National College of Ireland

WHITE BOX TESTING XML INJECTIONS IN WEBSITES

MSc Research Project
MSC. Cyber Security

Varun Rangaraj
Student ID: X19213573

School of Computing
National College of Ireland

Supervisor: Niall Heffernan

National College of Ireland MSc

Project Submission Sheet School of

Computing

Student Name:	Varun Rangaraj		
Student ID:	X19213573		
Programme:	MSc. In Cyber Security	**Year:**	2020-2021
Module:	Internship		
Lecturer:	Niall Heffernan		
Submission Due Date:	22-08-2021		
Project Title:	**White Box Testing XML Injections in Websites.**		

Word Count: 6759 **Page Count:** 17

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Varun Rangaraj

Date: 22-08-2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Abstract

The research is based on white box testing process that helps to analyze coding of software for verifying the input as well as output floor of the particular software. Moreover, the white box testing process also helps to analyze internal structure and design process of software and it also helps to increase the security of software. In this regard it has been observed that as every field has their own pros and cons, the other side of cyber security leads to damage to the reputation of business by several cyber-attacks. There are several problems related to cyber security in terms of applying XML injection methods into it. XML security is considered as one of our networks protocol types and the XML based network protocol helps to analyze structured data that are included within formatted information. The researcher has chosen positivism philosophy to identify the impact of white box testing in XML injection Websites. The research has followed the deductive approach as a research approach as it has been found to be effective for this study. Through this research approach, the casual relationships between the variables of the research can easily understand the concept of the research. Implementation of white box testing has been done in this project by considering some future work as well.

1. Introduction

1.0 Research background

The research is based on white box testing process that helps to analyze coding of software for verifying the input as well as output floor of the particular software. Moreover, the white box testing process also helps to analyze internal structure and design process of software and it also helps to increase the security of software. In this regard it can be said that hacker have the ability to exploit front end web application as well as backend web application in this server as there is an increased number of complexities in between communication channels. In addition to this it has been observed that web applications play an important role with the interaction process of optimum usability and security of software and internal Web services.

The research also includes the XML injection process. The mentioned processes are being applied while the white box testing is going on in any web application or software. The particular XML injection process helps any web application or software to make sure about the presence of malicious content in it. The research helps to figure out required solutions that can be effective for white box testing and can help to enhance white box testing efficiency for improving its usability towards any software or web application.

1.1 Problem Statement

The white box testing is related to cyber security and it has been noticed that cyber security is considered as one of the important factors that helps to protect various kinds of information and data. Moreover, the research helps to point out different solutions that are effective for increasing the improvement of white box testing usability. The improvement that is needed for enhancing white box testing process to users are also being discussed in this report. In this regard it can be said that the white box testing is considered as one of a cyber-security technology and it consists of potential threats from XML injection and the XML injection is considered as a cyber-security issue that is observed in various websites [4]. Different potential solutions that are helpful for mitigating cyber security issues and are able to give advanced experience to users are also being discussed in this research.

It has been analyzed that the white box testing is considered as the safest cyber security Technology, and it also makes sure about the execution of a system with meeting specific features

and also validates security features. The main issues regarding cyber security in terms of XML injection in websites are being discussed in this research. The major logic of the XML program and the way XML injection can be able to cause different malicious content that is being injected into a resulting message can be observed in this research. Moreover, it has been observed that the impact of white box testing is needed to mitigate or overcome the threats that come from XML injection in websites [8].

1.2 Research Aims and Objectives

Research Aims

The research helps to develop an overall idea on XML injection on websites and the effect of XML injection that can cause malicious content in web applications or software. Moreover, the research put focus on the effect of white box testing to overcome threads coming from XML injection on websites.

Research Objectives

- To determine the efficiency of white box testing as a cyber-security technology
- To analyze cyber security issues that occurs due to XML injection on website
- To signify the impact of white box testing to overcome XML injection threats in websites
- To recommend strategies that can help to increase the effectiveness of white box testing towards XML injection

1.3 Significance of the research

The research sheds light on the effectiveness of white box testing to overcome XML injection threat that occurs in websites and it causes malicious content in websites. Cyber security helps to defend or restore any operation eating system. Moreover, it has been observed that cyber security is also considered as a critical method because various types of records regarding exploitation information confidential data and government data are included in it [9]. The significance of cyber security is enhancing day by day and the world is intending on this particular Technology as it provides security to data. Moreover, it can be said that the white box testing approach is also considered as a part of cyber security Technology.

The white box testing helps to test the potential of positive as well as negative behavior of any software and it also involves data control flow, information control flow, coding, and fault management of any system. In addition to this the white box testing can also be done to analyze the execution of code and to detect the exploitable vulnerabilities. On the other hand, it has been observed that the XML injection is considered as a cyber-security issue that occurs in websites [11]. In this regard it has been observed that the white box testing includes programming language but in case of black box technique it helps in XML injection method by providing special advantage as the black box testing does not need source code to reduce any negative impact of XML.

2. Literature Review

2.0 Effectiveness of Cyber security and XML issues in website

Cyber security is considered as a key Technology nowadays as it protects different categories called 8 hours from being stolen or damaged. This data includes sensitive data, intellectual data, government related data, industry information related data, and health information related data and so on [28]. In this regard it can be said that as a cyber-security gives ample amount of security towards data and helps by providing security to protect data hence the data is being handled by the particular web server. In this regard it has been observed that as every field has their own pros and cons, the other side of cyber security leads to damage to the reputation of business by several cyber-attacks. There are several problems related to cyber security in terms of applying XML injection methods into it. XML security is considered as one of our network protocols types and the XML based network protocol helps to analyze structured data that are included within formatted information [18]. Several issues encountered by XML network protocol suggest text related issues, signature issues, and spurious validation errors and so on.

