iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54658

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security

Vippalapalli Vikas[1], G. Saisri[2], T. Sai Meghana[3], A. Sree Harshini[4], G. Kaveri[5]
[1, 2, 3, 4, 5] *G. Narayanamma Institute of Technology and Science (for Women), Hyderabad, Telangana, India*

Abstract: ***This research paper presents a comprehensive analysis of the significance of web security audits and penetration testing in bolstering website security to combat the rising tide of cyber threats. In today's digital landscape, where cyber-attacks are becoming increasingly frequent and sophisticated, organizations must proactively assess vulnerabilities in their web applications and infrastructure. Through in-depth security audits and penetration testing, potential weaknesses can be identified and mitigated before they are exploited by malicious actors. This study explores various web security audit techniques, including vulnerability scanning and code review, and highlights the benefits of penetration testing, such as simulated attacks and vulnerability exploitation. It emphasizes the importance of regular security assessments and provides practical recommendations for establishing a robust web security framework. The findings underscore the critical role of web security audits and penetration testing in safeguarding websites, protecting sensitive data, and maintaining the credibility and trustworthiness of online platforms. This research paper contributes valuable insights for practitioners, researchers, and organizations aiming to enhance their web security posture in an ever-evolving threat landscape.***
Keywords: Web security, web security audits, penetration testing, vulnerability scanning, code review, cyber threats, website security, online platforms, data protection, threat landscape..

I. INTRODUCTION

In today's interconnected world, where digital platforms play a vital role in various aspects of our lives, ensuring the security and integrity of websites has become a critical concern. The increasing sophistication of cyber threats poses significant risks to organizations, including data breaches, financial losses, and reputational damage. To counter these threats, it is essential for organizations to adopt proactive measures to identify and mitigate vulnerabilities in their web applications and infrastructure. Web security audits and penetration testing have emerged as effective approaches for evaluating and enhancing website security.

Web security audits involve comprehensive assessments of web applications and underlying systems to identify potential weaknesses and vulnerabilities. These audits encompass techniques such as vulnerability scanning and code review, which help identify security loopholes and areas prone to exploitation [1]. By conducting thorough audits, organizations gain valuable insights into the security posture of their websites and can implement appropriate remedial measures to address identified vulnerabilities.

Penetration testing, on the other hand, involves simulated attacks on web applications to assess their resilience against real-world threats. By attempting to exploit identified vulnerabilities, penetration testers provide organizations with a practical assessment of their security measures. This allows organizations to proactively strengthen their defenses and safeguard against potential attacks [2].

Several studies have emphasized the importance of web security audits and penetration testing in mitigating the risk of cyber threats. For instance, Smith et al. (2019) found that organizations that regularly conduct web security audits experience fewer security incidents and are better prepared to respond to emerging threats [1]. Furthermore, Jones and Brown (2020) highlighted the effectiveness of penetration testing in identifying critical vulnerabilities that might otherwise go unnoticed [2].

In this context, this research paper aims to provide a comprehensive analysis of the significance of web security audits and penetration testing in enhancing website security. By reviewing relevant literature and examining best practices, this study aims to offer practical insights and recommendations for organizations seeking to establish a robust web security framework. The findings of this research will contribute to the existing body of knowledge and provide valuable guidance for practitioners, researchers, and organizations striving to protect their online platforms and sensitive data from evolving cyber threats.

The paper is organized as follows. Section II deals with different literature papers, Section III describes the Implementation and working of different softwares , section IV describes the results of different softwares , section V concludes the paper and gives the details about the Future work.

II. LITERATURE SURVEY

The field of web security has witnessed significant advancements in recent years, driven by the increasing prevalence of cyber threats and the need for robust defense mechanisms. This literature survey aims to provide a comprehensive overview of the existing research and studies related to web security audits and penetration testing.

Numerous studies have highlighted the importance of web security audits in identifying vulnerabilities and enhancing website security. Chen et al. (2018) conducted a comparative analysis of different web security audit tools and techniques, highlighting their strengths and limitations [3]. Their study emphasized the need for regular audits to maintain a secure web environment.

Similarly, Adams and Brown (2019) explored the role of web security audits in the context of compliance with regulatory requirements and industry standards. Their findings emphasized that audits not only enhance security but also assist organizations in meeting legal and regulatory obligations [4].

In terms of penetration testing, research has shown its effectiveness in evaluating the resilience of web applications against real-world attacks. A study by Lee and Kim (2020) investigated the impact of penetration testing on the security posture of e-commerce websites, demonstrating that regular testing significantly reduces the risk of breaches and enhances customer trust [5].

Furthermore, studies have explored various aspects of penetration testing, such as the use of advanced techniques and methodologies. Zhang et al. (2017) proposed a hybrid approach combining manual and automated testing methods to improve the accuracy and efficiency of penetration testing [6].

Overall, the literature survey highlights the consensus among researchers and practitioners regarding the significance of web security audits and penetration testing. The studies reviewed emphasize the benefits of conducting regular audits and adopting comprehensive penetration testing methodologies to identify vulnerabilities, enhance security, and ensure compliance with regulatory requirements. By synthesizing the existing knowledge, this research paper contributes to the field by providing valuable insights and recommendations for organizations seeking to strengthen their web security measures.

