FACULTY OF SCIENCE, ENGINEERING AND COMPUTING

School of *(Kingston University)*

MSc DEGREE
IN
NETWORK AND INFORMATION SECURITY

PROJECT DISSERTATION

NAME: Akingbesote Oluwamayowa Samuel

ID NUMBER: K1941566

PROJECT TITLE: Web Application Firewall using barracuda

DATE: JANUARY, 2021

Supervisor: **Eckhard Pfluegel**

ACKNOWLEDGEMENT

ABSTRACT

This project has discussed the progress seen in the technological field, where it is seen that before the traditional approach to handling the general-purpose based services at the current time more specific applications and technologies have been developed. The development of the web application is one of the progress made by technology and has been providing services to the specific nature of any aspect. Even at the current time, the web application has been providing data handling and service providing to a more critical nature. This process of heavy dependence on the web-based application has initiated major issues to the system operation as a large number of the threats and security issues have been targeted to the web-based application. Hackers have tried to breach the security of the application and access the content in an unauthorized way. This research project aimed to examine the use of firewall technologies for web applications such that they can be able to mitigate the threats from hackers and protect the critical nature of the data stored in the web application. Various firewall technologies along with their issues and benefits have been discussed in this project and major focus has been given to the use of the Barracuda approach in system protection. Where the features of the Barracuda approach have been compared with the other technologies and even discussing the areas where this particular technology will be most effective. The features of the technology have been compared with the other similar firewall technology for the web application. Besides this, each of the selected technologies has been critically analyzed to see the positive features of each technology and highlight the limitations that can be seen with each of the processes. The main issue will be seen in the web application protection when the excessive dependency on the system will be seen, and this will result in the possibility of security attacks on the system. But when an adequate amount of the dependency will be seen in the web-based firewall such technologies will help to prevent strikes like SQL injection, file inclusion, XSS attacks, and many more. With all these issues addressed this project has attempted to implement a secure web application system.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background

With the advent of various web-based applications, the need to protect those applications from various issues have been a challenging process for developers and security engineers. The web-based applications have been developed in various areas including e-business, e-science, and e-health. The use of the firewall is an effective approach to develop such protection for the web-based application such that its security could be improved and protected from outside attack (Okumoku-Evroro, 2015). In the current time, a large number of attacks have been deployed to the web application layer, and this can see with the rapid development of such web-based applications. The fact that web applications have been developed as important tools to the system services have made them more popular, and a similarly large number of attacks have been initiated against them.

Previous studies related to the attacks by the criminal in the various platforms depicts that web application has become the prime cause of such attacks for the criminals and the data still show that those signs have been still increasing to be the most attacked platform (Prema Sindhuri & Kameswara Rao, 2018). The prevention of these attacks have been tried to be prevented with the use of various prevention strategies. Most of them have been concerning developing the web application firewall and the enablement of the issue with the process of conflict resolving. The other factor that has been assisting in the web application regarding the security issues is related to the use of the third-party application and provided handling authority to such applications(Effendi & Pravansta, 2017). Thus, such use of the third party application is seen to provide a further loophole for the network attackers to enter the application and misuse the regular operation of the system. This major issue is seen to come with the program logic of the system and can be utilized to violate the regular operation of the system. With the integration of a large number of third party applications to the web application, a large number of loopholes can be seen to enter the web application.

Firewall Is the technology that will help to protect the unwanted access to the system and only provides the access to the registered users to use the data in the system (Khosroshahi & Shahinzadeh, 2016). The firewall can broadly be divided into two main categories and these include, the host-based firewall and network-based firewall techniques. In the network based firewall, the internal and outside network from the system will be monitored with the placement of the firewall at the interface of two networks. This will help to monitor any system and only allow restricted access to the authorized users of the system. On the other hand, it can be seen that host-based firewalls will be directly implemented to the device and provide explicit control to the device from external threats (Effendi & Pravansta, 2017). This will be able to provide the second line defense system to the system from external attacks.

There are various types of solutions to these web-based applications to provide them with better security and enhancement. Some of the commonly used techniques include Mod Security, Imperva's secure sphere, barracuda network application gateway, breach security web defend, web sniper, and many more(Okumoku-Evroro, 2015). In this research project, a brief introduction to all the aspects will be done, but the work concerning the Barracuda network application gateway will be discussed in detail. Along with the analysis for the Barracuda method and determination of the advantages of this method, it will be compared to the existing other firewall techniques. Thus, the benefit that can be achieved with such a process can be understood and identified.

1.2 Aims and objectives

The primary aim of this project is to determine the issues that are seen in the web application, and later prevention of such issues with the use of firewall technique will be discussed. Besides this, using the Barracuda techniques will be analyzed, and its features will be compared to other techniques for the prevention of the attack on web applications. The objective of this research-based report has been listed in the following section.

- To discuss the web-based application's issues and prevention approaches for the web-based application with the use of the firewall
- To analyze the features and benefits seen with the use of the Barracuda technique for the prevention of the web-based application
- To compare other firewall techniques along with the Barracuda technique and compare the various factors

1.3 Summary of thesis

In this thesis, report work has been done regarding the issues commonly seen with web-based applications, and ways to prevent those issues. The primary focus is to analyze various issues that might come to any web application, such as the breach of data and misusing of the data. With such understanding ways to prevent those security issues have been discussed and the use of the firewall has been discussed in detail. Among them, the Barracuda approach has been discussed in full detail concerning its benefits and advantages in comparison to the other techniques.

1.4 Contribution and thesis outline

In the first chapter, the overall introductions to the research topic have been done. The work in this section has been related to understanding the scope of the research work and evaluating it from the reference of the security to the web application perspective. The chapter has then discussed the primary aim and objective of the research work. Thus, this chapter has provided an introduction to the overall report and also provided a summary of the topic.

The second chapter is related to the literature review, and the past works done by the researchers and academicians have been included in this section. Thus, past information about the topic and work that has been done in the field of web application security issues have been discussed in this section. With such information about the topic and material, it will be possible to gain preliminary information about the subject matter as a result of which the subject can be understood in further detail. Based on the collection of the basic information related to any subject matter, it will be possible to obtain and collect the details related to the field. Thus, a significant amount of work can be done in the field.

In the third chapter research methodology that will be used to perform the research-based project report will be discussed. As the project is research-based, several types of research methodology need to be used to perform, and these have been discussed in

this chapter. Use of the several approaches in the research methodology will help to obtain detailed information regarding the subject matter and even assist in contributing them in case any new information has been found.

In the fourth chapter obtained results and conclusions from the research-based report have been listed. With the understanding of this section of the chapter, it will be possible to grab the crucial information to the subject easily. Thus, by listing the information in this section, it will be possible to collect the related information more easily.

Finally, in the fifth chapter of this report, the conclusion and recommendation to the chapter have been stored. The overall summary after the conduction of research-based work has been placed as the summary of the subject. Similarly, any further recommendation that needs to be made to the current work done in the field has been suggested as the recommendation to the research work.

2. LITERATURE REVIEW

2.1 Overview

Past work related to the exploitation of the web application has been discussed in this section, along with the various prevention methods for such exploitation are also discussed. The work that has been done by the researchers with relation to the subject matter has been discussed, and based on such information, it will be possible to collect further information and even make a contribution to the subject matter.

2.2 Application Exploitation

As technology is growing at a rapid pace, it brings the exploitation of application-level threats and exploitation that may result in severe impacts on the respective organization (Kilari et al., 2012). According to Kilari et al. (2012), the main reason why this attack has increased all over these years is that vulnerabilities that are found in the network are highly patched. The lower levels have been patched to that point where it has been really difficult to penetrate those vulnerable layers. In addition to this, applications and web servers contain a huge number of users; therefore, it is easy to identify the vulnerabilities. Studies shows that about 72% of different companies' websites and web applications were hacked and malicious activities were performed. E-commerce business platforms and websites are found to be greatly affected by hackers and security weaknesses. Attackers are using different techniques to find out different kinds of loopholes in the system or the website. Attack on private customer information has become a serious problem. The hackers have harvested customer credentials, and financial information is used with the wrong intention (Trustradius, 2020). Various risks and threats to the web-based application have been discussed in the following section.

Among the various types of risk and threats that can occur to the web-based application, input validation is one of the types, where the attacker will attack any modified data that will be parsed by the users via the server (Shema, 2003). Some functions that need to be performed to the data will perform the specific task by the application. However, when the user modifies such data, this will cause an error inthe normal operation of the web application and cause a problem to the system. The study by

Ferrell (2020) shows that with such issues in the system, the normal operation of the system will be violated, and the system can face various problems. The use of the effective firewall approach to the system will cause the system to be well functional.

According to Begum et al.(2016) file inclusion is one of the attacks that will be seen with the web application and this includes the condition at which any files uploaded to the application will be vulnerable in the condition that privileges will be misconfigured. Thus allowing the ability to randomly use the data and hence undermine the confidentiality of the system overall. This will be a suitable condition for the hackers to access the files on a remote basis and tamper with such files as per their requirements.

Security misconfiguration is another type of attack that can be casted to the web application and it will hamper the overall security of the system. This overall issue can be seen with the security arrangement made to the system, where the preconfigured security process will be changed such that impact can be seen directly on the stability and security of the whole system. Once the security will be misconfigured, this will allow the attackers to manipulate the data and use them for personal benefits (Manaseer & Al Hwaitat, 2018).

SQL injection is another type of attack that is possible with the web-based application such that it will be possible to manipulate the normal operation of the web application (Mohd Yunus et al., 2018). In this type of attack, the application layer will be targeted by the attackers and will try to manipulate the database of the application with the use of the raw SQL statement. Thus, it will be possible to manipulate the original database of the system with the intended database by the user. The attacker even may attempt to provide arbitrary commands for the database of such an application. With the use of those arbitrary commands, any database can be misconfigured and tempered as per the wish of the attackers. In the process, the attacker will use an approach to attack the system, and later the SQL injection will be performed(Lin, 2005). This process will exploit the system to manipulate any existing system as per the requirement of the attacker. The process of any statements being verified by the database requires that they need to be verifiable by the system. Still, if the statement is correct, the attacker cannot enter the system. Once the system is gained access, the attacker can see and manipulate the confidential data like credit card numbers, and various other private information and use them as per their desire.

Another type of vulnerability to the web application is cross-site scripting, and this is even known as the CSS vulnerability. This will be caused by the failure of any web-based application to properly validate the input made by the users and entering into any client's web browser(Snyk, 2020). The main importance of cross-site scripting will be seen when the attacker will try to access the web application based on the malicious code entering the system. In the process, the attacker will inspect all the possible alternatives such that the system will not filter it, and later use them in the cross-site scripting to enter the system (Singh & Tomer, 2015). In the process, any malicious code will be inspected by the attackers by requesting the application. In this case, the application will not be able to filter that code; it will be provided access to the website. Once the access is provided to the system, it will be able to gain full access to the system and use it as if the authentic user of the system. In the making of such cross-site scripting, the attack will be relying heavily on the <script> tags of the application. The application will not be able to know that the entered user is authentic or not once the filter to the application will be passed (Snyk, 2020). Thus attackers will be able to

make any amount of data tampering to the original content of the system. So, this type of attack is very vulnerable and can impact the overall operation of the system.

Likewise, parameter tampering is another form of web-based attack where the attacker used specific parameters in the form of URL or web page field data that are used by the users and are changed without the consent and authorization of that user (Lin, 2005). Parameter tampering is done with the objectives of knockout of the server of the app off its usual operating behavior. This attack may bring identify risks and theft as the attacker can easily fool the web server as an authorized user to the system.

Buffer overflow is one of the many attacks that will be possible in the web application, and thus the regular operation of the system will be hampered. In this type of attack, the attacker will enter a larger amount of the data than expected in the program execution. With such an approach to the program execution, the program will not be able to operate in the normal manner as the allocated memory will not be able to operate on the provided number of the data to the web application (Gold, 2011). As the memory size will be filled the excess amount of the data will go to the undesired location of the web application, thus making the normal operation of the system to be difficult. This will be seen especially in the case of the web application that will be poorly written in code, and data will be entered into the system without checking the program size. This type of issue on the web application can be prevented with the use of the code that will be developed in the standard format of the code and the placing of the data checking approach. With this approach, the size of the entered data will be checked before entering the system such that only the supportable data will be made available to the system.

Moreover, IP spoofing is another type of attack that will be possible to the web application, where the attacker will try to access the network with another IP address particularly to enter the system network. Project by (Osanaiye, 2015) illustrates a network that must deal with the confidential data that will provide the firewall blockage to the devices entering the network so that only recognized devices could enter the network and access the content of the network. But, with an attack like IP spoofing, it will be possible for the unregistered attacker to enter the network and even access the file. Due to which there will be higher chances that such attackers will modify the content as per the requirement of their own. Generally, this type of attack will provide access to sensitive information for the attacker. The installation of the program, like the backdoor program, will provide the controllability to the attacker to enter the system.

Distributed denial of service is the full form of DDos. In DDosattck, the attacker tries to disrupt and destroy the normal flow of traffic of a targeted service or a network by sending a flood of traffic(Swetapadma Sahu & Pandey, 2014). DDoS attack receives efficiency and effectiveness by making use of compromised computer systems as a source of attack traffic. Attackers may exploit different computers, systems, network resources, and IoT devices.

Network eavesdropping is one of the threats to the web application, where the attacker will gain the information in the packet transfer and request made to the system (Li et al., 2014). This type of the information loss will occur with the process like the IP spoofing and man in the middle attack, due to all these processes it will be possible to lose the information about the system such that an unwanted person will gain access to the information of the system. In the whole process even though the data loss will

occur from the system, the victim will be unaware of the data loss so this type of network issue is very dangerous and can create serious issues to the system.

Similarly, session management attack is another type of attack that is very common in the system operation in which the vulnerabilities in the application that will be leading to the attack of the session management will occur (Wedman et al., 2013). This type of attacker will be able to manipulate the session token, such as the cookie or the URL parameter, session ID, and any obfuscated value to the system. Thus, the whole process will be able to cause the problem as the attacker being able to manipulate the normal operation of the system as per his desire and thus the system will not be able to work with the actual system function.

Data tampering is the form of the attack in the web-based application is the data tampering that will include the data changes and modification to the original data by the attacker (Moradian & håkansson, 2006). This type of tampering will be very suitable for the data that need to be transmitted through the network with the internet. Network-based hackers will be able to manipulate the data and modify them as per their desire such that they will be able to manipulate those data as per their motivation. As the data sent by the client-side will be manipulated by the attacker, the successful attack of this type will result in the tampered data that will impact the overall operation of the system. Also, the man in the middle attack is the other form of the attack that will be possible because SOAP messages need to pass through the various intermediate locations(Swetapadma Sahu & Pandey, 2014). Due to such a process, it will be impossible to specify the intermediaries that need to be visited by the SOAP message as it will travel through the various locations of the network. Thus, in each such intermediate location, the SOAP message will be the possibility of those messages being lost and hence critical information will be in the hand of unauthorized users. These unauthorized users will have the ability to modify such data and then make them useful for their benefit.

2.3 Attack Prevention Measures

According to the survey conducted by CSI/FBI computer crime in the year 2006, it was discovered that about 98% of the company used network firewall, 97% of the company used anti-virus programs, 69% of the company used IDS of some sort. Mathematically, 65% of these companies were under cyber-attacks and data breaching, 15% of them were attacked with network intrusion(Razzaq et al., 2014). These security measures worked under some conditions, but it showed those companies the wrong concept of security as they felt their organization systems and network were fully protected when they were not.

Security has been the main reason for the exploitation of the application. There are different measures to deal with web application security. According to the study and research conducted by WASC, it was discovered that about 13% of the sites were using automated scanning, 49% of the sites were vulnerable to risks and threats. Sites from the business area to the government area, everything was equally affected. Web security vulnerabilities increase the risk of the website. One of the effective measures can be considered as the “web application firewall”. There is a rapid increase in cyber-attacks, and they are not showing any downtime soon. According to the Data Connectors, it was discovered that about 780000 data records were either stolen or lost per day in 2017, and in 2021, the total costs of cybercrimes are expected to reach up to 6 trillion US dollars. A firewall is not only an idea it has been a great necessity to the IT world. A firewall is considered a great place to start if you want to keep the critical data of your company safe and secure (Pałka & Zachara, 2011). The firewall has the characteristics of isolating the computer and

the system from any kind of external threats (CR-T, 2019). You can control your network by using a firewall. It allows you to select the ports from where data goes out and comes in manually. A firewall can be a medicine to cyber-attacks that are mentioned above.

One of the security approaches for the web application from the unethical access by the cybercriminal is the use of mod security (Razzaq et al., 2014). This firewall is one of the open-source, free web applications that will be able to work in the Apache system and helps to provide security to the web application from unauthorized access by unauthorized personnel. The major feature that will be seen while using this firewall is that it helps to perform the simple filtering, filtering based on the regular expression, the encoding of the URL validation, Unicode encoding validation processes, auditing of the overall system process, prevention to the null byte attack prevention, uploading the memory limits and masking the server identity. With all these features main focus will be on providing security to the system and preventing unauthorized access to the system.

Barracuda network application gateway is the commercial firewall that will present the administration of the traffic related to the application ware. There is a various function with the use of the typical Barracuda firewall, and typical function of the barracuda firewall includes the inspection of the full state packet for the firewall, IPsec VPN and intelligent controlling of the traffic flow (Miller et al., 2013). The research performed, has shown that the Barracuda firewall is seen to have a higher capability of being higher availability.

F5-Big IP firewall will include the comprehensive, and built-in application authentication security policies for the frequent application as well as the regular policy building engine that will become accustomed to the application updates. The use of this firewall will be able to provide the services to control the main facilities related to the services such as controlling the traffic and blocking. The service provided by this firewall is one of the top ten services provided by the firewall that provides the security to the system protection related to the web application (Hao, 2020). So, it has been able to provide better services to the protection of the web application and help to perform the smooth operation of the web application.

Web sniper is another firewall service that will protect the web application and servers for the unauthorized disclosure to the behavioral attack patterns, and this includes the buffer overflow exploits, path traversals, injection of the SQL, and cross-site scripting with the implementation of the signature-based detection or the prevention. The use of the web sniper will initially supervise the request received by the internet and then differentiate from the request that is justifiable and illegal(Prema Sindhuri & Kameswara Rao, 2018). By doing this action, the firewall will help to block the unauthorized request and only provide access to the legitimate request. The use of this application will help to stop the zero-day attack and utter the management of them as the unique configuration process. The firewall will also be able to ensure and adapt as per the request sent by the web servers, thus will be able to protect the customers from protecting their data loss and theft and leaking of confidential data. This firewall will generally work as the desktop-based reverse proxy firewall. Likewise, I- sentry is the composite threat management firewall application that will be equipped with the web application and web services, that will be able to equip the security of the administration and provide reliable service to the system(Naveen Kumar & Nirmala, 2017). There are various functionalities of this firewall and among them, a major function that will be to provide the access control, assessment of the vulnerability, single

sign-in checking, discovery of the web application, acceleration of the content within the system, monitoring of the request, monitoring of the user authentication, access management to the users and even providing the data leakage protection from the system. Thus, with the use of this firewall, it will be possible to monitor and detect all the known and unknown attacks, thus, providing a security mechanism to the system related to the web application.

Secure IIS is one of the commonly used firewall techniques that is used to prevent the web application from unauthorized access to the system, and this will be used in the application layer of the web application. This firewall will be used to prevent the known exploits related to the system and unconstitutional web access such that tampering of the data content related to the web application will be possible (Veracode, 2020). With the use of this type of request, it will be possible to minimize the attacks related to the system confidentiality by the scrutinization of the request made to the system from the various level of the process that may be either on the network layer or kernel level of the system thus it will be possible to perform the protection of the system from the unauthorized access to the system. Secure IIS will be able to supervise the data as the IIS will route it and then only provide passage to the system request that is legitimate whereas to block the system request that is made from the unauthorized access to the system. With this approach, it will be possible for the web application for the process of being misused and accessed to tamper with the data content of the system.

Web defend is another process of the data protection scheme that will be able to prevent the web application from unauthorized use by the users; thus only legitimate access to the system can be executed. The process of the web can be done to the services that need to be protected from unauthorized access by the users at the outside (Naveen Kumar & Nirmala, 2017). With the use of the web defend firewall various functions can be performed and among them most of them include the process of compliance to the PCI DSS and the providing the detection to the known vulnerabilities and then later protection against that vulnerabilities. These threats could be the upcoming threat to the web application from various sources like google hacking, attempt to enter the system with the use of malicious bots, site scripting processes, and even the zero-day attacks. So, the configured web application with the web defends firewall will be able to prevent any type of attacks for the system. Thus, the process of the service provided with the web application can be made available suitably and appropriately. Such that legitimate requests made by the users will be provided access, and any unauthorized request can be blocked. Out of the many firewall techniques that are available for web application protection, the use of the archive is one of those. The use of this firewall will be able to provide various services in the web application, and these will range to various nature. Some of the commonly addressed solutions with the use of the archive based firewall technique are that it will perform the botnet protection to the system and this will be the attacks made by the group of the servers to the particular computer such that the network of that computer could be hampered. Thus ultimately, it will be possible to enter the network easily. Once the bots will be able to enter the network they will be able to attack the system by misusing the data stored in the system. Likewise, the other type of services provided by the archive firewall to the system includes the management of the bandwidth, such that available resources of the network could be used rationally. Once the available resources that could be used in the desired process, it will be able to provide the desired services to the demand made by the users. Similar other services that can be achieved with the use of this archive will be such that this firewall will also be able to provide the anti-malware prevention to the services that are provided by the system and then provide genuine service on the

request made by the users. Likewise, the enablement of web content auditing will also be provided with this service. With this system, it will be possible to check the contents of the web sites and later use them for the enablement of only the authentic system services based on the legitimate request made by the users. Thus, the web application can be protected from unauthorized access and only be used to perform the system functions based on the request made by legitimate users (Foo et al., 1999). In contrast, any illegal request to the system will be initially detected, and then service will be halted in the case of such unauthorized users.

Profense is one of the firewalls that can be used to protect against the unauthorized access made by the users to the web application such that they will be able to manipulate the system as per their requirement. This firewall is built in the approach of the positive and whitelisting security model that will work to protect against the various security issues (Kamara et al., 2003). The process will be able to provide various protection against the various threats and this includes the protection of the authentic request to the system. By identification of those authentic requests, all the other requests that are not authentic will be restricted from entering the system. The use of this firewall will also be able to protect against the zero-day attack, which will be most commonly seen due to the unknown threat to the system. Besides, this model will be able to identify the negative security model and prevent the access of those services as being legitimate users. Thus, it will be possible to protect the web application security with the use of the web application firewall as the province. The Types Of firewall will be able to provide the services only to the authentic and reliable users and prevent the illegal and illegitimate user from entering the web application.

Citrix is the other firewall for the web application and will provide inclusive web application security solutions for the known and unknown vulnerabilities that will be targeted against the web application (Citrix, 2020). Various actions will be performed by this firewall, and these include blocking the known as well as unknown attacks that will be seen against the web applications. The firewall will have the ability to implement the positive security model that will only allow for the accurate behavior of the application, and in doing so, the attack signatures will not be checked. Thus, with the services provided by this firewall, it will be possible to mitigate the threat to any web applications and provide reliable services only to legitimate users.

Among the various firewalls available to protect the web application, the web app security is one of them which will provide security to the web application with the HTTP traffic, which will flood freely through the conformist perimeter defenses. This firewall serves to block those applications that will not be a genuine request to the system by the user and hence the security to the system could be established. The firewall is also able to block the known as well as unknown viruses, worms, and attacks made to the web application via the process of whitelisting. Besides, it will be possible to prevent the URL parameter tampering, cookie-tampering, and SQL injections made to the web application and with all these efforts it will be possible to protect the web application from the attacks made by illegitimate persons (Su & Wassermann, 2006).

Another type of firewall that is available concerning the protection of the web application is the server defender AI, which will be useful in the detection of the web application threat and protect those attacks (Agarwal & Hussain, 2018). This firewall will be useful to the protection of the web application security life cycle management by the prevention of the data stored in the server of

the web application. With this type of the firewall, it will be possible to prevent the attack in the system and protect such threats from the vulnerabilities that will be possible in the system.

2.4 Web application firewall Types

Network-based web application firewalls (NWAF) are the oldest and based on traditional types of hardware and give latency decrease advantages because of the local installation (Daghmehchi Firoozjaei et al., 2017). In other words, NWAF is installed very near to the application so that we can have easy access to it. Also, NWAF provides different rules and setting replication in different conditions.

Host-based web application firewalls (WAF) acts as a module for a web server (Johns, 2011). HWAF is cheaper than NWAF, which is targeted for smaller web apps. The majority of the WAFs software is made in such a way that it is easily and effectively implemented within different web servers. We have to remember that web server attacks can circumvent WAF to disable its capabilities from inside. For instance, when there is an injection of malicious code, the server through insecure file transfer.

Cloud-based web application firewalls give comparable advantages to the other two WAF solutions, which are low price and the absence of on-premises resources that you should oversee(Bisht, 2019). CBWAF is considered the best choice when you prefer not to restrict yourself with the performance abilities or are expecting to keep away from the system that needs maintenance functionalities. Cloud specialist co-ops can offer boundless equipment pool with skillful setup and backing. Yet, eventually, the administration charges may become pretty steep, or you will arrive at the moment that you need an incredible custom arrangement dependent on your physical machine.

3. RESEARCH METHODOLOGY

3.1 Overview

The selected project is a research-based project so that various research methodologies have been applied to the conduction of the project; with the performance of these approaches the project has been completed to develop the best suitable information content. The various types of research methodologies have been discussed in the following section.

3.2 Research philosophy

Research philosophy is the area of the research method that will discuss the vast topic related to the research work, and its association with the selected project (Schlegel, 2015). Generally, the research philosophy will be related to pragmatism, positivism, realism, or interpretivism with the subject matter. With the use of this subject matter, the research work can be utilized as per the specific nature of the report. In the selection of the research philosophy, it will be impacted by the practical implication that will be required for the system, and each of these factors will be able to fulfil the necessity of the selected

project. The presence of the qualitative or the quantitative research method will be useful to determine the positivism and interpretive approach of the system (Antwi & Kasim, 2015). The latest trend in the selection of the research method has been seen to the selection of the pragmatism and realism philosophies in the business sector.

In the case of this web application firewall related topic, most of the topics are related to the qualitative nature due to which the realistic nature of the research philosophy approach has been selected. Thus, it has been possible to perform a general understanding of the data and work done in this sector. With the use of the realism approach of the research methodology, the realistic nature of the work has been selected, and this has been applied.

3.3 Research approach

The way of the conduction of the research work is the research approach that will be selected in any research work. The nature of the research approach selected will be suitable to determine the type of outcomes that will be obtained out of the system. Generally, there will be three types of research approach that will be possible to perform. These include the deductive research approach, inductive research approach, and abductive research approach. The deductive research approach is the research approach that will be used for the deductive inference based on the premises that are true such that the obtained conclusion will also be true as they will be obtained out of the correct premises (Burney & Saleem, 2008). Similarly, in the induction approach, the know premises will be used for the generation of the untested conclusions. Thus, induction will be able to develop the untested conclusion. Likewise, abduction is the process of obtaining detestable conclusion based on the premises that are previously determined such that an untested conclusion can be obtained. The abduction is the research approach that is used to generate the testable conclusion based on the premises that are previously known (Greenhill, 2004).

In the case of this research-based report, the deductive approach of the research has been followed. This research approach will help to identify the conclusion that will rely on the premises that are previously known.

3.3 Research methods

The specific procedures that will be used for the collection and analyzing the data are the research methods. These methods will be an integral part of the research design and will be used for the planning of the methods related to the project. The research methods that are generally selected will be the qualitative and quantitative approach, where the collection of the necessary data will be made out of the following sections (Sharma, 2018). The selection of the qualitative data will be useful in the selection of data that are related to the data that are theoretical and need to be interpretative. Generally, the selection of the data related to the philosophical nature will be of this nature. Whereas the other type of data that needs to be used is quantitative, this data will be of those related to natural science. Thus research works that are related to natural science will be related to the quantitative nature.

In the case of the selected research-based project, both qualitative, as well as quantitative nature of the data, will be used. As the research-based project will require both theoretical as well as the factual data so, both the qualitative and quantitative nature of both data will be used in the completion of the research proposal for the web application firewall. So, that it will be possible to gain the advantage of both the type of data in the selected project and complete the project.

3.4 Data collection

Data collection is a very essential process in the research-based project, where the use of the data will be an essential factor to the successful completion of the project (Alam et al., 2014). As the way to collect there are two ways to collect the data namely the primary mode of the data collection and the second mode of the data collection. The primary mode of the data collection is the direct approach of the data collection in which the data will be obtained from the direct experimental observation and work to the specific project. This type of data collection method will be useful to the project that should have the case-specific data and all the selected data need to be directly related to the project. The data of this type can be collected by the process of the direct experimental setup related to the system and collection of the related information with the process. Whereas any other method like data collection with the interview to the related person with the field, performing of the survey will also help to collect the primary data (Ajayi, 2017). The one limitation that will be seen with this model of data collection, even though it will be able to provide the best result on the outcome is that time to collect such data will be very long. So, it will be time-consuming to collect the data once the primary mode of data collection will be used. Hence, for the project that will be needed to be completed in a short period this method of data collection will not be suitable.

On the other hand, a secondary method of data collection will be the suitable approach where the data should not be in direct relation with the project and any general data will be able to fulfill the requirements of the project. The secondary method of the data collection can be useful to the situation where past data provided by other researchers and academicians can be used in the related project. With this approach of data collection, the time to complete any research work will be short, as there will be a possibility to complete such action in a shorter time. However, with this method the collected data may not be directly related to the project being performed.

In the case of this project, secondary data collection methods have been used to collect the related data. As the project is a research-based project the secondary works are done in the field and have been used in the project. Thus, the project can gain the benefits of a secondary method of data collection.

3.5 Limitations

The limitation related to the project is seen in the use of the data related to the project, which is only the secondary data have been used to perform the project. Due to which the data used for the project may not be in direct relation to the selected project. So, the findings that may be obtained with this type of research-based project will be limited and cannot provide an accurate understanding of the available firewall to project the web-based applications.

3.6 Ethical consideration

The research-based projects on the firewall analysis related to the web-based application have performed with consideration of all the ethical factors. In which the works did have been done without harm to any living creatures. Besides this, the work has been completed with full respect to the legal rights of all the associated persons and this project. In doing the work none of the living

creatures has been directly or indirectly harmed. Similarly, the work has been performed with the legal rights that are completely acceptable and will be justifiable to all persons.

3.7 Suitability of the firewall

As a suitable method, the Barracuda web application firewall has been selected and discussed in this report. The various issues and benefits of using this approach have been discussed in this section.

3.7.1 Barracuda Web Application Firewall

Barracuda CloudGen Firewall is defined as the collection of hardware devices, virtual devices, and other cloud-based appliances that provide protection to the architecture of the network and further enhance the network infrastructure (Barracuda, 2020). The firewall provides advanced security by implementing a comprehensive set of cloud-based firewall technologies that includes profiling the seven-layer application, prevention of intrusion, filtering web contents, protection from malware and other threats, protection from antispam, and controlling the network access. Besides these, the firewall also helps in the combination of highly resilient VPN technology with various traffic management and WAN optimization capabilities (Breeden, 2020). This factor will aid in the reduction of line costs and increment of the availability of the network, improvement of site to site connectivity, and make sure that the applications that are hosted in the cloud are uninterrupted.

3.8 Justification for artifact and design

1. Protect APIs and Mobile Application

APIs and Mobile applications are used widely almost everywhere in the field of IT and organization (Jain et al., 2015). APIs stands a backbone for every connected service. Therefore, it has been very important to ensure the security of APIs. Barracuda web application firewall does this work. It provides extensive security and availability of API. With Barracuda, we can protect APLs files such as JSON, XML against different types of attacks that involve API framing, and scraping. Besides, it also provides systems with a range of granular access control. Barricade also involves the built-in control functions which help in the reliable delivery of the app.

2. Block malicious bots and other automated attacks

Internet traffic is increasing with malicious automated bots (Dunham & Melnick, 2008). These types of bots steal your data and information with the wrong intention and other attacks named automated attacks lead to the compromisation of your web applications. Barracuda protects the websites against content scraping, data theft and breach, and a non-human flood of traffic. Barracuda WAFs built-in bot detection is a kind of technology that helps to distinguish between bad bots and good bots through different measures. Other methods like advanced bot protection make use of cloud based machines to detect bot, credentials prevention, request risk scoring and also client print fingering.

3. Secure app delivery and increase availability

Insecure delivery of the app may lead to the exposure of critical information. Therefore we can use barracuda WAF that helps in enabling the HTTP/HTTPseven for apps having a variety of legacy and SSL abilities. Barracuda ensures fast and secure web application delivery with the availability of hardened SSL/TLS attack

4. Control access and authentication

WAF acts as a center to control other Barracuda WAF deployments. All these deployments work together to ensure the policies, procedures, and provide all the tools that are important to produce ongoing security practices for the applications. Moreover, there are access controls like Devops, SecoPS, and NetOps that have their own rules to handle security at every layer of the lifecycle of the application.

5. Automate and orchestrate security

Barracuda Web Application Firewall has powerful REST API and integration and automation of tools such as terraform, puppet, AWS Cloud Formation, etc. to improve the agility of DevOps so that it can build security directly (Barraguard, 2020).

Besides the use of Barracuda, it is seen that analytics done with the use of the Cloudflare will make the whole process of determining any threats and protecting them very easy. Some of the features of the Cloudflare has been discussed in the following section (Clincy & Shahriar, 2018).

- The use of technology is very easy and thus system could be managed effectively to protect the web applications
- Cloudflare has a higher threat score, such that it will be possible to provide security with near-perfect accuracy.
- Cloudflare technology can integrate with the third party API interface, such that it will be easier for the data analytics and data visualization
- The technology has easier control to the system such that it will be able to provide reliable support for all the users level expertise

3.9 Without WAF protection

The main research method that has been used to collect information regarding the attack on the system is without WAF protection. With such technology used it was possible to identify the attacks seen in the system and later made a successful attempt to protect those from the unwanted attacks. Once this research method was utilized it was possible to identify the databases related to the system and thus protection to them could be achieved.

REFERENCES

Agarwal, N. & Hussain, S.Z. (2018) A Closer Look at Intrusion Detection System for Web Applications. *Security and Communication Networks*, 2018, pp.1–27. Available from: <https://www.hindawi.com/journals/scn/2018/9601357/>.

Ahmed, G., Khan, M.N.A. & Bashir, M.S. (2015) A Linux-based IDPS using Snort. *Computer Fraud & Security*, 2015 (8), pp.13–18. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1361372315300762>.

Ajayi, V.O. (2017) Primary Sources of Data and Secondary Sources of Data [Internet]. Available from: <https://www.researchgate.net/publication/320010397_Primary_Sources_of_Data_and_Secondary_Sources_of_Data>.

Alam, I., Khusro, S., Rauf, A. & Zaman, Q. (2014) Conducting Surveys and Data Collection: From Traditional to Mobile and SMS-based Surveys. *Pakistan Journal of Statistics and Operation Research*, 10 (2).

Antwi, S. & Kasim, H. (2015) Qualitative and Quantitative Research Paradigms in Business Research: A Philosophical Reflection. *European Journal of Business and Management*, 7 (3), pp.217–225.

Barracuda (2020) Barracuda CloudGen Firewall [Internet]. Available from: <https://www.barracuda.com/products/cloudgenfirewall/features>.

Barraguard (2020) Barracuda Web Application Firewall for Amazon Web Service [Internet]. Available from: <https://www.barraguard.com/WAF-AWS.asp>.

Begum, A., Hassan, M.M., Bhuiyan, T. & Sharif, M.H. (2016) RFI and SQLi based local file inclusion vulnerabilities in web applications of Bangladesh. In: *2016 International Workshop on Computational Intelligence (IWCI)*. IEEE, pp.21–25. Available from: <http://ieeexplore.ieee.org/document/7860332/>.

Bisht, P. (2019) Component-based Web Application Firewall for Analyzing and Defending SQL Injection Attack Vectors. *International Journal of Recent Technology and Engineering*, 8 (3), pp.4183–4190. Available from: <https://www.ijrte.org/wp-content/uploads/papers/v8i3/C4674098319.pdf>.

Borky, J.M. & Bradley, T.H. (2019) Protecting Information with Cybersecurity. In: *Effective Model-Based Systems Engineering*. Cham, Springer International Publishing, pp.345–404. Available from: <http://link.springer.com/10.1007/978-3-319-95669-5_10>.

Breeden, J. (2020) Barracuda WAF-as-a-Service [Internet]. Available from: <https://www.barracuda.com/waf-as-a-service>.

Burney, S.M.A. & Saleem, H. (2008) Inductive and Deductive Research Approach [Internet]. Available from: <https://www.researchgate.net/publication/330350434_Inductive_and_Deductive_Research_Approach>.

Citrix (2020) Introduction to Citrix Web Application Firewall [Internet]. Available from: <https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html>.

Clincy, V. & Shahriar, H. (2018) Web Application Firewall: Network Security Models and Configuration. In: *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. IEEE, pp.835–836. Available from: <https://ieeexplore.ieee.org/document/8377769/>.

CR-T (2019) Barracuda Firewall: An In-Depth Review [Internet]. Available from: <https://cr-t.com/blog/barracuda-firewall-an-in-depth-review/>.

Daghmehchi Firoozjaei, M., Jeong, J. (Paul), Ko, H. & Kim, H. (2017) Security challenges with network functions virtualization. *Future Generation Computer Systems*, 67, pp.315–324. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0167739X16302321>.

Dunham, K. & Melnick, J. (2008) *Malicious Bots*. Auerbach Publications. Available from: <https://www.taylorfrancis.com/books/9781420069068>.

Effendi, Y. & Pravansta, N.P. (2017) Perancangan dan Implementasi Kepatuhan PCI DSS Untuk Keamanan Aplikasi Web Menggunakan Web Application Firewall. *Jurnal JI-Tech*, 13 (2).

Ferrell, R.G. (2020) The 5 different types of firewalls [Internet]. Available from: <https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls>.

Foo, S., Chor Leong, P., Cheung Hui, S. & Liu, S. (1999) Security considerations in the delivery of Web‐based applications: a case study. *Information Management & Computer Security*, 7 (1), pp.40–50. Available from: <https://www.emerald.com/insight/content/doi/10.1108/09685229910255197/full/html>.

van Ginkel, N., De Groef, W., Massacci, F. & Piessens, F. (2019) A Server-Side JavaScript Security Architecture for Secure Integration of Third-Party Libraries. *Security and Communication Networks*, 2019, pp.1–21. Available from: <https://www.hindawi.com/journals/scn/2019/9629034/>.

Gold, S. (2011) The future of the firewall. *Network Security*, 2011 (2), pp.13–15. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1353485811700150>.

Greenhill, A. (2004) The Research Approach and Methodology Used in an Interpretive Study of a Web Information System: Contextualizing Practice. In: *IFIP Advances in Information and Communication Technology*. pp.213–231. Available from: <http://link.springer.com/10.1007/1-4020-8095-6_13>.

Hao, M. (2020) F5 BIG-IP TMUI Remote Code Execution Vulnerability (CVE-2020-5902) Threat Alert [Internet]. Available from: <https://nsfocusglobal.com/f5-big-ip-tmui-remote-code-execution-vulnerability-cve-2020-5902-threat-alert/>.

Hofstede, R., Jonker, M. & Sperotto, A. (2017) Flow-Based Web Application Brute-Force Attack and Compromise Detection. *Journal of Network and Systems Management volume*, 25, pp.735–758.

Huang, Y.-W., Huang, S.-K., Lin, T.-P. & Tsai, C.-H. (2003) Web application security assessment by fault injection and behavior monitoring. In: *Proceedings of the twelfth international conference on World Wide Web - WWW '03*. New York, New York, USA, ACM Press, p.148. Available from: <http://portal.acm.org/citation.cfm?doid=775152.775174>.

Al Ibrahim, M. & Shams, Y. (2014) The Reality of Applying Security in Web Applications in Academia. *International Journal of Advanced Computer Science and Applications*, 5 (10). Available from: <http://thesai.org/Publications/ViewPaper?Volume=5&Issue=10&Code=ijacsa&SerialNo=2>.

Jain, A., Adebayo, J., de Leon, E., Li, W., Kagal, L., Meier, P. & Castillo, C. (2015) Mobile Application Development for Crisis Data. *Procedia Engineering*, 107, pp.255–262. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1877705815010334>.

Jaiswal, A., Raj, G. & Singh, D. (2014) Security Testing of Web Applications: Issues and Challenges. *International Journal of Computer Applications*, 88 (3), pp.26–32. Available from: <http://research.ijcaonline.org/volume88/number3/pxc3893667.pdf>.

Jang Jaccard, J. & Nepal, S. (2014) A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80 (5), pp.973–993. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0022000014000178>.

Johns, M. (2011) Code-injection Vulnerabilities in Web Applications. *Information Technology*, 53 (5), pp.256–260. Available from: <http://www.degruyter.com/doi/10.1524/itit.2011.0651>.

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F. & Frantzen, M. (2003) Analysis of vulnerabilities in Internet firewalls. *Computers & Security*, 22 (3), pp.214–232. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0167404803003109>.

Kaur Chahal, J., Bhandari, A. & Behal, S. (2019) Distributed Denial of Service Attacks: A Threat or Challenge. *New Review of Information Networking*, 24 (1), pp.31–103. Available from: <https://www.tandfonline.com/doi/full/10.1080/13614576.2019.1611468>.

Khosroshahi, A.H. & Shahinzadeh, H. (2016) Security Technology by using Firewall for Smart Grid. *Bulletin of Electrical Engineering and Informatics*, 5 (3). Available from: <http://journal.portalgaruda.org/index.php/EEI/article/view/545>.

Kilari, N., Sridaran, R. & Dean (2012) A Survey on Security Threats for Cloud Computing. *nternational Journal of Engineering Research and Technology 2278-0181*, 1 (7).

Li, X., Dai, H.-N. & Zhao, Q. (2014) An analytical model on eavesdropping attacks in wireless networks. In: *2014 IEEE International Conference on Communication Systems*. IEEE, pp.538–542. Available from: <http://ieeexplore.ieee.org/document/7024861/>.

Lin, M. (2005) Global Information Assurance Certification Paper [Internet]. Available from: <https://www.giac.org/paper/gsec/4280/overview-session-hijacking-network-application-levels/106928>.

Manaseer, S. & Al Hwaitat, A.K. (2018) Centralized Web Application Firewall Security System. *Modern Applied Science*, 12 (10), p.164. Available from: <http://www.ccsenet.org/journal/index.php/mas/article/view/0/37039>.

Miller, S.K., III, T. & J., J. (2013) Diversity Trends, Practices, and Challenges in the Financial Services Industry. *Journal of Financial Service Professionals*, 67 (6), pp.46-57.

Mohd Yunus, M.A., Zainulariff Brohan, M., Nawi, N.M., Mat Surin, E.S., Azwani Md Najib, N. & Liang, C.W. (2018) Review of SQL Injection. *JOIV : International Journal on Informatics Visualization*, 2 (3–2), p.215. Available from: <http://joiv.org/index.php/joiv/article/view/144>.

Moradian, E. & håkansson, A. (2006) Possible attacks on XML Web Services. *IJCSNS International Journal of Computer Science and Network Security*, 6.

Naveen Kumar, S. & Nirmala, K. (2017) Cloud security: to prevent unauthorized access using an efficient key management authentication algorithm. *International Journal of Engineering & Technology*, 7 (1.1), p.607. Available from: <https://www.sciencepubco.com/index.php/ijet/article/view/10787>.

Okumoku-Evroro, O. (2015) Application Of Firewall System To Internet SECURITY. *International Journal of Information Technology and Business Management*, 15 (1), pp.64–71.

Osanaiye, O.A. (2015) Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. In: *2015 18th International Conference on Intelligence in Next Generation Networks*. IEEE, pp.139–141. Available from: <http://ieeexplore.ieee.org/document/7073820/>.

Pałka, D. & Zachara, M. (2011) Learning Web Application Firewall - Benefits and Caveats. In: *Proceedings of the IFIP WG 8.4/8.9 international cross domain conference on Availability, reliability and security for business, enterprise and health information systems*. pp.295–308. Available from: <http://link.springer.com/10.1007/978-3-642-23300-5_23>.

Prema Sindhuri, B. & Kameswara Rao, M. (2018) IoT security through web application firewall. *International Journal of Engineering & Technology*, 7 (2.7), p.58. Available from: <https://www.sciencepubco.com/index.php/ijet/article/view/10259>.

Razzaq, A., Latif, K., Ahmad, H.F., Hur, A., Anwar, Z. & Bloodsworth, P.C. (2014) Semantic security against web application attacks. *Information Sciences*, 254, pp.19–38. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0020025513005677>.

Rieger, C. & Majchrzak, T.A. (2019) Towards the definitive evaluation framework for cross-platform app development approaches. *Journal of Systems and Software*, 153, pp.175–199. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0164121219300743>.

Schlegel, D. (2015) Research Philosophy and Ethics. In: *Cost-of-Capital in Managerial Finance*. springer, pp.97–106. Available from: <http://link.springer.com/10.1007/978-3-319-15135-9_4>.

SenthilKumar, P. & Muthukumar, M. (2018) A Study on Firewall System, Scheduling and Routing using pfsense Scheme. In: *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*. IEEE, pp.14–17. Available from: <https://ieeexplore.ieee.org/document/8997167/>.

Sharma, R.K., Kalita, H.K. & Issac, B. (2014) Different firewall techniques: A survey. In: *Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, pp.1–6. Available from: <http://ieeexplore.ieee.org/document/6963102/>.

Sharma, S. (2018) Introduction to Research Methods [Internet]. Available from: <https://www.researchgate.net/publication/333220560_Introduction_to_Research_Methods>.

Shema, M. (2003) *Web Security Portable Reference*. McGraw-Hill.

Singh, A. & Tomer, S.S. (2015) Securing Server/Client side Applications against XSS attack via XSS-Obliterator. *(IJCSIT) International Journal of Computer Science and Information Technologies*, 6 (2), pp.1196–1203.

Snyk (2020) Snyk Open Source Security Management [Internet]. Available from: <https://snyk.io/product/open-source-security-management/?utm_medium=Paid-Search&utm_source=google&utm_campaign=nb_vulnerability&utm_content=cross site scripting&utm_term=%2Bcross %2Bsite %2Bscripting %2Bvulnerability&gclid=EAIaIQobChMIxILypvXg7AIVhgsrCh0->.

Sosnowski, J., Gawkowski, P. & Cabaj, K. (2011) Event and Performance Logs in System Management and Evaluation. In: *Information Systems in Management XIV, Security and Effectiveness of ICT Systems*. WULS Press.

Su, Z. & Wassermann, G. (2006) The essence of command injection attacks in web applications. *ACM SIGPLAN Notices*, 41 (1), pp.372–382. Available from: <https://dl.acm.org/doi/10.1145/1111320.1111070>.

Su, Z., Zhang, G. & Jiang, J. (2012) Multimedia Security: A Survey of Chaos-Based Encryption Technology. In: *Multimedia - A Multidisciplinary Approach to Complex Issues*. InTech. Available from:

<http://www.intechopen.com/books/multimedia-a-multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology>.

Sun, Y., Zhang, J., Xiong, Y. & Zhu, G. (2014) Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*, 10 (7), p.190903. Available from: <http://journals.sagepub.com/doi/10.1155/2014/190903>.

Swetapadma Sahu, S. & Pandey, M. (2014) Distributed Denial of Service Attacks: A Review. *International Journal of Modern Education and Computer Science*, 6 (1), pp.65–71. Available from: <http://www.mecs-press.org/ijmecs/ijmecs-v6-n1/v6n1-7.html>.

Trustradius (2020) A Guide to Web Application Firewall vs. Network-Level Firewall [Internet]. Available from: <https://www.trustradius.com/buyer-blog/web-application-firewall-vs-network-firewall>.

Veracode (2020) Cross-Site Scripting (Xss) Tutorial: Learn About Xss Vulnerabilities, Injections And How To Prevent Attacks [Internet]. Available from: <https://www.veracode.com/security/xss>.

Wedman, S., Tetmeyer, A. & Saiedian, H. (2013) An Analytical Study of Web Application Session Management Mechanisms and HTTP Session Hijacking Attacks. *Information Security Journal: A Global Perspective*, 22 (2), pp.55–67. Available from: <http://www.tandfonline.com/doi/abs/10.1080/19393555.2013.783952>.