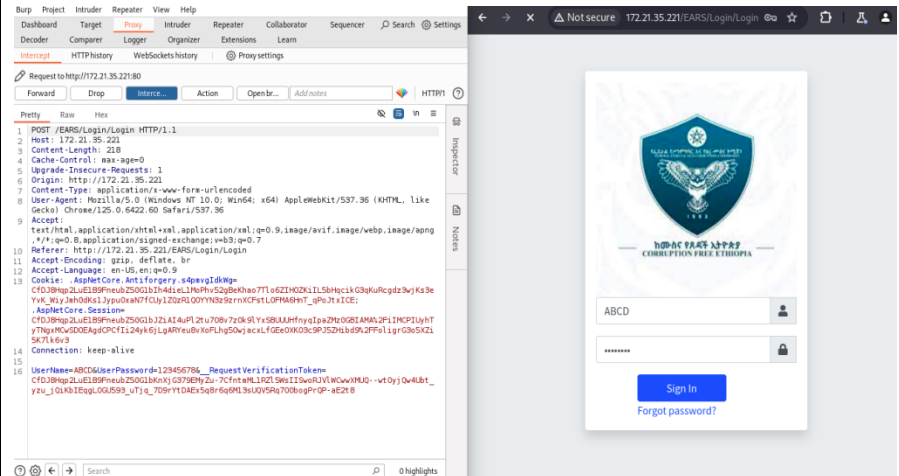
Countermeasure	Ensure that all data transmission occurs over HTTPS by configuring the server to redirect all HTTP traffic to HTTPS. Implement strong SSL/TLS protocols and avoid using deprecated protocols like SSLv2 or SSLv3. Regularly update SSL/TLS certificates.
Evidence:	 <p>The screenshot shows a web browser window with a login page. The page has a header with a logo and the text 'COMBATTION FREE ETHIOPIA'. Below the header, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'ABCD'. Below the input fields, there is a 'Sign In' button and a link that says 'Forgot password?'. In the background, the Burp Suite interface is visible, showing an intercepted HTTP POST request to the URL '/EARS/Login/Login'. The request body is displayed in the 'Raw' tab, showing the following data: 'Username=ABC&Password=123456789'. This indicates that the login credentials are being transmitted in clear text over the network.</p>

Fig 4.17 Clear text Login Credentials on Login Page

Table 4.9 Clear text Login Credentials Vulnerability Finding

4.2.3.8 Risk Calculation

Throughout the document, each risk calculated has been listed in a table 4.6 as a finding and categorized as a High-Risk, Medium-Risk, or Low-Risk. INSA used the following Risk calculation formula to calculate the risks.

$$\text{Risk} = \text{Likelihood} * \text{impact}$$

High risk: - these findings identify conditions that could directly result in the compromise of the web application. These include getting access to the website by resetting user accounts of different user levels i.e. normal user up to administrator user level. This will allow an attacker to perform tasks on administrator user level.

Medium risk: - these findings identify conditions that do not immediately or directly result in the compromise but do provide a capability to gain control on the web application. These includes the session cookie does not expire after the users click on log out. These will allow attackers to login and perform tasks using the cookie once they steal it from legitimate user.

Low risk: - these findings identify conditions that provide information that could be used in combination with other information to gain insight into how to compromise the web application. These include vulnerabilities like information disclosure and displaying server banners.

4.2.3.9 Conclusion

We conclude that the overall security of the 172.21.35.221/EARS needs improvement. We hope that the issues mentioned in this report will be addressed quickly as soon as possible by the responsible body. Experience has shown that a focused effort to address the problems outlined in this report can result in dramatic security improvements. For systems to remain secure, however, security posture must be evaluated and improved continuously, Assigning the responsible person or establishing the organizational structure that will support these ongoing improvements is essential in order to maintain control of information systems.

CHAPTER FIVE

5. Conclusion and Recommendation

5.1 Conclusion

Our internship at the Information Network Security Administration (INSA) has been a great experience; supply us with a wealth of practical skills, theoretical knowledge, and professional insights that will serve as a strong foundation for our future careers. INSA provided us with a dynamic environment where we could engage in hands-on learning, particularly in cybersecurity and development, while working on meaningful projects like the Laravel based task management system. Through this experience, we gained essential skills in programming, critical thinking, teamwork, and communication.

