# SECURITY AUDITING: ASSESSING VULNERABILITIES AND RISKS

*Thesis / Report by*

ALI HASIL A

In Partial Fulfillment of the Requirements

for the Degree Of

**MSc Computer Science with specialization in Cybersecurity**

Supervisors:

David Mathews, Design Engineer,

Kerala University of Digital Sciences, Innovation and Technology

A Pramoth,ASI,

Operations Officer, Kerala Police Cyberdome

**School of Computer Science and Engineering**

KERALA UNIVERSITY OF DIGITAL SCIENCES, INNOVATION AND TECHNOLOGY

04-09-2023

# Abstract

Vulnerability assessment, malware analysis, passive website security auditing, and network infrastructure security auditing are critical components of modern cybersecurity. Together, these practices form the cornerstone of a comprehensive cybersecurity strategy, safeguarding against ever-evolving cyber threats. This abstract provides an overview of the internship offered by the Kerala Police Cyberdome. It encompasses a comprehensive curriculum covering network configuration basics using Cisco Packet Tracer, static and dynamic malware analysis, ISO standards compliance, and vulnerability analysis. This internship involved a real-world security audit at a government organization, explicitly focusing on network and website security auditing. This abstract provides a glimpse into the program's significance and the practical experiences gained. Vulnerability assessment is a critical process in cybersecurity that involves systematically identifying and evaluating weaknesses within systems, networks, and applications. It plays a pivotal role in risk management by utilizing various tools and techniques to uncover potential security risks and prioritize remediation efforts. The internship provided me with practical experience in vulnerability analysis, equipping me to contribute to more robust cybersecurity defenses. Malware analysis is another vital aspect of cybersecurity, thoroughly examining malicious software. This analysis encompasses the dissection of code and behavior to understand the intent and impact of malware, facilitating the development of countermeasures and detection strategies. This helped to gain expertise in static and dynamic malware analysis, enhancing the ability to combat cyber threats effectively. Passive website security auditing relies on non-intrusive monitoring and analysis of web applications and sites to detect vulnerabilities and potential dangers. This approach safeguards sensitive data and user interactions, ensuring a secure online presence. The internship included practical passive website security auditing training that empowered to identify and address web-based vulnerabilities. Network infrastructure security auditing involves monitoring and analyzing network traffic, configurations, and logs to detect anomalies and potential threats proactively. This proactive approach enhances security by identifying and addressing vulnerabilities before they can be exploited. The hands-on training in network infrastructure security auditing enables us to secure network environments effectively. The curriculum also emphasized adherence to ISO standards, highlighting their importance in maintaining robust cybersecurity practices. This internship provided a holistic understanding of security auditing and equipped me with practical skills to enhance cybersecurity and protect against evolving threats.

# Acknowledgement

I am expressing my sincere gratitude and appreciation to everyone who contributed to the successful completion of my internship at the Kerala Police Cyberdome. This internship has been a valuable learning experience, and I am deeply thankful for the support and guidance I received throughout my time with the organization.

First and foremost, I would like to extend heartfelt thanks to my external guide, A Pramoth ASI, For Operations Officer, whose expertise and guidance from Kerala Police Cyberdome were instrumental in providing me with real-world perspectives and helping me apply my theoretical knowledge in a practical setting.

I would like to thank Digital University Kerala for enabling this internship opportunity. In particular, we are grateful to Vice Chancellor Dr. Saji Gopinath, Dr. Alex James, Dean of Academics, and Dr. Tony Thomas, Chair of Computer Science, for their support.

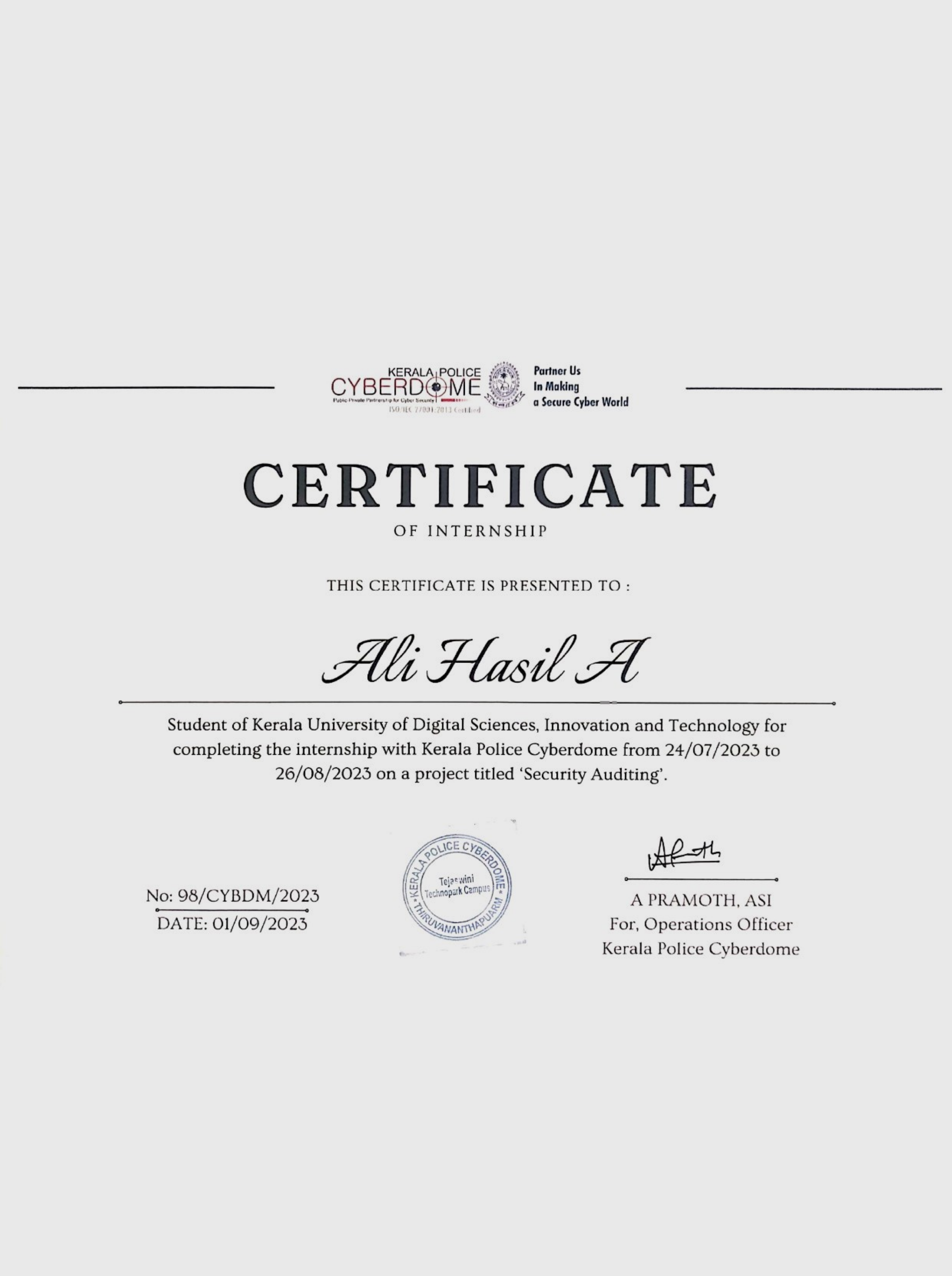
I am also grateful to David Mathews, my internal guide from the Digital University Kerala, for their unwavering support, mentorship, and valuable insights throughout this internship. Their guidance and expertise played a pivotal role in shaping my understanding of the field and helping me navigate the complexities of my tasks.

I would also like to acknowledge the exceptional training sessions conducted by Krishna Prasad, Pramod, and Jisha, cybersecurity professionals. These sessions provided me with practical knowledge and real-world insights that significantly contributed to my professional development.

I am incredibly thankful to the government organization that allowed me to conduct a security audit during my internship. The experience was invaluable and would not have been possible without their cooperation and openness.

Last but not least, I extend my gratitude to all the faculties and staff members of Digital University Kerala for their support and encouragement throughout my internship. Their willingness to share their knowledge and expertise enriched my learning experience.

# Organisation Certificate



KERALA POLICE CYBERDOME

Public-Private Partnership for Cyber Security

ISO/IEC 27001:2013 Certified

Partner Us
In Making
a Secure Cyber World

## CERTIFICATE

OF INTERNSHIP

THIS CERTIFICATE IS PRESENTED TO :

*Ali Hasil A*

Student of Kerala University of Digital Sciences, Innovation and Technology for completing the internship with Kerala Police Cyberdome from 24/07/2023 to 26/08/2023 on a project titled 'Security Auditing'.

No: 98/CYBDM/2023
DATE: 01/09/2023

KERALA POLICE CYBERDOME
Tejaswini
Technopark Campus
THIRUVANANTHAPURAM

A PRAMOTH, ASI
For, Operations Officer
Kerala Police Cyberdome

# Certificate

This is to certify that the thesis /report **SECURITY AUDITING: ASSESSING VULNERABILITIES AND RISKS** submitted by **Ali Hasil A (Reg. No: 221011)** in partial fulfillment of the requirements for the award of **MSc Computer Science with specialization in Cybersecurity** is a bonafide record of the work carried out at **Kerala University of Digital Sciences, Innovation and Technology** under my supervision.

Supervisor

David Mathews
Design Engineer
Kerala University of Digital Sciences, Innovation and Technology

# Contributions

1. (2010). AUDIT OF NARA'S NETWORK INFRASTRUCTURE.

   We referred this audit report to generate the security audit report of the organization visit.

2. Humphreys, E. (2016). Implementing the ISO/IEC 27001 ISMS Standard. Norwood: Library of Congress Cataloging-in-Publication Data.

   This book helped us understand how to implement ISO 27001 standards while conducting a security audit in an organization.

3. Clickjacking: Attacks and defenses - Microsoft Research. Microsoft Research.

   This paper has given an idea about clickjacking attacks

4. ZAP – Cross Site Scripting (DOM based). (n.d.). https://www.zaproxy.org/docs/alerts/40026/

   This official website of OWASP ZAP helped us to understand vulnerabilities such as cross-site scripting, SQL Injection, etc.

