

**CSE 473 – NETWORK AND INFORMATION SECURITY**

**TERM PROJECT**

**PENETRATION TESTING / ETHICAL HACKING**

**MERT GÜRŞİMŞİR**

**1901042646**

# CONTENTS

[CONTENTS 2](#_Toc167740730)

[INTRODUCTION 3](#_Toc167740731)

[Definition 3](#_Toc167740732)

[Importance 4](#_Toc167740733)

[Justification 5](#_Toc167740734)

[THEORETICAL EXPLANATION AND OTHER STUDIES 5](#_Toc167740735)

[Studies 6](#_Toc167740736)

[Automated Source Code Scanning 6](#_Toc167740737)

[Advanced Web Application Testing Tools 6](#_Toc167740738)

[Container and Cloud Security 7](#_Toc167740739)

[Enhanced Network Security Tools 7](#_Toc167740740)

[Mobile Application Security 7](#_Toc167740741)

[IoT and Embedded Systems Security 8](#_Toc167740742)

[POPULAR STUDIES 8](#_Toc167740743)

[Automated Source Code Scanning 9](#_Toc167740744)

[Advanced Web Application Testing Tools 10](#_Toc167740745)

[Enhanced Network Security Tools 11](#_Toc167740746)

[Mobile Application Security 13](#_Toc167740747)

[Comparisons of 4 Most Popular Studies 14](#_Toc167740748)

[CONCLUSION AND SUGGESTIONS 15](#_Toc167740749)

[BIBLIOGRAPHY 16](#_Toc167740750)

# INTRODUCTION

## Definition

In today's world, where technology is developing day by day, the importance of our data and the security of our applications are gaining importance day by day. Companies also run various security tests to analyze how secure these applications are. We call these tests penetration tests. Penetration test is offensive form of security testing designed to provide a deep technical analysis of a target environment’s vulnerability to exploitation and attack.

Security experts follows a test process to conduct an authorized, simulated attack to evaluate security. At the end of these simulated attacks, reporting process starts and this reporting is also very crucial in these tests. Results in a report listing identified vulnerabilities and recommended mitigations.

Everyone may follow a different methodology but here is the list of basic high-level methodology steps [1]:

* **Reconnaissance**: In this step, tester tries to find as many information as possible about the environment that is going to be tested. This information can be got from the available sources such as search engines, or with using the tools.
* **Scanning**: In this step, tester uses port and vulnerability scanners to discover and fingerprint open ports and services in the environment.
* **Testing**: In this step, tester conducts both automated and manuel testing to probe in-scope applications in the environment. Here, tester may use provided credentials to emulate an authorized user.
* **Exploitation**: Before get into this step, vulnerabilities are detected during the testing step. So exploitation is simply exploiting them to determine their impact and scope. The tester will utilize any advantage obtained through exploitation to further penetrate the environment, adhering strictly to the defined scope and the agreed-upon Rules of Engagement.

Penetration testing is a critical practice in the field of cybersecurity. What is being done while this testing process is, again, simulating cyberattacks on computer systems, networks, or web applications to identify vulnerabilities that malicious actors could exploit. The goal of this testing process is improve security by finding and fixing vulnerabilities before they are exploited.

There are different types of penetration testing. These types are listed below:

* **Network Penetration Testing**: Primary goal here is identifying vulnerabilities in network, including servers, firewalls, switches, routers and all other network devices.
* **Web Application Penetration Testing**: Here, target is the web application as the name implies. Goal is uncovering security flaws such as SQL injection, cross-site scripting (XSS), and other web-based vulnerabilities.
* **Mobile Application Penetration Testing**: Involves testing mobile apps on platforms iOS and Android to find vulnerabilities at mobile environments.
* **Wireless Penetration Testing**: In this pentesting, wireless networks and protocols are examined to detect vulnerabilities such as encryption flaws, and unauthorized devices.
* **Social Engineering**: Simulates attacks that exploit human psychology. Humans are the weakest link so here the attacks such as phishing are used to gain unauthorized access to sensitive information.
* **Physical Penetration Testing**: Here the main focus is the physical security control such as locks, surveillance, and security personnel to assess if an attacker can gain physical access to critical infrastructure in the company.

