

**VISVESVARAYA TECHNOLOGICAL UNIVERSITY**

**Belagavi-590018, Karnataka**

**A**

**Technical Seminar Report**

**On**

**“TESTING FOR SECURITY WEAKNESS OF WEB APPLICATION USING ETHICAL HACKING”**

*Submitted in partial fulfillment for the award of the degree in*

**BACHELOR OF ENGINEERING IN**

**COMPUTER SCIENCE & ENGINEERING**

Submitted by

SUMANT KUMAR

USN: 1BH20CS045

Under the guidance of

**Mrs. Neha Bhatt**

**Asst Professor**

**BANGALORE TECHNOLOGICAL INSTITUTE**

**(ISO 9001:2015 Certified Institute)**

Sarjapura Road, Kodathi, Bangalore-560035

**Department of Computer Science and Engineering**

**2023-24**

|  |  |  |
| --- | --- | --- |
|  | **BANGALORE TECHNOLOGICAL INSTITUTE**  **(An ISO 9001:2015 Certified Institute)**  **Off-Sarjapur Road, Kodathi, Bangalore – 560035**  **Department of Computer Science and Engineering** |  |

**CERTIFICATE**

It is certified that the Technical Seminar Work entitled **“Testing for Security weakness of web application Using ethical hacking”** carried out by **SUMANT KUMAR [1BH20CS045],** the Bonafide student of **Bangalore Technological Institute**, **Bangalore** in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering** of **Visvesvaraya Technological University, Belgaum** during the year **2023-2024**. Thus, it is certified that all corrections/suggestion indicated for Internal Assessment have been incorporated in the report submitted to the Department of Computer Science and Engineering. The technical seminar report has been approved as it satisfies the academic requirement in respect of technical seminar report prescribed for the said degree.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Mrs. Neha Bhatt Dr. Sreeramareddy G. M Dr. H S Nanda

Technical Seminar Guide Professor and Principal

Department of CSE H.O.D of CSE

|  |  |  |
| --- | --- | --- |
| A close-up of a card  Description automatically generated | **BANGALORE TECHNOLOGICAL INSTITUTE**  **(An ISO 9001:2015 Certified Institute)**  **Off-Sarjapur Road, Kodathi, Bangalore – 560035**  **Department of Computer Science and Engineering** |  |

**DECLARATION**

I am a student of eighth semester **B.E COMPUTER SCIENCE AND ENGINEERING, BANGALORE TECHNOLOGICAL INSTITUTE, BENGALURU**, hereby declare that the technical seminar entitled “**TESTING FOR SECURITY WEAKNESS OF WEB APPLICATION USING ETHICAL HACKING**” has been independently carried out me at **Bangalore Technological Institute, Bengaluru** and submitted in partial fulfillment of the requirements for the award of the degree in **Bachelor of Engineering in Computer Science and Engineering** of the **Visvesvaraya Technological University, Belagavi** during the academic year **2023-24**.

I also declare that, to the best of my knowledge and believe the work reported here does not form or part of any other dissertation on the basis of which a degree or award was conferred on an early occasion of this by any other students.

PLACE: BENGALURU DATE:

**SUMANT KUMAR**

**[1BH20CS045]**

# ACKNOWLEDGEMENT

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals and elders.

I would like to take this opportunity to thank them all. I heartily extend my gratitude to our Seminar Guide, **Mrs. Neha Bhatt** , for her valuable advice, encouragement and suggestion given to me in the course of my seminar work. I convey gratitude to his for having constantly monitored the development of the seminar report and setting up precise deadlines.

I express my heartfelt thanks to the technical seminar coordinators **Mr. Dilip S & Ms. Vidyashree R** for their immense support and guidance in the Semminar.

I would like to express my immense gratitude to the Head of Department of Computer Science and Engineering, **Dr. Sreeramareddy G. M**, for his unfailing encouragement and suggestions given to me in the course of the work.

I would like to take this opportunity to thanks Principal, **Dr. H S Nanda,** for giving me this opportunity to enrich knowledge.

I would like to express gratitude to the President **Dr. A Prabhakara Reddy** and Secretary**, Sri. C L Gowda** for having provided us with a great infrastructure and well- furnished labs.

Finally, a note of thanks to the Department of Computer Science and Engineering, both teaching and non-teaching staff for their cooperation extended. Last but not the least, I acknowledge the support and feedback of my parents, guardians and friends, for their indispensable help always.