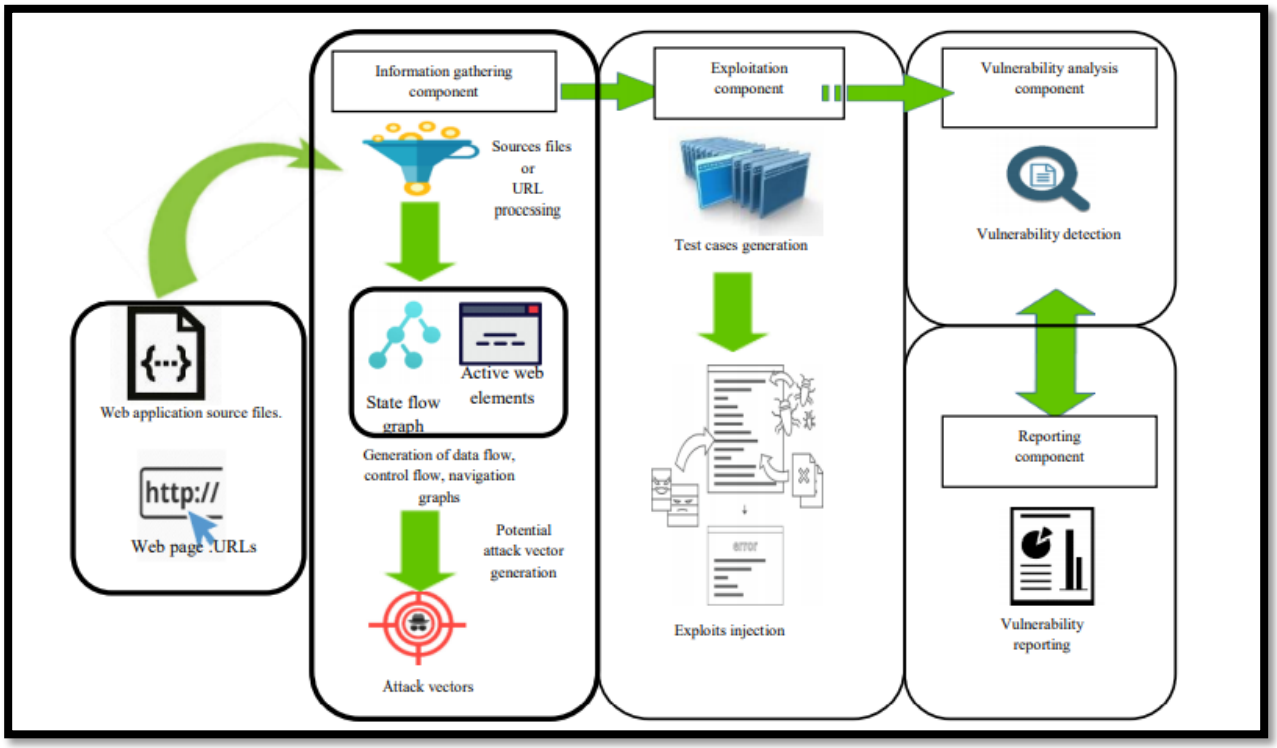


Figure 1: Web application security scanner
(Source: Acquired from [28])

The XML is used for transporting data from an application to another application. In this context it has been analyzed that the websites sometimes take content for their respective web pages from XML files. This is the process or way of including hypertext mark-up language and extensible markup language to work together. The XML files includes both tags as well as text file the extensible markup language (XML), is occupied with simple text-based format that represents structured information. There are several problems or issues related with "extensible markup language" or XML. As stated by [22], the XML is verbose. The world bows pattern indicates that whenever any user is trying to type in Raw XML there needs to be opening as well as closing tags. Moreover, the user needs to think on the tags every time even the editor tries to help the user. On the other hand, these tags get in a way of scanning for reading the particular text. This issue can be resolved by applying order using specialized XML editor.

As argued by [32], XML needs user specification for any particular language. As computers have not the ability to think of any particular language that is needed for any technical work. Hence the user needs to specify a particular language in XML for processing with any work. Moreover, the XML doesn't have any semantics. In this regard it has been observed that in XML syntax there is no meaning related to data that is marked up [16]. Moreover, the XML instructs users and asks their permission to close all the tags that have been opened by them. In XML it has been observed that there is no application processing system and more over the XML it's too dependent on HTML to read or write in a browser.

2.1 White box testing

The white box testing is considered as a software testing process. White box testing techniques, the internal structure of data, designing as well as coding of any software are being tested and also being verified with the flow of input output [26]. The key concept of using white box technique is to observe through the box concept.