All of these types are important in terms of security. Although, since there are more than 2 billion sites [2] on the world wide web, web application penetration testing is the main point of the pentesters concern.

## Importance

Penetration testing is an important component of cybersecurity for many reasons. The first one is identification of vulnerabilities. Pentesting helps organizations to identify weaknesses in their systems before attackers can exploit them. Second one is risk management. Discovering vulnerabilities helps organizations to manage and mitigate risks of vulnerabilities. This proactive approach enables organizations to reduce the potential impact of security breaches.

Penetration testing is an essential practice for identifying vulnerabilities, ensuring compliance, improving security posture, and managing risks. It provides a comprehensive evaluation of an organization’s defenses against cyber threats, helping to protect sensitive data and maintain the trust of customers and stakeholders.

## Justification

One of the advantages of ethical hacking is the fact that a broad range of threats are realized early and steps are taken to repair them. Since there are a wide variety of network threats from hackers, it is easier for a company, through ethical hacking, to deal with these threats before they become unmanageable, or before any damage to the network is done. [3]

Penetration testing is justified by its ability to identify and mitigate security vulnerabilities, manage risks efficiently and improve overall security of an organization. Pentesting also helps in cost savings and building trust for customers. While cyber threats are increasing day by day, ethical hacking remains an important practice for safeguarding organizational assets.

# THEORETICAL EXPLANATION AND OTHER STUDIES

Penetration testing, often abbreviated as pentest, is a process that is followed to conduct an in-depth security assessment or audit. A methodology defines a set of rules, practices, and procedures that are pursued and implemented during the course of any information security audit program. A penetration testing methodology defines a roadmap with practical ideas and proven practices that can be followed to assess the true security posture of a network, application, system, or any combination thereof. [4]

With the developing technology in the last 10 years, studies in the field of cyber security and especially penetration testing have also increased. With the developing artificial intelligence craze, companies started to use cyber security - artificial intelligence integrations.

As cyber threats continue to evolve, so must the techniques and tools used by ethical hackers. Continuous research and development are crucial to stay ahead of malicious actors. The field of penetration testing has seen significant advancements over the last decade, driven by the need to protect increasingly complex and interconnected systems. Research highlights the critical role of ethical hackers in identifying and mitigating security vulnerabilities across various sectors. As cyber threats continue to evolve, ongoing research and development are essential to enhance the efficacy and scope of penetration testing practices.

## Studies

### Automated Source Code Scanning

Fortify Software by Micro Focus, offers comprehensive static application security testing (SAST) tools that scan source code for vulnerabilities during the development process. It provides deep insights into code security, highlighting vulnerabilities early in the development lifecycle, which helps in reducing the cost and effort required to fix these issues later. The vulnerabilities that occur at the scan result can later deeply analyzed in the application, during the pentest. [5]

With cyber security blended with the DevOps methodology, which has become more common in recent years, a new concept in terms of security has emerged: DevSecOps.

Involving security in DevOps has been a challenge because traditional security methods have been unable to keep up with DevOps’ agility and speed. DevSecOps is the movement that works on developing and integrating modernized security methods that can keep up with DevOps. [6]

Integrating Fortify into pipelines created using Jenkins creates a preliminary protection to prevent possible security vulnerabilities in recent years. With the static scans created, it is very important for security to detect the code snippets that will cause findings in the application and replace these parts.