**SUMANTKUMAR**

**[1BH20CS045]**

# ABSTRACT

In the digit l world, everything gets connected through the network, and when various services are provided by web applications people are susceptible to hacking. According to the 2019 internet security threat report by Symantec’s, an average of 4, 800 websites are vulnerable to digital information theft (form jacking) attack. The main intent of this paper is to recognize openness and flaws in networks and web applications using penetration testing to protect the institutions from cyber threats. There are many scanning methods suggested by many authors to identify the weakness. But in our research, vulnerability analysis and assessment are done by the Nikto tool, [open web application security project] OWASP's Zed.

**TABLE OF CONTENTS**

**CHAPTERS PAGE NO.**

1. ABOUT SOFTWARE 1
   1. [Introduction 1](#_TOC_250003)
2. RELATED WORK 2-3
   1. [Keywords](#_TOC_250002)
   2. I.LITERATURE

3. INFORMATION GATHERING BY VARIOUS TOOLS 4-7

4. METHODOLOGY 8-11

5. RESULT AND DISCUSSION 12-13

6. CONCLUSION 14

[REFERENCES 15](#_TOC_250000)

**LIST OF FIGURES**

FIG. NO:TITLE OF FIGURE PAGE NO.

3.1Analysis Report by Sparta 4

3.2Analysis Report by Nmap tool 5

3.3Analysis Report by Zenmap tool 5

3.4

4.1

4.2

4.3

4.4

5.1

Analysis Report by virus total Steps for detecting vulnerabilities

Analysis report by OWASP ZAP tool Result Assessment Graph by OWASP Tool Analysis report by Nikto tool

The comparison result of OWASP ZAP and Nikto Tool

6

8

9

10

10-11

12

**CHAPTER 1**

# ABOUT SOFTWARE REUSE

### INTRODUCTION

In our daily life, all the domains from banking applications to government organizations and mobile applications use web services for sending and receiving information. Web applications are the most vulnerable to hacking. The foremost tactic of hackers is to identify loopholes in the network infrastructure, steal confidential data and passwords and hack the information from the organizations that could lead to financial loss. The cybercrime released by RSA security report 2019, mentioned 43% fraud increased in social media through web applications.

Ethical hacking or penetration testing or white-hat attacks is an important tool for testing of computer systems and network applications or web to locate security weaknesses. The hackers usually attack open websites by Client-side attack or Server-side attack in different methods to enter into networks for finding vulnerabilities. It is attainable by HTTP methods such as to get method (through URL), post method (body of the message), put and delete method or web cookies (Home Page), and the threats are performed through automated or manual testing. Nmap) have been tested through kali Linux platform and search engine. ZAP and Nikto tools are demonstrated in ten different domains to identify the security weakness. From the analysis medium, low-level attacks have been discovered by the ZAP tool. From the result comparison of the Nikto and zap tool, the Nikto tool identified more venerability than ZAP.

**CHAPTER 2**

**RELATED WORK**

## KEYWORDS

Cross Side Scripting, Ethical Hacking, Nikto, Nmap, OWASP ZAP, Penetration Testing, Sparta.

Cybercrime activities are increasing day by day and exploit the website due to the absence of security in network infrastructure. The protection of data is the highest priority level these days so the prominent work is to find security flaws in the network and web applications. The main goal of this paper is to find how hackers identify the loopholes in the network infrastructure for attacking web applications. Thus vulnerability analysis and web assessment techniques are used to gather information and cyber threat-related to it. This paper help to secure web applications in the future. The remainder of the article is organized as follows: section II forms literature review, section III briefly explains information gathering using various tools, section IV presents the methodology, section V vulnerability analysis and assessment for the testing environment, section VI presents the result and discussion and the last section gives the conclusion.

Hatfield discussed virtue ethics found lacking in firms while individuals are affected by human hacking; therefore he analyzed the ethical theory using penetration testing in social engineering with consideration of virtue ethics. Miriam et al. for cybersecurity researchers in fields related to vulnerability analyses. Zabicki, R& Ellis hackers have identified security weakness in networks and launch attacks because the internet is powerful in equipment, staff, code, network elements, and firmware. The case study is done on paper for a few tools. This paper has utilized different tools such as Nmap, Metasploit, and enterpriser in Kali Linux to find flaws. Patel introduced Penetration Testing (PT) and Vulnerability Assessment (VA) techniques to find security loopholes in an organization.