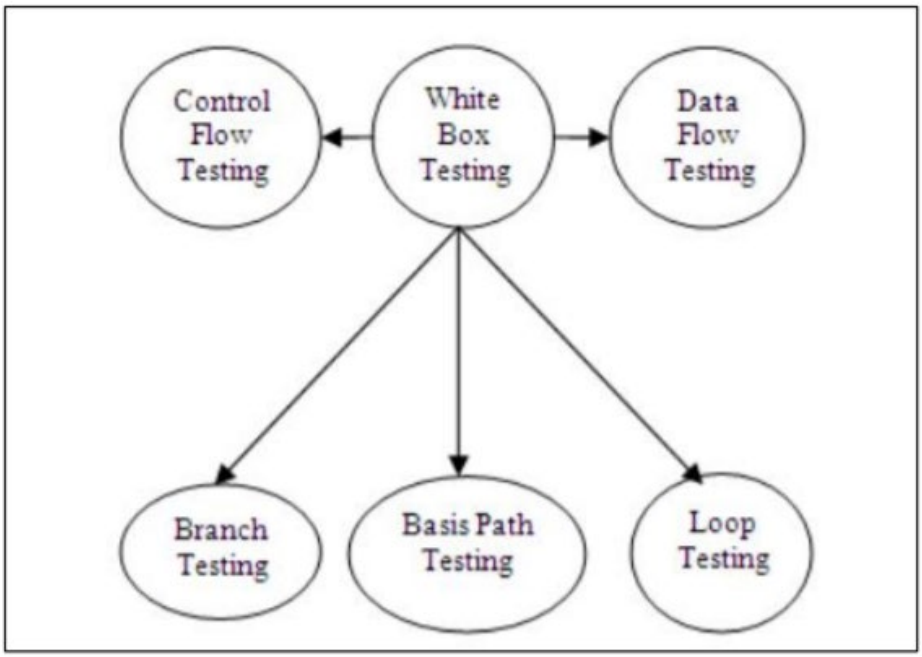


Figure 2: Technique variation in white box
(Source: Acquired from [31])

The white box testing also allows users to analyze the internal structure of a particular data. The major benefit of using white box testing is that it needs better knowledge of internal software that is going to be tested or that is under test. Moreover, the white box testing also allows to find out hidden errors or internal errors that cause harm to the internal functionality.

2.2 XML injection

XML injection can be stated as the attack technique that has been used to compromise or manipulate the logic of the service or application of XML. The injection of unintended content or structures of XML into the XML message has the ability to alter the intended logic of that application. In addition, XML injection can be considered as the reason for the insertion of the malicious content into resulting documents or messages. With the successful attack of XML injection, an attacker can steal a complete database or can log in as an administrator of a website [5]. Other issues regarding security like DOS and XSS attacks can occur with the malicious XML injections.

Determination of an application is vulnerable or not to XML injection can include attempts to examine whether that application is sanitizing the incoming data. The attack of XML injection can be needed to ensure the user input is successfully sanitized and managed before it has been granted to reach the code of the main program [10]. The best approach can be to consider all the input of the user to be unsafe and properly sanitize or monitor the input.

2.3 The ways through which white box testing help to overcome XML injections websites

The key purpose of the method of security testing is actually to ensure the system robustness in the face of failures of regular software or malicious attacks. White box testing has been performed based on that knowledge of the ways through which a system can be implemented. White box testing can impact XML injections websites. In the case of White-box testing, different kinds of search techniques are used to cover many structural targets at the same time (Moradin and Håkansson, 2016). In addition to that, those techniques can be easily applied and adapted in the detection of XML attacks in the application of front-end web. In the testing of traditional white-box, it can be seen often that multiple test cases with separate lengths are actually equivalent in terms of the scores of objectives.

As a result, prioritizing the shorter tests at a similar level of coverage helps to generate more concise tests. In terms of XML injection, the target TO can be easily covered through only one single solution and the other shorter strings of equivalent cannot be present. Therefore, it can be easily understood that the effectiveness of white-box testing to overcome the XML injections websites is that it helps in the detection of the viruses [21]. In addition to that, it has the intention to affect the information of the website and build the internal functions that can be regarded to be important for the efficient and effective website formulation without any kinds of issues regarding cyber security.

The testing of a white box requires knowing what makes software insecure or secure, the ways through which to be thought, such as the attacker and the ways through which different techniques and tools of testing can be used.

3. Methodology

3.0 Introduction

This portion has discussed different kinds of tools and methods to collect data and conduct data analysis based on those collected data. This portion has shown which research approach and philosophy have been followed. This portion has discussed the reason behind choosing the research tools and methods to fulfil the objectives of the particular study.

3.1 Research Philosophy

The researcher has chosen positivism philosophy to identify the impact of white box testing in XML injection Websites. Positivism philosophy relies on experience as the valid origin of knowledge. In addition to that, the findings of research in the positivist studies are not only descriptive; besides that, they have fewer chances of facing issues regarding in-depth research [2].

3.2 Research Approach

The research has followed the deductive approach as a research approach as it has been found to be effective for this study. Through this research approach, the casual relationships between the variables of the research can easily understand the concept of the research. The concepts regarding White box testing and XML injection can be measured easily and generalized the findings of the research to a certain context [24].

3.3 Research Design

In this case, descriptive research design has described the view and perception in a detailed manner [33]. Descriptive research designs have been considered as easy, cheap and quick for conduction. Descriptive research design has given an in-depth view of the topic. It is effective to identify the characteristics of white box testing and XML injection websites.

3.4 Tools and Techniques

Linux software has been used for XML injections and white box testing.

3.5 Data analysis

The researcher has implemented the tabular and graphical analysis of data to analyze the gathered information. Linux software has helped to visualize the influencing factors of white box testing in the XML injection website.

3.6 Summary

The research has focused on white box testing via Linux software to get authentic, valid and relevant information for the research of understanding white box testing for XML injection websites. White box testing is playing a vital role to use variety of techniques for software testing and that is effective to cope with different issues and problems at the same time. It is identified that control flow testing and data flow testing are effective to reduce different issues and problems.