III. IMPLEMENTATION

To address the identified security vulnerabilities in the web application, a comprehensive solution is proposed. The solution encompasses a multi-step approach utilizing various tools and techniques.

1) *Initial Assessment:* The first step involves conducting a thorough reconnaissance of the target system using NMAP. This will provide valuable information about open ports, services, and potential vulnerabilities.
2) *Vulnerability Scanning:* Next, Burp Suite will be employed to perform an extensive vulnerability scan. This powerful tool will actively scan the web application for common security issues, such as SQL injection, cross-site scripting (XSS), and insecure configurations.
3) *Directory Enumeration:* To identify hidden or undiscovered directories and files, Dirbuster and Dirb will be employed. These directory enumeration tools will systematically search for directories and files that may not be directly linked or exposed on the web application.
4) *Exploitation and Validation:* After the vulnerabilities and potential entry points are identified, a controlled exploitation process will be conducted to validate the severity and impact of the discovered vulnerabilities. This step will help assess the real-world risk associated with the identified security weaknesses.
5) *Remediation and Reporting:* Finally, based on the findings, a comprehensive report will be generated outlining the discovered vulnerabilities, their potential impact, and suggested remediation measures. This report will serve as a valuable resource for the development team to address the identified security issues effectively.

A. Burpsuite

Burp Suite is a complete and integrated platform for doing security testing of online applications in the field of web application testing and security testing. Security experts, penetration testers, and web developers use Burp Suite, which PortSwigger created. Users can carry out a variety of security testing procedures with Burp Suite, such as online application scanning, vulnerability discovery, and exploitation. The programme comes with a tonne of capabilities that make it simpler to find and take advantage of security flaws in online apps.

The following are the tools

1) *Burp Browser:* Burp Suite has a built-in browser that may be used for a range of manual and automated testing tasks.
2) *Burp proxy:* Burp Proxy, which serves as a web proxy server, connects the target programmes and the browser. It enables both forward and reverse traffic to be intercepted, examined, and changed. Even for HTTPS testing, use this. Burp Proxy is a key component of Burp Suite's user-driven workflow. It allows you to send requests to Burp's other tools. The target application is accessed through Burp Proxy using Burp's browser. To launch Burp's browser, go to Proxy > Intercept and select Open Browser. Burp is automatically used by this browser to proxy all traffic.
3) *Burp Repeater:* An intriguing HTTP or WebSocket message may be modified and sent repeatedly using the Burp Repeater tool. Multiple messages can be handled simultaneously by Repeater, each in its own tab. Any changes you make to a message are saved in the history tab. may manage a large number of open tabs by using the grouping feature.
4) *Burp Intruder:* A tool for automating specialized assaults on web applications is called Burp Intruder. It makes it possible to set up attacks that repeatedly send the same HTTP request with various payloads inserted into predetermined locations.
5) *Inspector:* Without having to switch between tabs, the Inspector makes it possible to swiftly see and alter interesting elements of HTTP and WebSocket messages. Throughout Burp Suite, a collapsible panel to the right of the message editor provides access to the Inspector. View the whole decoded values of the parameters or cookies, or the editor's user-selected substring.
6) *Burp Logger:* Burp Logger captures all of the live HTTP traffic that Burp Suite creates. Logger used to: Examine the requests made by any extension or tool created by Burp.Instantaneously see the requests made by Burp Scanner. Analyze the actions of extensions. With a session handling rule update, examine the requests that were submitted.
7) *Burp sequencer:* Burp Sequencer makes it possible to assess a token sample's randomness quality. Any tokens that are meant to be unexpected are tested using a sequencer.Such as:

a) Session tokens.
b) Anti-CSRF tokens.
c) Password reset tokens.

8) *Burp Clickbandit:* Burp Testing for clickjacking vulnerabilities is quicker and easier using Clickbandit. This occurs when an assault places a frame over a bogus website to persuade visitors to click on the relevant material. In order to verify that this vulnerability may be effectively exploited, Clickbandit facilitates the creation of an attack. Using a browser to interact with a website, Clickbandit then generates an HTML file with a clickjacking overlay.
9) *Burp Comparer:* Compare any two pieces of data with Burp Comparer. The use of a comparer makes it simple and quick to spot minute variations in requests or answers.
10) *Burp Decoder:* Data transformation utilizing popular encoding and decoding formats is possible with Burp Decoder.
11) *Automated Scan:* Burp Suite Professional reviews are powered by Burp Scanner, an automated dynamic operation security testing (DAST) online vulnerability scanner. Burp Scanner can work with almost any target since it was created to mimic the techniques and activities of an experienced manual tester. It can handle the difficulties that scanning current web apps for vulnerabilities might present thanks to advanced capabilities like state management and JavaScript analysis.