Suggested to launch security patches to minimize the threats and preventive steps against Owasp Top 10. T.Jain & N.Jain contributed two models for identifying web application flaws by python script scanner and minimize the vulnerabilities by ModSecurity. ModSecurity is a web technique firewall. Using this technique to find more flaws and differentiate into a low, medium or high level of attacks. Zaher and Babak examined the important factors and components considered for penetration testing and introduced some tools and processes in IT regulations. Renaud and Zimmermann presented a nudge testing for a stronger password for ethical suggestions in the authentication process from the various literature.Vance examined the importance of an ethical hacking course to protect computer networks. Ferda used the OWASP analysis tool to measure the vulnerability level in web application security development. Nagpure et al. used automation and manual testing to check vulnerabilities in web applications. A comparative analysis is executed automatically by OWASP ZAP, Acunetix and Burp Suite. The manual testing was done by Vulnerability Assessment and Penetration Testing (VAPT) tool and the result was 100% accuracy, and manual testing gave better results than automation testing. Cheng et al. outlined different attacks by cybercrime such as ransomware and spear- phishing in websites and evaluated test results using Vulscan and OWASP ZAP web vulnerability scanner. They would detect cross-site scripting (XSS) and SQL injection vulnerabilities. XSS a client-side attack where attackers inject scripts into web pages on a targeted page and SQL injection vulnerabilities are done on database servers when input is not fetched properly from the databases. Nirmal et al. explained that during the Software Development Life Cycle (SDLC) process web application vulnerability assessment was the major aspect in security phases. Therefore,external entity (XEE) and cross-site request forgery (CSRF) and Server Site Request Forgery (SSRF) risks have been discovered. The manual and automated assessment methods are used to predict flaws by machine learning and hybrid program analysis. Murthy and Shilpa proposed a finite state model identifying security weakness in the web application and implemented a Path generation algorithm and depth-first traversal-based test generation algorithm to execute initiate functional tests in the banking domain. Holikand Neradova introduced two phases such as application exploitation and reconnaissance to find security flaws in the web applications. Ghanem & Chen recommended Reinforcement Learning (RL) to learn complicated activities and suggested intelligent automated penetration testing system (IAPTS) to acquire information, imitate tests and learn from knowledges.

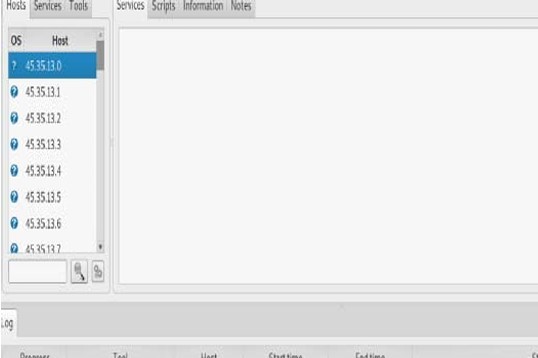
## CHAPTER 3

**INFORMATION GATHERING BY VARIOUS TOOL**

Here Sparta, Network Mapper (Nmap), Netcraft, Zenmap, Virus total, IP tracking tools are analyzed for finding vulnerabilities in the network as well as web applications.

1. **Sparta.**

It is a network infrastructure vulnerability analysis tool, python GUI implementation by the penetration expert, in the enumeration and scanning stage. It scans the web application’s open and close port and finds open ports more vulnerable to black hat attacks and advances to run extra tools against the detected services such as smbenum, snmpcheck, nikto and so on. Black hat attackers generally have vast knowledge about bypassing security policies and cracking into computer networks for financial gain, login credentials and personal recognition, political plan for a social change, but not authorized to accomplish any type of penetration testing activity . This scanning tool identified open ports. An utmost open port is an acquirable entry for attackers.



**Fig 3.1 Analysis Report by Sparta tool**

1. **Network Mapper (Nmap):**

Nmap (“Network Mapper”) is used for security evaluation and network location and for finding network log, monitoring host and handling resource upgrade program. It is more helpful to scan large networks. Nmap Command: Nmap –T4 –A – v Domain Name System (DNS) names are used to generate information such as application name, OS versions, etc. Nmap includes result viewer (Zenmap), debugging tool (Ncat) and response analysis tool (Nping) . The Zenmap analysis used to collect data about managing less secured services and ports and discover trace port in the hostname.

FIGURE 2.Analysis report by Nmap result is given below.