5. jquery 1.12.4 vulnerabilities — Snyk. (n.d.). Find Detailed Information and Remediation Guidance for Vulnerabilities.

   This website helped to identify the vulnerabilities in jQuery versions.

6. CVE - CVE. (n.d.). https://cve.mitre.org/

   Referred to this website to identify CVEs for vulnerabilities.

# Contents

# List of Figures

# Chapter 1

# Introduction

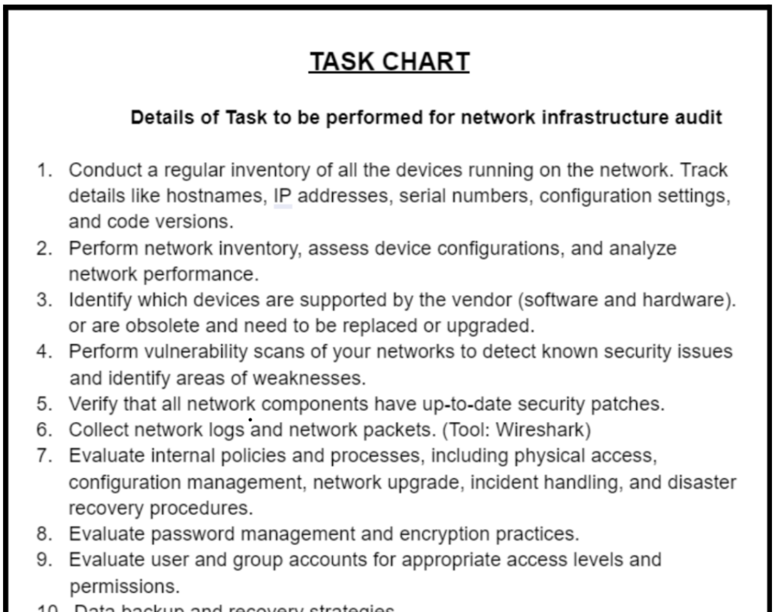
## 1.1 Introduction

The internship program serves as a light of preparation in the face of pressing cybersecurity difficulties in our modern world, where the significance of cybersecurity and network defense knowledge has reached unparalleled relevance. It emphasizes the crucial role of industry standards and guidelines in a landscape defined by strict data protection regulations and ever-evolving cyber threats. It has a meticulously crafted curriculum covering essential topics like security hierarchies, varied monitoring methodologies, specialized technologies, malware analysis, and unwavering adherence to ISO standards and cutting-edge information security principles. To meet the demands of a digital age marked by constant change, the program explores the complexities of web application security, OSI model levels, and the delicate elements of network architecture.

## 1.2 Security Auditing: Assessing Vulnerabilities and Risks

Security Auditing focuses on assessing vulnerabilities and risks within a government organization. This consisted of conducting two key audits: a Network Infrastructure Security Audit and a Website Security Audit. The network infrastructure security audit aimed to find vulnerabilities, misconfigurations, and potential entry points for cyber attacks by thoroughly examining the organization's network components, including routers, switches, firewalls, and servers. On the other hand, the Website Security Audit aimed to assess the security of the company's online presence, including its websites and web applications, by looking for vulnerabilities like cross-site scripting (XSS), SQL injection, and unauthorized access points. Keeping with the organization's commitment to upholding data integrity, confidentiality, and the general security of its digital assets, these audits ensured that the data and systems remained protected from cyber-attacks and illegal access.

The organization's security posture was evaluated methodically during the network infrastructure security audit. A checklist, task chart, and asset inventory were created to guarantee a thorough assessment. The Bandwidth Place web tool was used to assess bandwidth to evaluate network performance. Other settings and security standards were considered using tools like the advanced IP scanner, Nmap, and Wireshark. These technologies made it possible to examine network setups and find potential security holes thoroughly. An accomplished strategy was used for the website security assessment to detect and reduce hazards related to the organization's online presence. A whois lookup and Dmitry tools were used to learn more about the domain and hosting of the website as the first step in the information-gathering process.The website was then checked using VirusTotal to see whether any dangerous threats were there, assisting in maintaining a secure online environment.Both audits have a crucial place for vulnerability assessments. To find potential vulnerabilities in web applications and server configurations, a collection of specialist tools, including OWASP ZAP, Nessus, joomscan, and nikto, was used. These technologies helped in the creation of repair plans by providing a thorough examination of security flaws. Additionally, testing and analysis of the clickjacking vulnerability, a potential risk that could compromise user interactions on the website, were given special attention. The vulnerability was tested and evaluated using HTML and Python programs as part of this examination to make sure it was fully understood and that it could be effectively addressed.

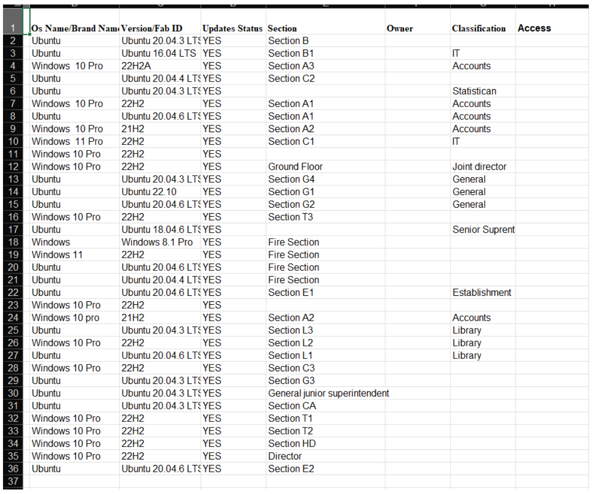


**TASK CHART**

**Details of Task to be performed for network infrastructure audit**

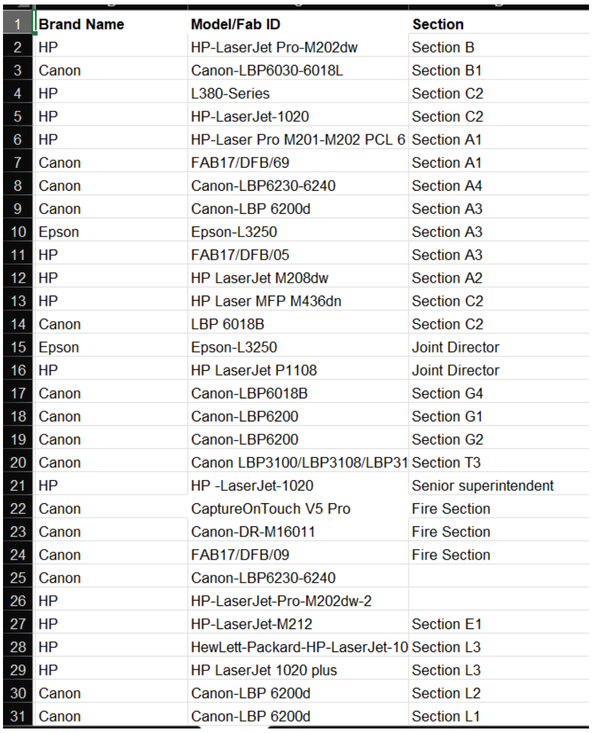
1. Conduct a regular inventory of all the devices running on the network. Track details like hostnames, IP addresses, serial numbers, configuration settings, and code versions.
2. Perform network inventory, assess device configurations, and analyze network performance.
3. Identify which devices are supported by the vendor (software and hardware). or are obsolete and need to be replaced or upgraded.
4. Perform vulnerability scans of your networks to detect known security issues and identify areas of weaknesses.
5. Verify that all network components have up-to-date security patches.
6. Collect network logs and network packets. (Tool: Wireshark)
7. Evaluate internal policies and processes, including physical access, configuration management, network upgrade, incident handling, and disaster recovery procedures.
8. Evaluate password management and encryption practices.
9. Evaluate user and group accounts for appropriate access levels and permissions.
10. Data backup and recovery strategies.
11. Ensure that personal devices do not expose the network.
12. Network bandwidth consumption.

Figure 1.1: Task Chart



| | Os Name/Brand Name | Version/Fab ID | Updates Status | Section | Owner | Classification | Access |
|---|---|---|---|---|---|---|---|
| 2 | Ubuntu | Ubuntu 20.04.3 LTS | YES | Section B | | | |
| 3 | Ubuntu | Ubuntu 16.04 LTS | YES | Section B1 | | IT | |
| 4 | Windows 10 Pro | 22H2A | YES | Section A3 | | Accounts | |
| 5 | Ubuntu | Ubuntu 20.04.4 LTS | YES | Section C2 | | | |
| 6 | Ubuntu | Ubuntu 20.04.3 LTS | YES | | | Statistican | |
| 7 | Windows 10 Pro | 22H2 | YES | Section A1 | | Accounts | |
| 8 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Section A1 | | Accounts | |
| 9 | Windows 10 Pro | 21H2 | YES | Section A2 | | Accounts | |
| 10 | Windows 11 Pro | 22H2 | YES | Section C1 | | IT | |
| 11 | Windows 10 Pro | 22H2 | YES | | | | |
| 12 | Windows 10 Pro | 22H2 | YES | Ground Floor | | Joint director | |
| 13 | Ubuntu | Ubuntu 20.04.3 LTS | YES | Section G4 | | General | |
| 14 | Ubuntu | Ubuntu 22.10 | YES | Section G1 | | General | |
| 15 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Section G2 | | General | |
| 16 | Windows 10 Pro | 22H2 | YES | Section T3 | | | |
| 17 | Ubuntu | Ubuntu 18.04.6 LTS | YES | | | Senior Suprent | |
| 18 | Windows | Windows 8.1 Pro | YES | Fire Section | | | |
| 19 | Windows 11 | 22H2 | YES | Fire Section | | | |
| 20 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Fire Section | | | |
| 21 | Ubuntu | Ubuntu 20.04.4 LTS | YES | Fire Section | | | |
| 22 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Section E1 | | Establishment | |
| 23 | Windows 10 Pro | 22H2 | YES | | | | |
| 24 | Windows 10 pro | 21H2 | YES | Section A2 | | Accounts | |
| 25 | Ubuntu | Ubuntu 20.04.3 LTS | YES | Section L3 | | Library | |
| 26 | Windows 10 Pro | 22H2 | YES | Section L2 | | Library | |
| 27 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Section L1 | | Library | |
| 28 | Windows 10 Pro | 22H2 | YES | Section C3 | | | |
| 29 | Ubuntu | Ubuntu 20.04.3 LTS | YES | Section G3 | | | |
| 30 | Ubuntu | Ubuntu 20.04.3 LTS | YES | General junior superintendent | | | |
| 31 | Ubuntu | Ubuntu 20.04.3 LTS | YES | Section CA | | | |
| 32 | Windows 10 Pro | 22H2 | YES | Section T1 | | | |
| 33 | Windows 10 Pro | 22H2 | YES | Section T2 | | | |
| 34 | Windows 10 Pro | 22H2 | YES | Section HD | | | |
| 35 | Windows 10 Pro | 22H2 | YES | Director | | | |
| 36 | Ubuntu | Ubuntu 20.04.6 LTS | YES | Section E2 | | | |
| 37 | | | | | | | |