### Advanced Web Application Testing Tools

It is difficult and time consuming to analyze all the aspects of the application since applications getting more complex. In the last 10 years some advanced web application testing tools are improved more and more. Key developments in the past 10 years include the introduction of Burp Suite Professional and Enterprise editions, enhanced scanning capabilities, and the addition of machine learning algorithms to improve vulnerability detection. With the applications like Burp Suite by Portswigger, it becomes easier and faster to penetration testing because these applications provides some advanced tools. Burp Suite is one of the most popular tools for web application security testing. It offers a range of features including [7, 8]:

* Burp Scanner: Automated vulnerability scanner that identifies vulnerabilities such as SQL injection, cross-site scripting (XSS), and more.
* Burp Intruder: A tool for performing automated attacks to find and exploit vulnerabilities.

### Container and Cloud Security

With the developing cloud and container technologies, the security of these structures has become very important. The widespread adoption of containerization, exemplified by Docker, has transformed software deployment, enabling agile applications. However, its popularity invites malicious exploits, heightening security incidents in containerized environments. [9]

In the last 10 years, some innovations have been done in this area. One of them is falco by Sysdig. It is a project that focuses on runtime security for containers and cloud environments. It uses rule-based detection to monitor and alert on suspicious activity.

### Enhanced Network Security Tools

Tools are present since the late 1990s but their development has accelerated in the past decade with features like agent-based scanning, cloud integrations, and improved vulnerability databases. Detection of network vulnerabilities is used to determine weaknesses of the network, the risk evaluation of attacks, the diagnosis and suggestions to solve the problems. [10]

There are many tools that are studied in this field such as the nessus. It is developed for pentesters to use for vulnerability scanning. Its extensive plugin library allows for comprehensive scans covering a wide range of known vulnerabilities​. There are so many tools that are used in the penetration testing and these will be examined in the next header.

### Mobile Application Security

There are a total of 8.93 million mobile applications today [11]. Therefore mobile application security is very crucial. This area has gained importance recently in order to ensure rapid security in the field of mobile applications and to prevent possible losses by eliminating vulnerabilities. MobSF which is mobile security framework is an open-source automated security testing framework for mobile applications. It performs static and dynamic analysis of Android, iOS, and Windows mobile apps, identifying vulnerabilities. It has been actively developed since its inception around 2015 and many researches are being done in this topic.

MobSF is an essential tool for mobile application security due to its comprehensive analysis capabilities, ease of use, detailed reporting, and ability to integrate with development workflows. Its open-source nature and strong community support make it a reliable and continually evolving solution for identifying and mitigating security vulnerabilities in mobile applications.

### IoT and Embedded Systems Security

The proliferation of Internet of Things (IoT) devices and embedded systems has transformed modern life, bringing significant convenience and efficiency. However, these devices also introduce unique security challenges. The security of IoT and embedded systems is a critical aspect of modern cybersecurity. These devices' extensive deployment and integration into everyday life, combined with their potential to handle sensitive data and impact physical safety, underscore the importance of robust security measures.

Several studies have been conducted in this area. For the result of these studies, a tool is generated: Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. The tool has received numerous updates in the last decade, improving its ability to analyze and extract firmware images, which is vital for IoT security research.​ [12]

# POPULAR STUDIES

Cyber ​​security tools and projects that have been developed and are being developed as a result of the studies played an important role in ensuring the security of applications and networks today. The development of these tools, which enable penetration tests to be carried out faster, more effectively and more reliably, has become more important with the increasing number of applications and users in the past 10 years.

The most popular studies are the ones that integrate DevOps methodologies with the cyber security or integrate artificial intelligence with the cyber security. Here is the 4 most popular studies in the examined articles:

* Automated Source Code Scanning
* Advanced Web Application Testing Tools
* Enhanced Network Security Tools
* Mobile Application Security

## Automated Source Code Scanning

Static Application Security Testing (SAST) tools purport to assist developers in detecting security issues in source code. These tools typically use rule-based approaches to scan source code for security vulnerabilities.