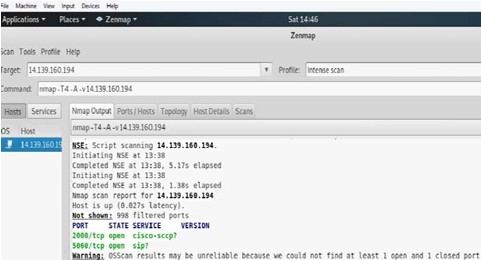
Nmap scan report for [www.kce.ac.in](http://www.kce.ac.in/) (216.70.123.73) Starting Nmap 7.70 (https://nmap.org) at 2019-07-09 03:19 EDT

* + PORT STATE SERVICE VERSION
  + 80/tcp opentcpwrapped
  + 113/tcp closed ident
  + 443/tcp open tcpwrapped
  + Public Key type: rsa
  + Public Key bits: 2048
  + Signature Algorithm: sha256WithRSAEncryption
  + Device type: VoIP
  + cpe:/h:firebrick:fb2700

**Fig 3.2 Analysis Report by Nmap tool**

1. **Zenmap :**

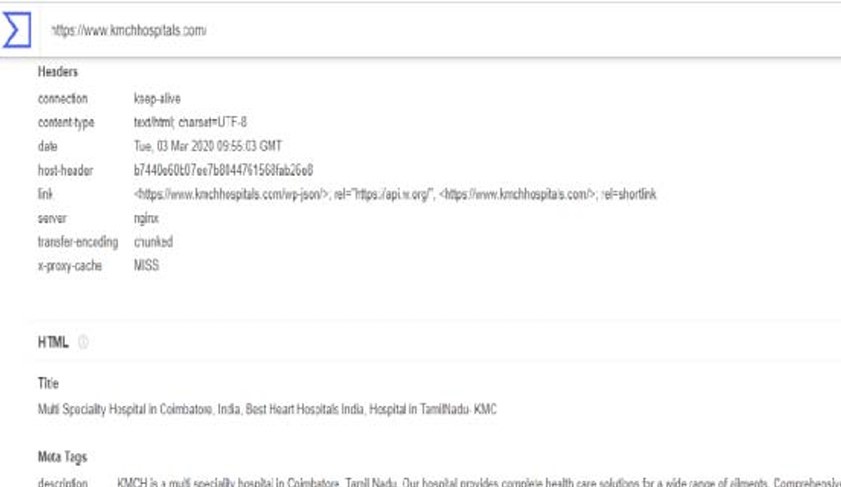
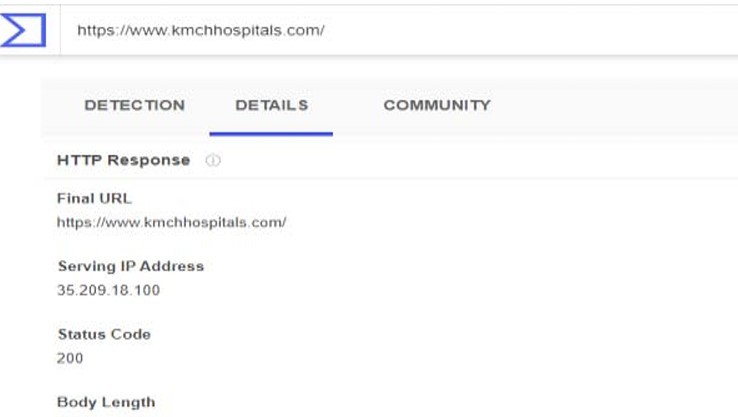
map Zenmap is also called network mapper. It is the Nmap security scanner with a graphical user interface (GUI) cross-platform for network discovery. The Zenmap tool discovered the open ports, HOP count and round trip time (RTT). The result is shown in FIGURE3.



**Fig 3.3 Analysis Report by Zenmap tool**

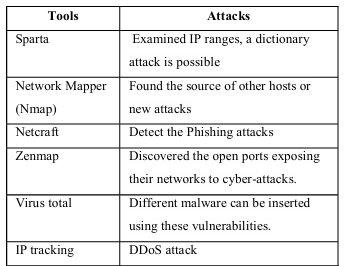
1. **Virus Total :**

The virus total service detects URLs for malicious code and suspicious files. https://[www.virustotal.com](http://www.virustotal.com/) is used to discover sub domains.