Working alongside seasoned professionals, we developed a deeper understanding of cybersecurity's role in safeguarding Ethiopia's digital infrastructure and the rigorous standards necessary for success in the field. We also strengthened our technical competencies, such as learning to use various tools, and built strong relationships with mentors and colleagues who supported us along the way.

In summary, our time at INSA has been invaluable, allowing us to apply our academic knowledge in a real-world context, refine our skills, and grow personally and professionally. This experience has deepened our commitment to the field of cybersecurity, and we look forward to building on the skills and knowledge gained at INSA as we advance in our careers.

5.2 Recommendation

5.2.1 Recommendation For The Company

INSA is a remarkable organization that plays a critical role in securing Ethiopia's digital infrastructure, handling numerous tasks each day with dedication and precision. We recommend that INSA continue its strong commitment to cybersecurity while also focusing on advancing its technological capabilities to keep pace with the rapidly evolving field. As the primary institution responsible for cybersecurity, INSA would benefit from expanding its reach across the country, ensuring that its presence and impact are felt in all regions.

Furthermore, we suggest implementing the task management system we developed during our internship. This platform could greatly enhance workflow efficiency by streamlining task assignments, tracking, and completion, helping teams to collaborate more effectively.

5.2.2 Recommendation For The Faculty

As faculty of electrical and computer engineering communications between faculty and company is low. Due to this reason many students have no idea which company best for their field of study and capable for best internship work place. So we would like to recommend that the university must work on communication between company and faculty in order to facilitate the internship program. In addition to this the school must give much information before the coming of internship program. We know that school give some information but we don't think it is sufficient.

5.2.3 Recommendation For Industrial Linkage

The Industrial Linkage department plays an essential role in connecting students with industry opportunities, yet there is significant room for enhancement to better serve students seeking internships. Currently, many students face challenges in identifying and securing suitable hosting companies for their internship period, often due to limited options and a lack of structured guidance on the process.

To address these challenges, we recommend that the Industrial Linkage department expands its network of partner companies, providing students with a wider variety of hosting options across different fields and industries. By building stronger partnerships with a range of companies, Industrial Linkage could offer students diverse choices that better align with their academic backgrounds and career aspirations, reducing the time and effort needed to secure an appropriate placement.

References:

Books

- 1) NEBIYOU EALIA, *INTRODUCTION TO LINUX*, 1st ed. ,Ethiopia
- 2) NEBIYOU EALIA, *FootPrinting & Reconnaissance*, 1st ed. ,Ethiopia
- 3) Bill, Naghmeh, Richard, *Lab 5: Web Attacks using Burp Suite*
- 4) Dr. Natarajan Meghanathan, *Secure Software Development Lifecycle*, Associate Professor of Computer Science Jackson State University
- 5) Robert W. Beggs, *Mastering Kali Linux for Advanced Penetration Testing*
- 6) Ministry of Communications and Multimedia Malaysia, *Guidelines for Secure Software Development Life Cycle (SSDLC)*
- 7) NEBIYOU EALIA, *Penetration Testing Process*, 1st ed. Ethiopia
- 8) Flavio Copes, *The React Beginner's Handbook*
- 9) Ash Allen, *The Clean Coder's Guide to Laravel*, United Kingdom

Websites

- INSA. (n.d.) Information Network Security Agency. Available at: <https://www.insa.gov.et/> (Accessed: 2 November 2024).
- Bahir Dar University. (n.d.) Home. Available at: <https://www.bdu.edu.et/> (Accessed: 2 November 2024).
- OWASP Foundation. (n.d.) Open Web Application Security Project. Available at: <https://owasp.org/> (Accessed: 2 November 2024).
- Offensive Security. (n.d.) Kali Linux. Available at: <https://www.kali.org/> (Accessed: 2 November 2024).
- Laravel. (n.d.) The PHP Framework for Web Artisans. Available at: <https://laravel.com/> (Accessed: 2 November 2024).
- Meta Platforms, Inc. (n.d.) React. Available at: <https://react.dev/> (Accessed: 2 November 2024).