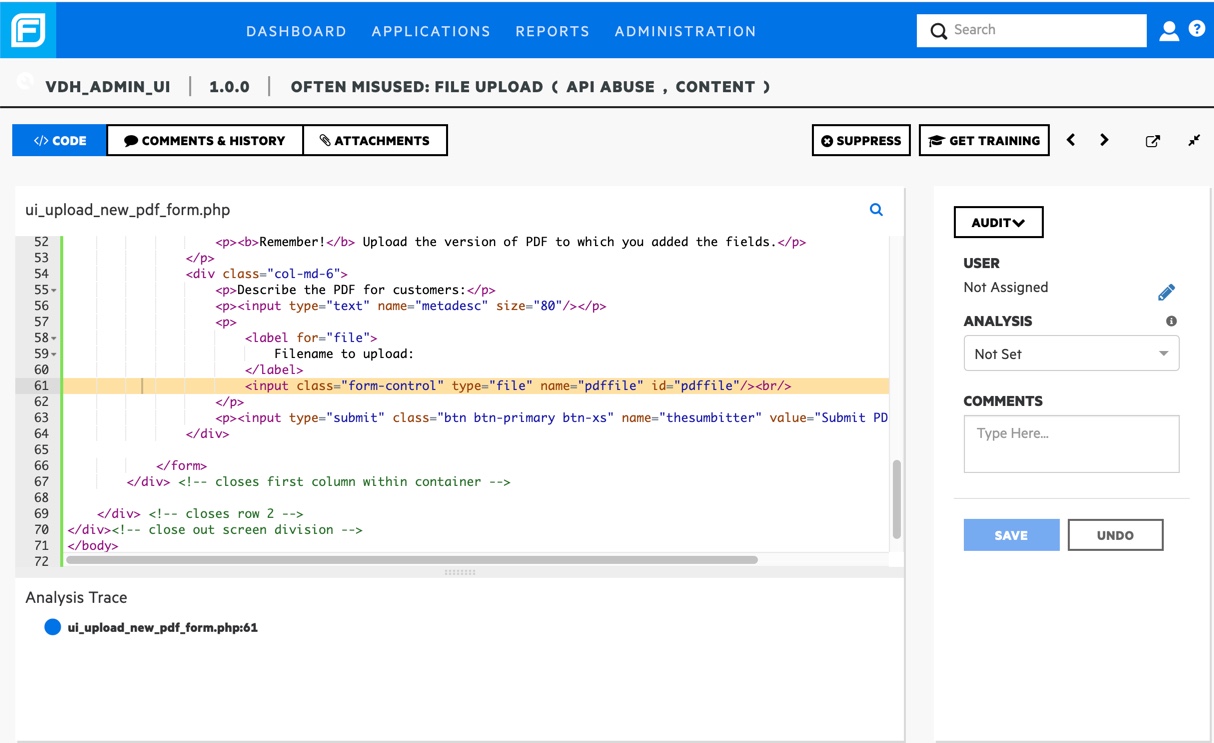
These tools are ideal for early development security with high privacy and integration with DevOps. They scan the source code to detect security vulnerabilities. It parses the code, constructs an abstract syntax tree (AST), and performs data flow analysis to identify insecure coding patterns, potential vulnerabilities, and compliance issues.

Techniques used:

* **Pattern Matching**: Utilizes predefined rules and patterns to match known vulnerabilities in the code.
* **Data Flow Analysis**: Tracks the flow of data through the application to identify how inputs are processed and where they might lead to vulnerabilities such as SQLi or cross-site scripting (XSS).
* **Control Flow Analysis**: Examines the execution paths within the code to detect logical vulnerabilities.

To make things faster and more efficient, DevOps integration is very popular method for this study. Therefore CI/CD pipelines are used here. Fortify can be integrated into Continuous Integration/Continuous Deployment (CI/CD) pipelines, enabling automated security testing during the build process. This ensures that security checks are a part of the software development lifecycle, allowing for continuous assessment and immediate remediation of identified vulnerabilities.