Figure 1.2: Asset inventory (Desktops and Laptops)



| | Brand Name | Model/Fab ID | Section |
|---|---|---|---|
| 2 | HP | HP-LaserJet Pro-M202dw | Section B |
| 3 | Canon | Canon-LBP6030-6018L | Section B1 |
| 4 | HP | L380-Series | Section C2 |
| 5 | HP | HP-LaserJet-1020 | Section C2 |
| 6 | HP | HP-Laser Pro M201-M202 PCL 6 | Section A1 |
| 7 | Canon | FAB17/DFB/69 | Section A1 |
| 8 | Canon | Canon-LBP6230-6240 | Section A4 |
| 9 | Canon | Canon-LBP 6200d | Section A3 |
| 10 | Epson | Epson-L3250 | Section A3 |
| 11 | HP | FAB17/DFB/05 | Section A3 |
| 12 | HP | HP LaserJet M208dw | Section A2 |
| 13 | HP | HP Laser MFP M436dn | Section C2 |
| 14 | Canon | LBP 6018B | Section C2 |
| 15 | Epson | Epson-L3250 | Joint Director |
| 16 | HP | HP LaserJet P1108 | Joint Director |
| 17 | Canon | Canon-LBP6018B | Section G4 |
| 18 | Canon | Canon-LBP6200 | Section G1 |
| 19 | Canon | Canon-LBP6200 | Section G2 |
| 20 | Canon | Canon LBP3100/LBP3108/LBP31 | Section T3 |
| 21 | HP | HP -LaserJet-1020 | Senior superintendent |
| 22 | Canon | CaptureOnTouch V5 Pro | Fire Section |
| 23 | Canon | Canon-DR-M16011 | Fire Section |
| 24 | Canon | FAB17/DFB/09 | Fire Section |
| 25 | Canon | Canon-LBP6230-6240 | |
| 26 | HP | HP-LaserJet-Pro-M202dw-2 | |
| 27 | HP | HP-LaserJet-M212 | Section E1 |
| 28 | HP | HewLett-Packard-HP-LaserJet-10 | Section L3 |
| 29 | HP | HP LaserJet 1020 plus | Section L3 |
| 30 | Canon | Canon-LBP 6200d | Section L2 |
| 31 | Canon | Canon-LBP 6200d | Section L1 |

Figure 1.3: Asset Inventory (Printers)

### 1.2.1 Malware Analysis

Malware analysis is a systematic and structured process for examining malicious files. To maintain the integrity of the original file, a copy is first made. A distinct hash value is then calculated for identification. To find out if the file is classified as malware, this hash is then compared to VirusTotal. The next step in the research entails looking up further information online and using the ' strings' tool to extract legible text from the file to expose crucial information such as domain names or file names. The choice of specialist analysis tools, such as ”olevba” for Office files, is guided by the file type. Malicious actions can be found via dynamic analysis in a controlled environment using tools like Procmon. To accurately classify threats and handle incidents, the gathered data is carefully examined to find signs of compromise. Collective defense against malware threats is strengthened by disseminating results to the larger security community.

### 1.2.2 ISO Standard 27001

A reliable Information Security Management System (ISMS) needs to be established within enterprises, and ISO 27001 is a widely accepted standard that is essential for this. Its main objective is the methodical protection of information assets, assuring their availability, confidentiality, and integrity. A structured framework is provided by ISO 27001 for developing security policies, identifying risks, and taking preventative measures to ensure information security. Certification fosters stakeholder trust and increases cybersecurity resilience by demonstrating a firm commitment to information security best practices. The ISO 27001 Control Checklist, which consists of 114 controls divided into 14 categories, is crucial to achieving ISO 27001 compliance because it offers an organized approach for implementing and maintaining information security while successfully protecting sensitive data.

## 1.3 Network Security

A key component of contemporary cybersecurity is network security, which uses various tools and procedures to guard against unauthorized access and online dangers. Using tools like firewalls, encryption, and stringent access restrictions guarantees data confidentiality, integrity, and availability. The knowledge necessary to manage, troubleshoot, and secure networks in both professional and private contexts by understanding IP and MAC addresses, the significance of port numbers, LAN configurations, and real-world networking scenarios. Hands-on experiences with tools like Cisco Packet Tracer reinforce this knowledge.

## 1.4 Motivation

The primary motivation behind my participation in the internship program was to acquire a profound understanding of the critical components of modern cybersecurity. Understanding the complexities of vulnerability assessment, malware analysis, passive website security auditing, and network infrastructure security auditing is essential in building a robust cybersecurity strategy. In a digital landscape where threats constantly evolve and become more sophisticated, I was driven to gain the expertise needed to assist organizations in identifying and mitigating risks, developing effective countermeasures against malware, ensuring online interactions' security, and proactively detecting anomalies in network infrastructure. This internship offered the invaluable opportunity to bridge theory and practice, providing hands-on experience securing critical systems and upholding industry-standard cybersecurity practices.

# Chapter 2

# Literature Review

## 2.1 Introduction

In today's digital landscape, cybersecurity is of paramount importance as organizations face ever-evolving cyber threats. One such threat is clickjacking, a deceptive technique that manipulates user clicks to perform malicious actions without their knowledge. Despite efforts to defend against it, clickjacking remains a serious concern. On a separate front, information security management is a crucial aspect of organizational security, and standards like ISO 27001 have emerged to guide organizations in this endeavor. The following combined literature review explores these two critical areas.

## 2.2 State-of-the-art approaches

Clickjacking

- Framebusting: An early approach to thwart clickjacking attempts involved preventing a website from being framed, thereby blocking UI redressing attacks.
- Randomizing UI Layout: By making the position of UI elements unpredictable, this approach seeks to prevent attackers from precisely overlaying deceptive elements.
- Confirmation Prompts: Users are prompted to confirm sensitive actions, adding an extra layer of protection against unintended clicks.
- Visibility Detection: Clicks are blocked if the UI element is not visible on the screen, aiming to counteract clickjacking attacks that involve hidden elements.

- Temporal Delays: Introducing action delays can thwart timing attacks, making it more challenging for attackers to achieve their goals.
- Pixel-based Filtering: This approach compares the rendering of clicked pixels across contexts, aiding in detecting UI redressing attempts.
- Cursor Customization Restrictions: Limiting the ability to spoof the mouse pointer helps prevent cursor-based clickjacking.
- Application Isolation: Treating UI security as an isolation problem by isolating UI elements to ensure their integrity.

  ISO 27001:

- Risk Assessments: Organizations employ methods like FAIR to quantify information security risks, guiding the selection of controls.
- Automated Compliance Scanners: Tools are used to assess the technical implementation of controls, ensuring they meet ISO 27001 requirements.
- Data Analytics: Security events and metrics are analyzed to gain insight into the effectiveness of controls, facilitating informed decision-making.
- Integration with COBIT: Organizations integrate ISO 27001 with frameworks like COBIT to bridge information security with overall enterprise governance.
- CMMI Models: Leveraging CMMI models helps mature the Information Security Management System (ISMS) across capability and process areas.
- Mapping to Threat Intelligence: Controls are mapped to cyberthreat intelligence to ensure emerging threats are addressed effectively.

## 2.3 Summary

Clickjacking:

Clickjacking attacks persist as a significant threat to online security. Despite the existence of defensive measures like framebusting and UI randomization, the paper ”Clickjacking: Attacks and Defenses” sheds light on the shortcomings of current mitigation strategies. It introduces innovative clickjacking attack variants that bypass existing defenses, with success rates ranging from 43

ISO 27001:

In the realm of information security management, ISO 27001 stands as a state-of-the-art framework. It provides a comprehensive approach to managing information security risks through 114 controls across 14 domains. The ISO 27001 Overview Poster offers a concise summary of the standard's purpose and structure, making it an invaluable resource for introducing ISO 27001 to stakeholders. On the other hand, the Internal Audit Checklist is a detailed tool for systematically assessing an organization's implementation of the standard. Covering leadership, planning, support, operations, performance evaluation, and continual improvement, it aids auditors and implementers in ensuring conformity across all 114 controls.

In conclusion, these two areas of research underscore the critical importance of cybersecurity and information security management in today's digital landscape. While clickjacking poses a deceptive threat demanding innovative defenses like InContext, ISO 27001 represents a robust framework for comprehensive information security management, aided by tools like the overview poster and audit checklist to facilitate adoption and conformity assessment.

# Chapter 3

# Methodology

## 3.1 Introduction

During the internship, a comprehensive strategy was implemented to enhance the organization's digital security. This involved conducting network structure security checkups and passive website security assessments within a government institution, leading to the creation of an audit checklist based on the training received.

The approach was grounded in ethical principles, prioritizing the protection of digital assets' privacy, availability, and integrity throughout the inspection process. The process began with a thorough information-gathering phase, which utilized a systematic checklist, task chart, asset inventory, interviews, and observations to ensure a structured examination of network structure security.