**Fig 3.4 Analysis Report by virus total**

**TABLE 3.1 Comparism Results of Different Tools**

****

**From the comparison results of different tools involved in identifying the attacks, it is cleared that cyberattacks can be possible.**

## CHAPTER 4

# METHODOLOGY

Organization, IT Industries, and then vulnerability analysis and assessment were executed for 100 websites using hostname The experiments are done using Intel (R) Pentium

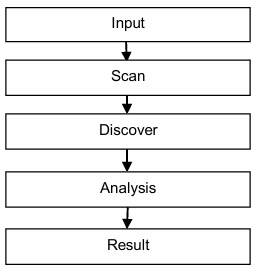
(R) CPU N3710 1.60 GHz with 4GB RAM. The data were collected from Hospitals, Engineering colleges, Government O rganizations, Schools, Healthcare Companies, Business Organization, Sports, Banks, Financial / host ID. The scanning process was performed on the kali Linux platform using penetration testing on the top ten websites of each domain.

### VULNERABILITY ANALYSIS AND ASSESSMENT

A vulnerability analysis and assessment are measures finding the security breaches in the network, computer system, or web applications of the institution with the appropriate knowledge understanding of network infrastructure, and knowing of the possible threats of the environment. The automated testing such as OWASP ZAP and Nikto tool is used to detect weaknesses in network infrastructure and web application.

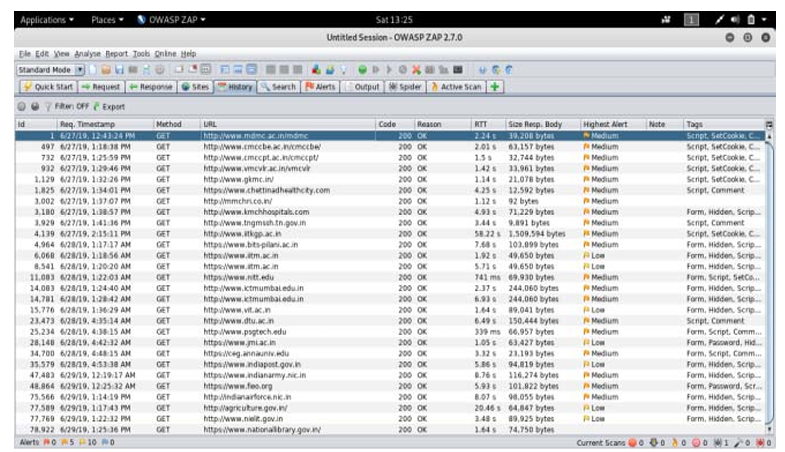
### A.OWASP ZAP (Zed Attack Proxy) Testing

OWASPs Zap is used as a security scanner for web applications. It has various modules such as Proxy for capturing, fuzzer for identifying vulnerability, Spider for discovering web applications, Scanner for active and passive attack and Dictionary method to access files [9]. The testing phase consists of five steps. Like the initial one, the Host Name/ Host ID should be given as input to attack. Next, the scanning process is carried out to identify the flaws in the network infrastructure.



**Fig 4.1 Steps for detecting vulnerabilities**

In ZAP, the four modes of attack such as standard mode, protected mode, attack mode, and safe mode are used to identify vulnerabilities on the web. Here scanning testing is demonstrated on standard mode to identify risks using Get method. The vulnerabilities found in this tool are explained below:



**Fig 4.2: Analysis report by OWASP ZAP tool**

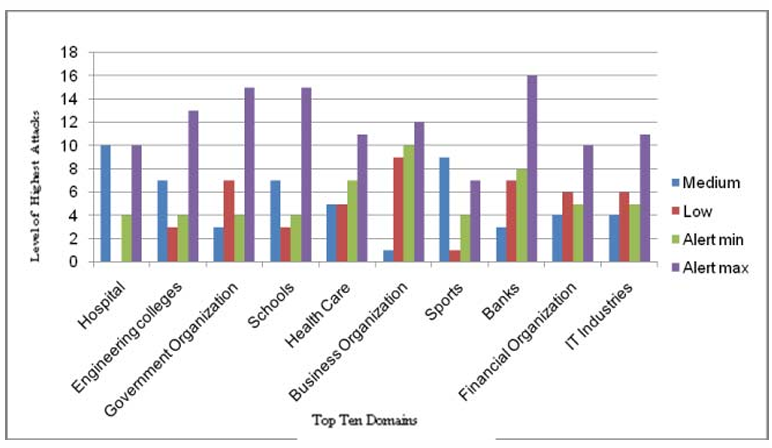
After the scanning process ZAP identifies medium and low-level risks and the vulnerabilities are explained below: OWASP ZAP detects the medium (high) level risks such as:

* URL rewriting-Third-party can attach to the session ID
* Application error disclosure-The sensitive information can be at risk in the hands of attackers leading to a ransomware attack
* X Frame Options(XFO) header not set- Without the user knowledge attacker will control the activities of the computer (clickjacking attack)
* SQL injection technique is used to attack the database layer flaws of an application and used to change the information with the help of DELETE, INSERT, ALTER queries to delete, add, and modify the data of the database.

The low (medium) level risk such as

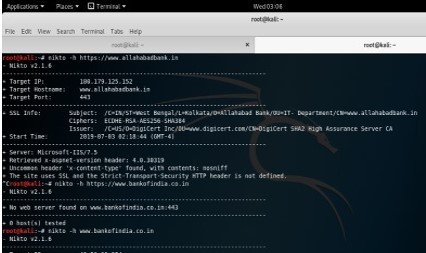
* Cross-Site Request Forgery (CSRF)- Through JavaScript code, the malicious file can be included through the various links attached to the source files and executing undesirable actions
* X-Content model missing –Threats of media type sniffing attacks cause a security vulnerability
* Secure pages include mixed content- Insecure HTTP connection leads to swamp video files, images and style sheets in the documents.
* Pragma HTTP and cache control– not implementing HTTP header properly.

From the testing environment, vulnerability and treats have been detected by scanning method and medium and low-level attacks have been discovered from the ten domains.



**Fig 4.3: Result Assessment Graph by OWASP Tool**

**A. NIKTO Testing**

Nikto is a free software command-line network security analysis automated scanner [20]. It is used to scan your web site and server immediately for known misconfigurations and security vulnerabilities. To identify vulnerability in the web applications, use the syntax Nikto –h hostname in the command-line.

Croot@kali:~# nikto -h <http://www.taekwondoindia.co.in/> - Nikto v2.1.6

+ Target IP: 167.88.160.3

+ Target Hostname: [www.taekwondoindia.co.in](http://www.taekwondoindia.co.in/)

+ Target Port: 80

+ Start Time: 2019-07-03 05:41:07 (GMT-4)

+ Server: LiteSpeed

+ Retrieved x-powered-by header: PHP/5.6.40

+ 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 &apos;x-redirect-by&apos; found, with contents: WordPress

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site differently to the MIME-type

**Fig 4.4 Analysis report by Nikto tool**

**Assessment through Nikto tool identified the vulnerabilities such as**

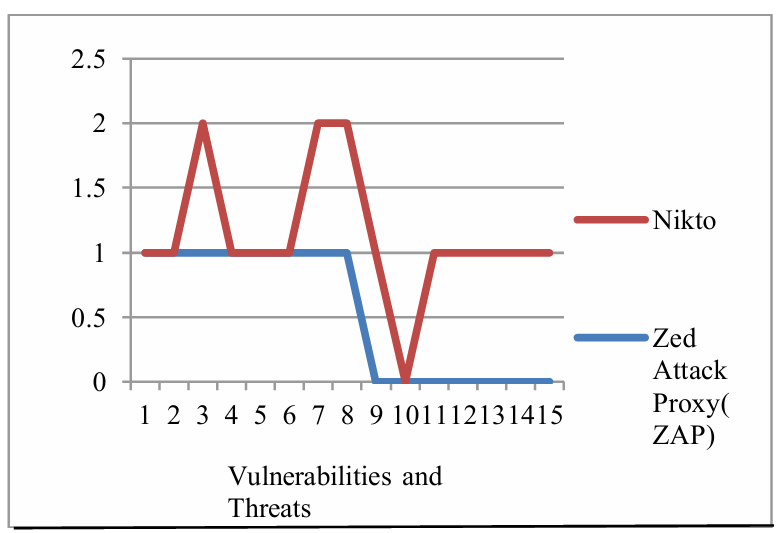
* Server leaks- report the affairs.
* XSS protection header is designed.
* Anti-click jacking non-existent.
* X-Frame-Options ineffective.
* An inadequate header in transport security.
* Retrieved x-aspnet-version header

From the assessment of the Nikto tool, only the top websites from a few domains exploit the header while the remaining domains do not use header files and informational alerts were found. The alerts and risk can be discovered using the OWASP ZAP scanning tool. Maximum alerts have been detected in the banking domain when compared to the remaining domains. The result is given in Figure 10

## CHAPTER 5

# RESULT AND DISCUSSION

In Figure 10 OWASP ZAP successfully discovered medium and low-level risks and found vulnerabilities at 19 (medium) and 81 (low). No high.