When scan is completed, tools generate detailed reports that list the vulnerabilities that are detected with their severity and potential impacts. Here users can also see the recommendations for fixing the issues.



*Figure 3.1: Static Application Security Testing Screen*

## Advanced Web Application Testing Tools

To make penetration tests easily practicable, people in cyber security field are studying new tools. The most popular and mostly used one is the Burp Suite. Security testing has become a vital part of software development in recent times. It helps us to identify vulnerabilities and loopholes in the software system and in turn fix the errors. Mainly there are two types of testing- manual and automated. Automated testing being advantageous over manual testing uses one of the many available tools Burp Suite [13].

With developing technology, time is very crucial. Therefore security tests should be done faster. Thanks to studies, penetration tests are being more efficient as well as being faster. Automated testing provides this approach.

CSRF PoC Generator can be given as an example for this. Formerly, what is needed to do for exploiting the CSRF vulnerability was creating a HTML page on your own. But with the help of Burp Suite and corresponding studies, now these HTML pages can be generated automatically.

A computer code with text

Description automatically generated with medium confidence

*Figure 3.2: Burp Suite CSRF PoC Generator [14]*

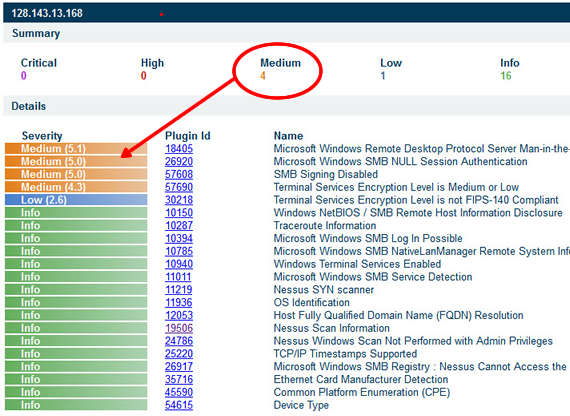
With the help of these web application testing tools, users can initiate scans on specific URLs or the entire application. Burp Scanner will crawl the application and identify potential vulnerabilities. As well as these automated scanning, manual testing and exploitation can also be done. With the help of Intruder pentester can configure attacks to test for specific vulnerabilities, such as SQL injection or XSS, by setting up payloads and attack positions and with the help of repeater pentesters can manually modify and resend requests to explore the application’s responses and identify security issues.

Thanks to all these studies that is held in the field of advanced web application testing tools, penetration testing becomes more efficient day by day.

## Enhanced Network Security Tools

As it is mentioned earlier, there are methodology steps for the penetration testing. For each of these steps, tools are created with the help of studies in this topics. These tools are designed to scan, identify, and mitigate vulnerabilities in networked systems.

There are many tools that are currently being developed more and more with the help of studies that is being conducted. First one is nessus. Nessus is primarily a vulnerability scanner used for identifying security weaknesses in networks and systems. It performs network scans, service detection, vulnerability assessment, and configuration audits.



*Figre 3.3: Example Nessus Report [16]*

Second one is nmap. Nmap (Network Mapper) is a versatile tool used for network discovery and security auditing. It performs host discovery, port scanning, service detection, and OS detection.

Third one is gobuster. Gobuster is a tool used for brute-force attacks on web directories and DNS subdomains. Primarily used to discover hidden resources within web applications.

SQLMap is another tool that is being studied in recent years. SQLMap is an open-source tool used for automating the detection and exploitation of SQL injection vulnerabilities. Automates the process of detecting and exploiting SQL injection flaws. SQLMap does exist for more than 10 years but it is integrating with other tools such as Burp Suite to designate more efficient automatic testing.

These are examples of tools that is used for network security. These tools complement each other and can be used together to provide a robust security testing framework for various environments.

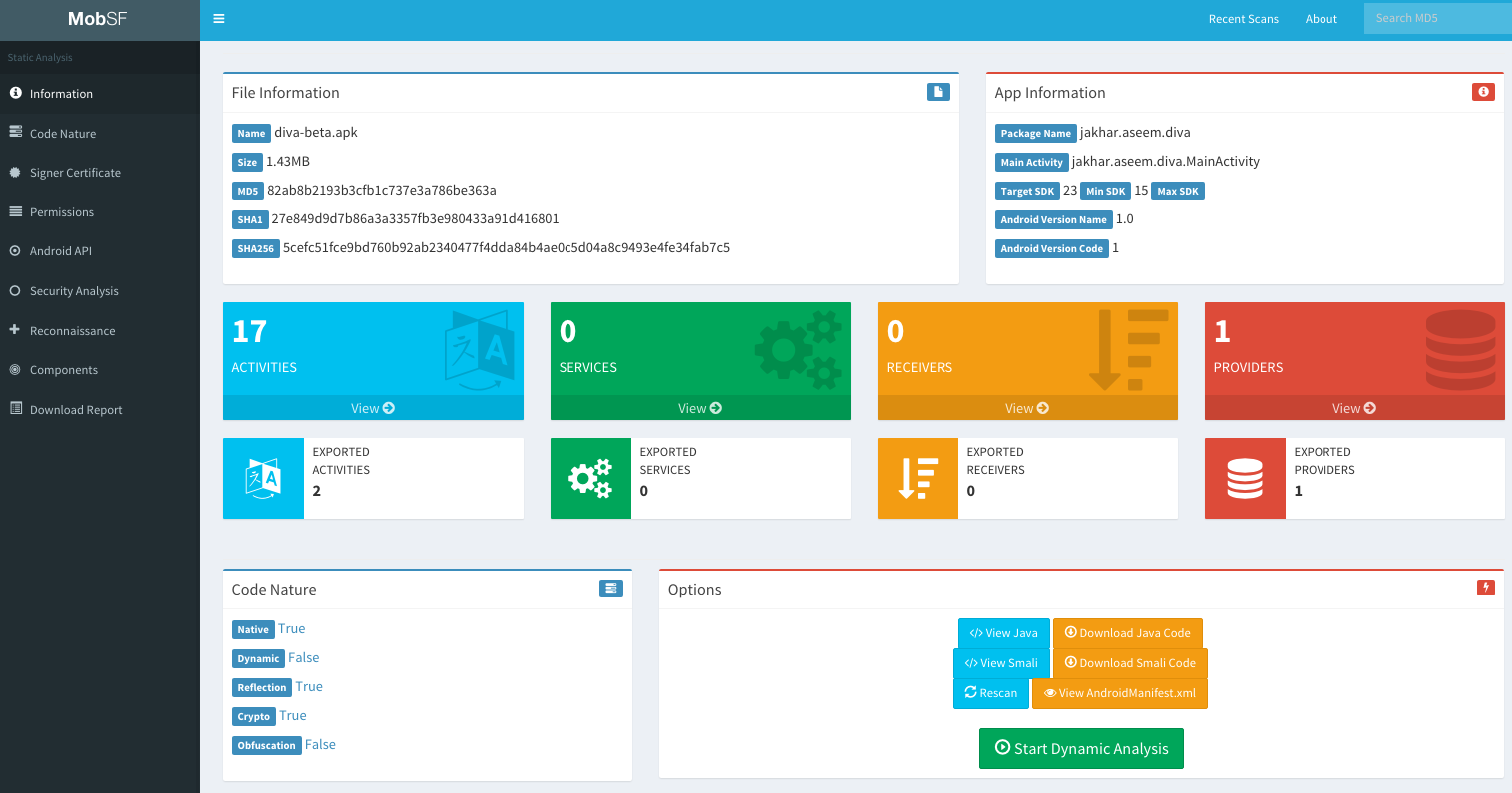
## Mobile Application Security

Mobile application security is very important in cybersecurity with the so much use of mobile devices and the sensitive data they handle. Penetration testing in this domain involves a thorough examination of mobile apps to identify and mitigate vulnerabilities that could be exploited by malicious actors. This process consists of both static and dynamic analysis.