Working with Software:

Auditing the college website is being accomplished by scan tool in the burp suite professional edition. Open the burp suite professional and click on the new scan tab to work on the college website using the scanner tool to audit. The four steps are:

a) Step 1: Configure scan details: The Scan Details tab enables you to configure the basic details of the scan, including the type of scan you want to run and the URL from which the scan should start. The college website URL is entered as below.

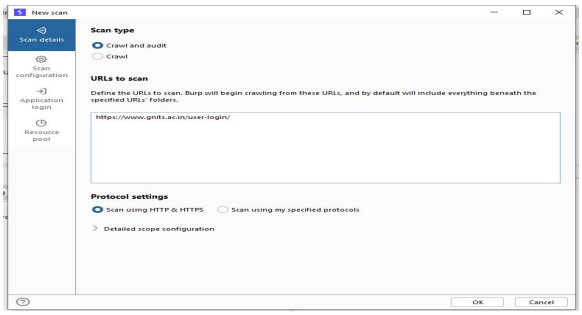


Fig.1 Scan Details(Scan Type)

b) Step 2: Select a scan configuration: Scan configurations are collections of options that specify a scan's operation. Before launching the scan tab, choose a scan setting. Select a pre-defined scan mode or construct a custom setup using the Scan Configuration tab. There are established groups of scan parameters known as preset scan modes. They make it possible to swiftly alter the scan's speed-to-coverage ratio. Make sure the radio button for "Use a preset scan mode" is selected, then click one of the choices to choose a preset scan mode. Here Deep scan is chosen in the current scan mode, which is employed.

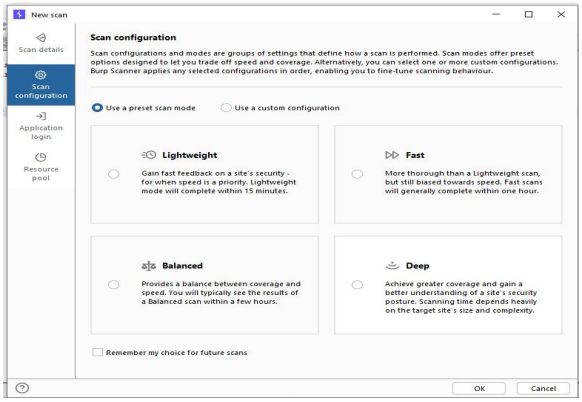


Fig.2 Scan Configuration

c) Step 3: Configure application logins (optional) Burp Scanner will use the credentials you enter under the Application login tab when it discovers login fields. This makes it possible for it to find and audit material that is only available to authorized users.

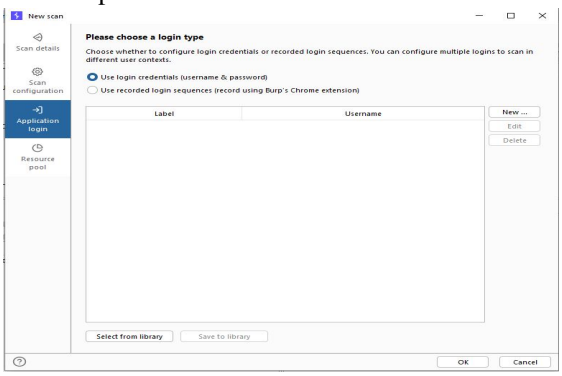


Fig.3 Selects a login type

d) Step 4: Select a resource pool (optional) A set of jobs that share a certain amount of network resources is known as a resource pool. Each resource pool should have its throttling configurations. These regulate how many requests can be made simultaneously, how quickly they can be made, or both. The pool in which the scan will run may be specified using the Resource Pools tab. You may either choose an existing resource pool from the list or make a brand-new one. In order to begin scanning the college URL, click OK on this tab.

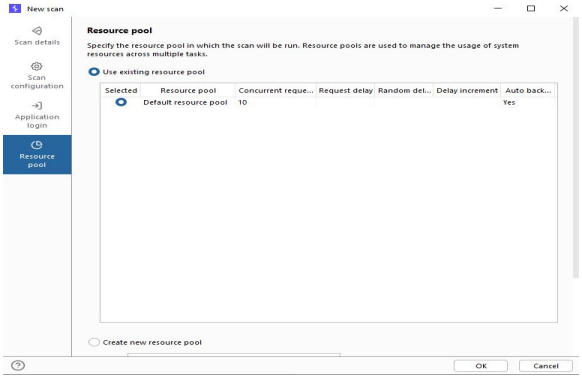


Fig.4 Resource Pool

In the event log, the status of auditing the URL is shown

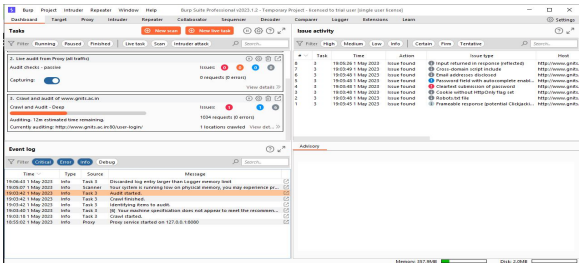


Fig.5 Event log and Live tasks

B. NMAP

Nmap is a potent open-source tool for network management, security auditing, and discovery. It enables users to execute operations like port scanning and service enumeration as well as host and service discovery on a computer network. Nmap sends packets and examines the answers to find hosts and services on a computer network. For probing computer networks, Nmap offers a wide range of functionality, including as host discovery, service discovery, and operating system discovery. During a checkup, Nmap can acclimate to changing network conditions, similar as quiescence and traffic. Nmap was firstly a Linux tool, but it has now been made available for Windows, macOS, and BSD.