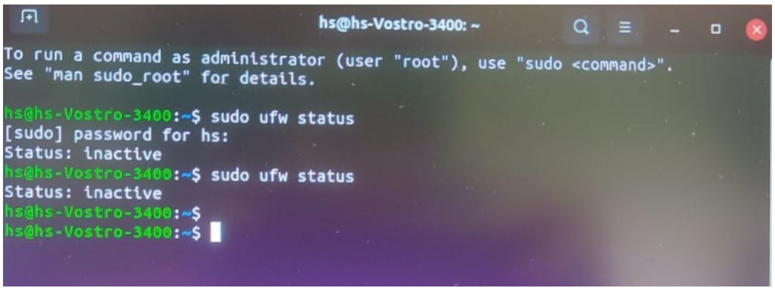
Ethical considerations remained paramount, guiding all actions within legal boundaries while respecting confidentiality and privacy. Technical tools such as Nmap, BandwidthPlace, Kaspersky password checker, Wireshark, VirusTotal, whois lookup, Dmitry, OWASP ZAP, Nessus, and Joomlascan were carefully selected to enable effective data collection and analysis. Throughout the inspection, a non-intrusive approach was maintained, focusing on minimizing disruption to the organization's regular operations while discreetly gathering essential information about network infrastructure, security vulnerabilities, and potential risks.

After thoroughly analyzing the collected data, problematic areas, potential weaknesses, and improvement recommendations were identified. This analytical phase formed the basis for an in-depth assessment, uncovering vulnerabilities and providing actionable solutions to enhance web operational security and overall organizational defenses.

## 3.2 Audit Methodology

### 3.2.1 Firewall Configuration Status

The command ’sudo ufw status’ was used to assess the firewall status of the Ubuntu system. This command allowed us to check the configuration and operational status of the Uncomplicated Firewall (UFW), a vital component for safeguarding the system against unauthorized access and network threats.

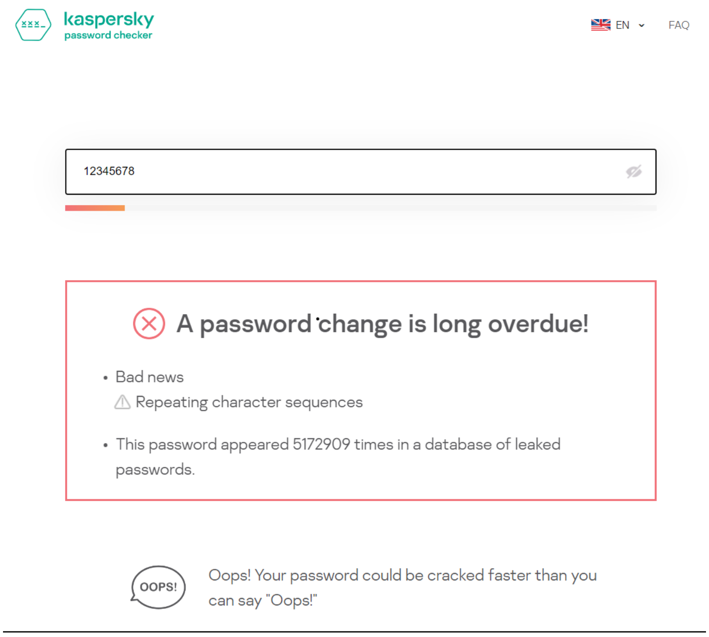


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hs@hs-Vostro-3400:~$ sudo ufw status
[sudo] password for hs:
Status: inactive
hs@hs-Vostro-3400:~$ sudo ufw status
Status: inactive
hs@hs-Vostro-3400:~$
hs@hs-Vostro-3400:~$ █
```

Figure 3.1: Firewall Configuration Status

### 3.2.2 Kaspersky Password Checker

The Kaspersky Password Checker was used to evaluate the strength of passwords in use by the organization.



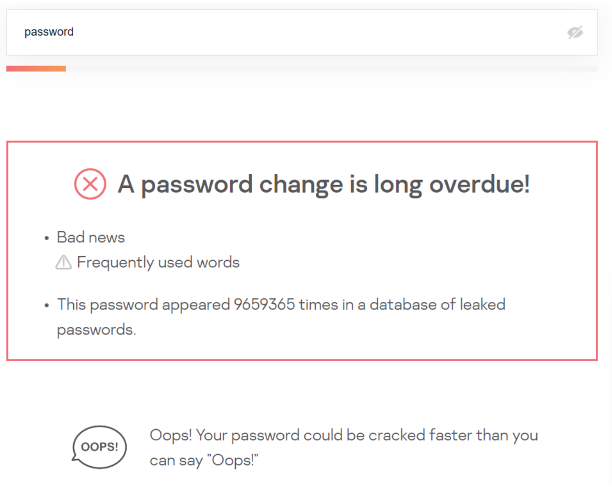
12345678

A password change is long overdue!

- Bad news
  ⚠ Repeating character sequences
- This password appeared 5172909 times in a database of leaked passwords.

Oops! Your password could be cracked faster than you can say "Oops!"

Figure 3.2: Password checker



password

A password change is long overdue!

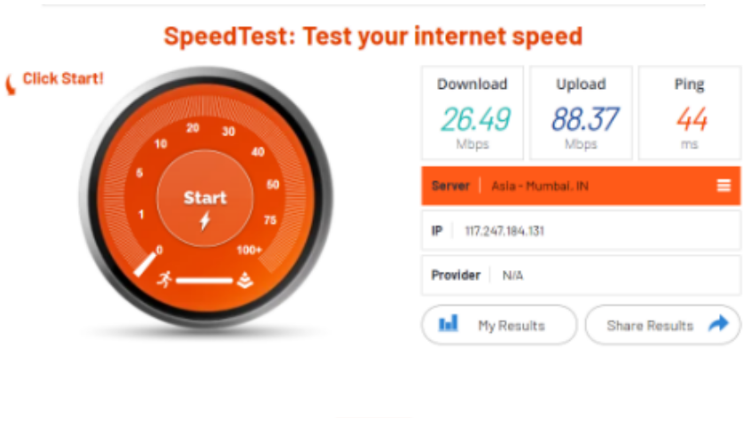
- Bad news
  ⚠ Frequently used words
- This password appeared 9659365 times in a database of leaked passwords.

Oops! Your password could be cracked faster than you can say "Oops!"

Figure 3.3: Password checker

### 3.2.3 Bandwidth Place

The ”bandwidth place” online tool was utilized to measure the network’s data transmission capacity, encompassing both download and upload speeds. This assessment was conducted to ensure that our organization’s network aligned with our specified internet speed requirements.



SpeedTest: Test your internet speed

| Download | Upload | Ping |
|---|---|---|
| 26.49 Mbps | 88.37 Mbps | 44 ms |

Server | Asia - Mumbai, IN

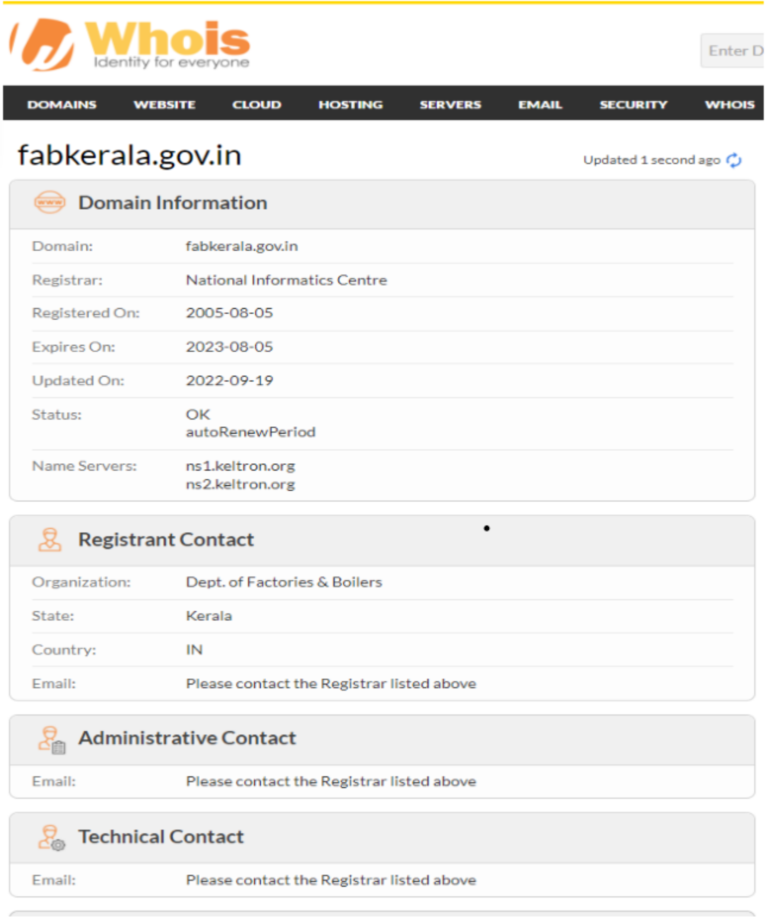
IP | 117.247.184.131

Provider | N/A

Figure 3.4: Bandwidth test

### 3.2.4 Whois lookup

WHOIS lookups were performed on the organization’s domains to acquire vital information like domain ownership, registration date, and contact details. These lookups serve multiple functions, including domain management, cybersecurity research, and confirming domain legitimacy.



fabkerala.gov.in

Updated 1 second ago

Domain Information

| | |
|---|---|
| Domain: | fabkerala.gov.in |
| Registrar: | National Informatics Centre |
| Registered On: | 2005-08-05 |
| Expires On: | 2023-08-05 |
| Updated On: | 2022-09-19 |
| Status: | OK<br>autoRenewPeriod |
| Name Servers: | ns1.keltron.org<br>ns2.keltron.org |

Registrant Contact

| | |
|---|---|
| Organization: | Dept. of Factories & Boilers |
| State: | Kerala |
| Country: | IN |
| Email: | Please contact the Registrar listed above |

Administrative Contact

| | |
|---|---|
| Email: | Please contact the Registrar listed above |

Technical Contact

| | |
|---|---|
| Email: | Please contact the Registrar listed above |

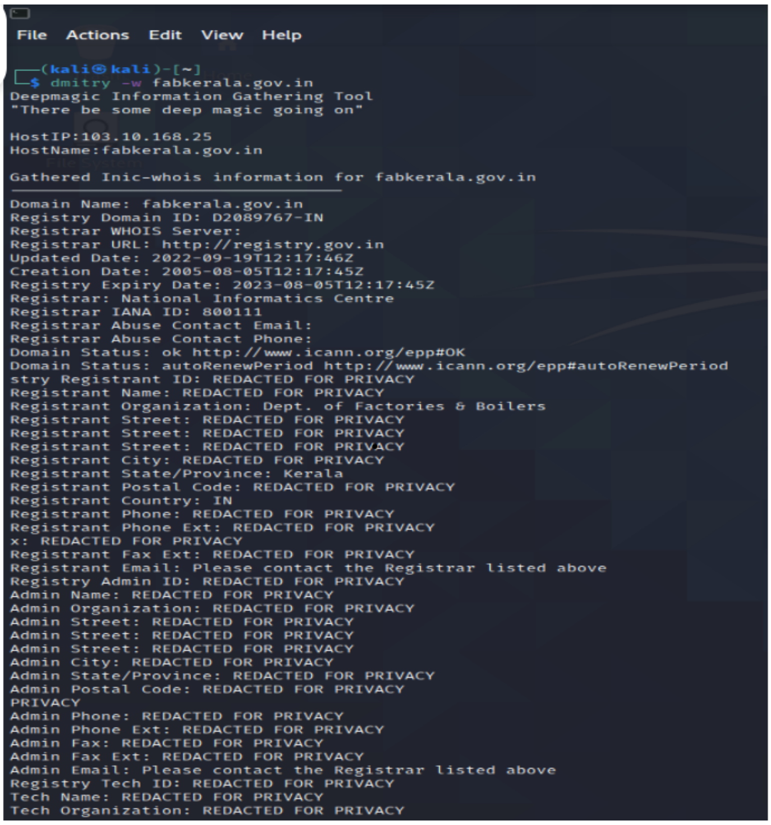
Figure 3.5: Whois lookup

### 3.2.5 Virus total

Using VirusTotal, a well-established online tool, comprehensive security audits were carried out on the organization's websites. This tool is purpose-built for assessing websites for potential security threats and vulnerabilities. The auditing process involves a thorough scan that utilizes multiple antivirus engines, web security scanners, and URL categorization databases.

### 3.2.6 Dmitry

The Dmitry tool was employed to gather data regarding the organization's digital assets, encompassing websites and email addresses. This process plays a crucial role in pinpointing potential vulnerabilities or security issues within their online infrastructure, facilitating the enhancement and fortification of their online security for increased safety.