Chapter 4: Design specification

Cyber security is very important in this modern world where the internet has been used widely in every sector. Therefore, it is a mandatory task to provide cyber security to a system. In this matter, a white box testing operation has been proposed in order to provide security to a web application or software. As per the views of Li *et al.* (2017), white box testing is also known as glass box testing or clear box testing. This method has been used in the process of software testing in order to provide cyber security to the system. On the other hand, it can be said that the design of this testing environment required some techniques and those are control flow testing, data flow testing, branch testing, statement coverage, decision coverage, and path testing. In addition, it has been found that this method has been used in different levels of the testing process including unit testing,

integration testing, and system-level testing of software.

In the process of white box testing, programming skills and coding knowledge are required for the test cases. Therefore, it can be said that a tester plays an important role in this process of providing cyber security to a website or web application. Cyber security is very important in order to avoid any type of important data being stolen or stolen from the web application or software [6]. In this matter, providing better security is a mandatory process to avoid any kind of data leak or damage. On this note, it can be said that these are the design specifications of this testing method in order to provide cyber security to a website or web application.

Chapter 5: Implementation

Implementation of white box testing is a very important process and, in this matter, the below-mentioned figure also provides a graphical representation of white box testing method from unit to system testing. The main process of implementing this testing method is as follows:

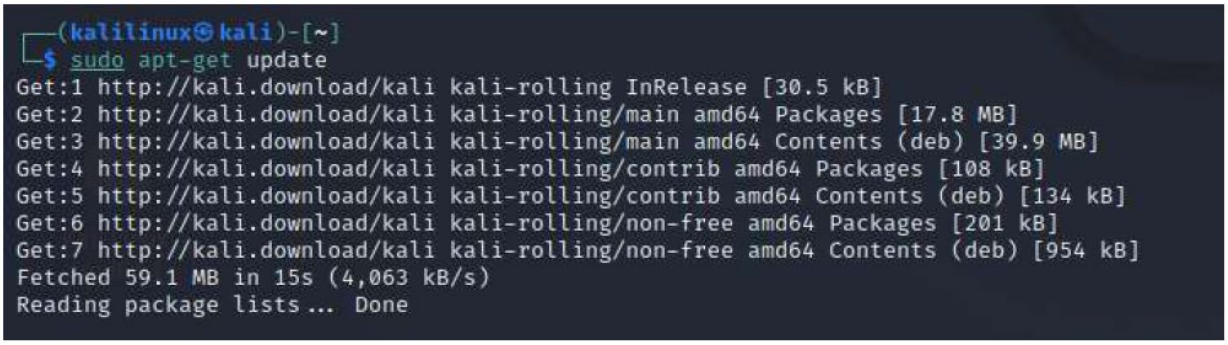
- Performing risk analysis to guide the whole process of white box testing activities. This process also can be said as threat modelling.
- Development of a proper strategy that will allow achieving the testing goals [25].
- Developing a proper testing plan in order to organize the subsequent process of testing [14].
- Preparation of the environment to execute the test properly.
- Execute all the test cases.
- Developing a report based on the result of this testing process.

There are some artefacts that are related to this white box testing process and those are risk analysis report, source code, security specification, quality assurance, and design documentation. According to the views of [12], the reporting mechanism of the white box testing process is very important to evaluate the effect of this process. However, in this matter, all the artefacts of this process are mentioned below for more clarification.

- Source code is one of the more important artefacts of this process in order to perform white box testing. Without implementing proper code, this testing process cannot be performed properly in any website or web application to provide cyber security. In this matter, Linux coding is required for the proper implementation of the method.

- Design and architectural risk analysis should be the main things in order to guide all the testing related activities. In this process, test planning, test case creation, test technique selection is also very crucial as part of the white box testing process.
- The process of documenting design is very essential as well in order to understand and develop effective use cases for this method. If the design documentation is not sufficient enough, then the test team could face many difficulties to answer each and every question related to the cyber security of a particular web application or a website.
- Security specifications are also important in this case. It is very important to understand the security functionality of the white box testing method. In this matter, it can be said that if the

security requirements are lacking, then the testing team could not obtain the information required from various stakeholders related to a web application or website.



- In this matter, it has been found that the security tested should have access to quality assurance of this proposed method. The process of quality assurance is very important in order to increase the acceptability of this white box testing method in providing cybersecurity.

There, it can be said that there are important artefacts of this white box testing method. As per the comment of [30], without implementing proper code, this testing process cannot be performed properly in any website or web application to provide cyber security. In this matter, Linux coding is required for the proper implementation of the method. If the design documentation is not sufficient enough, then the test team could face many difficulties to answer each and every question related to the cyber security of a particular web application or a website. In this process, test planning, test case creation, test technique selection is also very crucial as part of the white box testing process. This method has been used in the process of software testing in order to provide cyber security to the system [17]. On the other hand, it can be said that the design of this testing environment required some techniques and those are control flow testing, data flow testing, branch testing, statement coverage, decision coverage, and path testing. In addition, it has been found that this method has been used in different levels of the testing process including unit testing, integration testing, and system-level testing of software.