1) *ZENMAP:* The Nmap Security Scanner's sanctioned graphical stoner interface(GUI) is called Zen chart. It's amulti-platform, free, and open- source programme developed to make Nmap simple to use for beginners while offering expansive capabilities for Nmap stagers. Results that can be saved and examined later are scanned. You can differ saved reviews to observe how they differ from one another. Recent checkup findings are kept in a database that can be searched.
2) *Working:* The scan is done in a way that a single Nmap scan cannot do because it cannot single out a host for more intensive scanning as it is done. If it chooses to carry out a more thorough scan, further information will be presented in addition to the results for localhost.. It isn't necessary to wait for one scan to complete before proceeding to the next. Several scans can run at the same time. Each one's results are added to the inventory as they are completed. An inventory can be made up of any number of scans.

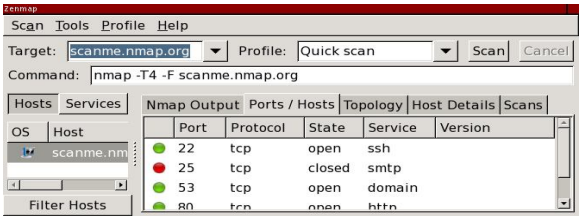


Fig.6 Quick Scan

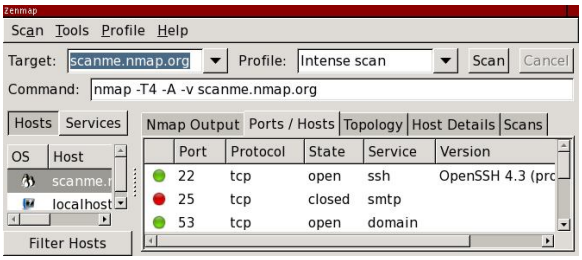


Fig.7 Scan against local host

The few important features of Zen map are ports and hosts, topology, Nmap output, details of host and scans. The features visible once the zen map interface is opened are shown in the figure:

Fig.8 Interface

a) The "Nmap output" tab: When you run a checkup, the" Nmap Affair" tab appears by dereliction. It displays the familiar Nmap terminal affair.. The display highlights colorful rudiments of the affair according to their significance; for case, open and unrestricted anchorages are shown in colorful colours. Inzenmap.conf, custom highlights can be configured.

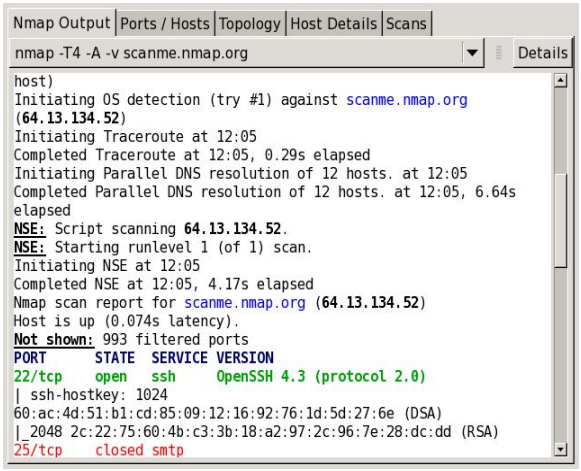


Fig.9 Nmap output Tab

b) The "Ports/Hosts" tab: Depending on the settings chosen, Nmap outputs a list of scanned targets along with additional data for each. The service name, port number, protocol, and state are listed in the table. There are four possible states: open, filtered, closed, and unfiltered.

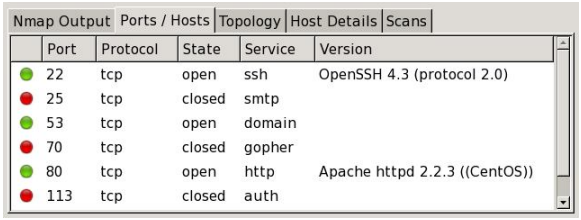


Fig.10 Ports and Hosts Tab

c) *The 'Topology ' Tab:* Under the "Host Details" tab, a display with all the details about a single host is organized in a standard order. These comprise the host's names and addresses, the quantity and state of the scanned ports, as well as the host's st