Studies conducted that doing both static and dynamic analysis increase the efficiency of penetration testing when we compare the speed and reliability of the results. Static analysis involves examining the mobile application's source code, binaries, or bytecode without executing the application. Dynamic analysis, on the other hand, involves executing the mobile application in a controlled environment to monitor its behavior in real-time.

As it is mentioned earlier, today, the technology trend is DevOps and therefore designing the process from development to operation as effectively and quickly as possible is very important. Here, we can include security tests in terms of cyber security into the process and prevent possible vulnerabilities. Integrating mobile application security testing into CI/CD pipeline ensures that security checks are part of the regular development process.

MobSF is being used actively in the sector as a result of the studies conducted in penetration testing field. Tools like Mobile Security Framework (MobSF) play a significant role in mobile application penetration testing. Its integration capabilities with CI/CD pipelines and detailed reporting features make it a valuable tool for developers and security professionals aiming to secure mobile applications effectively.



*Figure 3.4: Example Mobile Application Security Test Report*

## Comparisons of 4 Most Popular Studies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **METRIC** | **SAST** | **WEB APP TESTING TOOLS** | **NETWORK SEC TOOLS** | **MOBILE APP SECURITY** |
| *Privacy* | HIGH | MEDIUM | HIGH | MEDIUM |
| *Performance* | HIGH | MEDIUM | HIGH | MEDIUM |
| *Complexity* | MEDIUM | HIGH | LOW | MEDIUM |
| *Flexibility* | MEDIUM | HIGH | MEDIUM | HIGH |
| *Integration* | HIGH (DevOps) | HIGH (Manual & Automated) | MEDIUM | HIGH (Mobile DevOps) |
| *Ease of Use* | MEDIUM | MEDIUM | HIGH | MEDIUM |
| *Detection Accuracy* | HIGH | HIGH | HIGH | HIGH |
| *Coverage* | SOURCE CODE | WEB APPLICATIONS | NETWORKS AND SYSTEMS | MOBILE APPLICATIONS |
| *Automation* | HIGH | MEDIUM | HIGH | HIGH |
| *Manual Testing Support* | LOW | HIGH | LOW | MEDIUM |
| *Cost* | HIGH | MEDIUM TO HIGH | MEDIUM | LOW (Open Source) |
| *Community Support* | MEDIUM | HIGH | MEDIUM | HIGH |

As it can be seen, each studied field offers distinct advantages and is suited for different security needs:

* SAST: Ideal for early development security with high privacy and integration with DevOps.
* Web Application Testing Tools: Excels in flexible and comprehensive web application testing with strong community support.
* Network Security Tools: Perfect for network security with ease of use and high performance.
* Mobile Application Security: Provides thorough mobile application security with strong community backing and flexibility.

# CONCLUSION AND SUGGESTIONS

The studies that are read shows that advancements in technology and the increasing complexity of cyber threats in the world have necessitated the enhancement of penetration testing and ethical hacking tools. In the modern world, tools like Fortify, Burp Suite, Nessus, and MobSF play crucial roles in ensuring strong cybersecurity across various platforms.

As technology continues to develop, integrating security into every stage of the development lifecycle becomes more important day by day. Tools like Fortify show the importance of static application security testing (SAST) early in the development process. This integration helps identifying and mitigating vulnerabilities in the source code before they can be exploited, significantly reducing the cost and complexity of fixes.

To gain stronger security structure, organizations should do penetration testing at regular intervals. Finishing the whole project and then doing penetration test is not a good idea because there might be so many security vulnerabilities that need to be fixed. Instead the methodologies like DevSecOps should be used.