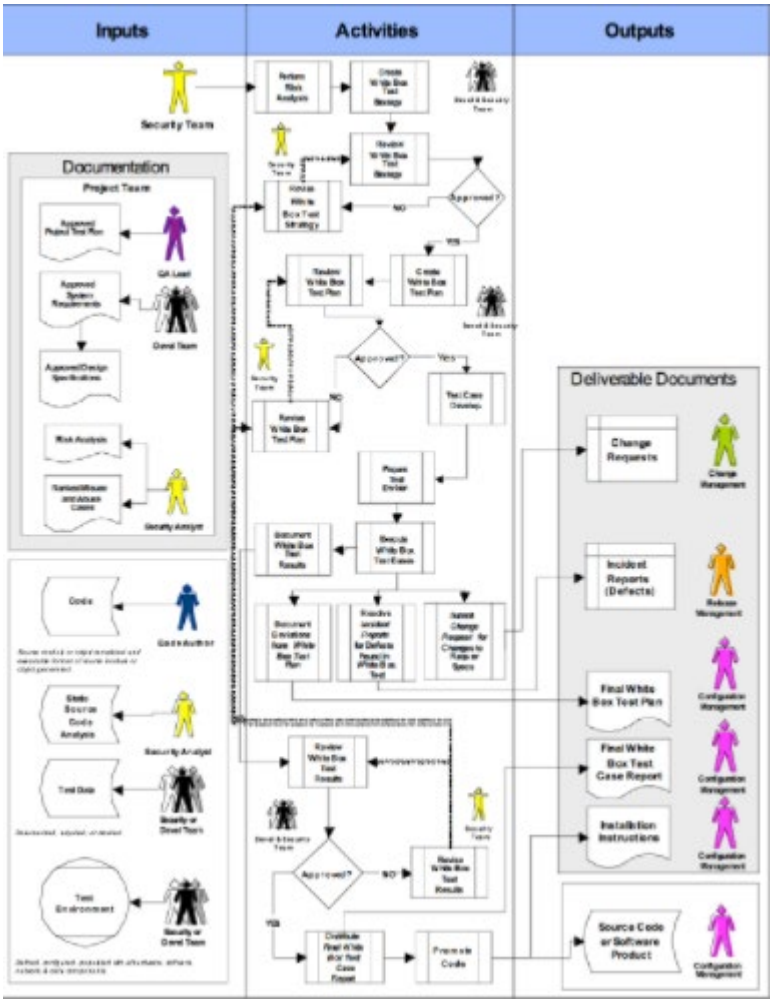


Figure 1: The process of security testing
(Source: [7]**)**

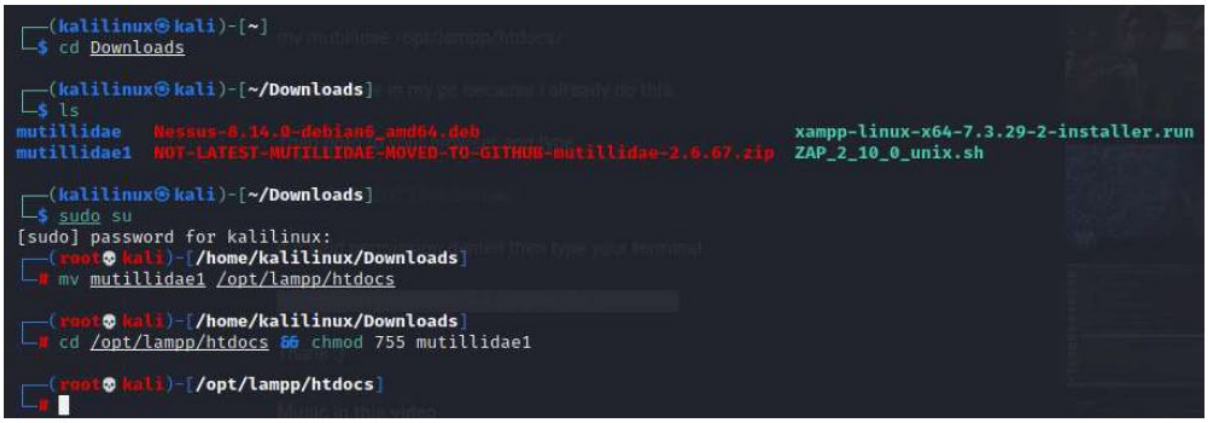
From this figure, it can be said that the first process of performing white box testing is developing a test strategy based on the risk analysis. In this matter, it can be said that the main purpose of defining test strategy is to define the major activities in this testing environment. As mentioned by [23], this normally includes testing technique, testing scope, environment, and skills of the test staff. In this matter, it can be said that test strategy has been divided into some other parts and those are test plan, test case development, test automation, test environment, and test execution.

Test plan

In this matter, it can be said that the test plan should manifest the strategy of this process. It has been mentioned before that the main purpose of having a test plan is to follow the testing process properly. As per the views of [29], the test plan of the white box testing method generally includes both high level and low-level data interpretation for providing cyber security to the software or web application. Therefore, it has been found that test planning is important for the administration and reporting at the time of performing this test smoothly.

Test case development

The development of test cases is also very important in the process of executing this white box testing. In this matter, it can be said that the development of test cases depends on different case descriptions. However, risk analysis, test plan, and test strategy help to develop test cases according to the requirements of the process [15]. The process of test application is very crucial in this matter in order to develop the test cases according to the criteria of a web application or software. All the members of the testing team are responsible for developing the test cases.



Test automation

Automation is all about automatic work. In this case, test automation of this process provides automated work on managing tests and repeating some past tests. Therefore, the development of test automation in this process is really a critical task incorporated with the process of providing cyber security to a web application or software. As per the comment of [27], the establishment of the environment for testing is important for test automation. The establishment of test automation is also important to identify any type of run time error and invalid data structures. However, it has been found that white box testing also requires some software development in order to support some particular tests.

Test environment

Testing of different phenomena of white box testing required a proper environment. It is very much critical to manage and establish a proper test environment in order to increase the effectiveness and efficiency of this testing process [1]. If the design documentation is not sufficient enough, then the test team could face many difficulties to answer each and every question related to the cyber security of a particular web application or a website. Therefore, the test environment is very important for white box testing.

Test execution

Execution of the test is all about running all the test cases in order to generate results. In this process, the first step of execution is validating the infrastructure which is required to run the test. This infrastructure is very important for encompassing test automation and the test environment required for white box testing. In this process, all the issues related to this execution have been sorted by the performed team for a seamless process of execution.

Chapter 6: Evaluation

This method has been used in the process of software testing in order to provide cyber security to the system. In this matter, providing better security is a mandatory process to avoid any kind of data leak or damage. On this note, it can be said that these are the design specifications of this testing method in order to provide cyber security to a website or web application. In addition, it has been found that this method has been used in different levels of the testing process including unit testing, integration testing, and system level testing of software [20]. This chapter provides the evaluation of the results of white box testing in a particular web application or software in order to provide cyber security. Therefore, the researcher of this project implemented this proposed technique in order to provide security.

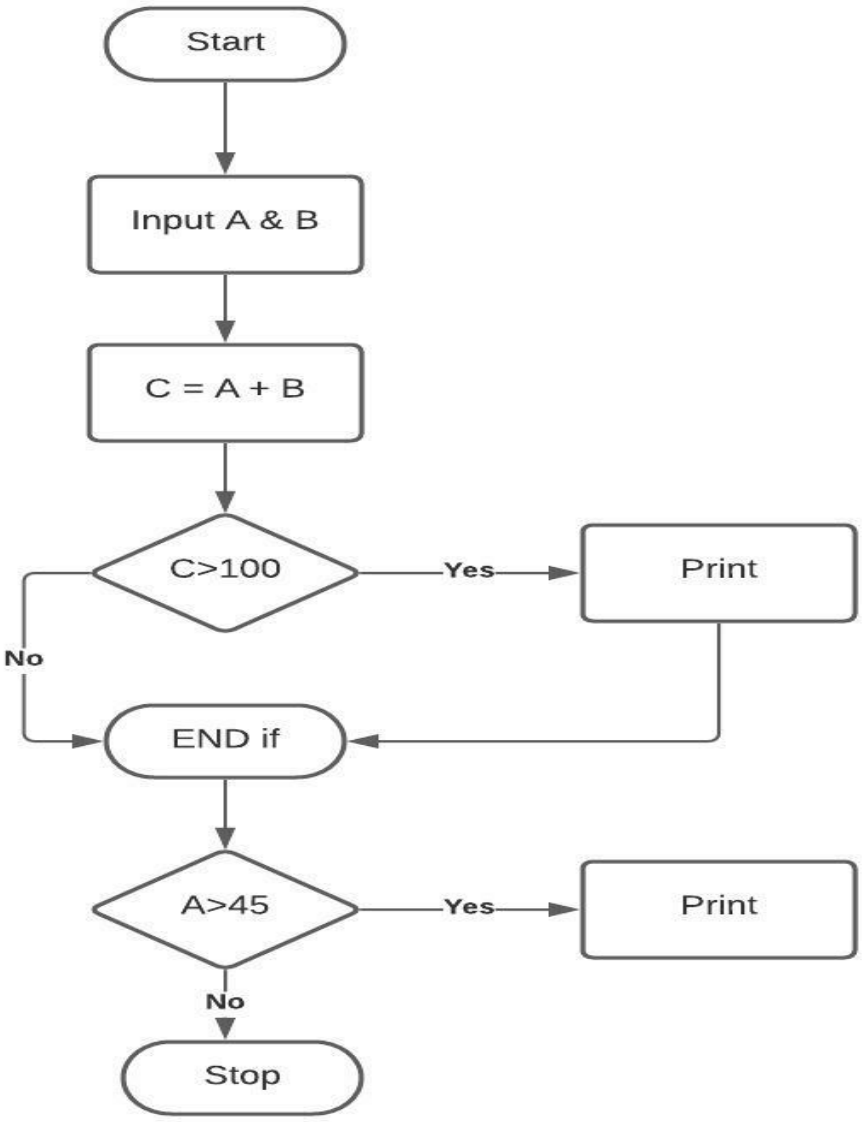


Figure 3: Flowchart of this proposed system
(Source: Created by author)

This figure shows the flowchart of performing white box testing on a website or a web application. In this matter, a Linux code has been implemented in order to evaluate this proposed white box implementation system in order to provide cyber security for protecting data and sensitive information properly.

```
INPUT B + A
C = B + A
PRINT "It's done"
END IF
IF A> 45
PRINT "It's pending"
END IF
```

In this matter, two test cases have been defined by the researcher in order to form this white box testing. In the first test cases, A = 50 and B= 60.
In the other case, A= 55 and B= 40.
However, the researchers of this project have decided to use the Veracode testing tool in order to identify and solve any type of software flaws quickly. This tool is also very acceptable in performing security testing of a desktop as well. According to the vision of [3], this tool supports programming languages like .NET, JAVA, and C++. In this matter, it has been found that white box testing has been done in this case in order to ensure all the independent paths. In addition, it also helps to verify all the logical decisions whether it is true or false in values. On the other hand, white box testing allows the researcher to perform all the execution of loops of an internal data structure of the website or web application.
In this matter, it has been also found that XML has been used in this testing for transporting data from one application to another. In this matter, the researcher of this project also analyzed that sometimes a website can take information from respective website pages as an XML file. However, XML injections are considered as one of the common applications in white box testing for providing cyber security to a website or web application. As per the comment of [13], XML normally depends on the HTML in order to read and write. Cyber security is very important in this modern world where the internet has been used widely in every sector. Therefore, it is a mandatory task to provide cyber security to a system. In this matter, a white box testing operation has been proposed in order to provide security to a web application or software. Implementation of white box testing is a very important process and, in this matter, the research of this project also provides a proper evaluation of the testing method of white box testing by representing the result with the help of this declared flowchart method.

6.1. Advantages

By performing the white box testing in order to provide cyber security, the researcher of this project found some advantages of this testing method. The main benefit of using white box testing is it helps to optimize the source code therefore; hidden errors are identified properly. As an example, it can be said that the researcher of this project easily uncovered the default formation of source code by a proper error handling mechanism. In this matter, it can be said that it helps to increase the productivity of testing. In addition, the other benefit of performing white box testing is it helps to execute some black box tests as well which is very hard to set up. All the test cases in the white box testing method are easily automated compared to the other testing methods. According to the views of [19], white box testing is more thorough compared to other testing

methods. In this matter, it can be said that this testing method covers all the code paths properly for thorough analysis. For this reason, the researcher of this project implemented this testing method for providing cyber security of a website. The other advantage of this white box testing is that it can be used in the SDLC phase as well without GUI.

The most important point of this discussion is this white box testing method helps to reduce cost and time as well. This testing method helps the researcher to assume quickly and validate proper design decisions. Therefore, it can be said that this method helps to increase the productivity of work. In addition, this method also helps to find any type of unintended features in a web application or website. In this matter, [6] said that security testing is not about identifying any type of vulnerabilities but also examining the useless functionality of a website or web application. Access to the source code allows the researcher to find more deeply about any type of gap in the security system of a web application or website.

6.2. Disadvantage

There are some disadvantages of this white box testing method, in this matter, it has been found that it is very time-consuming for the case of applications with large scale programming. Therefore, it can be said that it is useful for short types of applications that have less programming. In addition, it has been also identified that this testing is very complex and expensive as well. On the other hand, it has been also found that this testing method can also cause production errors as this is not a detailed process. In this matter, it can be said that performing testing methods requires skillful programmers who have a detailed understanding and knowledge of different programming languages and the process of implementation.

Chapter 7: Conclusion and future work

Thus, it can be concluded that white box testing using XML injections is a very complex process and requires a high level of understanding of programming knowledge in order to offer cyber security service to a particular web application or website. In this project, white box testing has been done on a website in order to provide cyber security. In this process, different types of outcomes have been found by the researcher which has been discussed in this research paper. Execution of the test is all about running all the test cases in order to generate results. In this process, the first step of execution is validating the infrastructure which is required to run the test. This infrastructure is very important for encompassing test automation and the test environment required for white box testing. In this process, all the issues related to this execution have been sorted by the performed team for a seamless process of execution. In this research project, the aims and objectives of this project have been achieved properly in order to determine the efficiency of the testing method as an important cyber security technology. On the other hand, issues related to XML injection also have been analyzed properly in this paper.

Cyber security is very important in this modern world where the internet has been used widely in every sector. Therefore, it is a mandatory task to provide cyber security to a system. In this matter, a white box testing operation has been proposed in order to provide security to a web application or software. In this matter, there are several possibilities for future work on this topic. There could be some new research on reducing the cost of this proposed testing method as it has been found that it is very much costly and time consuming as well. Therefore, could be another approach for future work to reduce the complexity of this testing method by implementing some new technology. That can reduce the time and cost as well and increase the efficiency of this method. In addition, it can be also said that some future work could be done on the topic of recommending some strategies in order to increase the effectiveness of white box testing methods by XML

injections in websites. Finally, there are future works, which can be performed in the near future in order to improve the cyber security of a website by performing white box testing.