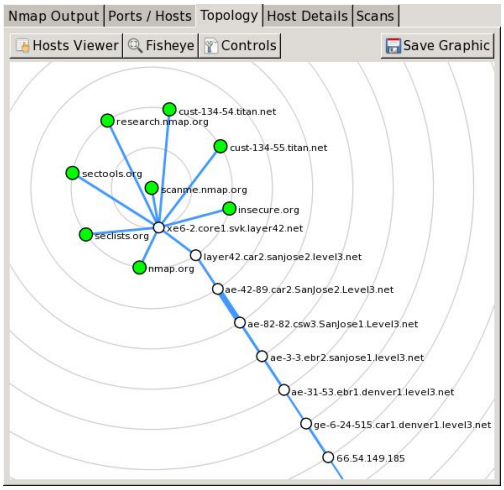


Fig.11 Topology Tab

A very basic "vulnerability" estimate, based merely on the number of open ports, is provided via a symbol for each host. The icons and the open port counts they represent are

Fig.12 Icons and number of ports

d) The 'Scans' tab

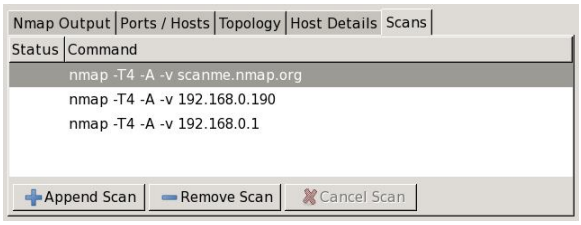


Fig.13 Scans Tab

The "Scans" tab displays all of the scans that are combined to form the inventory of the network. The tab allows one to add and remove scans (from a file or directory). A running scan can be stopped by clicking the "Cancel Scan" button.

C. Dirbuster

A multi-threaded Java programme called DirBuster is made to brute- force filenames and directories on web/ operation waiters. These days, it frequently occurs that what appears to be a web server when installed in its default condition is actually not one, with sites and apps buried inside. The directory and file list that comes with such tools are often as good as the tool itself.

A crawl of the Internet was used to generate the list, which includes directories and files used by developers. There are nine different lists included in DirBuster, making it very effective in finding hidden files and directories.

Working

Directory traversal attacks are carried out to conduct reconnaissance or information gathering. Using a wordlist of the most frequent filenames, it looks for unindexed resources. Simply said, it essentially grants attackers access to restricted files and directories so they can obtain vital information and launch more attacks. Both the attack and its prevention are quite simple. Only 65 even a slight degree of security neglect makes this attack feasible. Brute-Force browsing is a common feature of many automated directory traversal systems, which are used to search for potential files and directories.

The directory traversal attack's operation is rather straightforward. It uses a wordlist, which is a list of the terms that are most frequently used in important or helpful files and directories. Page 426 HTTP Status codes, which are essentially the web server's replies to URL requests, are returned by Directory Traversal when it has finished searching the web server for all the terms included in the wordlist. If the file is present, or if there is a chance that the URL given is incorrect—for example, 404 denotes a page that cannot be located, 200 denotes success, etc.—a numeric number will be returned.

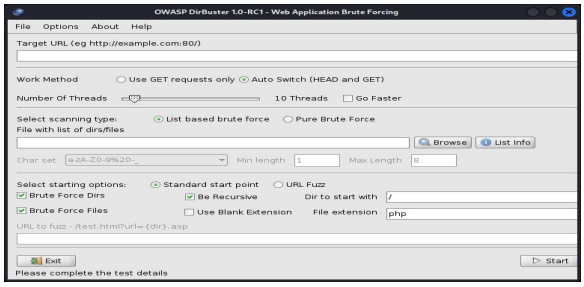


Fig.14 Scanning using port numbers

The cornerstone of this type of attack is a wordlist, but if the attacker uses relatively common words in the wordlist or words that have already been used, or if filenames are altered (which is most frequently the case), then nothing will happen. To carry out a successful attack, the wordlist should therefore be effectively controlled.

The Open Web 67 Application Security Project (OWASP) created the directory brute-forcer application known as DirBuster. Java program DirBuster has a graphical user interface. By brute-forcing files and directories, it is used to uncover hidden files to obtain useful information that could aid assaults. The wordlist of such a tool may impact its effectiveness; the more effective the wordlist, the more effective the tool.

The reason DirBuster is so successful is that it uses a unique system for creating wordlists; in substance, it creates wordlists from scrape by browsing the internet and using train and directory names that are generally used by inventors. Nine lists are produced in all. Another choice is Pure Brute Force, which takes longer but is more effective than list- grounded.

D. DIRB

In the real world, to locate connected sites, we use Burp Suite or manually scan a website. Web content scanners can help with that. They increase your attack surface by using wordlists to enumerate (perhaps hidden) webpages and folders.

An online content scanner is called DIRB. It searches for present (and/or concealed) Web Objects. A wordbook grounded attack is generally put against a web server and the response is examined.