```
┌──(kali㉿kali)-[~]
└─$ dmitry -w fabkerala.gov.in
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:103.10.168.25
HostName:fabkerala.gov.in

Gathered Inic-whois information for fabkerala.gov.in
---------------------------------
Domain Name: fabkerala.gov.in
Registry Domain ID: D2089767-IN
Registrar WHOIS Server:
Registrar URL: http://registry.gov.in
Updated Date: 2022-09-19T12:17:46Z
Creation Date: 2005-08-05T12:17:45Z
Registry Expiry Date: 2023-08-05T12:17:45Z
Registrar: National Informatics Centre
Registrar IANA ID: 800111
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok http://www.icann.org/epp#OK
Domain Status: autoRenewPeriod http://www.icann.org/epp#autoRenewPeriod
stry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Dept. of Factories & Boilers
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Kerala
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
x: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
```

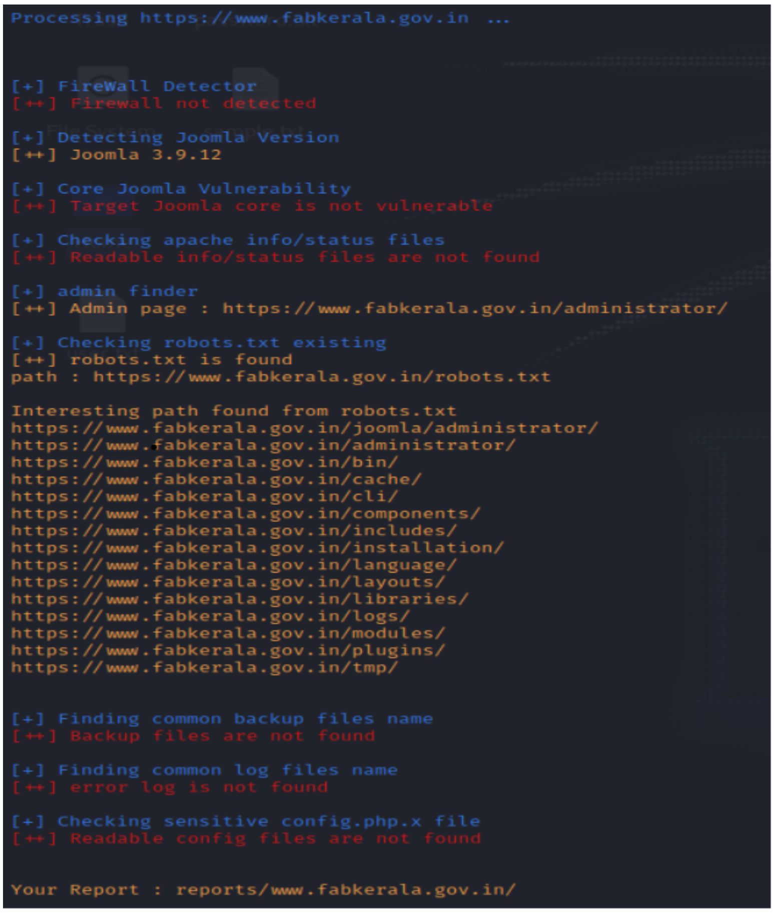
Figure 3.6: Whois lookup

### 3.2.7 OWASP ZAP

Website security audits were conducted using OWASP ZAP (Zed Attack Proxy). By spotting probable flaws and revealing information about potential attack vectors, this open-source security tool is specifically designed to find vulnerabilities in web applications. By doing so, it significantly improves the security of online applications. For establishing preventative security measures and boosting the general security of online applications, OWASP ZAP is a useful tool.

### 3.2.8 Joomscan

For assessing the security of the organization's Joomla-based websites, JoomScan, a specialized program designed to scan Joomla Content Management System (CMS) installations and identify potential vulnerabilities were employed. This tool plays a crucial role in ensuring the integrity and safety of Joomla-powered websites by proactively identifying and addressing security flaws.



```
Processing https://www.fabkerala.gov.in ...


[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 3.9.12

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page : https://www.fabkerala.gov.in/administrator/

[+] Checking robots.txt existing
[++] robots.txt is found
path : https://www.fabkerala.gov.in/robots.txt

Interesting path found from robots.txt
https://www.fabkerala.gov.in/joomla/administrator/
https://www.fabkerala.gov.in/administrator/
https://www.fabkerala.gov.in/bin/
https://www.fabkerala.gov.in/cache/
https://www.fabkerala.gov.in/cli/
https://www.fabkerala.gov.in/components/
https://www.fabkerala.gov.in/includes/
https://www.fabkerala.gov.in/installation/
https://www.fabkerala.gov.in/language/
https://www.fabkerala.gov.in/layouts/
https://www.fabkerala.gov.in/libraries/
https://www.fabkerala.gov.in/logs/
https://www.fabkerala.gov.in/modules/
https://www.fabkerala.gov.in/plugins/
https://www.fabkerala.gov.in/tmp/


[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found

Your Report : reports/www.fabkerala.gov.in/
```

Figure 3.7: Joomscan

### 3.2.9 Nessus

A reliable vulnerability scanner named Nessus was used for the web application test. This crucial tool thoroughly analyzed The organization's website, which uncovered security flaws, incorrect setups, and significant hazards. The website's security was improved, vital data was protected, and the integrity of the online presence was ensured thanks to Nessus' proactive approach to finding and fixing these vulnerabilities.

### 3.2.10 Nikto

The well-known open-source web server scanner Nikto was used to aid with the security evaluations. Nikto excels in locating possible weaknesses and security problems in web servers and apps. By efficiently identifying and mitigating possible vulnerabilities, its proactive scanning technique plays a crucial role in improving the overall security of web-based systems.

### 3.2.11 Advanced IP Scanner, Nmap, Wireshark

The security analyses used Advanced IP Scanner, Nmap, and Wireshark, each adding particular capabilities to our tests. While Advanced IP Scanner aided in network discovery and device identification, Nmap specialized in network mapping and vulnerability detection. For deep packet inspection and network traffic analysis, Wireshark was essential. This group effort helped to identify vulnerabilities, comprehensively assess the network architecture, and maintain a high degree of security.

## 3.3 Summary

The primary objective was to enhance the digital security of a government entity through a systematic and ethical approach. This involved conducting passive security checks on the website and performing network architecture audits supported by a comprehensive checklist and various technical tools. Ethical considerations were central, ensuring compliance with legal boundaries and respecting privacy during data gathering using task charts, checklists, interviews, and observations. The examination aimed to minimize disruption to the organization's operations while revealing critical information about network infrastructure and security weaknesses. The outcome involved identifying problem areas and vulnerabilities and offering practical recommendations for improvement, all contributing to enhancing web operational security and overall defense mechanisms for the organization.

# Chapter 4

# Results and Discussions

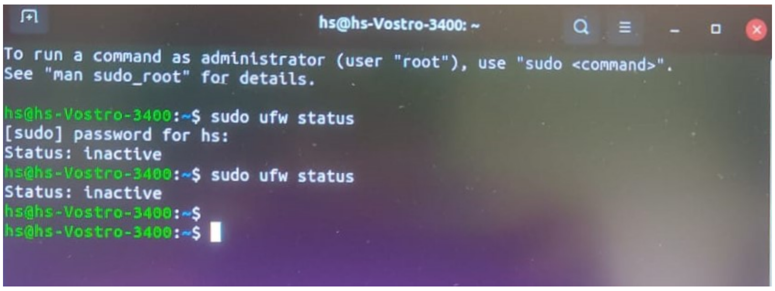
## 4.1 Introduction

A government institution's network architecture and website security were thoroughly audited, and the results provided important information about the organization's present state of digital security. This audit's primary objectives were to assess the organization's website, access controls, physical security measures, and network component security. For a non-intrusive website security assessment, passive security auditing techniques were used, evaluating publicly accessible data and configurations to spot potential vulnerabilities. The audit collected information and conducted thorough evaluations using various practical tools, including Nmap, advanced IP scanner, Wireshark, VirusTotal, whois lookup, Dmitry, OWASP ZAP, Nessus, and Joomscan. The findings have shown several serious problems that must be addressed immediately to improve the organization's overall digital security posture. Subsequent sections will provide detailed recommendations to enhance the management and technical controls over the network and website, addressing vulnerabilities, mitigating risks, and ensuring the practical safeguarding of the organization's digital assets.

## 4.2 Results

### 4.2.1 Firewall Status

Upon auditing the Ubuntu system, it was identified that the firewall was inactive. To rectify this security vulnerability, the firewall was activated using the command "sudo ufw enable." This proactive measure strengthens the system's security defenses by enabling the firewall, consequently enhancing protection against unauthorized access and potential security risks. Maintaining a robust firewall is imperative as a fundamental component of a holistic security strategy, ensuring the effective safeguarding of the system and its valuable resources.



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

hs@hs-Vostro-3400:~$ sudo ufw status
[sudo] password for hs:
Status: inactive
hs@hs-Vostro-3400:~$ sudo ufw status
Status: inactive
hs@hs-Vostro-3400:~$
hs@hs-Vostro-3400:~$
```

Figure 4.1: Firewall enabled

### 4.2.2 Network Segmentation

The organization's lack of network segmentation within its architecture raises significant concerns. Network segmentation is crucial to contemporary network design, providing security, performance, and manageability enhancements. Without proper segmentation, the network becomes susceptible to security breaches, unauthorized access, and the potential spread of issues throughout the entire infrastructure. This absence of segmentation exposes notable security risks that necessitate prompt and comprehensive mitigation to strengthen the organization's network security posture.