Reference

1. Aboelfotoh, S.F. and Hikal, N.A., 2019. A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. JOIV: International Journal on Informatics Visualization, 3(2), pp.157-176.
2. Aithal, P.S., 2017. ABCD Analysis as Research Methodology in Company Case Studies. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *2*(2), pp.40-54.
3. Ateşoğulları, D. and Mishra, A., 2019. White Box Test Tools: A Comparative View. International Journal on Information Technologies & Security, 3, pp.79-90.
4. Awlarijal, A.N., Almaarif, A. and Budiono, A., 2020. Vulnerability Assessment for Basic Data of Education Website in Regional Government X–A Black Box Testing Approach. *FoITIC*, pp.163-168.
5. Bravenboer, M., Dolstra, E. and Visser, E., 2020. Preventing injection attacks with syntax embeddings. *Science of Computer Programming*, *75*(7), pp.473-495.
6. Cabana, A., Charrier, C. and Louis, A., 2019. Mono and multi-modal biometric systems assessment by a common black box testing framework. Future Generation Computer Systems, 101, pp.293-303.
7. Cisa.gov (2017). White Box Testing. Available at: https://us-cert.cisa.gov/bsi/articles/best-practices/white-box-testing/white-box-testing [Accessed on: 16.08.2021]
8. Elkatatny, S. and Mahmoud, M., 2018. Development of new correlations for the oil formation volume factor in oil reservoirs using artificial intelligent white box technique. *Petroleum*, *4*(2), pp.178-186.
9. Fathurrahmad, F. and Ester, E., 2020. Automatic Scanner Tools Analysis As A Website Penetration Testing: Automatic Scanner Tools Analysis As A Website Penetration Testing. *JurnalMantik*, *4*(2), pp.1138-1144.
10. Gupta, A.N. and Thilagam, P.S., 2019. Attacks on web services need to secure XML on web. *Computer Science & Engineering*, *3*(5), p.1.
11. Gutiérrez, V., Ramos Ruiz, G. and Fernández Bandera, C., 2021. Impact of Actual Weather Datasets for Calibrating White-Box Building Energy Models Base on Monitored Data. *Energies*, *14*(4), p.1187.
12. Hasan, A.M., Meva, D.T., Roy, A.K. and Doshi, J., 2017, December. Perusal of web application security approach. In 2017 International Conference on Intelligent Communication and Computational Techniques (ICCT) (pp. 90-95). IEEE.
13. Jan, S., Panichella, A., Arcuri, A. and Briand, L., 2019. Search-based multi-vulnerability testing of XML injections in web applications. Empirical Software Engineering, 24(6), pp.3696-3729.
14. Kalin, J., Ciolino, M., Noever, D. and Dozier, G., 2020, September. Black Box to White Box: Discover Model Characteristics Based on Strategic Probing. In 2020 Third International Conference on Artificial Intelligence for Industries (AI4I) (pp. 60-63). IEEE.
15. Khera, Y., Kumar, D. and Garg, N., 2019, February. Analysis and Impact of Vulnerability Assessment and Penetration Testing. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 525-530). IEEE.
16. Laaziri, M., Benmoussa, K., Khoulji, S., Larbi, K.M. and El Yamami, A., 2019. A comparative study of laravel and symfony PHP frameworks. *International Journal of Electrical and Computer Engineering*, *9*(1), p.704.

17. Li, J., 2020. Vulnerabilities mapping based on OWASP-SANS: a survey for static application security testing (SAST). Annals of Emerging Technologies in Computing (AETiC), Print ISSN, pp.2516-0281.
18. Mansour, N. and Houri, M., 2017. White Box Testing Of Web Applications. *Journal of Systm and Software*, pp.1-9.
19. Marksteiner, S. and Ma, Z., 2019, November. Approaching the automation of cyber security testing of connected vehicles. In Proceedings of the Third Central European Cybersecurity Conference (pp. 1-3).
20. Mateo, F., Bermejo Higuera, J.R., Bermejo Higuera, J., Sicilia Montalvo, J.A. and Argyros, M.I., 2020. On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications. Applied Sciences, 10(24), p.9119.
21. Mouli, V.R. and Jevitha, K.P., 2016. Web services attacks and security-a systematic literature review. *Procedia Computer Science*, *93*, pp.870-877.
22. Noman, M., Iqbal, M. and Manzoor, A., 2020. A Survey on Detection and Prevention of Web Vulnerabilities. *International Journal of Advanced Computer Science and Applications*, *11*(6), pp.521-540.
23. Oka, D.K., 2020. Fuzz testing virtual ECUs as part of the continuous security testing process. SAE International Journal of Transportation Cybersecurity and Privacy, 2(11-02-02-0014).
24. Ørngreen, R. and Levinsen, K., 2017. Workshops as a Research Methodology. *Electronic Journal of E-learning*, *15*(1), pp.70-81.
25. Pan, Y., 2019, August. Interactive application security testing. In 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA) (pp. 558-561). IEEE.
26. Qian, Z.Z.J., 2018. Test Suite Augmentation via Integrating Black-and White-Box Testing Techniques. *International Journal of Performability Engineering*, *14*(6), p.1324.
27. Rani, S. and Nagpal, R., 2019. Penetration Testing using metasploit framework: An ethical approach. International Research Journal of Engineering and Technology (IRJET), 6(08).
28. Seng, L.K., Ithnin, N. and Said, S.Z.M., 2018. The approaches to quantify web application security scanners quality: a review. *International Journal of Advanced Computer Research*, *8*(38), pp.285-312.
29. Sugali, K., Sprunger, C. and Venkata, N.I., 2021. SOFTWARE TESTING: ISSUES AND CHALLENGES OF A RTIFICIAL INTELLIGENCE & MACHINE L EARNING. International Journal of Artificial Intelligence and Applications (IJAIA), 12(1).
30. Sun, X.D., Ren, Z., Yang, P.W., Li, J., Chen, H.Y. and Liu, T.Q., 2019, October. Artificial intelligence design research on the cyber security penetration testing of power grid enterprises. In IOP Conference Series: Earth and Environmental Science (Vol. 354, No. 1, p. 012104). IOP Publishing.
31. Syaikhuddin, M.M., Anam, C., Rinaldi, A.R. and Conoras, M.E.B., 2018. Conventional software testing using white box method. *Kinetik: game technology, information system, computer network, computing, electronics, and control*, pp.65-72.
32. Yang, J.H., Wright, S.N., Hamblin, M., McCloskey, D., Alcantar, M.A., Schrübbers, L., Lopatkin, A.J., Satish, S., Nili, A., Palsson, B.O. and Walker, G.C., 2019. A white-box machine learning approach for revealing antibiotic mechanisms of action. *Cell*, *177*(6), pp.1649-1661.
33. Zangirolami-Raimundo, J., Echeimberg, J.D.O. and Leone, C., 2018. Research methodology topics: Cross-sectional studies. *Journal of Human Growth and Development*, *28*(3), pp.356-360.