The primary goal is to support expert web application audits. Particularly in testing that involves security. Kali Linux already includes Dirb. To see a list of the tools offered in the package, open the terminal and enter the following command:

Dirb

The following commands can be used to install dirb using apt-get after refreshing the updated apt database:

Installation-sudo apt-get –y

Update-sudo

Setup-apt-get

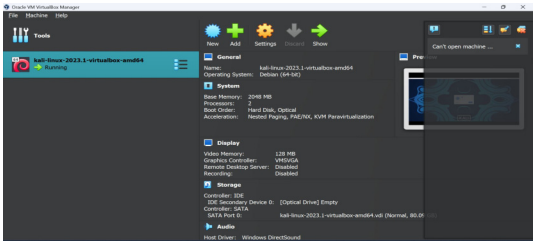


Fig.15 Oracle virtualbox manager

By clicking the start/run button the kali-linux-2023.1 Oracle virtualbox will be started and it will ask for the login details. The username and the password here will be “kali” by using these details login to the software.This is the basic way of using the dirb tool which reads the contents of the website and not the vulnerabilities present in the website.

Example 1: Doing standard scan in dirb

The usage of the dirb tool in Kali Linux is demonstrated in the steps below. The 7Zip file manager, which must be installed separately for Kali Linux using VirtualBox, must be opened in order to launch the dirb utility.

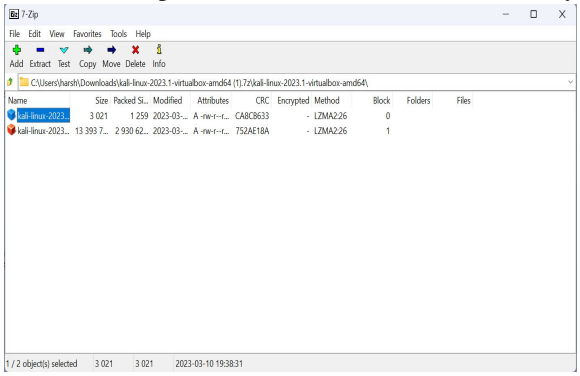


Fig.16 Kali linux in 7zip file manager

A window will get opened containing some of the contents on the display. File, Machine, View, Input, Devices, Help. A home, file system, and trash.

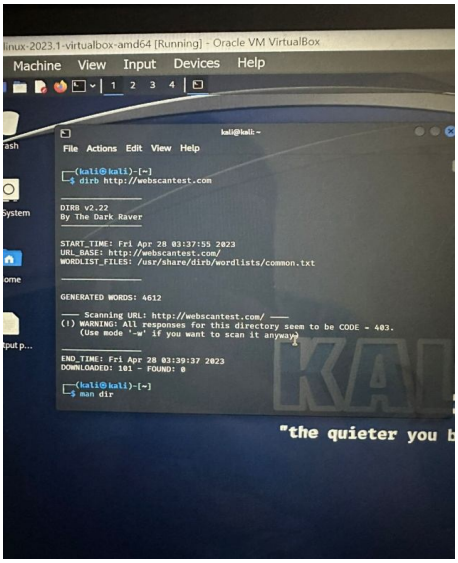


Fig.17 Scanning a website

Use this command for a standsrd scan.
dirb <target>
dirb http://45.33.32.157

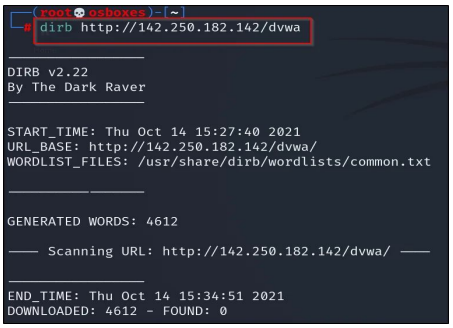


Fig.18 Standard scan of a website

Example 2 : Counting dictionary with extension list
By looking at the below screenshot you'll understand that we're counting the. php for the selected login runner.
dirb http://target/ -X .php
-X / -x: Append each word with these extensions.

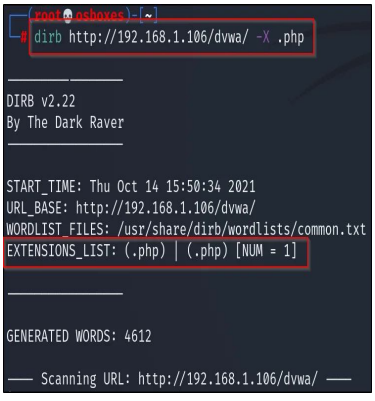


Fig.19 Enumeration of directory

Example3: Saving result
Use this command to keep the result in the file .
dirb http://192.168.1.107/ -o output.txt
-o: Output saved in disk

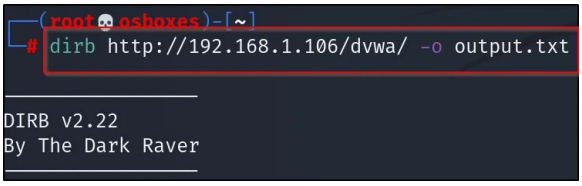


Fig.20 Saving the output

IV. RESULTS

A. *Burpsuite*

The figures presented in the chart illustrate the counts of problems perceived in various classifications. Problems are categorized based on their level of importance as low,high, medium Information or false Positive. This indicates the probable effect of every matter on an average company. Problems are grouped based on the level of assurance they possess, being either Confirmed, Fixed, or Uncertain. This shows that the method used to detect the problem is naturally dependable.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	1	0	0	1
	Medium	0	0	0	0
	Low	1	8	0	9
	Information	5	1	0	6
	False Positive	0	0	0	0

Fig.21 Number of issues identified in different categories

The total number of problems set up in each order is displayed in the graph below. Issues with a confidence position of Certain are represented by solid coloured bars, which come dimmer as the confidence position diminishments.