### 4.2.3 Logical Access Control

The assessment of logical access controls for network infrastructure devices and equipment revealed several vulnerabilities stemming from inadequate controls. In alignment with IT security guidelines, user identification using unique credentials is imperative to mitigate the risk of unauthorized access to network devices and servers. Notably, the absence of robust network access restrictions, permitting uncontrolled connections for any PC or personal device, emerged as a key weakness. Strengthening network access controls is crucial to enhance security and minimize the potential for unauthorized access and breaches. Additionally, the organization's ineffective implementation of its password policy underscores the need for improvements in logical access limitations.

### 4.2.4 Physical Access to Network Equipment and Cables outside the Computer Room

The physical security of the network hardware and cables kept outside the computer room has become a significant security problem. According to the audit, switches and firewalls inside specified racks weren't properly locked, posing a serious security risk. This carelessness can allow unauthorized people to access important parts, which might cause network interruptions. Implementing secure fastening techniques for important network gear within their enclosures is crucial for mitigating this risk efficiently and assuring the safety of crucial infrastructure parts.

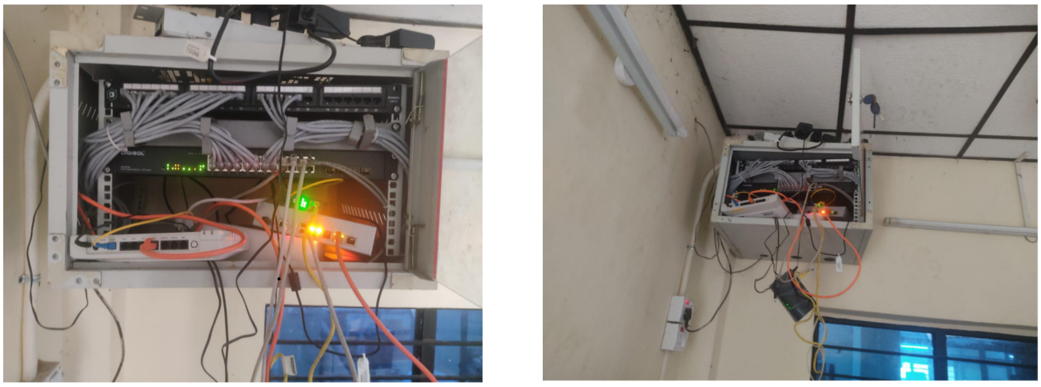


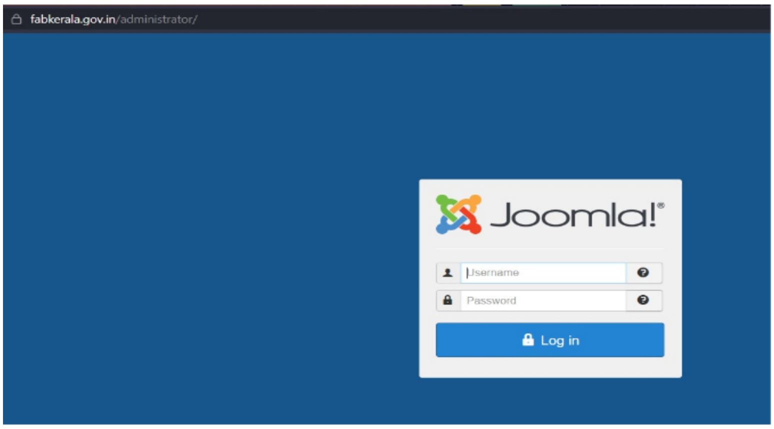
Figure 4.2: Network components rack

### 4.2.5 Network Bandwidth

The organization's network has a download speed of 26.49 Mbps and an upload speed of 88.37 Mbps, serving as a crucial reference point for evaluating its capacity and assessing alignment with its internet speed requirements. Consistent network speed assessments are essential in maintaining a dependable and efficient network environment, ensuring that it effectively meets the organization's connectivity needs.

### 4.2.6 Joomscan

Identifying an outdated Joomla website running version 3.9.12 and accessible through the administrator login page raises significant security concerns. Operating an outdated Joomla version exposes the website to known vulnerabilities, including the risk of brute force attacks and malware injection, which malicious actors can potentially exploit. It is imperative to prioritize the immediate update and patching of the Joomla installation to address these security vulnerabilities and ensure the website's robust protection against potential threats.

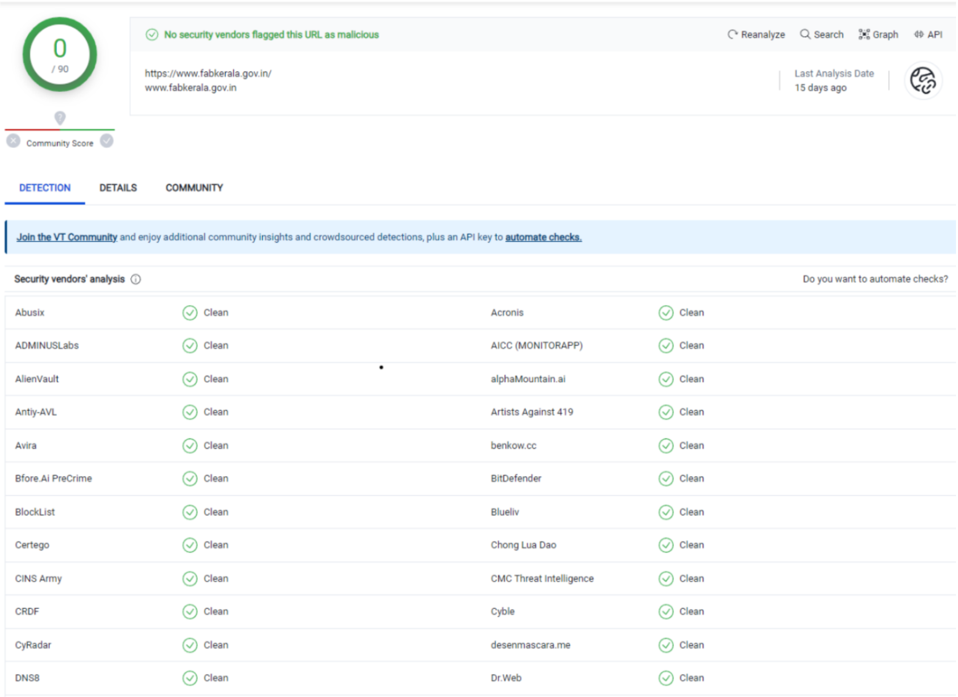


fabkerala.gov.in/administrator/

Figure 4.3: Joomscan

### 4.2.7 Virus Total

In the VirusTotal analysis of the website address, a score of zero implies the absence of noteworthy security threats or concerns identified during the assessment. This outcome signifies a robust security stance for the website, as there were no indications of malware, phishing attempts, or suspicious activities detected by VirusTotal's thorough scanning and analysis tools. Nevertheless, it remains crucial to maintain ongoing monitoring and periodic security assessments to uphold the website's integrity and remain vigilant against emerging threats.



No security vendors flagged this URL as malicious

https://www.fabkerala.gov.in/
www.fabkerala.gov.in

Last Analysis Date
15 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

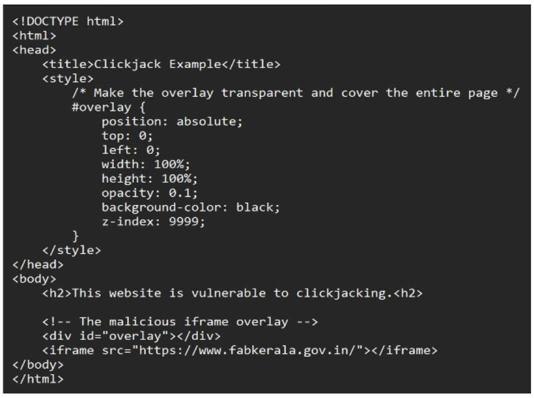
Do you want to automate checks?

| | | | |
|---|---|---|---|
| Abusix | ✓ Clean | Acronis | ✓ Clean |
| ADMINUSLabs | ✓ Clean | AICC (MONITORAPP) | ✓ Clean |
| AlienVault | ✓ Clean | alphaMountain.ai | ✓ Clean |
| Antiy-AVL | ✓ Clean | Artists Against 419 | ✓ Clean |
| Avira | ✓ Clean | benkow.cc | ✓ Clean |
| Bfore.Ai PreCrime | ✓ Clean | BitDefender | ✓ Clean |
| BlockList | ✓ Clean | Blueliv | ✓ Clean |
| Certego | ✓ Clean | Chong Lua Dao | ✓ Clean |
| CINS Army | ✓ Clean | CMC Threat Intelligence | ✓ Clean |
| CRDF | ✓ Clean | Cyble | ✓ Clean |
| CyRadar | ✓ Clean | desenmascara.me | ✓ Clean |
| DNS8 | ✓ Clean | Dr.Web | ✓ Clean |

Figure 4.4: Virustotal

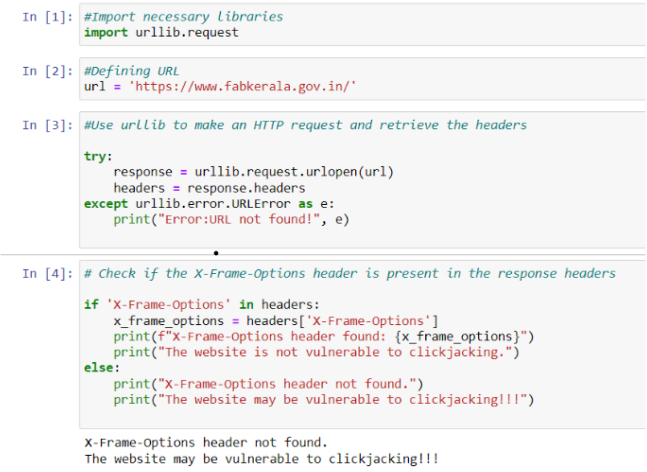
### 4.2.8 Clickjacking Testing and Assessment

The discovery of clickjacking activity on the website poses a significant security risk. Clickjacking is a deceptive attack that tricks users into clicking on web page elements without their knowledge. This method involves overlaying a hidden malicious page on top of a legitimate one, making it difficult for users to distinguish between them. Consequently, users may interact with the malicious content, unknowingly initiating potentially harmful actions or data theft, all while believing they are interacting with the genuine page. Testing conducted using HTML and Python has confirmed the website's vulnerability to clickjacking, emphasizing the urgent need to implement security measures to mitigate this threat effectively. Associated CVE : CVE-2019-18650 and CVE-2019-18674



```
<!DOCTYPE html>
<html>
<head>
    <title>Clickjack Example</title>
    <style>
        /* Make the overlay transparent and cover the entire page */
        #overlay {
            position: absolute;
            top: 0;
            left: 0;
            width: 100%;
            height: 100%;
            opacity: 0.1;
            background-color: black;
            z-index: 9999;
        }
    </style>
</head>
<body>
    <h2>This website is vulnerable to clickjacking.<h2>

    <!-- The malicious iframe overlay -->
    <div id="overlay"></div>
    <iframe src="https://www.fabkerala.gov.in/"></iframe>
</body>
</html>
```

Figure 4.5: Clickjacking tested using HTML

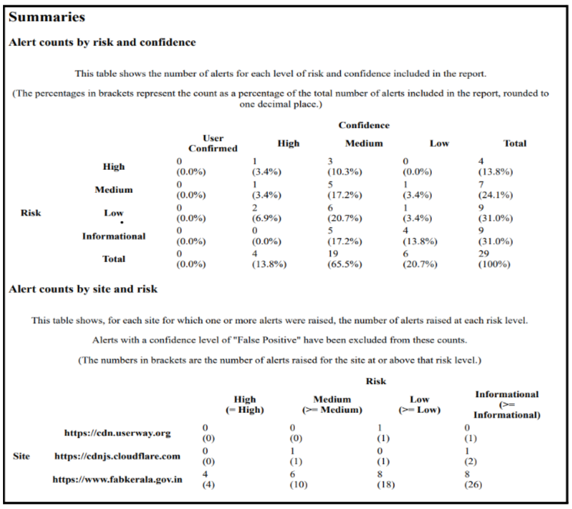


```
In [1]: #Import necessary libraries
        import urllib.request

In [2]: #Defining URL
        url = 'https://www.fabkerala.gov.in/'

In [3]: #Use urllib to make an HTTP request and retrieve the headers

        try:
            response = urllib.request.urlopen(url)
            headers = response.headers
        except urllib.error.URLError as e:
            print("Error:URL not found!", e)

In [4]: # Check if the X-Frame-Options header is present in the response headers

        if 'X-Frame-Options' in headers:
            x_frame_options = headers['X-Frame-Options']
            print(f"X-Frame-Options header found: {x_frame_options}")
            print("The website is not vulnerable to clickjacking.")
        else:
            print("X-Frame-Options header not found.")
            print("The website may be vulnerable to clickjacking!!!")

        X-Frame-Options header not found.
        The website may be vulnerable to clickjacking!!!
```

Figure 4.6: Clickjacking tested using Python

### 4.2.9 OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is a valuable open-source penetration testing tool for web application security. It excels in detecting and exploiting vulnerabilities in web applications, focusing on high-risk warnings such as Cross-site Scripting (XSS), Hash Disclosure, SQL Injection, and Server Side Template Injection (SSTI). XSS attacks inject malicious code, typically HTML or JavaScript, into a web application, compromising user data and trust. SSTI poses a severe threat by enabling attackers to inject malicious code into server-side templates, potentially leading to data breaches and remote code execution. SQL Injection is another vulnerability arising from dynamic database queries, which can be mitigated by avoiding string concatenation and sanitizing user-supplied input. These insights emphasize the importance of proactive security measures like input validation, output encoding, Content Security Policy (CSP), and code review to safeguard web applications against these critical threats.



Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

| | | Confidence | | | | |
|---|---|---|---|---|---|---|
| | | User Confirmed | High | Medium | Low | Total |
| Risk | High | 0<br>(0.0%) | 1<br>(3.4%) | 3<br>(10.3%) | 0<br>(0.0%) | 4<br>(13.8%) |
| | Medium | 0<br>(0.0%) | 1<br>(3.4%) | 5<br>(17.2%) | 1<br>(3.4%) | 7<br>(24.1%) |
| | Low | 0<br>(0.0%) | 2<br>(6.9%) | 6<br>(20.7%) | 1<br>(3.4%) | 9<br>(31.0%) |
| | Informational | 0<br>(0.0%) | 0<br>(0.0%) | 5<br>(17.2%) | 4<br>(13.8%) | 9<br>(31.0%) |
| | Total | 0<br>(0.0%) | 4<br>(13.8%) | 19<br>(65.5%) | 6<br>(20.7%) | 29<br>(100%) |

Alert counts by site and risk

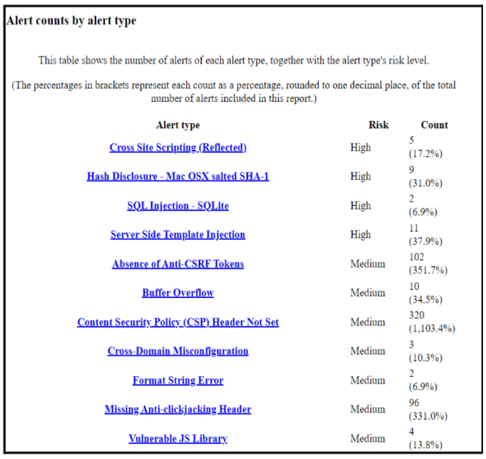
This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

| | | Risk | | | |
|---|---|---|---|---|---|
| | | High<br>(= High) | Medium<br>(>= Medium) | Low<br>(>= Low) | Informational<br>(>= Informational) |
| Site | https://cdn.userway.org | 0<br>(0) | 0<br>(0) | 1<br>(1) | 0<br>(1) |
| | https://cdnjs.cloudflare.com | 0<br>(0) | 1<br>(1) | 0<br>(1) | 1<br>(2) |
| | https://www.fabkerala.gov.in | 4<br>(4) | 6<br>(10) | 8<br>(18) | 8<br>(26) |

Figure 4.7: OWASP ZAP



Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

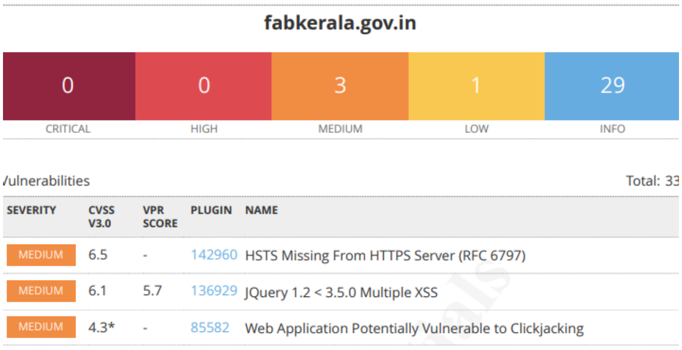
| Alert type | Risk | Count |
|---|---|---|
| Cross Site Scripting (Reflected) | High | 5<br>(17.2%) |
| Hash Disclosure - Mac OSX salted SHA-1 | High | 9<br>(31.0%) |
| SQL Injection - SQLite | High | 2<br>(6.9%) |
| Server Side Template Injection | High | 11<br>(37.9%) |
| Absence of Anti-CSRF Tokens | Medium | 102<br>(351.7%) |
| Buffer Overflow | Medium | 10<br>(34.5%) |
| Content Security Policy (CSP) Header Not Set | Medium | 320<br>(1,103.4%) |
| Cross-Domain Misconfiguration | Medium | 3<br>(10.3%) |
| Format String Error | Medium | 2<br>(6.9%) |
| Missing Anti-clickjacking Header | Medium | 96<br>(331.0%) |
| Vulnerable JS Library | Medium | 4<br>(13.8%) |

Figure 4.8: OWASP ZAP

### 4.2.10 Nessus

Nessus, a widely employed vulnerability scanning tool, is instrumental in evaluating and strengthening computer networks and system security. It efficiently identifies and prioritizes security weaknesses, misconfigurations, and potential threats within an organization's IT infrastructure, facilitating proactive vulnerability mitigation. After conducting a web application scan using Nessus, the results unveiled three medium-level vulnerabilities and one low-level vulnerability. Notably, these findings include the absence of HTTP Strict Transport Security (HSTS) on the HTTPS server, multiple cross-site scripting (XSS) issues related to jQuery 1.2 ¡ 3.5.0, and potential susceptibility to Clickjacking attacks. HSTS, in particular, is a vital web security measure that protects against various cyber threats, including man-in-the-middle attacks and cookie hijacking.

Addressing these vulnerabilities is essential to effectively reduce the risk of cyberattacks and data breaches.



fabkerala.gov.in

| 0 | 0 | 3 | 1 | 29 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

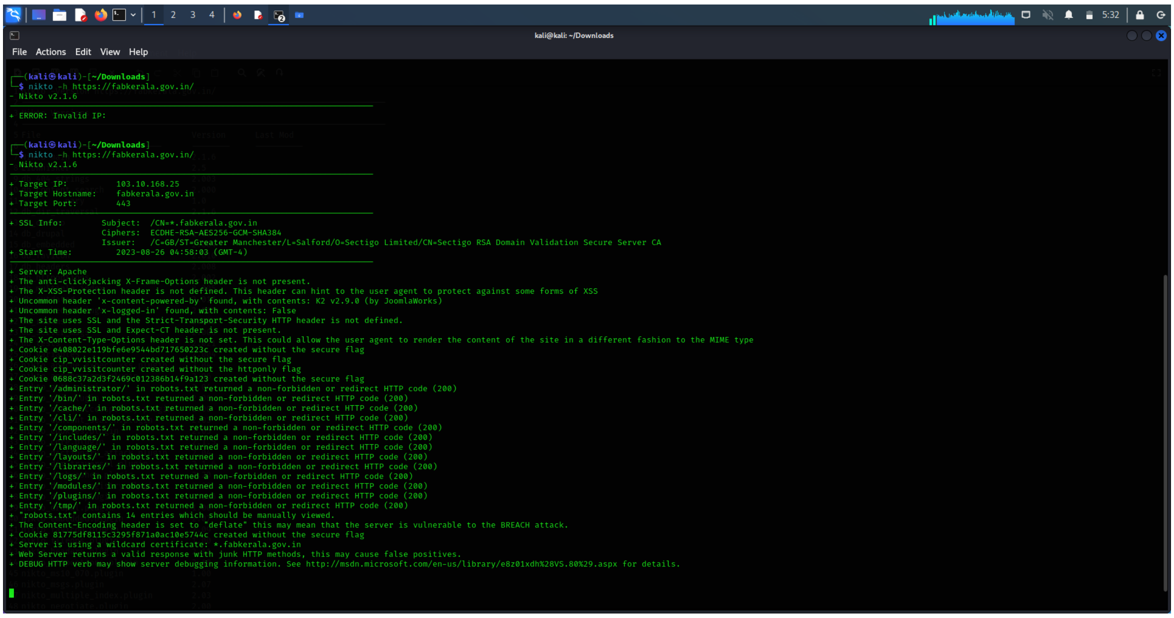
/ulnerabilities Total: 33

| SEVERITY | CVSS V3.0 | VPR SCORE | PLUGIN | NAME |
|---|---|---|---|---|
| MEDIUM | 6.5 | - | 142960 | HSTS Missing From HTTPS Server (RFC 6797) |
| MEDIUM | 6.1 | 5.7 | 136929 | JQuery 1.2 < 3.5.0 Multiple XSS |
| MEDIUM | 4.3* | - | 85582 | Web Application Potentially Vulnerable to Clickjacking |

Figure 4.9: Nessus

## 4.2.11 Nikto

The Nikto vulnerability analysis has revealed multiple vulnerabilities within the assessed website. Nikto's comprehensive scanning capabilities have successfully detected and documented these vulnerabilities, providing essential insights into potential security weaknesses that demand immediate and effective remediation. These findings are instrumental in improving the system's security posture and mitigating related risks.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nikto -h https://fabkerala.gov.in/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: Invalid IP:

┌──(kali㉿kali)-[~/Downloads]
└─$ nikto -h https://fabkerala.gov.in/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.10.168.25
+ Target Hostname:    fabkerala.gov.in
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.fabkerala.gov.in
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time:         2023-08-26 04:58:03 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-content-powered-by' found, with contents: K2 v2.9.0 (by JoomlaWorks)
+ Uncommon header 'x-logged-in' found, with contents: False
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie e408022e119bfe6e9544bd717650223c created without the secure flag
+ Cookie cip_vvisitcounter created without the secure flag
+ Cookie cip_vvisitcounter created without the httponly flag
+ Cookie 0688c37a2d3f2469c012386b14f9a123 created without the secure flag
+ Entry '/administrator/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/bin/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/cache/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/cli/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/components/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/language/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/layouts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/libraries/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/logs/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/plugins/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 14 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Cookie 81775df8115c3295f871a0ac10e5744c created without the secure flag
+ Server is using a wildcard certificate: *.fabkerala.gov.in
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
```

Figure 4.10: Nikto

### 4.2.12 Advanced IP Scanner, Nmap, Wireshark

The use of Nmap, Wireshark, and Advanced IP Scanner for network scanning and analysis raised concerns about the accuracy of the results. In particular, Wireshark showed standard packet transmission, while Advanced IP Scanner detected 254 IP addresses, significantly more than the expected number of devices (around 70) in the organization. The challenge lies in identifying which IP addresses belong to company devices and which may be associated with external or unidentified equipment. Several factors contribute to the difficulty in identifying all devices, including flexible network addresses, offline devices during the scan, network complexities, and security settings that limit scan visibility. Addressing these issues is crucial for enhancing network security and efficiency by accurately documenting all network components.

## 4.3 Results Comparison

The website vulnerability scans conducted through tools like ZAP, Nikto, and Nessus have unveiled a range of common vulnerabilities, including Cross-Site Scripting (XSS), Hash Disclosure, SQL Injection, and Server-Side Template Injection. The web server responds validly even to unconventional HTTP methods, and specific security headers such as X-Content-Type-Options and Expect-CT are absent. Furthermore, the jQuery library version 1.12.4 has been identified as vulnerable. The website lacks HTTP Strict Transport Security (HSTS) on its HTTPS server. These findings emphasize the immediate imperative of addressing and remedying these vulnerabilities to bolster the website's security posture.

## 4.4 Recommendations

To enhance overall security, the organization needs to implement a comprehensive set of recommendations. This includes configuring the Strict-Transport-Security (HSTS) header, ensuring reputable certificate authorities, employing a web application firewall (WAF), and keeping software consistently up to date. Upgrading jQuery to version 3.5.0 or higher is crucial, and both client and server sides must undergo identical security tests, incorporating character encoding and HttpOnly flags for session cookies. Critical steps include vigilance for visual cues indicating clickjacking, using modern browsers with security features enabled, and implementing frame-busting code. Security software should encompass anti-phishing and anti-clickjacking capabilities, with prompt reporting of suspicious activities. Strong password policies and Joomla updates are vital for web security. Mitigating brute force attacks necessitates changing the default administrator URL, implementing login attempt rate limiting, and employing CAPTCHA. Additionally, consideration of visitor verification, network segmentation, strict access controls, firewalls, encryption, intrusion detection systems, and the principle of least privilege is integral to network security. Adding MAC address-based access control is recommended.

Regular monitoring, employee training, and aligning with compliance requirements form essential components of a comprehensive security approach.

## 4.5 Summary

The audit of the government organization’s network infrastructure and website revealed several critical security issues. First, the absence of an up-to-date network diagram hinders effective security management. Mismanagement of firewalls and network switches poses operational and security risks. Password security is compromised by storing passwords on paper and not adhering to password policies. Network segmentation is lacking, increasing potential security risks. System inventory is not maintained, making it difficult to track assets. The organization’s firewalls are inadequately maintained, exposing the network to vulnerabilities. Adding MAC address-based access control is recommended. The website lacks critical security headers like X-Frame-Options, X-XSS-Protection, and HTTP Strict Transport Security, leaving it vulnerable to attacks. Lastly, the possibility of SQL injection exists due to insecure database query construction. Implementing these recommendations is crucial for enhancing the organization’s network and website security.

# Chapter 5

# Conclusions and Future Work

## 5.1 Conclusions

In conclusion, the Kerala Police Cyberdome internship has given me essential knowledge and practical skills in cybersecurity. It emphasized the importance of vulnerability assessment, malware analysis, passive website security auditing, and network infrastructure security auditing as critical components of modern cybersecurity. I learned systematic approaches to identifying and mitigating vulnerabilities, deciphering malicious software, and safeguarding online assets. Additionally, the program highlighted the significance of adhering to ISO standards. Overall, this internship has transformed my understanding and equipped me to proactively defend against cyber threats, contributing to a safer digital environment.

## 5.2 Limitation

This passive website security auditing has limitations and might not be able to provide an accurate picture of how secure a particular website is. The functionality, dynamic character, or user interactions of the website are not assessed. Therefore, passive auditing should be used with other security evaluations, such as active vulnerability scanning, penetration testing, and manual testing, to reduce the risk of false positives and negatives and the potential for missing real-time threats.

## 5.3 Future Work

In the future, our audit will continue to address the limitations of passive website security auditing by actively requesting access to the organization's website for comprehensive scanning and advanced testing. This proactive approach ensures a more accurate assessment of vulnerabilities, reducing the potential for false positives and providing a clearer view of security risks. Furthermore, we will expand our efforts to enhance the organization's security posture by conducting awareness programs on password policies and firewall security, fostering a security-conscious culture among personnel. Our commitment to proactive security testing and education will remain a central focus. Revisiting the organization periodically, we will reevaluate network infrastructure and utilize tools like Nmap and Wireshark to identify changes and emerging risks, ensuring ongoing security resilience and alignment with evolving threats and technologies.

# References

[1] V. K. P. S. N. K. D. P. P. K. A. V. G. Kumar B.P, ”Analysing Cyber Security Vulnerabilities using Click Jacking and HostHeader Injection,” in International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru,India, 2023.

[2] ”AUDIT OF NARA’S NETWORK INFRASTRUCTURE,” 2010.

[3] ”Zed Attack Proxy,” [Online]. Available: https://www.zaproxy.org/docs/alerts/40012/.

[4] ”jQuery 1.12.4 vulnerabilities: Snyk,” [Online]. Available: https://security.snyk.io/package/npm/jquery/1.12.4.

[5] ”HTTP — MDN,” [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security.

[6] ”Joomla! Developer Network™,” [Online]. Available: https://developer.joomla.org/security-centre/794-20191001-core-csrf-in-com-template- overrides-v

[7] A. M. H. W. S. S. C. J. Lin-Shung Huang, ”Clickjacking: Attacks and defenses,” in 21st USENIX Security Symposium, USA, 2012.

[8] E. Humphreys, Implementing the ISO/IEC 27001 ISMS Standard, Norwood: Library of Congress Cataloging-in-Publication Data, 2016.