**Fig 5.1 The comparison result of OWASP ZAP and Nikto Tool**

Figure 13 mentions different vulnerabilities and threats are mentioned below;

1. Session ID in URL rewrite
2. Application error disclosure
3. X Frame options Header not set
4. Cross-domain JavaScript source file inclusion
5. Content-type header missing
6. Web browser XSS protection not enabled
7. X-content type options header missing
8. Cookie no HTTP only flag and without secure flag
9. The X-XSS-Protection header is not defined
10. Uncommon header found
11. SSL and the strict-transport-security not defined
12. Security HTTP header is not defined
13. Server leaks inodes via ETags 1

4. Retrieved x-powered by header

The red line indicates flaws detected by Nikto tool and blue line ZAP tool vulnerabilities. Nikto tool identifies vulnerability as the OWASP tool does. Nikto tool finds some additional information such as server, ciphers and Secure Socket Layer (SSL) information. SSL cryptographic protocols are used in computer networks for communication security. The vulnerabilities and threats discovered by the Nikto tool are higher than those by the OWASP ZAP tool, and by comparison, it is clear that some vulnerability missed by the OWASP ZAP tool is found by Nikto tool. The lack of security may lead advanced hackers to exploit those flaws. In the future, a high level of risk is possible and therefore identifying loopholes at an early stage in the network and web application is necessary. “Prevention is better than cure” is the best motto for securing cyberspace from attackers.

## CHAPTER 6

# CONCLUSION

Using penetration testing, security weakness has been detected in all areas of domains finding medium and low-level alerts with the OWASP ZAP tool. Our research and experimentation using automated testing have detected more vulnerabilities such as The X- XSS-Protection header is not defined, Uncommon header found, SSL and the strict transport- security HTTP header is not defined, Server leaks inodes via ETag, Retrieved x-powered by a header from the Nikto tool than from OWASP ZAP. Different vulnerabilities such as cookie without secure flag, cross-site request forgery (CSRF), URL rewriting and application error disclosure alerts have been detected by both the tool in web applications testing. This paper has a detailed security weakness using penetration testing and discussed security weaknesses in network infrastructure and web applications. Protecting the web applications and the infrastructure from attacks is very important in future research work.

# REFERENCES

1. Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. Computers & Security, 83, 354-366.
2. Sönmez, F. Ö. (2019). Security Qualitative Metrics for Open Web Application Security Project Compliance. Procedia Computer Science, 151, 998-1003.
3. Denis, M., Zena, C., &Hayajneh, T. (2016, April). Penetration testing: Concepts, attack methods, and defense strategies. In 2016 IEEE Long Island Systems, Applications, and Technology Conference (LISAT) (pp. 1-6). IEEE.
4. Huang, H. C., Zhang, Z. K., Cheng, H. W., & Shieh, S. W. (2017). Web application security: threats, countermeasures, and pitfalls. Computer, (6), 81-85.
5. Nirmal, K., Janet, B., & Kumar, R. (2018, July). Web Application Vulnerabilities- The Hacker's Treasure. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 58-62). IEEE.
6. Aarya, P. S., Rajan, A., Sachin, K. P. S., Gopi, R., &Sreenu, G. (2018, June). Web Scanning: Existing Techniques and Future. In 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 123-128). IEEE.
7. Nagpure, S., & Kurkure, S. (2017, August). Vulnerability assessment and penetration testing of Web application. In 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1 6). IEEE.
8. Murthy, P. V. R., & Shilpa, R. G. (2018, September). Vulnerability Coverage Criteria for Security Testing of Web Applications. In 2018 International Conference on Advances in Computing, Communications, (ICACCI) (pp. 489-494). IEEE. and Informatics
9. Holík, F., &Neradova, S. (2017, May). Vulnerabilities of modern web applications. In the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1256-1261). IEEE.
10. Renaud, K., & Zimmermann, V. (2018). Guidelines for ethical nudging in password authentication. SAIEE Africa Research Journal, 109(2), 102-118.