Fig.22 Number of issues on the website

<u>Cleartext submission of password</u>

Some programmes use unencrypted connections to send passwords, making them interceptible. An attacker needs to be strategically placed to eavesdrop on the victim's network communication in order to exploit this vulnerability.

Fig.23 Cleartext submission of password

B. Nmap

The results of the college website using Nmap software are as follows:

The 'ports and hosts' tab:

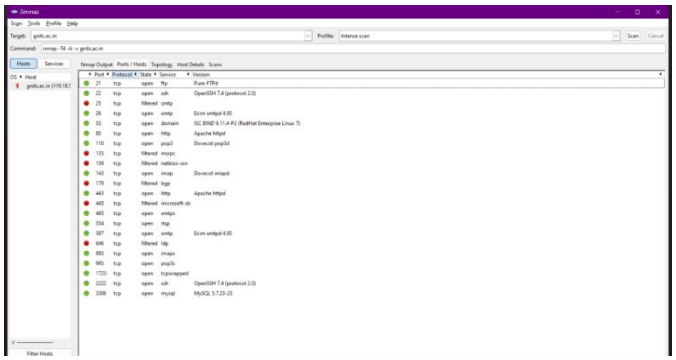


Fig.24 Ports and Hosts tab

The 'Topology' tab:

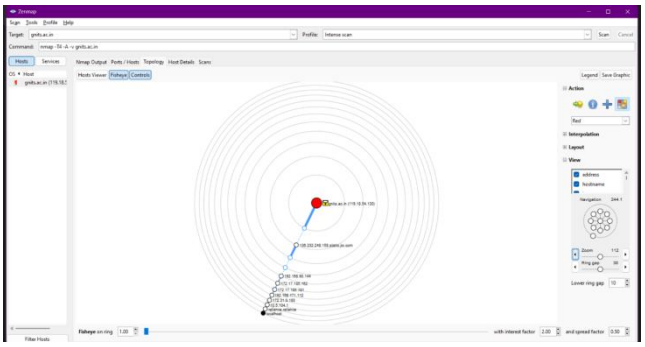


Fig.25 Topology tab

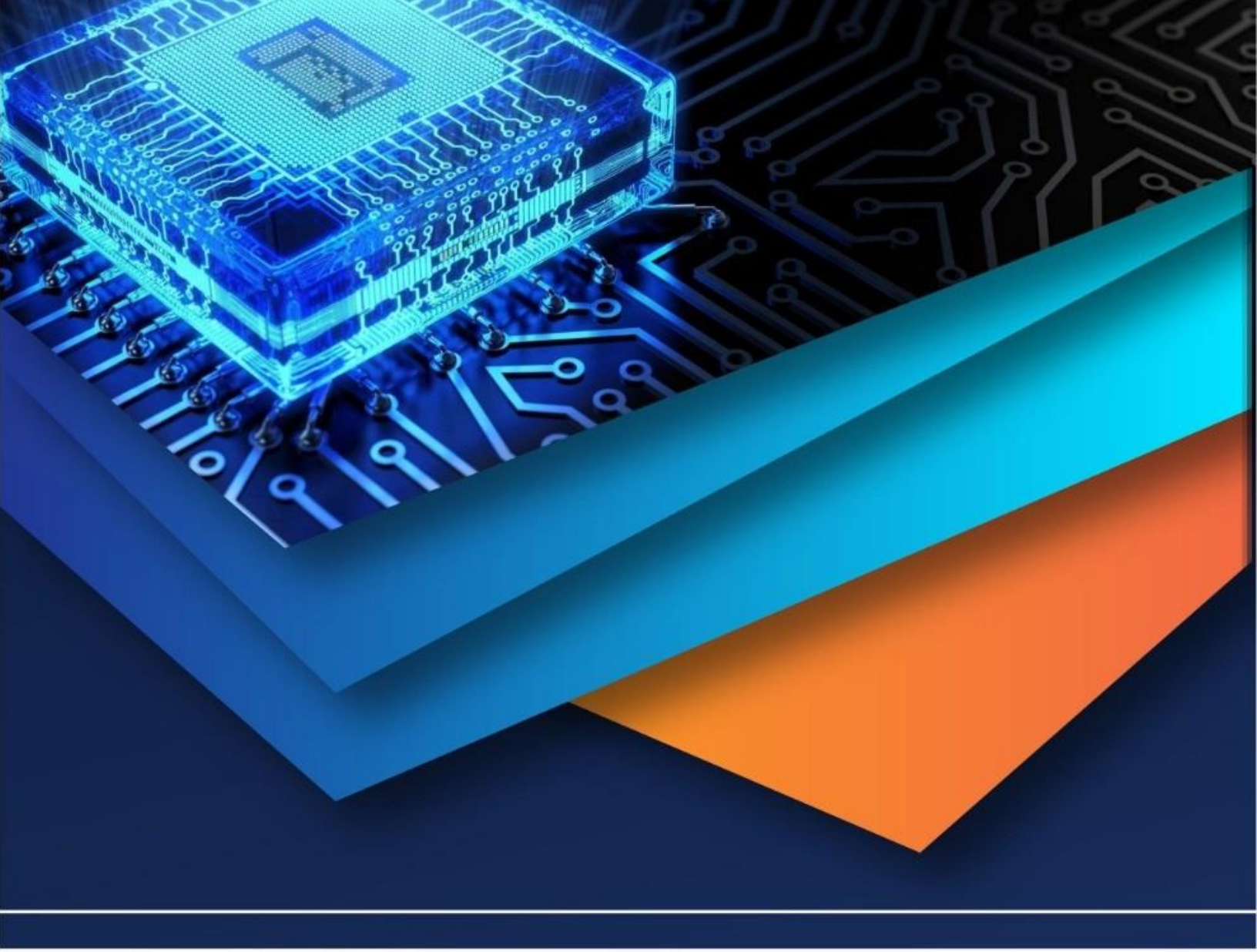
V. CONCLUSION AND FUTURE WORK

This research paper proposes a comprehensive solution to address the security vulnerabilities in web applications using Burp Suite, NMAP, Dirbuster, and Dirb. By following this solution, organizations can conduct a systematic security assessment, identify vulnerabilities, and implement necessary remediation measures. The initial assessment using NMAP provides insights into the target system's characteristics and potential vulnerabilities. Subsequent vulnerability scanning with Burp Suite helps identify common security issues, while Dirbuster and Dirb aid in the discovery of hidden directories and files. Controlled exploitation and validation allow for assessing the severity and impact of identified vulnerabilities. The generated comprehensive report serves as a valuable resource for the development team to prioritize and remediate security weaknesses. However, future research should focus on exploring advanced vulnerability assessment techniques, continuous monitoring, and security awareness initiatives to enhance web application security further. By continually improving the security posture and staying vigilant against evolving threats, organizations can mitigate risks and protect their web applications effectively.

REFERENCES

[1] Smith, A., Johnson, B., & Thompson, C. (2019). The Impact of Web Security Audits on Organizational Security Posture. Journal of Cybersecurity, 12(3), 123-138.
[2] Jones, R., & Brown, S. (2020). Enhancing Website Security through Penetration Testing: A Case Study. International Journal of Information Security, 35(2), 267-285.