Security should be integrated early in development. Incorporating tools like Fortify into the CI/CD pipelines allows for continuous security checks, providing immediate feedback to developers and catching vulnerabilities early in the development process. This proactive approach ensures that security is built into the software from the start.

Studies show that tools such as nmap, mobsf, sqlmap, fortify, burp suite do a very good job in their fields. However, each of them is an advanced tool for micro tasks. Instead, in the future, applications can be developed that capture requests, automatically run tools such as sqlmap and nmap, and automate penetration testing processes. With this way, it can be combined that the studies mentioned in this report.

Implementing these suggestions can help penetration testers leverage the strengths of each study.

# BIBLIOGRAPHY

[1] “M Safe Computing.” University of Michigan Ross School of Business, 13 May 2024, safecomputing.umich.edu/.

[2] “Web App Development: A Detailed Guide.” JayDevs, 25 Sept. 2023, jaydevs.com/web-app-development-a-detailed-guide/.

[3] “Ethical Hacking Research Paper Example | Topics and Well Written Essays - 1250 words”, n.d.

[4] “Kali Linux - Assuring Security by Penetration Testing” Lee Allen, Tedi Heriyanto, Shakeel Ali. April 2014.

[5] Yang, Jinqiu, et al. "Towards better utilizing static application security testing." 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP). IEEE, 2019.

[6] Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: a multivocal literature review. In Software Process Improvement and Capability Determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4–5, 2017, Proceedings (pp. 17-29). Springer International Publishing.

[7] Tomás de J. Mateo Sanguino, "Enhancing Security in Industrial Application Development: Case Study on Self-Generating Artificial Intelligence Tools", Applied Sciences, vol.14, no.9, pp.3780, 2024.

[8] R. Bouafia, H. Benbrahim and A. Amine, "Automatic Protection of Web Applications Against SQL Injections: An Approach Based On Acunetix, Burp Suite and SQLMAP," 2023 9th International Conference on Optimization and Applications (ICOA), AbuDhabi, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICOA58279.2023.10308827.

[9] D. Mubanda, N. Mandela, T. Mbinda and C. Ayesiga, "Evaluating Docker Container Security through Penetration Testing: A Smart Computer Security," 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), Greater Noida, India, 2023, pp. 415-419, doi: 10.1109/ICCSAI59793.2023.10421124.

[10] KUSHE, R. Comparative study of vulnerability scanning tools: Nessus vs Retina. Security & Future, 2017, 1.2: 69-71.

[11] “How Many Apps Are There in the World.” BankMyCell, 8 Apr. 2024, [www.bankmycell.com/blog/number-of-mobile-apps-worldwide](http://www.bankmycell.com/blog/number-of-mobile-apps-worldwide).

[12] S. Lee and E. -S. Cho, "Toward Firmware-Type Analysis Using Machine Learning Techniques," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, pp. 977-978, doi: 10.1109/COMPSAC.2018.00172.

[13] A. Kore, T. Hinduja, A. Sawant, S. Indorkar, S. Wagh and S. Rankhambe, "Burp Suite Extension for Script based Attacks for Web Applications," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 651-657, doi: 10.1109/ICECA55336.2022.10009116.

[14] Creating a CSRF POC using Burp Pro?. Enciphers Labs Pvt Ltd. (n.d.). https://www.enciphers.com/web-app-security/creating-a-csrf-poc-using-burp-pro

[15] Vavkamil. (n.d.). Vavkamil/awesome-bugbounty-tools: A curated list of various bug bounty tools. GitHub. <https://github.com/vavkamil/awesome-bugbounty-tools?tab=readme-ov-file>

[16] How to read A nessus report - uva its. (n.d.). <https://virginia.service-now.com/its?id=itsweb_kb_article&sys_id=75e70054dbb553404f32fb671d9619d5>

[17] ALANDA, Aide, et al. Mobile application security penetration testing based on OWASP. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020. p. 012036.