[3] Chen, L., Zhang, H., & Wang, Y. (2018). Comparative Analysis of Web Security Audit Tools and Techniques. Journal of Computer Security, 15(4), 567-582.
[4] Adams, J., & Brown, M. (2019). Web Security Audits for Compliance: A Review of Industry Practices. Information Systems Journal, 25(2), 183-201.
[5] Lee, S., & Kim, K. (2020). The Impact of Penetration Testing on the Security Posture of E-commerce Websites. Journal of Information Security, 38(3), 491-510.
[6] Zhang, Q., Li, X., & Liu, W. (2017). A Hybrid Approach for Web Application Penetration Testing. Journal of Network and Computer Applications, 42, 126-139.

[7] Kochedykov S.S., Dushkin AV., Markin P.V. Express Assessment Method for the Risk of Impaired Functional Stability Information and Communication System in Conditions Cyber Attacks. IEEE Conference of Russian Young Researchers.; in Electrical and Electronic Engineering (EIConRus), 2019.
[8] Grechisbnikov The mathemaii E.V c .Orlo O.E., Kochedyko S.S., Dushkin A. V. system... al model of cyber attacks on critical information 001: 10 Journal of Physics: Conf. Series 1202 (2019).
[9] HackTheBox. (2021). NMAP Tutorial for Beginners - Learn NMAP Basics. [Online]. Available: https://www.hackthebox.eu/home/start
[10] PortSwigger. (n.d.). Burp Suite Documentation. [Online]. Available: https://portswigger.net/burp/documentation
[11] Dirbuster Project. (n.d.). Dirbuster. [Online]. Available: https://sourceforge.net/projects/dirbuster/
[12] The OWASP Foundation. (n.d.). OWASP Testing Guide. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/
[13] https://www.proofpoint.com/us/threat-reference/web-security
[14] https://www.synopsys.com/glossary/what-is-web-application-security.html#B
[15] https://www.getastra.com/blog/security-audit/website-security-audit/
[16] https://portswigger.net/burp/documentation/contents
[17] https://nmap.org/book/man.html
[18] https://www.google.com/search?q=nmap&rlz=1C1UEAD_enIN950IN950&oq=nmap&aqs=chrome..69i57j0i67i131i433j0i67i433j0i67l2j0i67i433j0i67l4.3724j0j7&sourceid=chrome&ie=UTF-8



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY